BLACKHOLE DETECTION TECHNIQUE IN WSN - A REVIEW

Mayur Srivastava[1], Dr. Amit Dixit[2]
[1]Research Scholar Uttarakhand Technical University Dehradun, India
[2]Professor & Dean Quantum School of Technology, Roorkee, India

Abstract
W**ireless sensor network consists of many tiny motes, which actually communicate with each other for data transmission. Only three processes are involved to complete the motive of wireless sensor network and they are Sensing, Processing and Transmitting. The issue in this process arises when any intruder hack any particular sensor node and reprogrammed that node in the network to block the packet. Due to which the information received to any malicious node, is not further transmit to any neighboring node or destination so such node is called blackhole node in that network. In our present work a study about blackhole attack with different blackhole detection techniques and tools have**
Keywords: Blackhole attack, Detection technique, Different tools

I. INTRODUCTION OF BLACK HOLE ATTACK

Blackhole attack comes under Dos (Denial of service) attack in the network layer of OSI Model. In this attack an intruder hack a particular node which block the packet instead of forwarding it to the destination node. Due to this all the information sends to the malicious node or blackhole node is opted and consumes there only instead of reaching it to the destination. [8]. The most challenging blackhole attack is occurred due to crash between group leader and the other nodes. The main aim of blackhole attack is to completely dribble the packets. A randomized data acknowledgement mechanism is used to detect this attack [1].

REWARD (Receive, Watch, and Redirect) is called a routing method which provides a measurable security service for geographic ad-hoc routing [2]. For blackhole and scheduling attacks the algorithms creates a distributed database.

Low-Energy Adaptive Cluster Head (LEACH) is one of the most popular routing protocols which disperse the energy load among the various sensor nodes. The effect of attack is more if the attacker becomes the cluster head. In that case it can affect the data of the whole cluster attached to it [9].

Multi-Protocol Oriented Middleware-level Intrusion Detection generates two detection methods. Anomaly base detection and Misuse based detection [27]. Normal operations of the member are profiled and a certain amount of deviation from the normal behavior is flagged anomaly whereas in misuse based detection only known attack is detected.

The blackhole attack which is a denial of service attack, the adversary nodes try to attract as many data packets as possible and tend to discard all the packets afterwards [29].

A blackhole receives all the data packets and drop them maliciously. Basically when a node selects a blackhole node as one of its candidates, it expects malicious candidate to forward received packets according to its priority in the candidate set.

In Blackhole attack, it exploits the trustworthiness of a network by promising routing of data packets to the sink node, reporting falsely that it has a shortest path but in reality it drops all the packets and consequently threatens reliability [31]. A Blackhole is a malicious node that falsely replies for any Route Request (RREQ) without having active route to specified sink and drops all the receiving packets. If such compromised nodes work

together in a group, then damage caused will increase significantly. Such attack is sometime referred as cooperative Black-Hole attack.

To detect blackhole attack in wireless sensor network using various soft computing algorithms like genetic algorithms, ant colony optimization algorithms, Particle swarm optimization, BAT algorithm, cuckoo search, gravitational search algorithm, Artificial fish swarm algorithm etc. [32].

Blackhole attacks occur in grid layer due to the capturing, pulling and blocking of packets by an attacker by means of reprogramming a set of nodes in the network instead of allowing them to pass to the base station resulting in making itself a sink node. This result in information capture in the blackhole area. They can be easily constitute and are capable of downgrading the performance of network by dividing the network, thus preventing important event information reaching the base station [33].

Blackhole attack is also known as packet drop attacks. There are two protocols used in wireless sensor networks and they are Ad-hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR). For finding the routes DSR uses two types of routing packets and they are Route Request packets (RREQ) and Route Response Packets (RREP). An RREQ has the address of the destination node and it goes to all the nodes attached to that network. When it receive the destination address, it creates an RREP in response and sends it back to the original sender [14].

II. TECHNIQUES USED IN THE LITERATURE FOR BLACKHOLE DETECTION

Table-I

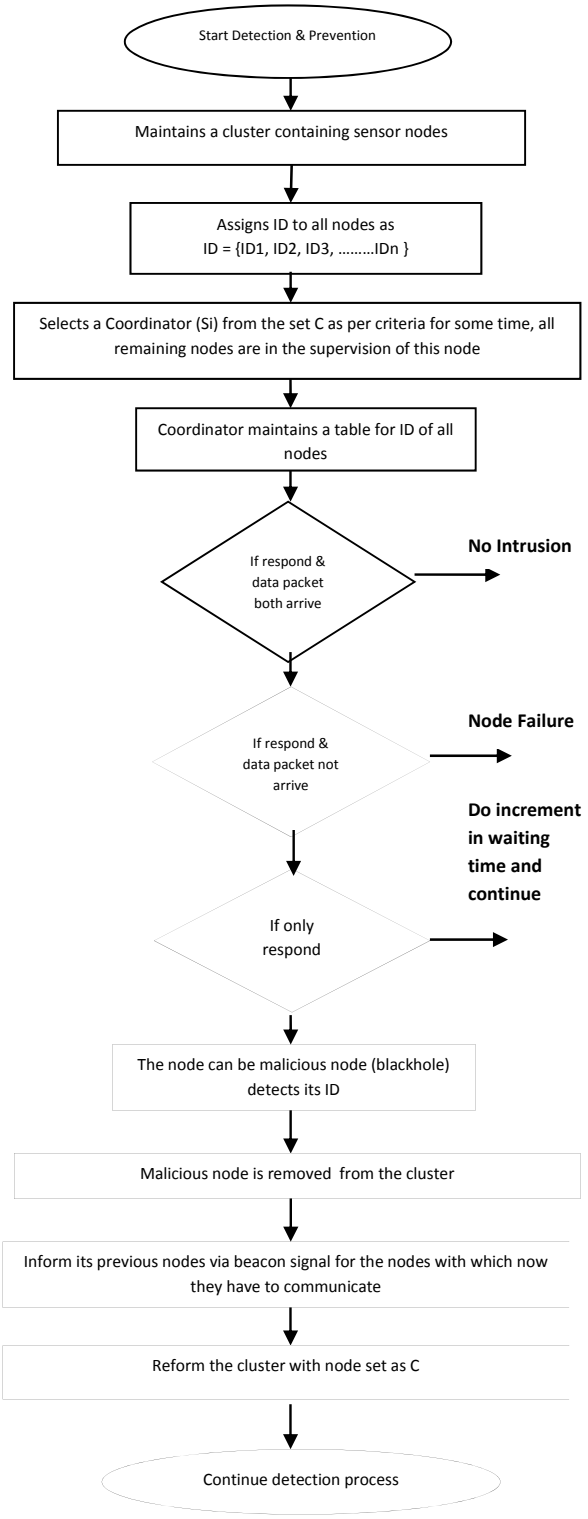
First Author	Technique Used
Jian Yin ,2006[1]	Randomized data acknowledgement scheme proposed.
Zdravko Karakehayov,2007[2]	REWARD (receive, watch, redirect) Algorithm. The algorithm utilizes two types of broadcast messages, MISS and SAMBA. MISS (material for intersection of suspicious sets) message. SAMBA (suspicious area, mark a blackhole attack) message.
Mukesh Tiwari,2009[3]	Specification based Intrusion Detection System. These specifications for detecting black hole and selective forwarding attack scan simply be a rule on the number of messages being dropped by a node.
Anoosha PrathapaniI,2009 [4]	Honeypot based detection scheme. In detecting such attacks, we explore the use of intelligent agents called Honeypots which are roaming virtual software agents that generate a dummy Route Request (RREQ) packets to lure and trap blackhole attackers.
Kashif Saghar,2010 [5]	Formal Modelling. This formal model confirms thatmARAN(secure ad-hoc routing protocol) indeed is vulnerable to attacks such as Invisible node attack (INA), black hole, and wormhole despite the use of expensive public key cryptography to prevent these attacks.
Tao Shu,2010 [6]	Randomized Dispersive Routes. In this algorithm, multiple paths are computed in a randomized way each time an information packet needs to be sent, such that the set of routes taken by various shares of different Packets keep changing over time.
Chia-Mu Yu ,2011 [7]	En-route filtering scheme (Constrained Function-based message Authentication (CFA) scheme)
Sheela.D	This system is designed to

,2012 [8]	defend against black hole attack using multiple base stations deployed in network by using **mobile agents.**
Meenakshi Tripathi, 2013 [9]	LEACH: (Low Energy Adaptive Clustering Algorithm). LEACH is one of the most popular routing protocols which disperse the energy load evenly among the various sensor nodes.
Moham mad Wazid,20 13 [10]	Topology Based Efficient Service Prediction (TBESP) Algorithm.
Mohammad Wazid, 2013 [11]	A node can be coordinator for some period of time defined by tm_lmt (threshold) Battery_pow (threshold) is the battery power of a coordinator node which decides whether the node is going to act as coordinator or not
Vidhya, S., & Sasilatha, T.,2014 [12]	Message Digest 5 Algorithm MD5 algorithm is a cryptographic function with a 128-bithash value. It is used in our work for the security part and used to check the integrity of files. MD5 hash is typically expressed as a 32–digit hexadecimal number.
Baadache, A., & Belmehdi, A.,2014[13]	end-to-end authenticated ACK based approach
Taylor, V. F., & Fokum, D. T.,2014[14]	ADIOS: Advanced Detection of Intrusion on Sensor Network
Sharma, H., Banerjee, K., & Chaurasia, B. K.,2014[15]	Blackhole tolerant AODV (btAODV).

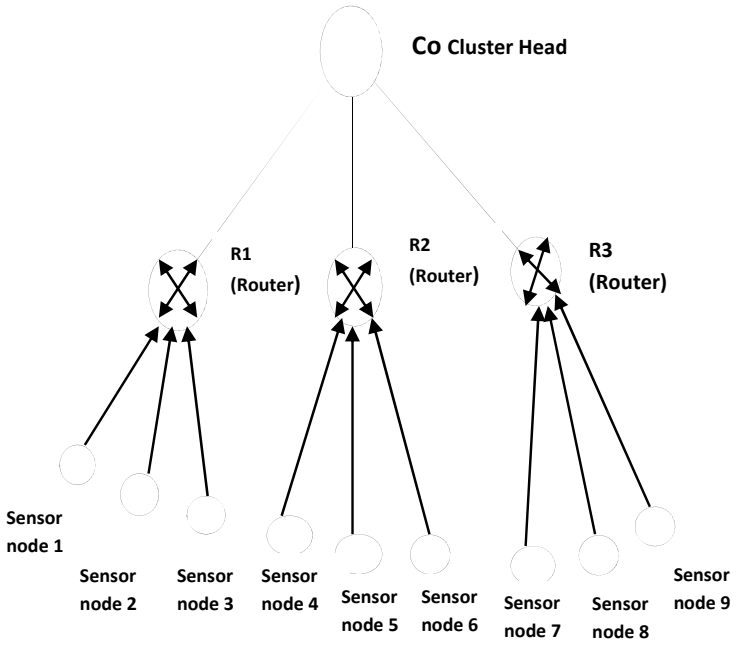
Saghar, K., Kendall, D., & Bouridane, A.,2014[16]	RAEED: Robust formally Analyzed protocol for wireless sensor networks Deployment
Dutta, C. B., & Biswas, U,2014[17]	IDS are proposed to detect the new blackhole attack.
Arfaoui, I., Bellazreg, R., & Boudriga, N.,2014 [18]	Geometric Method: Proposed new scheme based on polygonal cycles to localize and identify the radio holes.
Dongare, S. P., & Mangrulkar , R. S.,2015[19]	LEACH (Low Energy Adaptive Clustering Hierarchy)
Karuppiah, A. B., Dalfiah, J., Yuvashri, K., & Rajaram, S.,2015[20]	Exchange of control packet between sensor nodes and base station.
Trong, N. D., Le, N. P., Van Hau, P., & Van Khanh, N.,2015[21]	Propose two protocols : 1.Hole boundary detecting protocol HBD 2.Hole boundary updating protocol HBU
Moon, P. S., & Ingole, P. K., 2015[22]	Enhanced Adaptive Acknowledgment (EAACK) mechanism is used for detecting black-hole attack
Yan, F., Vergne, A., Martins, P., & Decreusefo nd, L.,2015[23]	we adopt two types of simplifies complex called Čech complex and Rips complex to capture coverage holes of a WSN
Salunke, A., & Ambawade, D.,2015[24]	Dynamic Sequence Number Thresholding (DSNT) Protocol for securing network against blackhole attack.
Motamedi, M., & Yazdani, N.,2015[25]	UAV (unmanned aerial vehicles) using Sequential Probability

	Ratio Test.
Salehi, M., Darehshoorzadeh, A., & Boukerche, A.,2015[26]	OR Modelling Using DTMC (Opportunistic Routing Using Discrete Time Markov Chain) The proposed model is modified to include the effect of Black-hole attack
Guo, Q., Li, X., Xu, G., & Feng, Z., 2016[27]	MP-MID: Multi-Protocol Oriented Middleware-level Intrusion Detection Methods , generates two detection methods: 1. Misuse base detection 2. Anomaly based detection.
Ravichandran, S., Chandrasekar, R. K., Uluagac, A. S., & Beyah, R., 2016[28]	PROVIZ: Is used to visualize a WSN and show how the tool enables visual debugging to identify a security breach such as a black-hole attack.
Salehi, M., Boukerche, A., & Darehshoorzadeh, A., 2016[29]	Descrete Time Markov Chain (DTMC) Model
Li, W., & Wu, Y.,2016[30]	Tree-based coverage hole detection:
Dongare, S. P., & Mangrulkar, R. S.,2016[31]	Algorithm for Detection and Prevention of Black-Hole and Gray-Hole Attack 1. Select Maximum Energy Node as CH in first Round of CH selection using equations in 5, 6. 2. SNCH broadcast RREQ packet. 3. INCH receives RREP, RIE of INCH. 4. IF Received timestamp of RREP by INCH< TF_GH, Make current INCH as Gray-Hole attacked node. OR IF DNCHSeqNo>last(DNCHSeqNo) but HopCountLast(DNCHSeqNo) > TF_BH at Node INCH ,ake Current INCH as Black-Hole Attacked Node and delete RIE of INCH from Source Routing Table. ELSE Route Data Packets to INCH. Current_IN = NHN_CH. 5. IF INCH is found Compromised Node, Broadcast FRqst_CH to NHN_CH. 6. Receive FRp_CH and RIE of requested NHN_CH. 7. IF NHN_CH is not malicious, Route data packets to selected NHN_CH. NHN_CH= SNCH. 8. Repeat from step 1 while NHN_CH is not DNCH.
Rani, S., & Singh, C., 2016[32]	Proposed Different Algorithm to detect Black Hole 1. Genetic Algorithm(GA) 2.Ant Colony Optimization (ACO). 3.Particle Swarm Optimization (PSO). 4.Gravitational search algorithm (GSA). 5.Artificial Fish Swarm Algorithm (AFSA). 6.AODV (Ad hoc On Demand Vector) Protocol
Krishnan, S. N., & Srinivasan, P. 2016[33]	The proposed methodology aims at black hole defence that protects the primary QOS parameters of delay in packet delivery, throughput efficacy and delay increment.
Aljumah, A., & Ahanger, T. A. 2017[34]	A method has been proposed against blackhole attack that detects attacker node and prevents it before it affects the network.

III. BLACKHOLE ATTACK DETECTION AND PREVENTION FLOW CHART



Demonstrate the traffic in wireless sensor network



Sensor Nodes sense the environmental condition and extract the information then deliver it to the respective routers.
Routers are the intermediate nodes reporting to the cluster coordinator.
Routing is the process of moving data from source node to sink.
Cluster Coordinator detects the intruder node in the cluster.

Step 1: Cluster Coordinator assigns IDs to all the nodes
Step 2: Cluster Coordinator sends the Authentication Packets to each of the router nodes.

IDR1	Auth.

Authentication Packet Field

Step 3: All intermediate nodes respond to the authentication packet being sent by the coordinator nodes.

IDR1	Ack.

Respond Packet Field

Step 4: Sensor nodes sends, sensed data packet to the routers, routers nodes further process this information and pass it to the cluster coordinator in the form of data packet (DP)

IV. WSN Layers attacks and its countermeasures

Table 2.

Layer	Attacks	Defense
Physical	Jamming	Priority message, region mapping, mode change
Link	Crash Exhaustion Unfairness	Error correcting code Rate limitation Small Frames
Network	Spoofed & Selective forwarding Sinkhole Sybil Wormhole Grayhole & Blackhole Hello Flood	Authentication, Monitoring, Filtering Redundancy Probing Authentication, Monitoring, redundancy Authentication, Probing Monitoring, authentication Authentication, Packet curbs by using geographic & temporal info.
Transport	Flooding De-synchronization	Client puzzles Authentication

Blackhole attack occurred in network layer that's why I

Focused my research on network layer and attacks fall under this layer.

Spoofed routing information: As the name indicate spoofed routing means an alteration or spoof in direct routing information by the attacker.

Selective forwarding: In a multi-hop networks such as WSN, an accurate flow of message is required from one to another node. But in this attack an attacker may select some nodes on which message is not forwarded means selective forwarding technique is used.

Sinkhole: In this attack, an adversary introduces an attractive dump or adjusted node by forging the routing information. Due to attractive nature the neighbor node select the compromised node as the next-hop to pass the information. As a result a large amount of data which used to flow in large area in the network would now focus on a compromised node.

Sybil attack: It is an attack where one node presents more than one identity in a network. It was originally described as an attack intended to defeat the objective of redundancy mechanisms in distributed data storage systems in peer-to-peer networks

Wormhole: A wormhole is low latency link between two portions of a network over which an attacker replays network messages. This link may be established either by a single node forwarding messages between two adjacent but otherwise non-neighboring nodes or by a pair of nodes in different parts of the network communicating with each other. The latter case is closely related to sinkhole attack as an attacking node near the base station can provide a one-hop link to that base station via the other attacking node in a distant part of the network.

Blackhole and Grayhole: In this attack, a malicious node falsely advertises shortest path to the destination node during the path-finding process (in reactive routing protocols), or in the route update messages (in proactive routing protocols). The intention of the malicious node is to intercept all data packets being sent to the destination node. A more delicate form of this attack is known as the grayhole attack, where the malicious node intermittently drops data packets thereby making its detection more difficult.

HELLO flood: Protocols that uses HELLO packets make the naïve assumption that receiving such a packet implies that the sender is within the radio range of the receiver. An attacker may use a high-powered transmitter to fool a large number of nodes and make them believe that they are within its neighborhood.

V. TECHNIQUE RELATED TO BLACK HOLE ATTACK

Based on the survey done we can categories technique related to blackhole detection as follows:

Table 3.

Detection technique related to blackhole attacks		
S.N	**Technique Name**	**Reference No.**
1.	Randomized data acknowledgement scheme	[1]
2.	REWARD (Receive, Watch & Redirect Algorithm)	[2]
3.	Specification based Intrusion detection system	[3]
4.	Honeypot based detections scheme	[4]
5.	Randomized Dispersive Routes	[6]
6.	Mobile Agent Based Technique	[8]
7.	Topology Based Efficient Service Prediction Algorithm (TBESP)	[10]
8.	Advanced Detection of Intrusion on Sensor Network (ADIOS)	[14]
9.	Unmanned Aerial Vehicle Technique (UAV)	[25]
10.	MP-MID (Multi-protocol oriented middleware level intrusion detection method for WSN)	[27]

VI. SUMMARY

As we have gone through the literature and reviewed most of the recent techniques related to blackhole detection almost all the previous related technique recognize the blackhole node on the basis of End-to-end delay. End-to-end delay refers to the time taken for a packet to transmit across a network from source to destination. This review paper mainly focuses on the working of various related techniques, different steps involve in detection of attacks in WSN. Further work will be done on comparative analysis of some popular algorithms used for detecting intrusion attacks in wireless sensor networks.

References

[1] Yin, J., & Madria, S. K. (2006, June). A hierarchical secure routing protocol against black hole attacks in sensor networks. In Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on (Vol. 1, pp. 8-pp). IEEE.

[2] Karakehayov, Z. (2007, September). Security-lifetime tradeoffs for wireless sensor networks. In Emerging Technologies and Factory Automation, 2007. ETFA. IEEE Conference on (pp. 646-650). IEEE.

[3] Tiwari, M., Arya, K. V., Choudhari, R., & Choudhary, K. S. (2009, November). Designing intrusion detection to detect black hole and selective forwarding attack in WSN based on local information. In Computer Sciences and Convergence Information Technology, 2009. ICCIT'09. Fourth International Conference on (pp. 824-828). IEEE.

[4] Prathapani, A., Santhanam, L., & Agrawal, D. P. (2009, October). Intelligent honeypot agent for blackhole attack detection in wireless mesh networks. In Mobile Adhoc and Sensor Systems, 2009. MASS'09. IEEE 6th International Conference on (pp. 753-758). IEEE.

[5] Saghar, K., Henderson, W., Kendall, D., & Bouridane, A. (2010, July). Applying formal modelling to detect DoS attacks in wireless medium. In Communication Systems Networks and Digital Signal Processing (CSNDSP), 2010 7th International Symposium on (pp. 896-900). IEEE.

[6] Shu, T., Krunz, M., & Liu, S. (2010). Secure data collection in wireless sensor networks using randomized dispersive routes. IEEE transactions on mobile computing, 9(7), 941-954.

[7] Yu, C. M., Tsou, Y. T., Lu, C. S., & Kuo, S. Y. (2011). Constrained function-based message authentication for sensor networks. IEEE Transactions on Information Forensics and Security, 6(2), 407-425.Chicago

[8] Sheela, D., Srividhya, V. R., Asma, B. A., & Chidanand, G. M. (2012). Detecting Black Hole Attacks in Wireless Sensor Networks Using Mobile Agent. In International Conference on Artificial Intelligence and Embedded Systems (ICAIES (pp. 15-16).

[09] Gaur, M. T. M., & Laxmi, V. (2013). Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN. In The 8th International Symposium on Intelligent Systems Techniques for AdHoc and Wireless Sensor Networks (Procedia Computer Science 19 (2013) 1101--1107. DOI= 10.1016/j. procs. 2013.06. 155.

[10] Wazid, Mohammad, Avita Katal, and R. H. Goudar. TBESP algorithm for wireless sensor network under blackhole attack. Communications and Signal Processing (ICCSP), 2013 International Conference on. IEEE, 2013.

[11] Wazid, Mohammad, et al. "Detection and prevention mechanism for Blackhole attack in Wireless Sensor Network." Communications and Signal Processing (ICCSP), 2013 International Conference on. IEEE, 2013.

[12] Vidhya, S., & Sasilatha, T. (2014, October). Performance analysis of black hole attack detection scheme using MD5 algorithm in WSN. In Smart Structures and Systems (ICSSS), 2014 International Conference on (pp. 51-54). IEEE..

[13] Baadache, A., & Belmehdi, A. (2014). Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks. Computer Networks, 73, 173-184.

[14] Taylor, V. F., & Fokum, D. T. (2014, April). Mitigating black hole attacks in wireless sensor networks using node-resident expert systems. In Wireless Telecommunications Symposium (WTS), 2014 (pp. 1-7). IEEE

.[15] Sharma, H., Banerjee, K., & Chaurasia, B. K. (2014, November). Blackhole Tolerant Protocol for ZigBee Wireless Networks. In Computational Intelligence and Communication Networks (CICN), 2014 International Conference on (pp. 782-786). IEEE.

[16] Saghar, K., Kendall, D., & Bouridane, A. (2014, January). 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 on (pp. 191-194). IEEE.

[17] Dutta, C. B., & Biswas, U. (2014, May). A novel blackhole attack for multipath AODV and its mitigation. In Recent Advances and Innovations in Engineering (ICRAIE), 2014 (pp. 1-6). IEEE.

[18] Arfaoui, I., Bellazreg, R., & Boudriga, N. (2014, September). A hole detection scheme based on polygonal cycles for the irregular radio range in WSN. In Proceedings of the 12th ACM international symposium on Mobility management and wireless access (pp. 31-38). ACM.

[19] Dongare, S. P., & Mangrulkar, R. S. (2015, March). Implementing energy efficient technique for defense against Gray-Hole and Black-Hole attacks in wireless sensor networks. In Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in (pp. 167-173). IEEE.

[20] Karuppiah, A. B., Dalfiah, J., Yuvashri, K., & Rajaram, S. (2015, February). An improvised hierarchical black hole detection algorithm in Wireless Sensor Networks. In Innovation Information in Computing Technologies (ICIICT), 2015 International Conference on (pp. 1-7). IEEE..

[21] Trong, N. D., Le, N. P., Van Hau, P., & Van Khanh, N. (2015, December). A Distributed Protocol for Detecting and Updating Hole Boundary in Wireless Sensor Networks. In Proceedings of the Sixth International Symposium on Information and Communication Technology (pp. 171-178). ACM.

[22] Moon, P. S., & Ingole, P. K. (2015, March). An overview on: Intrusion detection system with secure hybrid mechanism in wireless sensor network. In Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in (pp. 272-277). IEEE..

[23] Yan, F., Vergne, A., Martins, P., & Decreusefond, L. (2015). Homology-based distributed coverage hole detection in wireless sensor networks. IEEE/ACM Transactions on Networking, 23(6), 1705-1718.

[24] Salunke, A., & Ambawade, D. (2015, January). Dynamic Sequence Number Thresholding protocol for detection of blackhole attack in Wireless Sensor Network. In Communication, Information & Computing Technology (ICCICT), 2015 International Conference on (pp. 1-4). IEEE.

[25] Motamedi, M., & Yazdani, N. (2015, May). Detection of black hole attack in wireless sensor network using UAV. In Information and Knowledge Technology (IKT), 2015 7th Conference on (pp. 1-5). IEEE.

[26] Salehi, M., Darehshoorzadeh, A., & Boukerche, A. (2015, November). On the effect of black-hole attack on opportunistic routing protocols. In Proceedings of the 12th ACM

Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks (pp. 93-100). ACM.
[27] Guo, Q., Li, X., Xu, G., & Feng, Z. (2016). MP-MID: Multi-Protocol Oriented Middleware-level Intrusion Detection method for wireless sensor networks. Future Generation Computer Systems.
[28] Ravichandran, S., Chandrasekar, R. K., Uluagac, A. S., & Beyah, R. (2016). A simple visualization and programming framework for wireless sensor networks: PROVIZ. Ad Hoc Networks, 53, 1-16.
[29] Salehi, M., Boukerche, A., & Darehshoorzadeh, A. (2016). Modeling and performance evaluation of security attacks on opportunistic routing protocols for multihop wireless networks. Ad Hoc Networks, 50, 88-101.Chicago.[30] Li, W., & Wu, Y. (2016). Tree-based coverage hole detection and healing method in wireless sensor networks. Computer Networks.
[31] Dongare, S. P., & Mangrulkar, R. S. (2016). Optimal Cluster Head Selection Based Energy Efficient Technique for Defending against Gray Hole and Black Hole Attacks in Wireless Sensor Networks. Procedia Computer Science.
[32] Rani, S., & Singh, C. (2016). A Survey of Various Algorithms to Detect Black Hole Attack in Wireless Sensor Network.
[33] Krishnan, S. N., & Srinivasan, P. (2016). A QOS Parameter based Solution for Black hole Denial of Service Attack in Wireless Sensor Networks. Indian Journal of Science and Technology.
[34] Aljumah, A., & Ahanger, T. A. (2017). Futuristic Method to Detect and Prevent Blackhole Attack in Wireless Sensor Networks. International Journal of Computer Science and Network Security (IJCSNS),