International Journal of Engineering & Technology, 7 (4.41) (2018) 139-144

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Simulative Study of Black Hole Attack for Wireless Networks and Network Performance Analysis Over NS2

Monika Jain[1]*, Rahul Saxena[1*], [2]Aashis Kumar, [2]Tushar Sadana, [2]Vidyanshu Jain, [2]Siddharth Jaidka

[1]Assistant Professor, Manipal University Jaipur
[2]Student, Manipal University Jaipur
**Corresponding author E-mail: rahulsaxena0812@gmail.com*

Abstract

Wireless networks are the most popular and widely used class of networks in the world. Because of its extreme level usage, it is more prompt to attack in the network. In recent times there has been increase in the frequency of cyber-attacks for example Ransomware that has affected various organization of different sectors (Health care, defense etc). In order to prevent such attacks on our systems it is important to understand the methodology of these attacks and how they impact the efficiency of available network. This paper provides us the insight about how such an attack is performed and what are the counter measure we can take to improve the security of network system in place around the world. The major objective of the paper is the simulation of Black hole attack on a wireless network and studying its effects. We have also evaluated the network efficiency with varying number of nodes under the conditions of with and without attack.

Keywords: *Security, efficiency, black hole attack*

1. Introduction

Communication between mobiles, laptops and other devices is a most common phenomenon occurs on a day-to-day basis. The most common configuration in the wireless network is an *Ad hoc configuration*. An adhoc network is a network in which every node present in the network will perform as router. Nodes location and topology is not fixed, nodes can join and leave network according to accessibility and thus they are highly dynamic in nature. They are autonomous in nature where the messages are exchanged from node to node. Biggest challenge in adhoc network is to maintain power consumption and available memory in the network. Adhoc networks are highly adaptable in nature. The communication between these nodes are done through routing protocol. Fig. 1.1 Shows the example of wireless network in which all the nodes available in the network connect to the centralized router and router maintains the network and basic exchange of data between nodes.

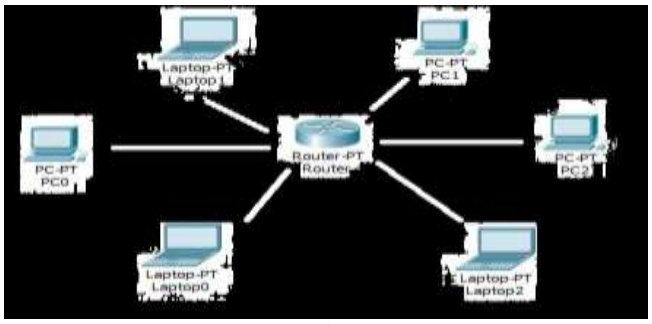

Fig.1.1: Example of Wireless Network

Fig. 1.2 Describe the exchange of data between the devices, note that these devices do not need centralized router for communication between the nodes. Wireless adhoc network are distributed in nature in which each node is autonomous and capable of sending and receiving the data. If the nodes are within the network, it can communicate with any device present on the network. Every node can join and leave the network according to the scenario.

Fig. 1.2: Example of Wireless Adhoc network

Fig. 1.3 Describe the architecture of one of the specialized part of wireless adhoc network i.e., Mobile adhoc networks. First layer is the enabling technologies in which it specifies the MAC, Antennas the protocols supported are 802.11, Bluetooth. The other layer is transport and network layer protocols in which protocol supported are TCP, IP routing, Addressing, Location etc. The next layer is the middleware in which it specifies services Location, Group communication shared memory

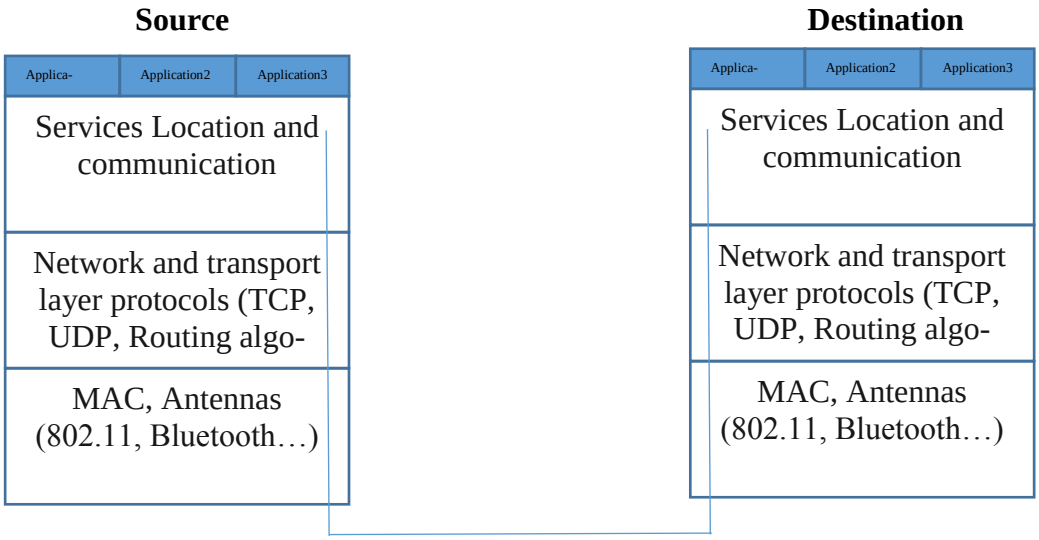

Fig. 1.3: Architecture of wireless adhoc network [1]

Challenges in Wireless Adhoc networks

There are some challenges in Adhoc networks, which affect the performance of the networks [2]. Like highly mobile nature of nodes, which makes it difficult for sending and receiving of messages due to frequent join and disconnect of the nodes. Lots of power needed for nodes to process the messages and sending the messages to destination through intermediate nodes, so limited power available is another flaw in the wireless adhoc networks. Packets loss is another issue, because of the frequently changing the topology of the system hence quality of service is degraded. Security is the biggest challenge in wireless network, because the messages send by the source node are broadcast messages, which are received by every node present in the network, so security is always the major concern in wireless network.

2. Security in Wireless sensor network

What brings the comfort also bring some kind of side effects. Due to the wide usage of wireless communication between nodes, it is vulnerable to many kind of attacks. Various attacks are possible in each layer of OSI [13]. These kinds of attacks directly impact the availability, confidentiality, and integrity of the nodes. Wireless networks are more susceptible because of its distributed nodes, node mobility and no infrastructure [14]. As all the nodes has to participate through routing, nodes have to trust the other nodes available on the network. Because of these attacks, there is a huge impact on performance of the network. Security in wireless adhoc network is a broad area because there are different attacks possible on each layer of OSI. We have focused on two attacks i.e. Denial of service attack and black hole attack because they severely damage the network and directly affects the performance of nodes.

2.1 Denial of Service attack (DoS)

It is a common attack is a very common and special kind of attack where the attacker directly attacks on the resources available. As shown in Fig. 2.1 it disrupts the services offered to the host provided by the internet. Generally, these kind of attacks can be done by sending flooded requests to the resource. These requests are not valid and they overload the system such that the resource becomes unavailable to the genuine host. Many requests at the same time are sent to the resource node. When the resource node sends the authentication approval message, attacker does not fulfill the authentication thus creating endless waiting for the server. In this way, server gets busy by multiple requests. There are serious consequences of DoS attack like the services offered becomes unavailable, inaccessible while increasing the network traffic. Unfortunately, there are not many solutions available for the DoS attacks but some precaution we can take to prevent Denial of service attack. Like filtering, the types of data receive to prevent the data received from the unknown traffic. Usage of antivirus and firewall can also prevent the Denial of service attack from happening.

Fig. 2.1: DoS attacks on wireless network

2.2 Black hole attack

It is a famous kind of attack in which intruder act as intermediate node between the devices and accepts the packet from the source claiming to reach at the destination through shortest path. Malicious node discovers and uses the route discovery process, and these malicious nodes make themselves undetectable to the network, it can only be detected when special monitoring occurs in the network for lost data.

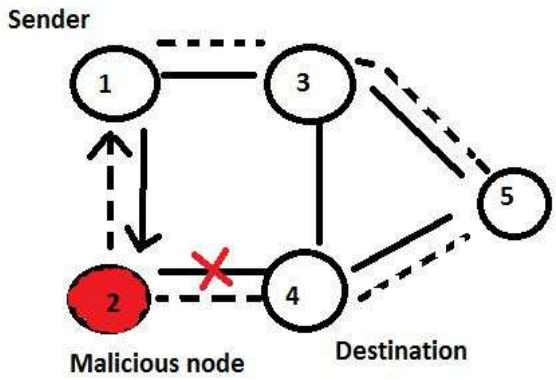

Fig. 2.2: Description of black hole attack

As depicted in Fig. 2.2 node 1 is the source node who wants to send data to node 4; node 2 is a mischievous node which claims that it is directly reachable to node 4. After receiving data from the node 1, malicious node drops the packet and send the acknowledgment to the source that it has send the packet. This misrouting of packets can be easily done on wireless network as it is open to route discovery query.

3. Related work

Mohammad Al-Shurman et.al, discusses "Black hole attack in mobile Ad Hoc networks" in which author has discusses in detail about black hole attack, and two solutions has been proposed for black hole the first is to have more one route for the destination and other is the use of the sequence number [3]

C.V. Anchugam et.al, discusses "Detection of Black Hole Attack in Mobile Ad-hoc Networks using Ant Colony Optimization – simulation Analysis" in this paper AODV routing protocol is modified by the concept of ant colony optimization for increasing the throughput and packet ratio [4]

Fihri et. al, discusses "The Impact of Black-Hole Attack on AODV Protocol", where it has implemented black hole attack [5]

Rooshabh Kothari et.al., discusses "Implementation of Black Hole Security Attack using Malicious Node for Enhanced - DSR Routing Protocol of MANET" in which the analysis of black hole attack is done over the proposed scheme for performance analysis using different number of nodes. But in this paper only black hole attack is studied with different number of nodes [6]

Debarati Roy et.al., discusses "Implementing and Improving the Performance of AODV by Receive Reply Method and Securing it from Black Hole Attack" discusses the solution of black hole attack to increase the performance of AODV by receive and reply method [7]

Ashwini et.al, discusses "Implementation of Black Hole Attack Detection and Mitigation in MANET Using Advance BFO Algorithm" in which it detects black hole attacker which reduces the energy consumption and packet delivery, however the detection can be improved by adding additional method [8]

Amandeep Kaur et.al, "Implementation of Black hole attacks in WSN using Genetic Algorithm and PSO" discusses paper implemented black hole attack and comparison have been done for GA and PSO for AODV routing protocols [9]

4. Implementation

We have implemented a black hole attack in network simulator 2.35. It is an open-source event-driven simulator designed specifically for research in computer communication networks.

Table1: Network Parameters used for simulation of black hole attack

Network Parameters	
Processor Used	Intel core i5
Ram	4 gigabytes
Operating System	Linux (Ubuntu)
Software	NS 2.35
Routing Protocol	AODV
Channel type	Wireless Channel

5. Simulation Results

The simulation of wireless networks with and without black hole attack and the performance of both the networks are analyzed over here, Fig. 5.1 and Fig. 5.2 Shows the Simple wireless network simulation on network animator without black
hole attack. In this scenario node 0 and node 2 are source nodes and node 3 and node 5 are destination nodes. The received throughput in wireless network is 300.04 and sender to receiver packet ratio is 1. Likewise, we have simulated black hole attack as shown in Fig. 5.3 and Fig. 5.4 on wireless network by making node1 as malicious node, the source node is again node 0 and node 2 and target nodes are node 3 and node 5. The received throughput after the attack of malicious node decreases from 300.04 to 200.58 and sender to receiver packet ratio decreases from 1 to 0.66. Packets get lost in the transmission due to the black hole created between the sender and receiver.

Table II. Shows the Simulation steps implemented in NS2

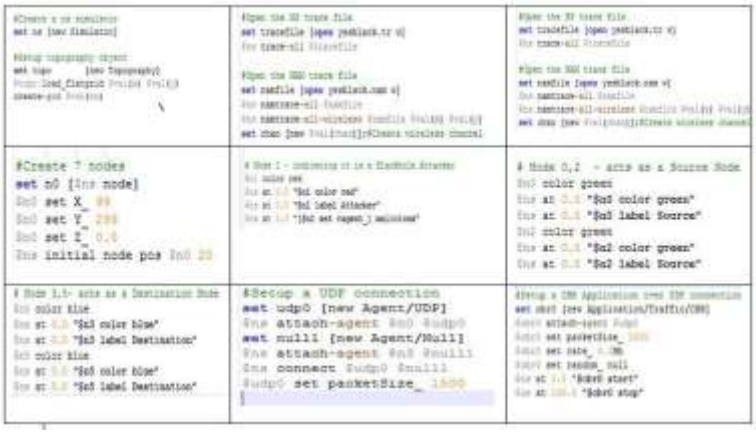

Fig.5.1: Simple wireless network stimulation on network animator without black hole attack

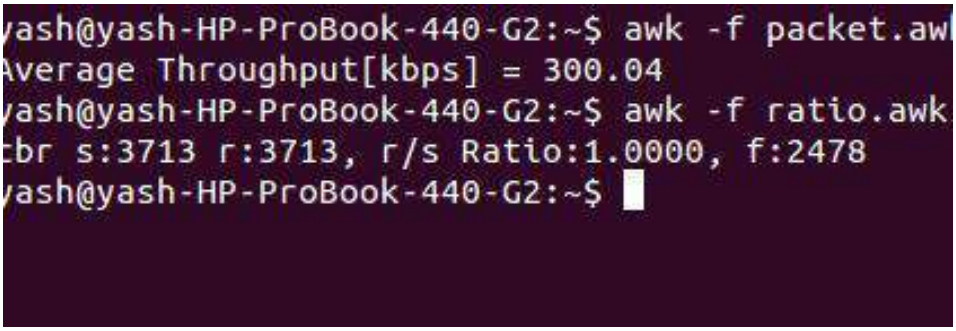

Fig.5.2: Snapshot of received Throughput and sender to receiver packet ratio

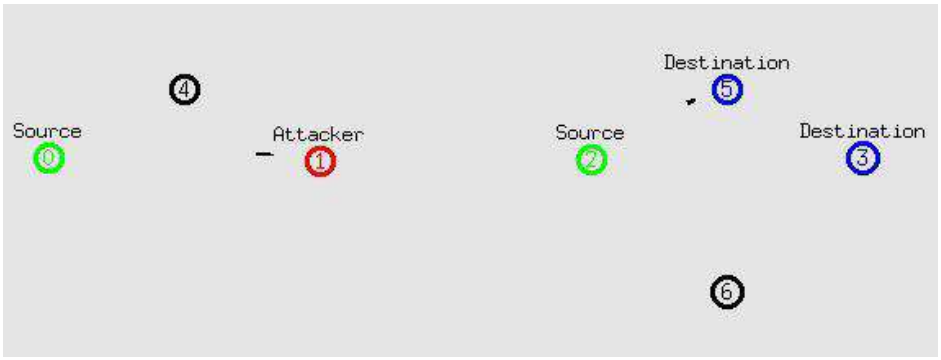

Fig.5.3: Black hole attack stimulation on network animator

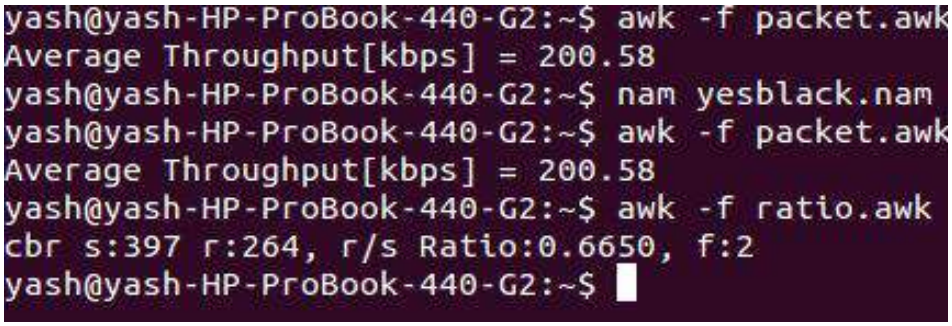

Fig.5.4: Snapshot of Average Throughput and sender to receiver ratio

We have extended our work by varying different number of nodes with different number of attackers. Simulation of work done is as follows:

- 7 nodes with one malicious node and without any malicious node
- 17 nodes with one malicious node and without any malicious node
- 26 nodes with 3 malicious nodes and without any malicious node
- 51 nodes with 3 malicious nodes and without any malicious node

Throughput obtained in these above scenarios with and without black hole attack is shown in Fig. 6.1 Sender to receiver ratio obtained in these scenarios is shown in Fig. 6.2 Black hole attack severely damages and degrades the throughput and sender to receiver ratio.

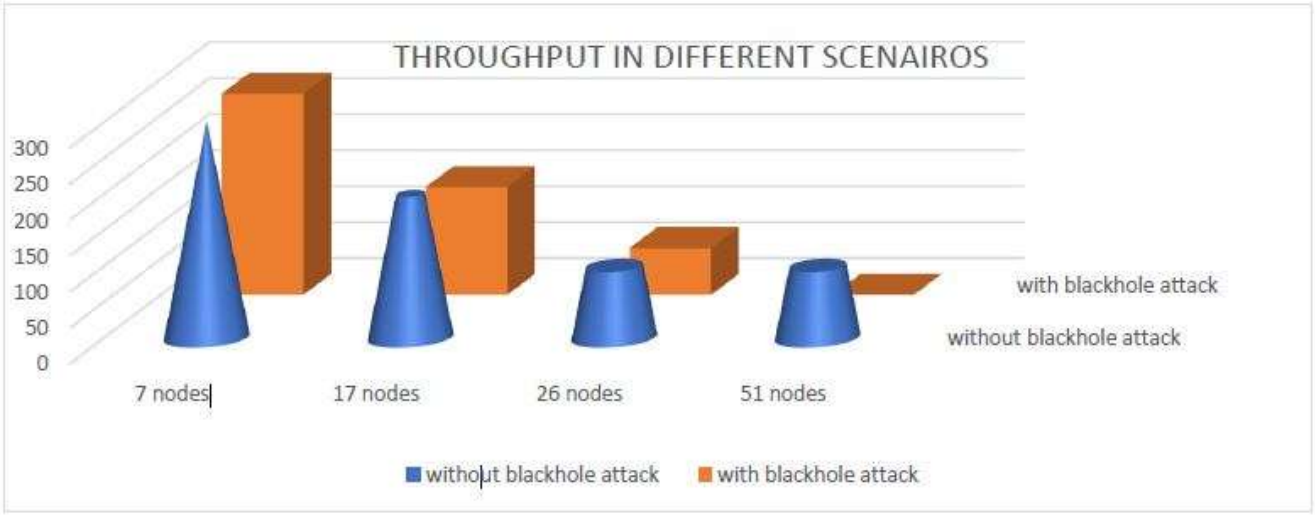

Fig. 6.1: Throughput comparison in different scenarios

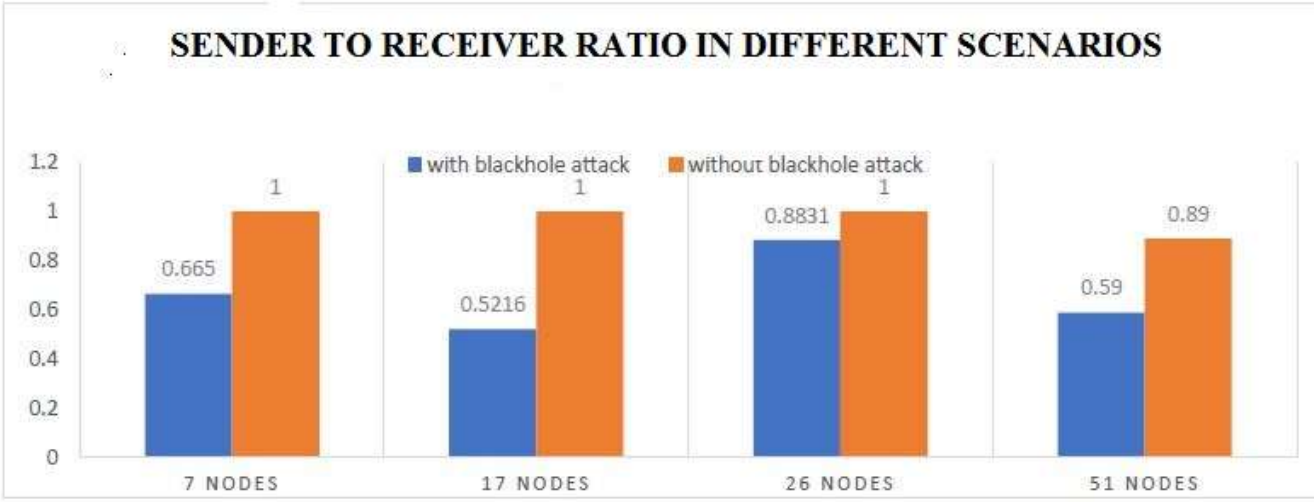

Fig. 6.2: Sender to receiver ratio comparison in different scenarios

6. Solution to black hole attack

Some solutions are proposed for black hole attack like trust based routing, intrusion detection system, sequence number comparison and data routing information tableIn trust based routing [10], a trust model has been developed which manage different trust levels, basically it estimates the level of trust to each node to help the source node. The other method is Intrusion Detection System [11]. As the name implies, it is a system which monitors the network for an unusual activity. It uses alarm filtering techniques to distinguish malicious activity from false alarms. Sequence number prevents black hole attack by checking the difference between the sequence number of source node and intermediate node that sent the message [12]. If the large sequence number is detected in comparison with source node, the intermediate node is marked as malicious node and forcefully removed from the network. The other solution is data routing information table in which data table is maintained and stored in a router which stores all the routes available along with the metrics. From these methods the intermediate route can be analyzed and better decision can be taken by the source node.

7. Conclusion

The wise usage of wireless network along with their characteristics have been discussed. Along with enormous facilities provided by wireless ad hoc network yet it is vulnerable to some possible attacks. In this paper, we have seen that black hole reduces the efficiency of overall network and directly affects the performance of the system. Simulation of general scenario and attacked scenario is discussed by comparing the average throughput and packet ratio of Black hole attack. From these simulations, we can say that the throughput and packet ratio is more for simple network than the attacked network. Thus, it can be concluded by saying that attacks reduce the efficiency of the network. By increasing the nodes to 7, 17, 26, 51, average throughput and packet ratio have been calculated. The future work, which can be further carried out, is the implementation of prevention or the solution for the scenario when the attack has taken place by causing minimal loss of data or without affecting the throughput and data loss of the network.

References

[1] Jai Shree Mehta, Shilpa Nupur, Swati Gupta: An Overview of MANET: Concepts, Architecture & Issues, International Journal of Research in Management, Science & Technology (E-ISSN: 2321-3264) Vol. 3, No. 2, April 2015.

[2] Iqbaldeep Kaur, Navneet Kaur, Tanisha, Gurmeen, Deepi: Challenges and Issues in Adhoc Network, IJCST Vol. 7, Issue 4, Oct - Dec 2016 ISSN: 0976-8491 (Online) | ISSN: 2229-4333 (Print)
[3] Mohammad Al-Shurman, Seong-Moo Yoo, Seungjin Park: Black hole attack in mobile Ad Hoc networks, ISBN:1-58113-870-9 doi>10.1145/986537.986560.
[4] C.V. Anchugam* and K. Thangadurai: Detection of Black Hole Attack in Mobile Ad-hoc Networks using Ant Colony Optimization – simulation Analysis, Indian Journal of Science and Technology, Vol 8(13), DOI: 10.17485/ijst/2015/v8i13/58200, July 2015.
[5] FIHRI Mohammed, LAVETE, Morocco, LAVETE: The Impact of Black-Hole Attack on AODV Protocol, International Journal of Advanced Computer Science and Applications (IJACSA).
[6] Rooshabh Kothari discusses: Implementation of Black Hole Security Attack using Malicious Node for Enhanced - DSR Routing Protocol of MANET, International Journal of Computer Applications, (0975 – 8887) Volume 64– No.18, February 2013.
[7] Debarati Roy, LeenaRagha, Dr.bNilesh Marathe: Implementing and Improving the Performance of AODV by Receive Reply Method and Securing it from Black Hole Attack, International Conference on Advanced Computing Technologies and Applications (ICACTA2015), https://doi.org/10.1016/j.procs.2015.03.109.
[8] Ashwini Hosgouda, Shobha m s, Akshay Shivanand: Implementation of Black Hole Attack Detection and Mitigation in MANET Using Advance BFO Algorithm, International Journal of Advanced Research in Computer Science and Software Engineering, 2015.
[9] Amandeep Kaur, Praveen Kaur, Harish ran Aggarwal: Implementation of Black hole attacks in WSN using Genetic Algorithm and PSO, Advances in Wireless and Mobile Communications. ISSN 0973-6972 Volume 10, Number 4 (2017), pp. 717-726.
[10] S. Biswas, T. Nag and S. Neogy: Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET, 2014 Applications and Innovations in Mobile Computing (AIMoC), Kolkata, 2014, pp. 157-164. doi: 10.1109/AIMOC.2014.6785535
[11] N. Boumkheld, M. Ghogho and M. El Koutbi: Intrusion detection system for the detection of blackhole attacks in a smart grid, 2016 4th International Symposium on Computational and Business Intelligence (ISCBI), Olten, 2016, pp. 108-111. doi: 10.1109/ISCBI.2016.7743267.
[12] A. Salunke and D. Ambawade: Dynamic Sequence Number Thresholding protocol for detection of blackhole attack in Wireless Sensor Network, 2015 International Conference on Communication, Information & Computing Technology (ICCICT), Mumbai, 2015, pp. 1-4. doi: 10.1109/ICCICT.2015.7045745
[13] Jain, Monika, and Rahul Saxena. "Overview of VANET: Requirements and its routing protocols." Communication and Signal Processing (ICCSP), 2017 International Conference on. IEEE, 2017.
[14] Jain, Monika, and Rahul Saxena. "VANET: Security Attacks, Solution and Simulation." Proceedings of the Second International Conference on Computational Intelligence and Informatics. Springer, Singapore, 2018.