International Journal of Scientific Research & Engineering Trends
Volume 6, Issue 2, Mar-Apr-2020, ISSN (Online): 2395-566X

A Review on Suspicious Attack Detection

Ranu Dilware
Dept. of Electronic and Communication (Digital Communication)
Sagar Institute Of Research & Technology
Indore,ranudilware123@gmail.com

Asst.Prof. Dr Dev Kumar Rai
Dept. of Electronic and Communication
SAGE Univesity Indore
dev47076@gmail.com

Dr. Akhilesh Upadhyay
Head of Institution
Dept. of Electronic and Communication
SAGE university Indore
akhileshupadhyay@gmail.com

***Abstract* – Wireless Sensor Networks (WSN) is a drifting innovation inside the present time and contains a major choice of utilizations, for example, front line observation, traffic reconnaissance, woodland fire recognition, flood location and so forth. A few scientists have led very surprising location strategies and calculations to proposed contrasting sorts of discovery plans. Wireless sensor end up being such a lot of common in numerous fields in view of its handiness in military, current region and so on. The blackhole nodes will dispatch blackhole attack to save its asset or to perform attack that decrease the system. Right now, the current arrangements and talk about the best in class steering strategies. This paper audits the current condition of workmanship strategies to identify the blackhole attack in Wireless Sensor Networks.**

***Keywords* – MANET, Blackhole attacks, Wireless Sensor Networks, AODV, DSN.**

I. INTRODUCTION

The wireless sensor networks are formed by the collection of nodes that are geographically distributed. The sensor node consists of three things such as communication component, sensing component, and computation, or data processing component. These device nodes collect the information, method the information, and transmit to the sink node or base station by operating along. The basic unit of a wireless sensor network is a device node that consists of aboard sensors, power offers, memory, processor, and wireless electronic equipment. A device converts a natural phenomenon like sound, light, heat, etc. into electrical or different signals that act as an electrical device. A WSN is an assortment of numbers of device nodes that unit of measurement distributed in the atmosphere. It's extremely a special form of Ad-hoc network. The key feature of WSN includes its use of things as a result of it's self-organizing and self-maintaining. As a result of the infrastructure-less atmosphere and wireless nature of WSN, they are a heap of laid low with many types of security attacks.

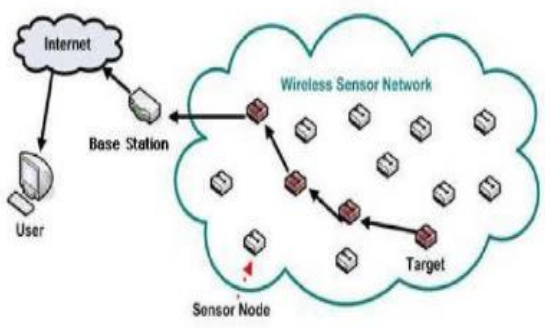

Fig.1.Basic Structure of Wireless Sensor Network.

There are several types of attacks that can be done by malicious nodes to damage the network and make that network unreliable for communication and proper working. Some of such kinds of attacks are:

1. Wormhole Attack
In a wormhole attack, the attacker records packets at one place and tunnels those to another place in the network. Due to this, it creates a False scenario that the main sender is a neighbor of the remote location. Wormhole forms by tunneling procedure in sensor networks.

2. Tempering
its tempers hardware configuration of a sensor and gain physical access for making node as adversary node. Tempering can be done at the physical layer.

3. Jamming
this attack is related to troublemaking or interfering radio frequencies, which are used by sensor nodes. By gating physical access of some nodes, the attacker can create jams in the network to disturb the network.

4. Sybil Attack
In a Sybil attack, a malicious node illegally takes multiple identities. In this, an adversary can appear in multiple places at the same time. A node presents multiple identities to other nodes in the network by stealing or fabricating the identities of authenticated nodes. This attack is made on the network layer.

5. Hello Flood Attack
It uses HELLO packets as a weapon to convince the sensors in WSN. In this attack, an attacker has a high radio transmission range and processing power. They

send HELLO packets to several sensor nodes that are in a large area within a WSN.

6. Black Hole Attack

In the black-hole attack, the advertises of the wrong paths as good paths to the source node by a malicious node during the pathfinding process as in reactive routing protocols or the route updating messages as in proactive routing protocols.

II. BLACKHOLE ATTACK

Blackhole attacks are one of the attacks in WSNs. It is an attack that is mounted by an external adversary on a subset of the sensor nodes (SNs) in the network. In the black hole attack, a malicious node advertises the wrong paths as right paths to the source node during the pathfinding process as in reactive routing protocols or the route updating messages as in proactive routing protocols. The right way means the shortest path from the source node to the destination node or the most stable track through the sensor network[7]—Fig. 2 to illustrate these terms. In the figure, are black hole node is represented by a red border, and dotted lines serve the black hole region. When the source node selects the path, which includes the attacker node, the traffic starts passing through the adversary node, and this node start dropping the packets selectively or as a whole. Blackhole region is that the entry purpose of an outsized variety of harmful attacks.

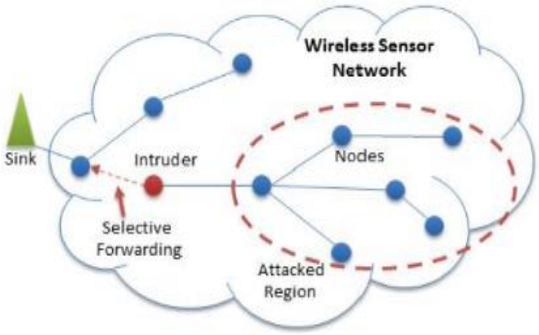

Fig. 2. Blackhole attack in Wireless Sensor Networks.

Security against this attack is a challenging problem that can be detected and prevents various techniques. Several researchers have proposed different detection and prevention techniques.

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 receives the destination address, it creates an RREP in response and sends it back to the original sender

III. REVIEW OF LITERATURE

Taylor Vincent F, Fokum Daniel T [1] discussed Wireless sensor networks comprise of autonomous, self-organizing, low-power nodes that cooperatively measure data in an environment and cooperate to route this data to its intended destination. Blackhole attacks are potentially devastating attacks on wireless sensor networks in which a malicious node utilizes spurious route updates to attract network movement that it then drops. We propose a robust and flexible attack detection scheme that uses a watchdog mechanism and lightweight expert system on every node to detect anomalies in the behavior of neighboring nodes. Utilizing this scheme, regardless of the possibility that malicious nodes are inserted into the network, high nodes will have the capacity to identify them based on their behavior as inferred from their network activity. We examine the resource-preserving mechanisms of our system utilizing simulations and demonstrate that we can allow groups of nodes to all in all evaluate network activity and identify attacks while regarding the limited hardware resources (handling, memory, and capacity) that are typically accessible on wireless sensor network nodes.

R. Lakhwani, et., al. [1] proposed a new approach called the Agent-based method to detect and eliminate black hole attacks. Agent-based mostly technique won't solely expeditiously notice the parts; however, utterly overcome the matter by eliminating the black hole from taking part in painter so rising the protection of the AODV. In simulation victimization NS - a pair of.33, the Agent-based AODV has shown outstanding results as compared to AODV in the presence of black holes. Results obtained from simulation have shown that Agent-based mostly technique doesn't introduce high overhead for the period of secure time (no attacks) and supply higher performance throughout attack time (presence of Blackhole) 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 unicasts 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 supply can check those acknowledgments, and process them 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 could be a malicious node, so an alarm message will be broadcast to warn the network about this node.

N. R. Yerneni and A. K. Share [3] found an algorithm that is based on how the malicious node behaves to perform the black hole attacks. To attract traffic towards it, a malicious node sends a 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, it sends RREP without checking its routing table. So, for the malicious node, the ratio of the number of RREQs transmitted to the number of RRSPs transmitted is very less. The 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 a weight and reply weight. The request weight in the routing table indicates the quantity of RREQs that area unit forwarded by the corresponding node. Similarly, Reply weight indicates the number of RRSPs forwarded. The proposed method has two modules-updating request/reply weights and collecting feedback.

K. Bar, et., al., [4] In the proposed work, a new parameter is known as 'trust value' is calculated against all the intermediate nodes. This trust price is calculated, relying upon the flexibility to forward packets and, therefore, 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 factors W1 and W2, are introduced. W1 is the ratio of several packets sent from a node to the number of packets received to that node. A high price of this magnitude relation indicates that the node has a greater ability to forward the packets. Thus, the chance of loss of packets is a smaller amount. The maximum value of W1 maybe 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 the number of RREQ received to the number of RREP sent. This magnitude relation detects the nodes that incessantly receive the RREQ from its neighbor nodes; however, ne'er reply to that request by causation the reply, i.e., the silent node. Thus, the upper price of this quantitative relation implies 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 will send a packet, then the trusted price is enlarged; otherwise, it's reduced. This trust price is saved within the routing table of that node. And within the route discovery step of the AODV routing protocol, the trail is established per that trust price instead of the shortest path. Thus, the less trusty node may be avoided throughout the route institution in the AODV routing protocol.

R.Biswas, el., al., [5] 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 of the source node. Many researchers have proposed different solutions for preventing a black-hole attack. In the 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 attacks and proposed a solution based on the trust of the individual nodes to detect and prevent black-hole attacks 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], the effects of the 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 the network, and it can be optimised by using the fuzzy and GA algorithm. A theoretical network was made for the simulation purpose then monitored for a variety of parameters. The model for various nodes is simulated. The initial position for the node is specified in a movement scenario file created for the simulation using MATLAB. The nodes move randomly among the simulation area. So, the detection and interference of part attack within the network exist as a difficult task.

Sonia and H. Kaur [7] The protocol used to enhance the security is to Enhance AODV (Ad-hoc on-demand distance Vector), the key concept used in the procedure is that of multipoint relays. MPRs have selected nodes that advancing broadcast messages during the flooding process.
This technique considerably reduces the message overhead as associated with a classical flooding instrumentality, where every node retransmits each message when it receives the first copy of the message. In spontaneous mobile 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. One of the recent researches works performed to prevent Blackhole attack. Aims and objectives of this thesis work are to design and implement IMPROVED BACTERIA FORAGING OPTIMIZATION protocol with the smartest hole attack and prevent the system for threat using this hybridization. At last, evaluate the parameter explain in the problem statement.

I. Woungang, et., al., 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 before the actual routing process. This is achieved by mistreatment faux route request packets.

M. B. M. Kamel el. al., [10] Mobile accidental networks (MANET) could be a sort of network that consists of autonomous nodes connecting directly while not a top-down specification or central controller. The absence of base stations in MANET forces the nodes to rely on their adjacent nodes in transmitting messages. The dynamic nature of Edouard Manet makes the connection between nodes untrusted because of the quality of nodes. A malicious node might begin denial of service attack at the network layer to discard the packets rather than forwarding them to a destination that is thought of as a region attack. In this paper, a secure and trust-based approach supported spontaneous on-demand distance vector (STAODV) has been planned to enhance the safety of the AODV routing protocol. The approach isolates the malicious nodes that attempt to attack the network betting on their previous data. A trust level is connected to every taking part node to find the extent of the trust of that node. Each incoming packet is going to be examined to forestall the region attack.

J. M. Chang, et., al., [11] a mechanism [cooperative bait detection theme (CBDS)] is providing effectively detects the malicious nodes that attempt to launch gray hole/collaborative black hole attacks. In our theme, the address of Associate in the Nursing adjacent node is employed as the bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes square measure detected using a reverse tracing technique. Any malicious detected node is kept in a blackhole list so that all other nodes
that participate in 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 goal above.

A. A. Bhosle et., al. [12] AODV is an important on-demand reactive routing protocol for mobile ad hoc networks. There are no security provisions against a "Black Hole" and "Wormhole" attacks in existing AODV protocol. Blackhole nodes are those malicious nodes that conform to forward the packet to the destination. But they do not forward the packet intentionally to the destination node. The black hole nodes degrade the performance of the network eventually by participating in the network actively. The proposed watchdog mechanism detects the black hole nodes in a WSN. This method first detects a black hole attack in the network and then provides a new route to this node. In this, the performance of original AODV and modified AODV in the presence of multiple black hole nodes find out based on 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 black hole 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 might even cause a lot of devastating injuries if two or a lot of black hole nodes work with one to launch an attack. This type of attack is known as a collaborative black hole 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 unit of measurement 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 cooperative blackhole attacks in MANETs - in terms of network output rate and minimum packet loss proportion, when collaborative black hole nodes are present in the network.

G. S. Bindra, el., al., [14] proposed a mechanism to detect and remove the black hole and gray hole attacks. The solution we tend to square measure proposing tackles these attacks by maintaining AN Extended information Routing data (EDRI) Table at every node additionally 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 a chain of cooperating malicious nodes that drop a significant fraction of packets.

A. Mishra el. al. [15] proposed a mechanism to identify multiple black hole nodes cooperating as a group in an ad hoc network. the proposed mechanism works with slightly modified AODV protocol and makes use of the data routing information table (DRI) with 'check bit' in addition to the cached and current routing table. We have found out misbehavior nodes in the mobile ad hoc environment and also find a secure route to the destination. And enhance the performance of the network by eliminating a cooperative black hole attack. This type of attack is thought of as a Cooperative region attack. We projected a mechanism to mitigate a single region attack likewise as a cooperative region attack to get a secure

route to the destination by avoiding attacks. In this paper, we proposed an approach for better analysis and improved the security of AODV, which is one of the popular routing protocols for WSN. Our theme is predicated on the AODV protocol that is improved by deploying the Advanced DRI table with an extra bit. The Simulation on NS2 is dispensed, and therefore, the planned theme has created results that demonstrate the effectiveness of the mechanism in detection and elimination of the attack and maximizing network performance by reducing the packet dropping magnitude relation in the network.

S. K. Dhurandher, el., al., [16] we, therefore, analyze MANETs under single and collaborative Black Hole attack and prevent it by diverting traffic from the Black Hole. The WSN, therefore, mentioned I use the AODV routing protocol, and also, the technique therefore projected is predicated on causing confirmation packets that square measure verified by the destination to visualize 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 know 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 to avoid being caught. If they randomly add many faked neighbors into broadcast Hello messages, they can be easily identified. If a certain node refuses to exchange neighbor information, 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, the 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 moved dynamically in the network. In the OSI network layer, there's a heap of attack however introduces a solely cooperative part and wormhole attack. A group of black hole nodes easily employed against routing in mobile ad-hoc networks called collaborative black hole attack. When two malicious nodes are creating a tunnel is called a wormhole attack. This paper instigates to detect and avoided of wormhole attack and collaborative black hole attack using a trusted AODV routing algorithm.

K. S. Arathy and C. N. Smith [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 cooperative part attacks. Three additional elements are used in the proposed algorithms, specifically, a fake RREQ with the 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 a 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 set up between source and destination. CRCMD&R scheme uses AODV to form a path during path discovery. In the 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.

IV. CONCLUSION

Wireless sensor networks have gained much popularity over the past few years. Security is the biggest threat in WSNs. In this paper, we describe Attacks which degrade the performance of a wireless sensor network. The black hole attack is the active type of attack, which reduces network performance in terms of various parameters. This paper reviews various techniques that are used for the detection of malicious nodes and discussed in terms of various parameters. This paper mainly focuses on the working of various related techniques; different steps involved in the detection of attacks in WSN.

REFERENCES

[1]. Taylor Vincent F, Fokum Daniel T "Mitigating Black Hole Attacks in Wireless Sensor Networks Using NodeResident Expert Systems," Washington, DC,pp.1- 7, IEEE,2014.

[2]. 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.
[3]. 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.
[4]. 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.
[5]. R. K. Bar, J. K. Mandal, and M. M. Singh, "QoS of WSN through trust-based AODV routing protocol by the exclusion of black hole attack," Procedia Technology, vol. 10, pp. 530-537, 2013.
[6]. 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.
[7]. R. Kumar and R. Chadha, "Mitigation of black hole attack using genetic algorithms and fuzzy logic," International Journal of Engineering Sciences & Research Technology, vol. 5, no. 6, pp. 818-826, 2016.
[8]. 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.
[9]. 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.
[10]. 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.
[11]. 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.
[12]. 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.
[13]. 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.
[14]. Woungang, S. K. Dhurandher, R. D. Peddi, and I. Traore, "Mitigating collaborative black hole 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.
[15]. G. S. Bindra, A. Kapoor, A. Narang, and A. Agrawal, "Detection and removal of a co-operative black hole and gray hole attacks in WSN," in Proceedings of International Conference on System Engineering and Technology (ICSET), Bandung, Indonesia, 2012, pp. 1-5.
[16]. 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.
[17]. 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.
[18]. 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.
[19]. N. Arya, U. Singh, and S. Singh, "Detecting and avoiding of wormhole attack and collaborative black hole 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.
[20]. 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.
[21]. 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.