DOI: http://doi.org/10.46632/daai/2/4/7

Data Analytics and Artificial Intelligence
Vol: 2(4), 2022
REST Publisher; ISBN: 978-81-948459-4-2
Website: http://restpublisher.com/book-series/data-analytics-and-artificial-intelligence/

Detection of Worm Hole Attack and Prevention Using DSR in Wireless Sensor Network

***Stella K, Subashri M, Keerthana P, Harini L**
Veltech High tech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai, India
*Corresponding author Email: stellaakk16@gmail.com

Abstract. Security is one of the most important and essential issues in the network of sensors due to their inherent liabilities, i.e., physical size. Because of the fact that community sensors don't have any routers, every node inside the network must use the same routing protocol, which helps in each and every transmission that takes place in packets. Wormholes are remarkable examples of such assaults that they cause the greatest risk despite their difficulty in detecting and stopping. In this paper, we have proposed a methodology for spotting and preventing wormholes. It has been implemented with a DSR routing protocol, which uses neighbor discovery and transmission variety mechanisms.
Keywords: Wireless Sensor Network, Security, Worm hole attack, DSR.

1. Introduction

A collection of a wireless sensor network with a couple of specialised transducers bedded with an imparting structure has a capability of attaining at different locales is an idea for monitoring and having data in that condition. Temperature, wind speed, direction, pressure, and other factors, particularly the body's mortal functions that are independent of any sensor node in the network where all the nodes are connected with sensors of communication span, are made up of four introductory regions. The watch units consist of a battery, a transceiver (i.e., a transmitter and a receiver), and a processor. The physical volume grounded on an electrical transducer is generated while an enormous computer is processed to store the detector event. Likewise, onward data sharing is processed by a transceiver that receives inputs from the main computer. Processes used here are powered by a battery. Unlike wired networks, wireless spotting networks should have spatially scattered bumps along with order less and neglected terrain. As a result, the possibility of an attack is extremely high. Thus, nodes are safeguarded from an enormous detector attack.

WSN Security Threats in Network Layer: The network layer of sensor networks is designed with data centric and attribute-based addressing. The possible attacks in the network layer are

- Spoofed, Altered routing information
- Sink hole attack
- Selective forwarding attack
- Wormhole attack

Spoofed, Altered Routing Information: An attacker may try to spoof or alter the information during the exchange of data between nodes to disrupt the traffic in the network, as shown in Fig.1.

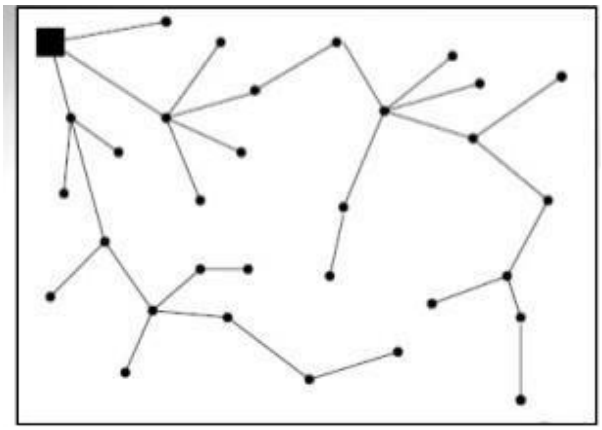

FIGURE 1. Spoofed, altered routing information attack

The disruptions are caused by attacks on network traffic, making routing nodes generate false messages with errors, increasing end-to-end delay and also partitioning of the network. The defence against these attacks is to add a Message Authentication Code (MAC) code at the end of the message.

Sinkhole Attack: The compromised nodes are created by the attacker and make those nodes very attractive to surrounding nodes, and routing information is forged, which is shown in Fig.2. Then the surrounding nodes select those compromised nodes as the next neighbour node to forward the data.

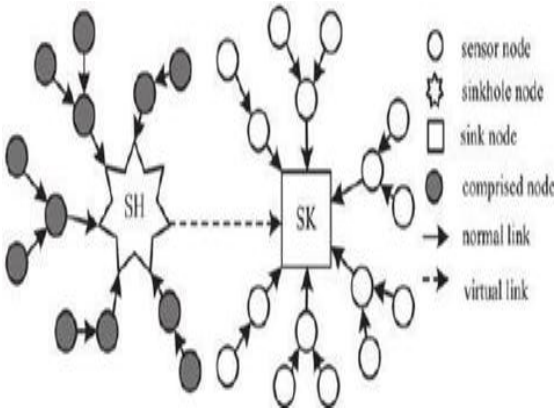

FIGURE 2. Sinkhole attack

Selective Forwarding Attack: The malicious nodes are created by the attacker and forward only selected messages, as shown in Fig.3. It is also called a "black hole attack," which drops all packets it collects. The guard against these strikes is by using numerous ways to forward the details.

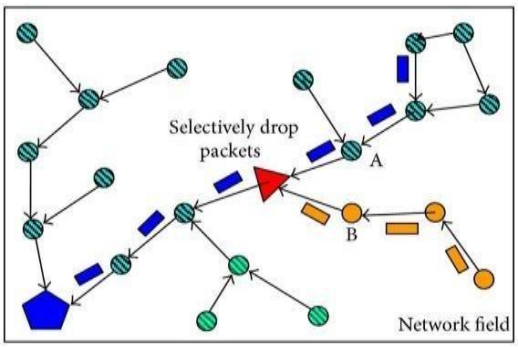

FIGURE 3. Selective forwarding attack

Wormhole Attack: A low-latency link is created by an attacker between two portions of the network. Actually, wormhole nodes make their own fake route that will always be smaller in size than the actual route, as shown in the fig.4. Request routing

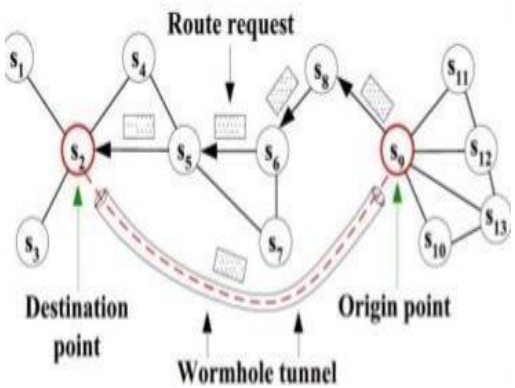

FIGURE 4. Wormhole attack

A wormhole attack confuses the routing mechanisms. The attacking node seizes the packets from one location and transfers them to the other location node. It can be easily launched by an attacker without knowledge of a network.

2. Related Works

Parmar, Amisha, and V.R. Vaghela (2016) developed a way for determining and helping to recognize wormholes present in the network efficiently by implementing the AOMDV protocol. The parameters used are delivery charge, mean of the end-end detection, and mean output of the packet. The difference between the values in the output protocol that has been proposed by a methodology like AOMDV Thus, the network's performance determines the parameters, and by using this

algorithm, the network's thickness is increased. In this ideology, no special hardware is needed. They've done this by calculating the round-trip time (RTT) of each and every route that premedicated the threshold of RTT.

Jitendra Kurmi, Ram Singar Verma, and Sarita Soni, (2017) found an effective and predictable technique for wormhole detection in wireless sensing element networks. The paper presents a well-organized wormhole detection and segmentation-based strategy with the premise of perception of the gigantic sum of web activity that will be pulled in by the wormholes. This framework is employed to distinguish the wormhole attack and ensure the wireless sensing element web by using bundle drop, delay, altering bundles, foes misleading the multi-hop directing, and that they have designed a trustworthy based vitality effective system for location of wormhole attack in remote sensor web. Preferences of the Proposed Framework is depending direct not on the specialized equipment. The proposed strategy gives the location of the wormhole attacking in reduced time. Effortlessly recognize suspected junction or assailant hub. The planned methodology employments a vitality watcher and belief supervisor to calculate the execution. The time period of the network is restricted as a result of these depends on the energy of specific junction within the web.

Hardeep Singh, along with Surinder Singh (2018), found a certainty-based methodology for wormhole attacks over wireless sensing element networks. This paper is a lightweight countermeasure to a wormhole attack. Liteworp handles the critical DSR protocol for protection method put off following hoppy symptoms. The Delphi is an overview of the AODV protocol safety method, which reduces the loss of packets by about 40%, 43%, and 35%. The attacking node will detect the register by developing its acknowledgment information and routing mechanism. Then more attacked nodes are left in the network layer. Some of the safety methods are to reduce the packet ratio. LITEWORP in wireless sensing element systems uses DSR routing methodology for the transfer of facts within the network. It ensures two-hop neighbourhood declaration and close-by observation among the monitoring movements to find hubs occupied alongside wormhole attacks. The Delphi Technique, wormhole location used in both the leap count and delay data of disjoint methods, MOBORP to re-create the wormhole attack, has been accomplished numerous times, notably sensing element organization with a double protocol. The benefit of this technique is that many methodologies are used to ensure wormhole attacks in a wireless sensing element network. This attack's disadvantage accelerated packet fall and disrupted the network's routing mechanism.

Tejaswini R. Murgod and Dr. S. Meenakshi Sundaram (2020), found collection-based and decreased methods to determine wormhole attack. The detecting device's bumps were set down consistently deep inside the ocean. To determine data and broadcast it to the CH, a specific portion of the detecting device bumps was used. The cluster head transmits every single piece of information and counts them. The base station where the procedure for the tested information will occur was connected with CH. The selection method will be similar to EEHRCP. In the planned system, each node ensures the below-given statistics. The packets will be transferred by RTT, which is a period from the source until they get an adjustment. The hop count will be pointed out between source and destination, and the estimated delivery time (EDT) was evaluated. To secure the lost packets, the threshold term was set. The transmission and reception of packet counts were conserved as PS and PR from the source to their destination. The attributes like outturn, consumption of energy, detention of end-to-end, and packet delivery rate of packets are approached. All the attacker node does is easily sit and look for the network with a connection, and also the path that passes through the vicious node is a nearby way to the destination.

3. Worm Hole Attack

Two or more venomous attacker gets packets of data of sensing element network from a position, transmits it to the tunnel of the wormhole, and makes them free into another position which gives two nodes sight that closes together. Let us consider a multi-hop Ad hoc network ignoring of their nodes in the sensing element network are conveyable or motionless as appeared in fig.5 for well understanding.

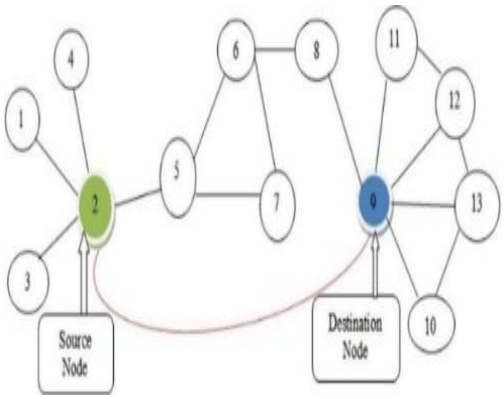

FIGURE 5. Wormhole attack in wireless sensor network

From the above representation, a node of the network is given as a circle and the relation between two nodes were represented by the line. In the case of node 2 wants to convey a message to node 9. Before transmission, the source node would find a route to transmit the message by implementing predetermined energetic or non-energetic protocols for routings. If node 2 is a source node that had preserved before a routing table (i.e. energetic routing) also it will maintain routing protocols about every single node in the sensing network This will be implemented to provide transmission to the destination but suppose the source node has non-energetic routing protocol also it does not have a table for routing hence before transmission of any information it needs to find routing data. RREQ transmission uses an In non-energetic routing protocol

sender for its one-hop down neighbours in the sensing element network. Every single node that admits RREQ transmission will verify whether RREQ is intended for itself or not and if not then it will retransmit RREQ transmission after fixing its node identity in transmission and when request transmission is arrived by the destination node it will unicast route reply transmission with route protocols to sender through the same route from which request transmission had entered to the node.

Significantly directing conventions choose the way that's a most limited sense of bumps in Adhoc web have restricted transmission capacity and control. Subsequently, we will say that junction 2 will shoot the communication through junctions 2,5,6,8, and 9. Within the web, the middle of the junction act as switches that shoot the communication to the desired goal. Let us expect that the Adhoc web specified over is beneath a wormhole attack. Assume that two bushwhackers are set in the region of junction 2 and junction 9 and these bushwhackers are associated with each other through a highspeed machine. It may be conceivable that bushwhacker is not a portion of the web but still it can listen stealthily transmission due to the spread mind Adhoc web.

At whatever point any venomous attacker junction gets transmission by bumps on whose surrounding bushwhacker is false, redelivering is made by another bushwhacker in the web. In this manner, bumps are bush whackers' deceptions that may junction 2 and junction 9 is done to accept that both of these are associated by themselves specifically. Subsequently a false connect is developed using bushwhacker in the web. In-between junction 2 and junction 9. Because of these false connections, junction 2 will shoot transmission to junction 9 specifically using wormhole lair. Subsequently, now the way is 2 and 9. All directions in the web that will penetrate using junctions 2,5,6,8 and 9 are presently supplanted by junctions 2 and 9. Therefore most extreme representation of transfer in the web can be coordinated to a wormhole that makes the bushwhacker in a certifiably important place equal as like bumps within the web. Bushwhacker can misbehave like a false interface by putting away all transport moving to the web that can be approached by dismembering substance in fact on the off chance that the bushwhacker will not have hidden keys. Bushwhacker junction generally identifies the transmission of junction that affect alertness along with wholeness parameters of the secured system.

In this manner, a Wormhole attack is avoided for an advance attack like wiretapping, activity, spoofing bundle loss and Wormhole attack is one of the Denials-of- benefit attacks which influence the web in the absence of a doubt the information of any hidden ways. Wormhole attack is certifiably fragile for descry. That can be propelled by two or advance bumps. Two finished wormhole bundles are burrowed through a wormhole connected from source to goal junction and on entering bundles, the final junction recommunicates them to the near conclusion.

Classification of Wormhole Attack: Open Wormhole: The venomous attacker nodes consider themselves in the packet following the path detecting process. Bumps of the network are attentive to the existence of venomous bumps on the direction but they will act like the venomous bumps of their direct neighbors. Half-Open Wormhole: The venomous attacker nodes do not identify the coverage of the packet. They can easily underpass through the packet from one end of wormhole to another end and it also duplicates the packet. Closed Wormhole: Here both the source and the destination consider themselves as just one- hop down from each other. Therefore, false adjustment nodes are developed.

4. Detection and Prevention of Worm Hole Attack

The two neighbour nodes such as A and B are to be checked. When the transmission range of node A, B and C is r, node A meets C Node C ∈ N(B) but C /∈ N(A) and its transmission range is adjusted to R = 2r as shown in in Fig.6. All the neighbours of node C become neighbours of node A and also it meets that C ∈ N(A) and N(B) ⊆ N(A). The wormhole link is created between Node A and B. Node C and node D both meet that C, D ∈ N(B). Node A, B and D are become mutually neighbours due to the wormhole link. Node B and D lay in node A's neighbour list due to the wormhole link. Node C is away from the wormhole end point and thus free from wormhole attack.

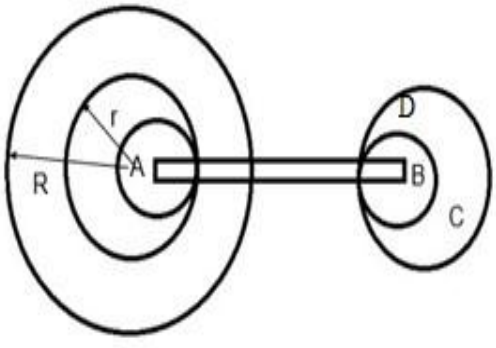

FIGURE 6. Worm hole node with neighbour nodes

The transmission range of these four nodes is r at first. Then transmission range of node A is expanded to R = 2r. Node D is node A's neighbour connected by the wormhole link. However, since nodes A and B are multi-hops away from each other, node C is still not a neighbour of node A even though the span of node A is repeated twice. Even after enlarging the span of node A any specific adjacent node of node B is not an adjacent node of A, So it results that D ∈ N(A) and C/∈ N(A). At last, not every single surrounding node of node B will transform into adjacent nodes of node A , which encounters that N (B)/⊂ N(A). This approach can be helpful to examine the wormhole existence in between nodes.

Flow Chart: Every single node will forward its own adjacent node statistics to its surrounding node with the help of a beacon frame so that every single node can have its surrounding data within a hop count of two. A try-out node will upgrade its surrounding node data in the succeeding beacon period. By collating its existing adjacent node data with the past data, the try-out node can estimate the actuality of misleading topology. Also, the neighbor node provides a path if the transmission range is higher than the distance of transmission range between source to destination then it is identified as a wormhole. By examining the range of transmission of nodes in the WSN, the essence of the node, trustable or malicious, can be determined.

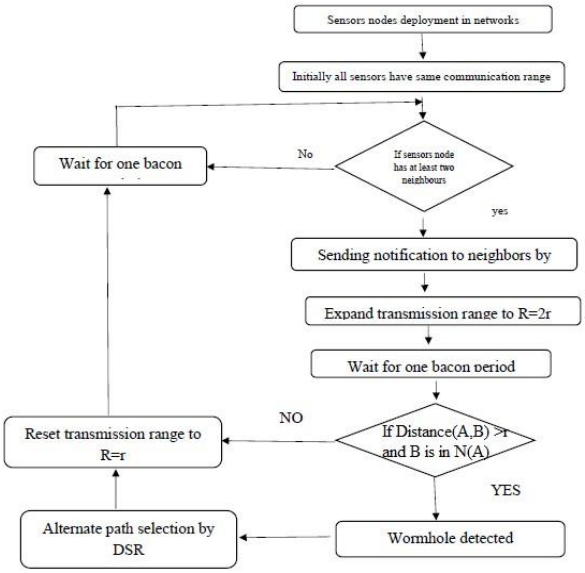

FIGURE 7. Flow chart for Worm hole node detection and prevention using DSR

5. Results And Discussion

Using NS2 simulation software the functioning of wormhole attack had been examined. There are 25sensors nodes in the WSN in the simulated system. Nodes 23 and 24 were wormhole and node 20 was a node from the entire nodes. The red colour was used to represent the sink node. Every node in our model has an existing list of neighbours. However, the list of neighbours will be updated regularly. To get the list from its neighbour each node can transmit beacon message to them. At last, every node can able to know about statistics of one hop and two hop adjacent node. When a node begins a procedure to detect the wormhole, it first broadcasts beacon message with a packet to apprise its surrounding node, this will increment the range of transmission. The node will not change its coverage of transmission which are all receiving this notification in the succeeding beacon period. After broadcasting the message, the transmission coverage of node A was expanded by 2r. If neighbour of node B which are neighbour of Node An even after increment of transmission range, then the node A would search in next beacon period. Suppose one of the node C in neighbour nodes B is still not the neighbour node of A, then that particular node will be detected as a wormhole. The neighbour list has N(A) and N(B). (1) the condition $N(B) \subseteq N(A)$ fulfils, then there will no wormhole link in between node A and node B : (2) There will be wormhole link between node A and B when the neighbour list fulfils the condition $N(B)/\subset N(A)$. The simulation output of detection of sink hole attack is shown in fig.8.

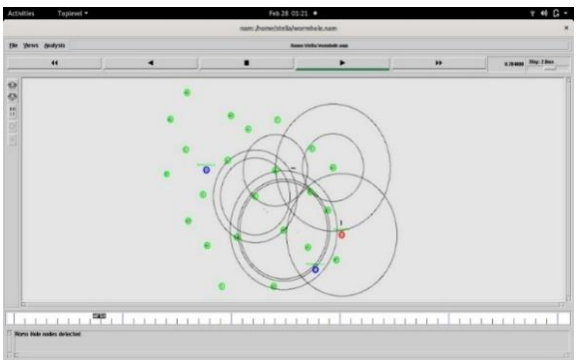

FIGURE 8. Simulation output of wormhole attack

In the existing TRM algorithm, the rate of detection will not be 100% because some of the neighbor nodes around the wormhole cannot able to detect the wormhole link. Because the nodes do not have local neighbor hoods to check the information, the detection may fail using this method. This happens in very spare or isolated sensor nodes, which is low probability in practical application. But in our proposed method, the detection rate is increased in our method wormhole is

detected using both transmission range and the distance between 2 nodes. The network simulation parameters and their values are shown in Table.4.1. If the distance between nodes A and B are greater than transmission range 'r' and node B is in the neighbor lists of node a, then those nodes are detected as wormhole nodes. If a wormhole is detected, then it will select the alternate path using the DSR routing protocol. The rate which holds high symbols will not work well for strut spacing because these objects cross the strut height consistently. Also, incrementing the height of the strut frequently won't be an option since the depth and height of the tall symbols are measured or approximated and there will be some other rows that will have a normal line of height.

6. Conclusion

Wireless sensor network are widely achieved great realization in every zones by virtue of its execution nature in all locality in wireless channels. Executing performance of a WSN may be affected if the wormhole presents in that certain network. He maximum preceding works on this attack are placed more concentration on detecting the attack rather than preventing it. Here we come up with a refinement algorithm for identifying and prevention methods for the attack in the absence of any special hardware, by applying on basis of DSR protocol in NS2. The trustable or malicious node can be identified by examining the transmission range of node in networks. The malicious node can be exterminated with hop count of prior route reply information. By utilizing throughput delay and packet delivery ratio, the accuracy can be calculated. The proposed algorithm has present the hopeful results by observing the visualization results

References

[1]. Neha Singh, Kamakshi Rautela [2016], International Journal of Engineering and Computer Science ISSN: 2319 – 7242, Volume 5, pp. no. 17544-17548.

[2]. Wazid, Mohammad & Das, Ashok Kumar & Kumari, Saru& Khan, Khurram [2016], Design of sinkhole node detection mechanism for hierarchical wireless sensor networks. Security and Communication Networks. 9.10.1002/sec.1652.

[3]. K. Saghar, M. Tariq, D. Kendall and A. Bouridane, "RAEED: A formally verified solution to resolve sinkhole attack in Wireless Sensor Network," 2016 13th International Bhurban Conference on Applied Sciences and Technology [IBCAST], 2016, pp. 334-345, doi: 10.1109/IBCAST.2016.7429899.

[4]. Mittal, Vikas, Sunil Gupta, and Tanupriya Choudhury. "Comparative Analysis of Authentication and Access Control Protocols Against Malicious Attacks in Wireless Sensor Networks." Smart Computing and Informatics. Springer, Singapore, 2017, pp. 255-262.

[5]. Yasin, N. Mohammaed, et al. "ADSMS: Anomaly Detection Scheme for Mitigating Sink Hole Attack in Wireless Sensor Network." Technical Advancements in Computers and Communications (ICTACC), 2017 International Conference on. IEEE, 2017

[6]. Jan, Mian, et al. "PAWN: a payload-based mutual authentication scheme for Wireless sensor networks." Concurrency and Computation: Practice and Experience 29.17 [2017].

[7]. Kumar, Gulshan and Rahul Saha, "Securing range free localization against wormhole attack using distance estimation and maximum likelihood estimation in Wireless Sensor Networks." Journal of Network and Computer Applications 99 (2017): pp. 10-16.

[8]. Vidhya, S, "Sinkhole Attack Detection in WSN using Pure MD5 Algorithm." Indian Journal of Science and Technology 10.24 (2017).

[9]. S. Aryai and G. S. Binu, "Cross layer approach for detection and prevention of Sinkhole Attack using a mobile agent," 2017 2nd International Conference on Communication and Electronics Systems (ICCES), 2017, pp. 359-365, doi: 10.1109/CESYS.2017.8321299.

[10]. Zhang, Z. et al. M optimal routes hops strategy: detecting sinkhole attacks in wireless sensor networks. Cluster Computer 22, pp. 7677-7685 [2019].

[11]. K. E. Nwankwo and S. M. Abdulhamid, "Sinkhole attack Detection in A Wireless Sensor Networks using Enhanced Ant Colony Optimization to improve Detection Rate," 2nd International Conference of the IEEE pp. 1-6.

[12]. K. Karthigadevi and M. Venkatesulu, "Based on Neighbor Density Estimation Technique to Improve the Quality of Service and to detect and Prevent the Sinkhole Attack in Wireless Sensor Network," 2019 IEEE International Conference on Intelligent Techniques in the control, Optimization and Signal Processing (INCOS), Tamilnadu, India, 2019, pp. 1-4.

[13]. Stella K, E N Ganesh, Distributed Energy Efficient ZonalRelayNodeBasedMultiPathSecureRoutingProtocol(DEZMSR)for WirelessSensorNetworks, Journal of computational and theoretical Nano science"Vol. 15, No.2, pp. 403–408, Feb 2018.

[14]. AbdulmalikDanmallam Bello, Dr. O. S. Lamba, 2020, How to Detect and Mitigate Sinkhole Attack in Wireless Sensor Network International Journal of Engineering Research & Technology (IJERT) Volume 09, Issue 05.

[15]. K Stella, Manikandan T and Ganesh E N 'Detection of optimized intermediate sensor nodes using carrier sensing power and genus factor for energy efficient multipath routing protocol in wireless sensor networks' in "Sensor letters", Vol. 17, No. 4, pp. 290-295, April 2019.

[16]. K Stella, Manikandan T and Ganesh E N 'Experimental analysis of Fault tolerant Authentication in non-invasive Epidermal Glucose Sensor using SQEZLMRP based information transmission in Wireless Sensor Networks' in "Sensor Letters", Vol.16, No.3. pp. 224-233, Mar 2018.

[17]. SumitPundir et al. [2020] designed efficient sinkhole attack detection mechanism in egde based IoT deploymen.

[18]. Dhivya M et al. vol.2, 2021, Detection and Prevention of Sinkhole Attack in Wireless Sensor Network using Armstrong 16-digit Key Identity and GAN Network.

[19]. SihemAissaoui& Sofiane Boukli, Sinkhole attack detection based on SVM in wireless sensor network, international journal of wireless networks and broadcast technologies, IGI Global, vol. 10(2), pages 16-31, July.

[20]. SemagnShifere et al. Department of Computer Science Woldia University, Ethiopia , Volume 6, Issue 2, February – 2021 International Journal of Innovative Science and Research Technology ISSN No:-2456-2165.

