IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol. 8, Issue.10, October 2020 E-ISSN: 2347-2693

Survey of Black Hole Attack Detection Techniques in Wireless Sensor Network

R. Chinthamani[1*], V. Selvi[2]

[1,2]Dept. of Computer Science, Mother Teresa Women's University, Kodaikanal, Tamilnadu

**Corresponding Author: sindhuvelmukull@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v8i10.127132 | Available online at: www.ijcseonline.org

Received: 04/Oct/2020, Accepted: 15/Oct/2020, Published: 31/Oct/2020

Abstract— Secure sending is a problematic task because of the partial nature of wireless sensor network properties. This paper provides solution to recognize malicious nodes in wireless sensor networks concluded prevention of black hole attack. It is basically a set of portable hosts associated wirelessly without slightly central management, where respectively node acts as a packet contributor, packet receiver, and a router at the same time. According to the landscape of this system, the active topology and the absence of a central management source some security problems and occurrences, such as the black hole attack, the wormhole attack, and the impression and negation attack. In this survey, we are going to introduce the Black Hole attack security issues and some of the recognition systems used to distinguish the black hole attack. In this kind of attack (black hole attack) the interlopers manipulate the normal performance of the network, by introduc0069ng themselves as the node with the shortest path to the destination. Interlopers can do a malicious behaviour over the network. Our future approach based on a new routing algorithm which educations shortest path in order to avoid malicious node path. Our results demonstrate the success and the effectiveness of our proposed routing procedure.

Keywords— WSN, HMM, Black Hole, Malicious, Shortest path

I. INTRODUCTION

A device network is a complex, of sensing, dispensation, message ability to detect and respond to events in a definite environment. WSN is usually collected of tens to thousands of nodes. Which collect process and transmit accommodatingly data to a central location [1].

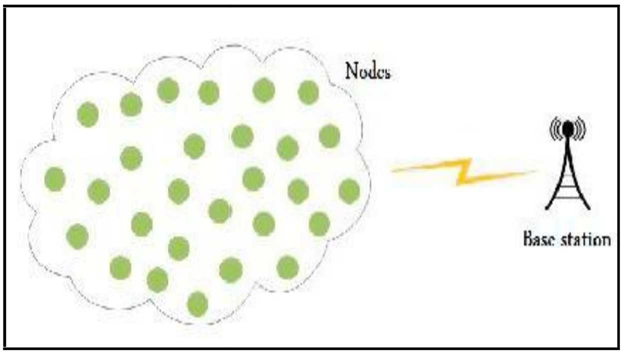

Fig.1. Wireless sensor network

WSN technology proposals many advantages associated to conservative networking solutions such as reducing budgets, consistency, scalability, give, accuracy and ease of arrangement. The fast Advance of technology makes the devices smaller and cheaper although billions of them are being organized in dissimilar applications. Some of the possible requests domains are military, atmosphere, healthcare and security [2]. The enterprise of such a network is partial by many factors such as: responsibility production costs, effective environment, sensor network topology, hardware limitations, transmission media and power ingesting. These factors are used as a guideline to design procedures and algorithms for manufacturing well-organized sensor network [3-4-5].

Moreover, security in WSNs is an significant trial, especially if they have life-threatening tasks. Sensor networks are organized in applications where they cooperate physically with the environment, people and other objects making them more susceptible to security threats [6]. The detached of security in WSN is to protect information and properties in contradiction of attacks and misbehaviour [7].

BACKGROUND AND MOTIVATION

Due to the widespread use of wireless ad hoc networks in daily requests worldwide, it is much essential to pay kindness to the rising security needs of the network and the of the members of such a type of net. There are some methods already applied for detection of the malicious nodes from the network. But the main difficult in doing so is that they need to eavesdrop the whole system's message which over products a security issue and cannot be a dependable solution. Thus, a method to distinguish the attack of black hole in wireless ad hoc network without cooperating the network's integrity or security has to be established and with that in mind, this method has been planned.

II.CLASSIFICATION OF ATTACK

Based on the source of the attacks [1]:

1. ***External attack:*** the external attack happens due to nodes that are not fragment of the network.
2. ***Internal attack:*** the internal attack happens complete the nodes going to the network (compromised nodes).

Based on the behaviour of attacks [1]:

1. ***Passive attacks:*** they find information from the exchange of data in the network, but do not source any change of the data or do not intersect the communication in growth [2].
2. ***Active attacks:*** get material from the exchange of information in the network and adjust the data or intersect the communication in progress [2].

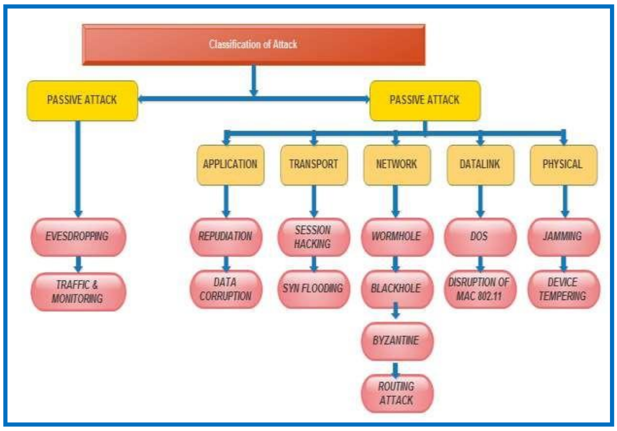

Figure 2: Classification of Attacks

III. BLACK HOLE ATTACK

Black Hole attack happens under Dos (Denial of service) occurrence in the network layer of OSI Model. In this kind of occurrences the malicious node forgery other nodes by declaring a straight false route to the terminus then interests extra traffic and drops frequently the packages. During data program the source node sends a Route REQuest (RREQ) message to all the nodes as well as malicious node. Assumed that a malicious node may developed energetic by receiving RREQ message and responses using Route REPly (RREP) message. It appeals further traffic by incorrectly demanding the straight route to the destination [16]. This causes blocking and cumulative the energy consumption in each node, leading to the development of directing holes which disturb or stop the network functionality [17, 18].

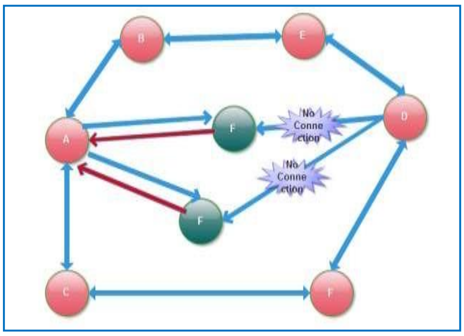

Figure 3: Collaborative Black hole Attack

The Fig. 2 illustrates the Black hole attack: while the source node A programs an RREQ infrastructures to regulate the route for transmission packets to destination node C. An RREQ program from node A is received by neighbouring nodes B, D and the malicious node E. The RREP communication sent by the malicious attacker node E is the first communication reaching the source node. This last informs its routing table for the new route to the planned node destination, removal any RREP message from other adjacent nodes including the actual node end point and starts transfer the buffered data containers immediately. In the same time the Black hole node drops all approaching data packets rather than forwarding [19].

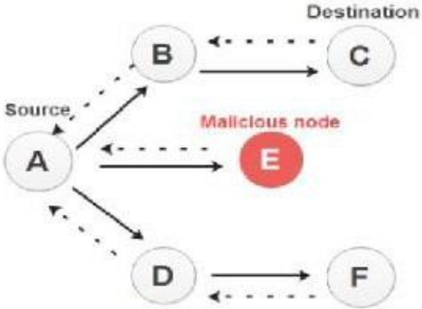

Fig. 3. Black hole Attack schematic design using RREQ and RREP Packet

In Blackhole Attack, a disagreeable node communicates the total adjoining node that has the smallest path to the destination node deprived of looking at its routing table. Source will show data to this malicious node. And after having found all the data, it is not forwarded to the end point, but all data is removed [3].

Figure 3 explains how the black hole problem occurs. Node A sends information to node D and starts the process of discovery the path. Send RREQ message to all end-to-end nodes. Node C is an unfriendly node and declares that it has the smallest path to the end point node. Then it will refer the RREP message to node A. Node A will accept that this is the shortest way and will disregard all other answers. When node C receives all data packages, it compresses all data. Thus, disagreeable node attracts all network traffic to itself, broadcasting that it has the smallest path to the destination node, hereafter the loss of data in the network.

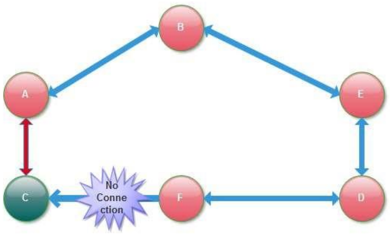

Figure 4: Black hole Problem

In AODV, we can organize a black hole attack [1] in two types:

(i) *Internal attack of the black hole:*

In this type of attack, an disagreeable inner knot is introduced between the sender and the receiver. Once it has a chance, the unpleasant knot becomes an approved knot. Then, it may interrupt the message in progress of the network.

(ii)*External attack of the black hole:*

An external attack essentially remainders external the network and refuses contact to network traffic or makes bottlenecks in the system or intersects the process of the entire network. It can develop an internal attack when it takes control of the disagreeable internal node and accomplishes it to hit other nodes in the network area.

IV. Attack of a single black hole

In the occurrence of a single black hole, there is only one malicious node in an area. The extra nodes will be an authorized node [4]. As shown in Figure 3. Node A is the opening node and Node D is the ending node. Node C is a malicious node and replies to the RREQ package sent by the initial node A and wrongly answers that it has the smallest path to the ending node. Therefore, node A have confidence in that the path finding process has been accomplished and starts sending data packages to node C. In MANET, a malicious node eliminates all data packets. This problematic is known as the black hole problem in MANET.

V. Collaborative attack of the black hole

In this black hole attack, more than one malicious node is present in the system. It is also known as Black Hole Attack with harmful nodes [4]. Figure 4 shows the cooperative BlackHole Attack, where the two malicious nodes are C and D. Node A is the basic node and node G is the end point node.

IV. LITERATURE SURVEY

Before ***"DR scheme and cross-checking scheme" [5, 6]*** Hesiri Weerasinghe planned an algorithmic program to regulate the accommodating attack of the black hole. In this case, a trivial change is made to the AODV routing protocol by addition an additional table, that is, a data routing information (DRI) table and a irritated check using the additional request - FREQ and the extra response - FREP. The DRI table supports to track whether the node has participated in data transmissions with its neighbours. Each access within the table comparative to its neighbour designates whether the node has sent data finished or from that neighbour node. If there are no paths to the end point, the source node can send a route appeal packet: RREQ to look for a innocent path to the end point node, just like in the ODV. Once the middle node receives RREQ, it will reply to the request or, once again, communicate it to the network, this will depend on the accessibility of a new route to the end point. If the end point includes a answer, all intermediate nodes update their directing entry for that end point. The source node also sends data on the direction because it beliefs the destination and informs the DRI table with all the transitional nodes between the source and, therefore, the destination.

"Detection, prevention and reactive AODV (DPRAODV)" [7] The new set called ALARM is used in the DPRAODV system. In this scheme a additional check on the beginning value is carried out. The sequence number REP is patterned to see if its value is superior than or equal to the threshold value. If the value of the RREP sequence number is better than the verge value, the node is called a malicious node and is efficient to the blacklist. ALARM is sent to end-to-end nodes, each with a black list. As soon as RREQ comes from a node, the middle nodes check if the sending node is in the blacklist, if it is, it will simply discard the packets from that node. This chunks RREP of the malicious node. The benefit of DDPAODV is that it has a higher package delivery ration than the original ODV, but it includes a higher routing above and an end-to-end delay. It does not sustenance the helpful attack of the black hole.

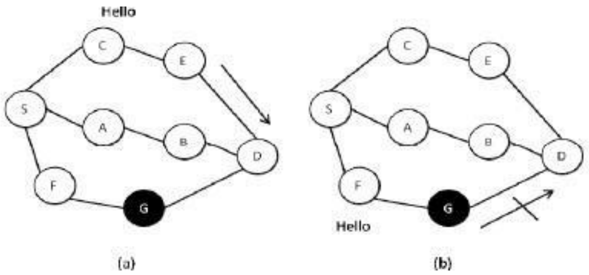

Figure 5

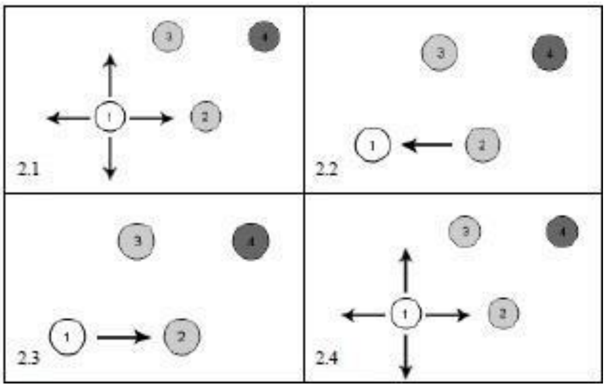

Figure 6

"Time-based threshold detection scheme" [8] The main idea is that, once the first appeal is found, the collection of requirements from other nodes is done via a device. The Route Collection Response Table (CRRT) is used to gather arrangement numbers and time values. By linking the arrival time of the first request and the edge value, the value of the network direction-finding request is measured. The result of the reproduction shows that a higher percentage of package transfer is attained with negligible delay and overload. The disadvantage is the end-to-end delay when the malicious node is far from the source node.

"Trusted table method" [9] In this method, respectively node is given a data structure called a reliable table. This table is in control for management the addresses of the trusted nodes. An additional field called as a belief field is involved to the RREP package. This field designates the dependability of the reply node. Only if RREP is spread from a consistent node, the basis does not send its information through it, then an additional RREP is expected.

The "Routing and neighbourhood recovery scheme" [10] In this method distinguishes a black hole attack based on the data in the next to set. It consists of two parts: recognition and response. Two main steps in the finding procedure are the gathering of data from neighbouring sets and the pursuit for the black hole attack. In the response procedure, the source node sends a path entry modification control packet (MRE) to the destination node to procedure a detailed path by adapting the routing entries of the middle nodes from the source to the destination. This system is more effective at distinguishing black hole attacks through less network control overhead. The disadvantage of this arrangement is that it becomes useless when the attacker approves to fabricate the packages of wrong answers.

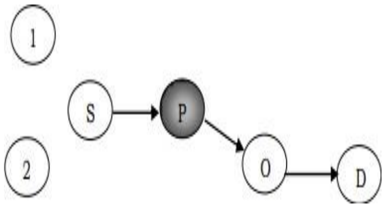

Figure 7

Then the neighbour node will be observed if it is advancing the packets. Packets sent to field in the neighbour table are incremented as the data program goes on. Forwarded packets will be incremented or stay still according to the neighbour's action. Neighbour ratings [2] will be considered when the timer goes off. If the ratio of advanced packets and sent to packets is less than threshold, the neighbour node will be added to black hole list, routes through that node will be cleaned up and alert message will be sent to neighbours. Upon getting an alert message, the node will be checked if the sender is in the black hole list and then inform its black hole list. When a node meets a new neighbour node, it will ask its neighbours rating on the new one. By the time a reputation request is received, the sender will be checked whether it is a black hole and if it is not neighbour ratings will reset neighbour rating calculating time and calculate at once. Then the reply will be sent to the demanded node.

Node 1 wants to send information to node 4 but it does not have the way. RREQ packet will be sent to its neighbours by node 1 like in Fig 2. In this figure, node 2 responses the RREQ by transfer RREP to node 1 that it has the way to node 4. Node 1 accepts the reply and starts not only advancing data packages but also monitoring node 2's package forwarding behaviour. Fig. 2 establishes node 1's actions. Node 1 keeps monitoring and it discoveries out that node 2 is reducing the packets, in its place of forwarding them to the next stage node or send them to the end point. When node 1 is sure that node 2 is purposely dropping the packages, it will improve node 2 in the black hole list. Before route clean-up procedure will takes place and all the route accesses to node 2 or through node 2 will be removed from node 1's routing table. In conclusion, node 1 sends prepared message to its neighbours informing node 2 is a black hole.

Advantage: Due to the occurrence of neighbour rating table, the Black Hole problematic avoidance rate increases.

Drawback: This technique includes much work overhead while skill with the updates on the neighbour evaluation table.

A. Contest with Black Hole Attack in AODV routing protocol in MANET

In this paper, a method has been planned to combat black hole attack in AODV routing protocol [3]. In this method any node uses amount rules to interpretation about morality of reply's sender. To contribute in data transfer procedure, a node must establish its honesty. Early of reproduction, all nodes are able to transmission data; consequently, they have sufficient time to show its truth (Though every node can be an effect less one). If a node is the initial receiver of a RREP packet, it onwards packets to basis and pledges judgment process on about replier. The judgment development is based on opinion of network's nodes about replier. The actions of a node are logged by its neighbours. These neighbours are demanded to send their view about a node. When a node gathers all thoughts of neighbours, it chooses if the replier is a malicious node. The choice is base on number rules [3]. The decision is base on node's activity in network.

Rule1: If a node distributes many data packets to destinations, it is expected as an honest node.

Rule2: If a node accepts many packets but don't sent same data packets, it's probable that the current node is a misbehaviours node.

Advantages: Faster recognition of the malicious nodes as the message goes over the set of rules. It avoids overhearing the network.

Drawback: There is no well-organized detection of malicious nodes this technique is based on neighbour's opinions and on node's honesty.

B. Performance Study and Prevention of Grey Hole and Black Hole Attack in MANET

The procedure that is planned in this paper is based on a sequence-based scheme [4]. That is, a node does not detect every node in the neighbour, but only detects the next hop in existing route path. For example, in Figure 1, S is the basis node; D is the end point node; and P is a black hole. Node S is transfer information packets to node D over the course S, P, Q, D. In this classification, Node S only watches Node P, which is the following hop; but does not care Node 1 and Node 2.

If the eavesdrop rate of next hop is less than edge worth (TH) then the node is restrained as a Black Hole. After applying detection algorithm, the presentation of the system is more improved by feast over dynamic threshold method. The node at which the attack is noticed keeps the path of Black hole detection time. If Detection Time is less than probable Time then threshold values are efficient. Due to active threshold values the presentation of network growths. Proposed algorithm separates the black hole or Gray hole node from path structure phase. To stop Black hole node, the noticing node redirect the packet to extra available path till no black hole or gray hole node is noticed in path. DSR protocol directs the route Request for the package and starts the way discovery process again.

Advantage: Each node is accomplished to detect the Black Hole attack separately without the essential to overhear the whole system or dealing with the neighbouring node's views.

Drawback: Sometimes, there are wrong alarms produced that lead to announcing a non-malicious node as malicious.

V. PROPOSED METHOD

We have graphed and studied all the above methods and have definite to device and do some more work on the technique mentioned in the last paper that is, Presentation Analysis and Prevention of Grey Hole and Black Hole Attack in MANET as in the earlier methods there is a problematic of eavesdropping of the entire system which is overcome in the last paper.

VI. CONCLUSION

In ad-hoc network, there is no robust networking infrastructure as it is just a brief set up of nodes in order to create joining between them for a limited period of time. The black hole attack is a shared threat to the wireless ad-hoc networks where the malicious nodes enter the system and give out wrong responses the route demanding nodes in the network. These nodes then grasp the packets and as an alternative of passing them through, they drop the packets. This is a possible risk to the entire system as the packets do not get moved and information loss occurs.

REFERENCES

[1]. Filippini, Massimo, and Lester C. Hunt. "*Energy demand and energy efficiency in the OECD countries: a stochastic demand frontier approach*." Energy Journal**32 (2): 59–80. 2011**

[2]. Sohraby, K., Minoli, D., and Znati, T. "*Wireless sensor networks: technology, protocols, and applications.*" John Wiley and Sons. **2007**

[3]. Rawat, P., Singh, K. D., Chaouchi, H., and Bonnin, J. M."*Wireless sensor networks: a survey on recent developments and potential synergies*." The Journal of supercomputing **68(1): 1–48. 2014.**

[4]. Kalkha, H., Satori, H., and Satori, K "*Performance Evaluation of AODV and LEACH Routing Protocol*." Advances in Information Technology: Theory and Application. **.2016.**

[5]. Kalkha, H., Satori, H., and Satori, K. ()"*A Dynamic Clustering Approach for Maximizing Scalability in Wireless Sensor Network.*Transactions on Machine Learning and Artificial Intelligence **2017.**

[6]. Akyildiz, I. F., Su, W., S Sankarasubramaniam, Y., and Cayirci, E. "*Wireless sensor networks: a survey.*" Computer networks, 38(4):393–422. **2002.**

[7]. Zia, T., and Zomaya, A. "*Security issues in wireless sensor networks.*" In Systems and Networks Communications. ICSNC'06. International Conference IEE. 40. **2006**

[8]. Sunitha, K., and Chandrakanth, H. "*A survey on security attacks in wireless sensor network*." International Journal of Engineering Research and Applications (IJERA), **2(4), 1684–1691. 2012.**

[9]. SARVARI, S., et al.: Wireless Local Area Network. "*A Comprehensive Review Of Attacks And Metrics.*" Journal of Theoretical & Applied Information Technology. **95, no. 13. 2017**

[10]. Abraham, A., Falcon, R., and Koeppen, M. "*Computational Intelligence in Wireless Sensor Networks: Recent Advances and Future Challenges*". **Vol. 676. 2017** Springer .

[11]. Singh, G., and Singh, J. "*Prevention of Blackhole Attack in Wireless Sensor Network using IPSec Protocol.*" International Journal of Advanced Research in Computer Science, **4(11). 2013**

[12]. Saghar, K., Kendall, D., and Bouridane, A. "*Application of formal modeling to detect black hole attacks in wireless sensor network routing protocols.*" In Applied Sciences and Technology (IBCAST), 2014 11th International Bhurban Conference. IEEE. **191–194. 2014, January**

[13]. Wazid, M., Katal, A., Sachan, R. S., Goudar, R. H., and Singh, D. P. (2013, April). "*Detection and prevention mechanism for blackhole attack in wireless sensor network*." In Communications and Signal Processing (ICCSP), **2013** International Conference.IEEE. 576–581.

[14]. Gondwal, N., and Diwaker, C.() "*Detecting blackhole attack in WSN by check agent using multiple base stations.*" American International Journal of Research in Science, Technology, Engineering & Mathematics, **3(2), 149–152. 2013**

[15]. Baadache, A., and Belmehdi, A.()"*Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks*." Computer Networks, **73, 173–184. 2014**
Irshad Ullah and Shoaib Ur Rehman, "*Analysis of Black Hole Attack on Mobile Ad Hoc Networks using Different Manet Routing Protocols*" **June 2010.**

[16]. Sevil Sen, John A. Clark, Juan E.Tapiador, "*Security Threats in Mobile Ad Hoc Networks".*

[17]. Tarunpreet Bhatia, A.K.Verma, "*Security Issues in MANET: A Survey on Attacks and Defense Mechanism*", International Journal of Advanced Research in Computer Science and Software Engineering, **vol.3, issue 6, pp.1382- 1394, 2013.**

[18]. Kriti Gupta, Maansi Gujral and Nidhi, "*Secure Detection Technique Against Blackhole Attack For Zone Routing Protocol in MANETS*", International Journal of Application or Innovation in Engineering & Management (IJAIEM), **Volume 2, Issue 6, June 2013.**

[19]. Hesiri Weerasinghe and Huirong Fu, Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation, Intenational Journal of Software Engineering and its Application, **Vol.2, Issue 3, July 2008.**

[20]. Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K, Prevention of Cooperative Black Hole Attack in Wireless Ad

Hoc Networks, Paper presented at the International Conference on Wireless Networks, Las Vegas, Nevada, USA, **23-26 June 2003.**

[21]. Raj PN, Swadas PB, DPRAODV: A Dynamic Learning System against *Blackhole Attack in AODV based MANETs*, International Journal of Computer Science Issue, **Vol. 2, pp 54-59, 2009.**

[22]. Tamilselvan L, Sankaranarayanan V, *Prevention of Blackhole Attack in MANET*, 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, **27-30 August 2007.**

[23]. Yaser khamayseh, Abdulraheem Bader, Wail Mardini, Muneer BaniYasein, in "*A New Protocol for Detecting Black Hole Nodes in Adhoc Network*, Internalional Journal of COllununication Networks and Infonnation Se curity (IJCNlS), **Vol. 3, No. I,April 201**

[24]. .Sun B, Guan Y, Chen J, Pooch UW , *Detecting Black-hole Attack in Mobile Ad Hoc Networks*, 5th European Personal MobileCommunications Conference, Glasgow, United Kingdom, **22-25 April 2003.**

[25]. Chethan K C, Shobha rani A, Dr. T G Basavaraju,*Scalable Local Route Repair-Hybrid Wireless Mesh Protocol (SLRR-HWMP) for IEEE 802.11*, International Journal of Computer Science and Engineering, **Volume 8 Issue 5,page no: 173-184**

[26]. Adetoye Adeyemo *Comparative Analysis of Various Denials Of Service (Dos) Attack Mitigation Techniques*, International Journal of Computer Science and Engineering, **Volume 8 Issue 4,page no: 162-167**

AUTHORS PROFILE

*Mrs.R.Chinthamani i*s a Research Scholar in the field of Wireless Sensor Network, currently working as an Assistant Professor in Department of Computer Science at EMGYWC, Madurai, India. She completed her M.Sc., from MGYWC (Tamil Nadu) and undergoing Ph.D at Mother Teresa Women;s University (Kodaikanal), India .
Email :sindhuvelmukull@gmail.com

Dr.V.Selvi, Assistant Professor, Department of Computer Science, Mother Teresa Women’s University, Kodaikanal, Tamil Nadu. She was a Website Committee Member in Mother Teresa Women’s University.
Email: selvigiri.s@gmail.com