IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 77-82

A Survey Of Collaborative Black Hole Attack And Non-Collaborative Black Hole Attack In Wireless Sensor Networks

K. Sutha, S. Srividhya
M.Phil Research Scholar. , Department of Computer science, Sri Ramakrishna College of Arts and Science for women, E-mail:suthakailasam@gmail.com
Assistant Professor, Department of Computer Science, Sri Ramakrishna College of Arts and Science for women E-mail: vidhyacs@srcw.ac.in

Abstract: *Wireless Sensor Networks (WSN) is a trending technology now-a-days and has a wide range of applications such as battlefield surveillance, traffic surveillance, forest fire detection, flood detection etc. The many researchers have conducted different detection techniques and algorithms to proposed different types of detection schemes. But wireless sensor networks are susceptible to a variety of potential attacks which obstructs the normal operation of the network. The blackhole nodes will launch black hole attack to conserve its resource or to perform attacks that reduce the network. In this paper, survey the existing solutions and discuss the state-of-the-art routing methods. In this paper analysis the different type black hole attacks detection techniques in addition conceive the open issues and future trends of black hole detection and prevention in WSN based on the survey results of this paper.*

Keywords: *Mobile Ad-hoc networks, Blackhole attacks, machine learning, pre-processing, classification*

I. Introduction

A Wireless Sensor Network (WSN) consists of large number of sensor nodes working in cooperation manner to gather the information from the monitoring region. Generally, WSN have little or no infrastructure. There are two types of WSNs: structured and unstructured. In unstructured WSN there are huge numbers of nodes deployed randomly to monitor the region. Due to unavailability of physical presence on the region, network maintenance activities are difficult. In a structured WSN, all the nodes are deployed in fixed and planned manner. Positive point of a structured network is that fewer nodes can be deployed and requires fewer maintenance and management cost. In a WSN the object performing task of sensing is called a sensor. Sensor nodes are low power devices equipped with one or more sensors, processor, memory, power supply, a radio, and an actuator. A variety of mechanical power, thermal sensor, biological, chemical, optical sensor, and magnetic sensors can be attached to enhance the power of sensor nodes. Since the sensor nodes have limited memory and are deployed in harsh environment and in difficult locations, radio transmitter is implemented to transfer the collected data to base station. WSNs have many applications such as military target tracking and surveillance, disaster relief, health monitoring, environment exploration seismic sensing to measure the environment.

A WSN is assortment of numbers of sensing element nodes that area unit distributed in atmosphere. It's really a special variety of Ad-hoc network. The key feature of WSN includes its use things because it is self-organizing and self-maintaining. As a result of infrastructure less atmosphere and wireless nature of WSN, they're a lot of suffering from many varieties of security attacks.

There are many varieties of attacks is done by malicious nodes to break the network and build that network unreliable for communication and proper working. a number of such types of attacks are:

- Wormhole Attack: in wormhole attack, assailant records packets at one place and tunnels those to a different place in network. Due to this it creates False situation that main sender is neighbor of remote location.
- Tempering: Its tempers hardware configuration of sensor and gain physical access for creating node as somebody node. Tempering is done at physical layer.
- Jamming: This attack is expounded with trouble making or interfering radio frequencies that are employed by sensor nodes. By gating physical access of some node's assailant will produce jam in network to disturb the network.
- Sybil Attack: In Sybil attack a malicious node illegally take multiple identities. Throughout this, a someone can appear in multiple places at the same time. A node presents multiple identities to completely different nodes in network by stealing or fabricating the identities of authenticated nodes. This attack is completed on network layer.
- Hello Flood Attack: Its uses hello packets as a weapon to persuade the sensors in WSN. During this attack an assailant have high radio transmission range and process power. They send hello packets to number of sensor nodes that are in a massive space among a WSN.

Wireless Sensor Network is used in various applications like to monitor physical environmental conditions, battlefield applications. So, we require security over these networks. There are some threats to these

networks in the forms of various attacks like black hole attack, Sink hole attack, worm hole attack etc. But black hole attack is very common and critical attack because it stops communication from source end to destination end. Black hole attack is attack in which malicious node sends fake message to source node claiming that it has the optimized fresh and shortest path to send all packets to the required destination node or base station. User sends all its data through this path that is get by falsely information and lost all information.

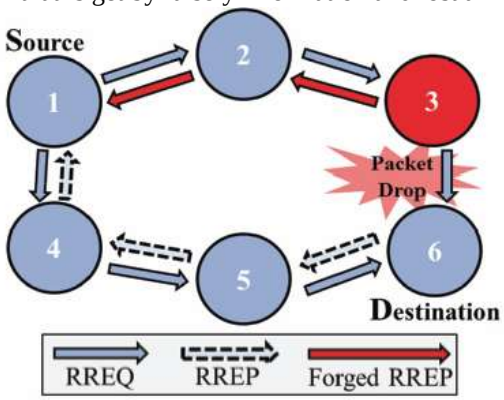

Fig.1. Black hole attack based on forged route reply packet

Security against this attack is challenging problem which can be detect and prevents by various techniques. Several researchers have proposed different detection and prevention techniques.

II. Related Work

Security is one of the main research topics in computer networks. One of the most famous attacks done by attackers is Black Hole attack. A black hole attack is an attack where the malicious node forcibly obtains the route with greatest sequence number and less hop count and subsequently overhears or drops all data packets. The wide usage of Ad Hoc networks in martial environment and other security sensitive usages have made the security a basic requirement for these networks. Because nodes participate in the routing process, they can destroy the network. As routing is based on some kind of trust between nodes, it provides a good chance for attackers to disorder routing process. It is of two types:

1.1 Non-cooperative Black Hole Attack Detection and Prevention

A non-cooperative black hole attack means that a malicious node forges false information to accomplish its misbehavior without cooperating with other malicious nodes. For example, a malicious node is able to declare it has the shortest path to destination node so that other nodes mis transmit packets to the malicious node. However, the malicious node drops these packets as well as a black hole attack and transmits fake routing packets to destroy regular routing operation.

R. Lakhwani, et., al., [1] in this paper proposed a new approach called Agent based method to detect and eliminate black hole attack. Agent based method will not only efficiently detect the black holes but completely overcome the problem by eliminating the black hole from participating in MANET thus improving the security of the AODV. In simulation using NS - 2.33, the Agent based AODV has shown outstanding results as compared to AODV in presence of black holes. Results obtained from simulation have shown that Agent based method does not introduce high overhead for the duration of secure time (no attacks) and provide better performance during attack time (presence of Black hole) in the network.

N. Sharma and A. Sharma [2] The first proposal is to find more than one route to the destination (redundant routes, at least three different routes). Then, the source node unicast a ping packet to the destination using these three routes (we should assign different packet IDs and sequence number, so any node who receive the first packet will not drop the second one if it exists in both paths). The receiver and the malicious in addition to any intermediate node might have a route to the destination will reply to this ping request. The source will check those acknowledgements, and process them in order to figure out which one is not safe and might have the malicious node. The second proposed solution exploits the packet sequence number included in any packet header. The node in this situation needs to have two extra tables; the first table consists of the sequence numbers of the last packet sent to every node in the network, and the second table for the sequence number received from every sender. During the RREP phase, the intermediate or the destination node must include the sequence number of last packets received from the source that initiates RREQ. Once the source receives this RREP, it will extract the last sequence number and then compare it with the value saved in its table. If it matches the transmission will take place. If not, this replied node is a malicious node, so an alarm message will be broadcast to warn the network about this node.

N. R. Yerneni and A. K. Sarje [3] This algorithm is based on how the malicious node behaves in order to perform the black hole attacks. To attract traffic towards it, malicious node sends false RREP packet as a response RREQ packet. It sends RRE P even if it does not have the path towards the destination as requested by the source of RREQ. It does not broadcast RREQ, instead sends RREP without checking its routing table. So, for the malicious node the ratio of number of RREQs transmitted to the number of RREPs transmitted is very less. Modified algorithm makes use of this fact to detect the black hole attack. Two extra fields are used in the proposed algorithm OAODV (opinion AODV) - request weight and reply weight. Request weight in routing table indicates the number of RREQs that are forwarded by the corresponding node. Similarly Reply weight indicates the number of RREPs forwarded. Proposed method has two modules-updating request/reply weights and collecting feedback.

R. K. Bar, et., al., [4] In the proposed work a new parameter known as 'trust value' is calculated against all the intermediate nodes. This trust value is calculated depending upon the ability to forward packets and the RREQ forwarding ability of a node. To obtain this ability the number of packets received and the number of packets sent is counted. Two weight factor W1 and W2 are introduced. W1 is the ratio of number of packets sent from a node to the number of packets received to that node. A high value of this ratio indicates that, the node has a greater ability to forward the packets. Thus, the probability of loss of packets is less. The maximum value of W1 may be 1, where all the received packets are forwarded and no packet is dropped. From this value we can also detect the untrusted nodes in the network. The other weight vector W2 is the ratio of number of RREQ received to number of RREP sent. This ratio detects the nodes which continuously receive the RREQ from its neighbor nodes but never respond to that request by sending the reply i.e. the silent node. Thus, the higher value of this ratio means that, the nodes can frequently respond to the route request of its neighbor node. Then this two-weight factor is multiplied to get the trust value of that node. Here we check if any nodes have the W1 value greater than the threshold value. If it can send a packet then the trust value is increased otherwise it is decreased. This trust value is saved in the routing table of that node. And in the route discovery step of AODV routing protocol the path is established according to that trust value rather than the shortest path. Thus, the less trusted node can be avoided during the route establishment in AODV routing protocol.

S. Biswas, el., al., [5] In this paper black-hole attack is one of the most severe routing attacks that is often encountered in MANET. In this attack, a malicious node sends fake RREP to a source node that initiates route discovery, and consequently deprives data packets from the source node. Many researchers have proposed different solutions for preventing black-hole attack. In MANET network topology changes continuously. But most of the solutions do not consider the mobility of nodes that is an important characteristic of nodes in MANET. In this paper, we have analyzed black-hole attack and proposed a solution based on trust of the individual nodes to detect and prevent black-hole attack in MANET. Trust has been calculated based on a few important parameters of a node such as rank, mobility, available battery power, etc.

R. Kumar and R. Chadha [6] In this paper, the effects of black hole attack in the performance of fuzzy and GA are analyzed. The simulation results show that when the black hole node exists in the network, it can be affected and decreased the performance of network and it can be optimized by using fuzzy and GA algorithm. A hypothetical network was constructed for the simulation purpose and then monitored for a number of parameters. The model for various nodes is simulated. Initial position for the node is specified in a movement scenario file created for the simulation using a MATLAB. The nodes move randomly among the simulation area. So, the detection and prevention of black hole attack in the network exists as a challenging task.

Sonia and H. Kaur [7] The protocol used to enhance the security is Enhance AODV (Ad-hoc on-demand distance Vector), the key concept used in the procedure is that of multipoint relays. MPRs are selected nodes which advancing broadcast messages during the flooding process. This technique significantly reduces the message overhead as associated to a classical flooding apparatus, where every node retransmits each message when it receives the first copy of the message. In mobile ad hoc networks, the movement of the network nodes may quickly change the topology resulting in the surged overhead message in topology maintenance that is why clustering techniques are used. In one of the recent researches works performed, to prevent Black hole attack. Aims and objectives of this thesis work are to design and implement IMPROVED BACTERIA FORAGINING OPTIMIZATION protocol with smartest hole attack and prevent the system for threat using this hybridization. At last evaluate the parameter explain in problem statement.

I. Woungang, et., al., In this paper, an improved version of a dynamic source routing (DSR) protocol (so-called detecting blackhole attack based on DSR (DBA-DSR)) is proposed to combat against blackhole attacks in mobile ad hoc networks. Unlike other solutions, which adopt a reactive approach in which blackhole nodes are identified only after the attack has been carried out on the network, our DBADSR scheme detects and isolates the blackhole nodes prior to the actual routing process. This is achieved by using fake route request packets.

M. B. M. Kamel, el., al., [10] Mobile ad hoc networks (MANET) is a type of networks that consists of autonomous nodes connecting directly without a top-down network architecture or central controller. Absence

of base stations in MANET force the nodes to rely on their adjacent nodes in transmitting messages. The dynamic nature of MANET makes the relationship between nodes untrusted due to mobility of nodes. A malicious node may start denial of service attack at network layer to discard the packets instead of forwarding them to destination which is known as black hole attack. In this paper a secure and trust-based approach based on ad hoc on demand distance vector (STAODV) has been proposed to improve the security of AODV routing protocol. The approach isolates the malicious nodes that try to attack the network depending on their previous information. A trust level is attached to each participating node to detect the level of trust of that node. Each incoming packet will be examined to prevent the black hole attack.

1.2 Collaborative Black Hole Attack Detection and Prevention

A collaborative black hole attack coordinates several malicious nodes cooperate to forge fake packets for reaching their misbehavior. For example, a fake RREQ or RREP sent by single attacker may be detected due to the inconsistent information of hop count or sequence number. However, two or more attackers are able to collaborate with each other for deceiving above-mentioned detection schemes.

J. M. Chang, et., al., [11] In this paper, a mechanism [cooperative bait detection scheme (CBDS)] is presented that effectively detects the malicious nodes that attempt to launch grayhole/collaborative blackhole attacks. In our scheme, the address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique. Any detected malicious node is kept in a blackhole list so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list. Unlike previous works, the merit of CBDS lies in the fact that it integrates the proactive and reactive defense architectures to achieve the aforementioned goal.

A. A. Bhosle et., al., [12] AODV is an important on-demand reactive routing protocol for mobile ad hoc networks. There is no any security provision against a "Black Hole" and "Wormhole" attacks in existing AODV protocol. Black hole nodes are those malicious nodes that conform to forward packet to destination. But they do not forward packet intentionally to the destination node. The black hole nodes degrade the performance of network eventually by participating in the network actively. The propose watchdog mechanism detect the black hole nodes in a WSN. This method first detects a black hole attack in the network and then provide a new route to this node. In this, the performance of original AODV and modified AODV in the presence of multiple black hole nodes is find out on the basis of throughput and packet delivery ratio. In a wormhole attack, intruders tunnel the data from one end of the network to the other, leading distant network nodes to trust they are neighbors' and making them communicate through the wormhole link.

I. Woungang, el., al., [13] A blackhole is a malicious node that can falsely reply for any route requests without having an active route to a specified destination and drop all the receiving data packets. The attack may even lead to more devastating damage if two or more blackhole nodes cooperate with each other to launch an attack. This type of attack is known as collaborative blackhole attack. In this paper, a novel scheme Detecting Collaborative Blackhole Attacks (so-called DCBA) for detecting collaborative blackhole attacks in WSN is introduced. Simulation results are provided, demonstrating the superiority of DCBA compared to Dynamic Source Routing (DSR) and the Bait DSR scheme (so-called BDSR) [1] - a recently proposed scheme for detecting and avoiding collaborative blackhole attacks in MANETs - in terms of network throughput rate and minimum packet loss percentage, when collaborative blackhole nodes are present in the network.

G. S. Bindra, el., al., [14] In this paper we propose a mechanism to detect and remove the blackhole and grayhole attacks. The solution we are proposing tackles these attacks by maintaining an Extended Data Routing Information (EDRI) Table at each node in addition to the Routing Table of the AODV protocol. The mechanism is capable of detecting a malicious node. It also maintains a history of the node's previous malicious instances to account for the gray behavior. Refresh packet, Renew Packet, BHID Packet, Further request and Further reply packets are also used in addition to the existing packets (RREQ and RREP). Our technique is capable of finding chain of cooperating malicious nodes which drop a significant fraction of packets.

A. Mishra, el., al., [15] In this paper we have proposed a mechanism to identify multiple black hole nodes cooperating as a group in ad hoc network. the proposed mechanism work with slightly modified AODV protocol and make use of the data routing information table (DRI) with 'check bit' in addition to cached and current routing table. We have found out misbehavior nodes in mobile ad hoc environment, and also find secure route to the destination. And enhance the performance of network by eliminating cooperative black hole attack. This type of attack is known as Cooperative Black Hole attack. We proposed a mechanism to mitigate single black hole attack as well as cooperative black hole attack to discover a safe route to the destination by avoiding attacks. In this paper we proposed an approach for better analysis and improve security of AODV, which is one of the popular routing protocols for WSN. Our scheme is based on AODV protocol which is improved by deploying Advanced DRI table with additional check bit. The Simulation on NS2 is carried out and the proposed scheme has produced results that demonstrate the effectiveness of the mechanism in detection and

elimination of the attack and maximizing network performance by reducing the packet dropping ratio in network.

S. K. Dhurandher, el., al., [16] In this paper we therefore analyses MANETs under single and collaborative Black Hole attack and prevent it by diverting traffic from the Black Hole. The WSN so discussed employ the AODV routing protocol and the method so proposed is based on sending confirmation packets that are verified by the destination to check for Black Hole presence in the GAODV routing protocol so proposed. The GAODV algorithm was then simulated in both static as well as mobile node environment and it was observed that its data delivery ratio is significantly better than the conventional AODV.

R. J. Cai, el., al., [17] A proactive security-routing protocol, SCS, and its enhanced version were proposed with the necessary assumption that internal attackers have the knowledge about how the prevention mechanism works in WSN. Our scheme could be applied on top of conventional routing protocols as a complimentary security measure. The key idea is that every node is required to exchange neighbor information before route discovery and then uses previously collected neighboring information to verify each received RREP. As the attackers do not know who will be the requested destination in the next RREQ message, they have no idea what neighbor information they need to fake in order to avoid being caught. If they randomly add many faked neighbors into broadcast Hello messages, they can be easily identified. If certain node refuses to exchange neighbor information, definitely, it will be caught if it behaves as an active black hole attacker in the next second. If attackers provide faked neighbor information after they know the requested destination, liar-checking operation will function. By utilizing previously collected neighboring information, we can greatly increase the robustness of our prevention system.

N. Arya, el., al., [18] A mobile ad-hoc network is a wireless network such that nodes are move dynamically in network. In OSI network layer there is lot of attack but introduce only collaborative black hole and worm hole attack. A group of black hole node easily employed against routing in mobile ad-hock networks called collaborative black hole attack. When two malicious nodes are creating a tunnel is called worm hole attack. This paper instigates to detect and avoided of worm hole attack and collaborative black hole attack using trusted AODV routing algorithm.

K. S. Arathy and C. N. Sminesh [19] To shield AODV from single and collaborative black hole attacks, it is essential to discover noxious nodes amid the route discovery process, when they send malicious RREPs to attract the source node. We propose two algorithms for mitigating single and collaborative black hole attacks. Three additional elements are used in the proposed algorithms specifically, a fake RREQ with nonexistent target address, a list of black hole nodes (BH list) and a list of collaborative black hole nodes (CBH list). The proposed Detection of Multiple Black Hole attack (D-MBH) algorithm detects single and multiple black hole nodes, computes a threshold for DSN (ADSN), creates BH list and invokes the proposed Detection of Collaborative Black Hole attack (D-CBH) algorithm. Using ADSN, BH list and next hop information extracted from RREP, the proposed D-CBH algorithm creates the CBH list.

S. Sharma and S. Gambhir [20] The CRCMD&R scheme is an on demand AODV like protocol that avoids malicious node attacks during route setup between source and destination. CRCMD&R scheme uses AODV to form path during path discovery. In CRCMD&R scheme, every CH node maintains the Neighbor Table, Legitimacy Value Table and Reputation Level Table which are used to keep information about all the nodes. In the route discovery phase of CRCMD&R scheme, an intermediate node will attempt to create a route that does not go through a node whose replied information is wrong or Prime Product Term is not fully divisible or reputation value of that node crosses the lower threshold value (level 1 or level 2) or reputation value greater than 1. Compared with AODV, the proposed CRCMD&R scheme has the following differences in message format and type.

III. Problem Statement And Solutions

In WSN there are several disadvantages of routing protocols thus researchers have conducted numerous techniques to propose different types of detection and prevention mechanisms for black hole attack. All of these methodologies have some or the opposite drawbacks, either it might be having higher overhead, higher packet loss, doesn't support cooperative black hole attack or increased end to end delay. This supports cooperative black hole attack and additionally offers way to facilities the server node to overcome the failure. The packets are dropped by the black-hole node, so the source does not receive acknowledgement from the destination and therefore decrements the rank of all nodes in that route.

The future work may be to reduce false positives in the propose protocol and enhance version AODV could further improve the security at the reduce routing overhead and minimizing end-to-end delay. There is no doubt at all that collaborative black hole detection method will still be a hot research issue in the future. First of all, a hybrid routing protocol is proposed by composing reactive and proactive routing methods to improve their defects.

The primary idea is that source node sends bait RREQ packets with empty target address before route discovery. Note that the bait RREQ packets only survive a while to economize the use of network throughput. Black hole nodes can be easily found because they reply forged RREP packets with destination address to the source node. As a result, source node is capable of recognizing malicious nodes because it should not receive any reply packet due to the design of empty target address. The brand-new idea can be applied to all routing protocols with a slight modification.

IV. Conclusion

The survey on wireless sensor network security is vast with various attack models and counter measures proposed by various researchers. Various methodologies are presented for ensuring security at the network layer in WSNs has been surveyed. We have discussed different issues and attacks that spoil the functioning of the network layer. We have also covered the countermeasures and potential solutions against those network layer attacks. Hopefully by reading the survey, the readers can have a better view on issues, attacks and their countermeasures at network layer in WSNs. Sensor networks are still at an early stage in terms of technology as it is still not widely deployed in real world and this opens many doors for research. The standard models of current attacks and countermeasures are able to help increase security developers' understanding and pave the way for building more secure WSNs.

References

[1] R. Lakhwani, S. Suhane, and A. Motwani, "Agent based AODV protocol to detect and remove black hole attacks," International Journal of Computer Applications, vol. 59, no. 8, pp. 35-39, 2012.

[2] N. Sharma and A. Sharma, "The black-hole node attack in WSN," in Proceedings of 2nd International Conference on Advanced Computing & Communication Technologies, Rohtak, India, 2012, pp. 546-550.

[3] N. R. Yerneni and A. K. Sarje, "Secure AODV protocol to mitigate black hole attack in mobile ad hoc," in Proceedings of 3rd International Conference on Computing Communication & Networking Technologies (ICCCNT), Coimbatore, India, 2012, pp. 1-5.

[4] R. K. Bar, J. K. Mandal, and M. M. Singh, "QoS of WSN through trust based AODV routing protocol by exclusion of black hole attack," Procedia Technology, vol. 10, pp. 530-537, 2013.

[5] S. Biswas, T. Nag, and S. Neogy, "Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in WSN," in Proceeding of Applications and Innovations in Mobile Computing (AIMoC), Kolkata, India, 2014, pp. 157-164.

[6] R. Kumar and R. Chadha, "Mitigation of black hole attack using generic algorithms and fuzzy logic," International Journal of Engineering Sciences & Research Technology, vol. 5, no. 6, pp. 818-826, 2016.

[7] Sonia and H. Kaur, "Proficient and enhance the mobile ad-hoc network using routing protocol and EBFOA (Enhanced Bacteria Foraging Optimization Algorithm)," International Journal of Modern Computer Science, vol. 4, no. 6, pp. 88-94, 2016.

[8] I. Woungang, S. K. Dhurandher, M. S. Obaidat, and R. D. Peddi, "A DSR-based routing protocol for mitigating blackhole attacks on mobile ad hoc networks," Security and Communication Networks, vol. 9, no. 5, pp. 420-428, 2016.

[9] S. Kumar and K. Dutta, "Intrusion detection technique for black hole attack in mobile ad hoc networks," International Journal of Information Privacy, Security and Integrity, vol. 2, no. 2, pp. 81-101, 2015.

[10] M. B. M. Kamel, I. Alameri, and A. N. Onaizah, "STAODV: a secure and trust based approach to mitigate blackhole attack on AODV based WSN," in Proceedings of IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 2017, pp. 1278-1282.

[11] J. M. Chang, P. C. Tsou, I. Woungang, H. C. Chao, and C. F. Lai, "Defending against collaborative attacks by malicious nodes in WSN: a cooperative bait detection approach," IEEE Systems Journal, vol. 9, no. 1, pp. 65-75, 2015.

[12] A. A. Bhosle, T. P. Thosar, and S. Mehatre, "Black-hole and wormhole attack in routing protocol AODV in MANET," International Journal of Computer Science, Engineering and Applications (IJCSEA), vol. 2, no. 1, pp. 45-54, 2012.

[13] I. Woungang, S. K. Dhurandher, R. D. Peddi, and I. Traore, "Mitigating collaborative blackhole attacks on DSR-based mobile ad hoc networks," in Proceedings of the International Symposium on Foundations and Practice of Security, Montreal, Canada, 2012, pp. 308-323.

[14] G. S. Bindra, A. Kapoor, A. Narang, and A. Agrawal, "Detection and removal of co-operative blackhole and grayhole attacks in WSN," in Proceedings of International Conference on System Engineering and Technology (ICSET), Bandung, Indonesia, 2012, pp. 1-5.

[15] A. Mishra, R. Jaiswal, and S. Sharma, "A novel approach for detecting and eliminating cooperative black hole attack using advanced DRI table in ad hoc network," in Proceedings of 3rd IEEE International Advance Computing Conference (IACC), Ghaziabad, India, 2013, pp. 499-504.

[16] S. K. Dhurandher, I. Woungang, R. Mathur, and P. Khurana, "GAODV: a modified AODV against single and collaborative black hole attacks in WSN," in Proceedings of 27th International Conference on Advanced Information Networking and Applications Workshops, Barcelona, Spain, 2013, pp. 357-362.

[17] R. J. Cai, X. J. Li, and P. H. J. Chong, "A novel self-checking ad hoc routing scheme against active black hole attacks," Security and Communication Networks, vol. 9 no. 10, pp. 943-957, 2016.

[18] N. Arya, U. Singh, and S. Singh, "Detecting and avoiding of worm hole attack and collaborative blackhole attack on WSN using trusted AODV routing algorithm," in Proceedings of International Conference on Computer, Communication and Control (IC4), Indore, India, 2015, pp. 1-5.

[19] K. S. Arathy and C. N. Sminesh, "A novel approach for detection of single and collaborative black hole attacks in WSN," Procedia Technology, vol. 25, pp. 264-271, 2016.

[20] S. Sharma and S. Gambhir, "CRCMD&R: cluster and reputation based cooperative malicious node detection & removal scheme in WSN," in Proceedings of 11th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 2017, pp. 336-340.