Volume 9, Issue 6, June – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1551

A Study on Different Types of Blackhole and Wormhole Attack in MANET

Prajeet Sharma
Research Scholar Rabindranath Tagore University
Bhopal

Pratima Gautam
Professor, Rabindranath Tagore University
Bhopal

Abstract:- Ad-hoc mobile networking (MANET) is an important technology in wireless networks with mobile nodes. Where nodes are collaborate with each other in a distributed manner and to provide multiple communications between sources and destination node. In general, the basic assumption of MANET is that each node is a trusted node. However, in a real case, there are some untrusted nodes that misbehave and attack the network like a black hole and wormhole. Where black hole nodes attract all traffic, providing false information about small hop count path to destination and with very sequence number to destinations. In wormhole attack, attacker collect data packets at one place and tunnels this data packet to another place in the network. For this attacker will give false information to the source node that the attacker node has the shortest path between sender and receiver. Source node will eventually choose that path for transmission. Once the path is established, both the nodes will drop all the incoming and outgoing packets and this causes denial of service attack, using wormhole attacks in this paper, we will discuss black hole and worm hole attack and discuss the different techniques which is used to detect and prevent these two attacks by different researchers.

Keywords:- *MANET, Routing Protocols, Worm Hole Attack Black Hole Attack, Performance Metrics.*

I. INTRODUCTION

Mobile Ad Hoc Network (MANET) is the form of wireless networks which do not require any fixed infrastructure or base stations. Mobile Ad Hoc Network is a collection of wireless mobile nodes which is capable of not only to communicate but also route the data from one node to another node which are in its radio range without any centralized master node or administrator. In a Mobile Ad Hoc Network (MANET), the nodes are tasked with the dynamic discovery of other nodes for communication purposes. Given the limited range of wireless network interfaces, a wireless mobile node might need to rely on other hosts to forward a packet to its final destination. Each mobile node functions as both a host and a router, facilitating the forwarding of packets for other nodes that are not directly within each other's transmission range. These nodes utilize an ad hoc routing protocol, enabling them to find multi-hop paths throughout the network to reach any other node. This type of network is termed infrastructureless networking, as the mobile nodes autonomously establish routing among themselves, creating the network spontaneously [1].

II. ATTACKS IN MANET

Due to the flexible nature of MANET, it is venerable to attacks. There are different types of attack. Which are mentions are as follows.

In MANET attacks are classified into External attack and internal attack. In which external attack is takes place with the use of node which is not the part of the network while in the internal attack, attack takes place with the use of internal node.

Attack can also be classified as Active attack and Passive attack. In active attack attacker node grab the data from the network and alter that data which is being exchanged into the network. In Passive attack the attacker node simply listens and record the data which is being exchanged into the network and then used that information in the future.

Attacks are also classified as on layer basis which is given into the table. [2]

Table 1 Layer Wise Attacks

Layer	Attack
Physical Layer	Jamming, interceptions, Eavesdropping
Data Link Layer	Traffic analysis, monitoring
Network Layer	Wormhole, Black hole, gray hole, message tempering, Byzantine, Flooding, resource consumption, location disclosure attacks
Transport Layer	Session hijacking, SYN Flooding
Application layer	Repudiation Malicious code

As we focus on network layer attack only so here, we discussed so of the network layer attack.

- Wormhole attack - In this attack attacker collects data packets at one place and tunnels this data packet to another place in the network. For this attacker will give false information to the source node that the attacker node

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1551

has the shortest path between sender and receiver. Source node will eventually choose that path for transmission. Once the path is established, both the nodes will drop all the incoming and outgoing packets and this causes denial of service attack, using wormhole attacks.

- Black hole attack - Where black hole nodes attract all traffic, providing false information about small hop count path to destination and with very sequence number to destinations.
- Gray hole attack – A Gray hole attack is a upgraded version of black hole attach as the attacker node is the part of network so it can easily participate in the data transfer route and when the data packet is received by this attacker node the it cannot drop all the packet but it can only drop specific packet or random packet. So, by this nature it is not the easy task to find out this type of attacker node. Because legitimate node also drops some data packet due to many legal reasons. [3]
- Message tempering - This kind of attack can be done when attacker wants to alter the incoming data to it and send the altered data back into the network to its original destination.
- Byzantine attack – This type of attack is done by the group of attacker nodes. All the attacker nodes pass the data packet to one another and creates a loop so the data packet trapped into the loop and discarded from the network when it's time to live field becomes zero. Another way is also used by the attacker nodes that they can divert the data packet to the non-optional path so it's time to live field become to zero and the data packet simply discarded from the network.
- Flooding attack – In this type of attack, the attacker node creates a scenario that maximum traffic is come to the victim node side and due to this, victim node does not able to send or receive the authentic data packet to and from the network.
- Resource Consumption - In this attack, the attacker node keeps continuously broadcast route request packet (RREQ) into the network. This is done because that maximum nodes are involve in replying the route request (RREQ) and do not do legal work into the network.[4]
- location disclosure attacks – In this attack, the attacker node simply acts as a legitimate node and listen the traffic flow into the network and record it. Then use this information in the future for other attacks.[5]

III. BLACKHOLE ATTACK

In Blackhole attack [6], the attacker node present in the path between source and destination launches its attack by not forwarding packets or dropping packets. It is an active attack which occurs at network layer and affects the functioning of the layer. The mechanism of Blackhole attack can be explained as: In Fig.1, assume that node S, node D, node 5 are source, destination and attacker respectively. In order to convey data packets from sender node S to target node D, node S commences route finding process. To accomplish this, node S rushes the network with Route Request message (RREQ). All the neighbouring nodes answers it with Route Reply message (RREP). Upon intercepting RREQ message from the source, a malicious node asserts that it is having the shortest and freshest way to the destination by misguiding the network nodes. Attacker node 5 tries to gain the confidence of source by sending a reply with less number of hops and higher sequence number. This makes source node believe that it is a legitimate node. After this, node S starts forwarding the information through that path believing that it is the shortest and most fresh route. When the packets fall in Node 5, it drops them. This is blackhole attack.

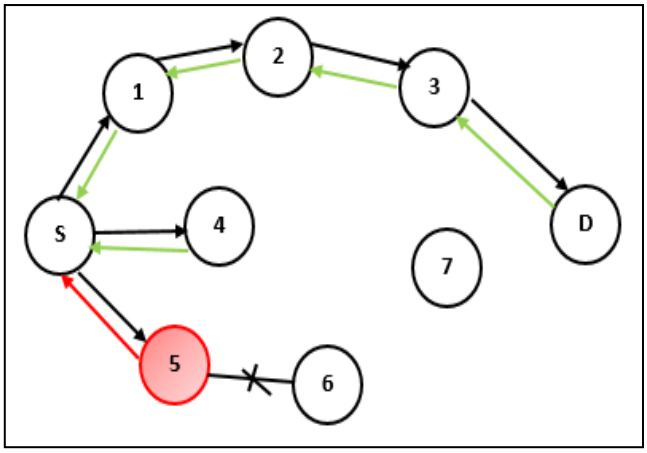

Fig 1. Blackhole Attack

IV. BLACKHOLE ATTACK PREVIOUS WORK

In the research of many people, they have suggested many solutions to the black hole attack and drives many algorithms for black hole detection and prevention. Some of the technique that served are:

Arathy et al. [7] have proposed algorithm - D-MBH and D-CBH in which three elements are used: Black Hole node List, a collaborative black hole node list and a fake route request. This algorithm is capable of identify both single and collaboration attacks in black hole. This algorithm reduced computational and routing overhead into the network.

Noguchi et al. [8] Prevent malicious nodes by sending different replies from the intermediate nodes. A black hole node is identified when the average number of input nodes at the origin is greater than the destination ID. If the generator ID is the same as the original node ID, the response packet is dropped. The simulation results are compared with original AODV and SRD-AODV which combines 40 real destination sequences for pseudo destination sequences. Failure can be considered as the waiting time for several RREPs by the source node.

Saurabh et al. [9] tried to divide the nodes into clusters with each node having a master node. During discovery, each node has checkpoints to count and send packets received from other clusters. A packet sent from the source is checked if the probability of sending a packet is less than a threshold, if true, the black hole node is listed as suspicious and from other groups of destination nodes to read more about it. A positive acknowledgment is sent. Delivery of the package. The proposed method does not explain the energy

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1551

consumption during cluster head formation in MANET.

Kame et al. [10] First, each node is assumed to be reliable, and each collaborating node maintains trust level and malicious node tables. After that a safety score is calculated to determine the safety of the route response. If there is an uncertain replay, the value of the confidence level is reduced by 1, and a negative value indicates that the node is attacker node. When comparing the results with the original AODV, the throughput graph, PDR and end-to-end delay results are better, but adding an extra table to the protocol shows that it increases.

Shivare et al. [11] did propose an index for each node in the Network. Whenever a black hole node or an undamaged node is detected, the node index is incremented or decremented by 1 for every 10 packets dropped. Simulations are performed for flow rate, PDR and residual energy. The technique does not prevent many black holes.

Dorri [12] framed some packet which is named as data control packet and a table that have "from and "through " column and named that table as DRI table. Source send random number and it will be compared by the received random number. This is done to find out the attacker node. Researchers uses Packet overhead, throughput, delay as a performance matrix element.

Tamilselvi et al. [13] proposed an algorithm in the DSR protocol to detect and remove malicious nodes. On the step of route discovery, the source and destination share a symmetric key to encrypt the data. The source sends routing requests and encrypted messages to intermediate nodes. Simple nodes will easily decrypt the encrypted data and return it to the source. Therefore, the source node can easily detect the black hole node because it cannot decode the next message and only sends a false response to the route.

Jasmine et al. [14] assessed the efficiency of the "AODV" protocol in the presence and absence of Blackhole

Attacks by measuring the end-to-end latency of packets and the packet delivery rate. As the number of nodes rises, the regular "AODV" has a higher packet delivery rate compared to the "AODV" under assault. Additionally, the end-to-end latency of the normal "AODV" increases, whereas the end-to-end delay of the "AODV" under attack reduces significantly.

Sharma et al. [15] examined the impacts of Blackhole Attacks on the performance of MANETs using the Qualnet network simulator. The experimental findings demonstrate that the conventional "AODV" exhibits greater "throughput", packet delivery rate, and end-to-end latency compared to Blackhole Attacks.

Semih et al. [16] using the NS2 network simulator to examine the effects of Blackhole Attacks on MANET. They conducted 100 simulations and quantified the packet loss in the system under two conditions: with and without Blackhole nodes.

Table 2 Summarization of Technique in Blackhoel Attack

SIMULATOR	PROTOCOL	ALGORITHM	DETECTION TECHNIQUE	PERFORMANCE E L E M E N T S	RESULTS	SHORTCOMING
Not Define	AODV	D-CBH , D-MBH (2016)[7]	Single and combined.	Routing overhead and Computational	Reduced computational and routing overhead	No Simulation Result
NS-2	AODV	Based on Multiple RREPs (2018) [8]	Single and combined	PDR, Routing Overhead, Throughput,	Increased throughput PDR, valid RREPs is discarded	Time delay due multiple RREPs
NS-2	AODV	Based on Cluster (2017) [9]	combined	PDR, Energy, Throughput	As compare to modified DSR Rate of Detection and throughput is three times higher	energy consumption for cluster head is not define
NS-2 (v. 2.35)	AODV	STAODV (2017) [10]	Single	PDR, End to End delay, Throughput	Better constant overhead, throughput and PDR	Fake sequence number can be forged
NS-2 (v. 2.35)	AODV	Based on Indexing Algorithm	Single	PDR, Residual Energy Throughput,	More PDR and throughput,	Fails for combined black hole nodes

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1551

		(2017) [11]			Lower energy consumption,	
OPNET 14	AODV	Table-based (DRI table) (2017)[12]	combined	Throughput, Packet overhead, delay	Decrease in packet loss, delay, packet overhead	Energy consumption increased
NS-2	DSR	Encrypted Message (2017)[13]	Single and combined	PDR, Packet drop, overhead, Throughput, Routing	Less retransmission, packet drop, the overhead for no black hole list	Computational overhead
NS-2	AODV	Based on threshold [14]	Single	end-to-end latency of packets and the packet delivery rate	End to end latency decresed and packet delivery ration incresed	Through put must be included
Qualnet	AODV	Based on IDSand trust system [15]	Single and combined	throughput", packet delivery rate, and end-to-end latency	Throughput, Packet delivery ratio increases and end to end latency decreases	Enhance it without the use of trust management system
NS-2	AODV	Based on threshold [16]	Single	end-to-end latency of packets and the packet delivery rate	End to end latency decresed and packet delivery ration incresed	Through put must be included

V. WORMHOLE ATTACK

In wormhole attack attacker records packets at one placed tunnels those to another place in the network. Due to this, it creates a false scenario that main sender is neighbour of the remote location. Wormhole forms by tunnelling procedure in sensor network. This attack requires at least two attacking nodes, working in coordination. These malicious nodes mostly have the high-speed link between them. The nodes use high speed channel (tunnel) to transmit the RREP packet to the sender at very fast rate. It creates illusion to the source node that the replying node (attacker) has the shortest path between sender and receiver. Source node will eventually choose that path for transmission. Once the path is established, both the nodes will drop all the incoming and outgoing packets and causes denial of service [17], using wormhole attacks.

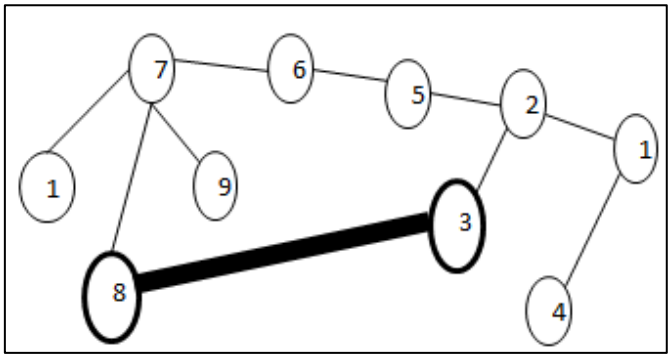

Fig 2 Wormhole Attack

VI. WORMHOLE ATTACK PREVIOUS WORK

Kim et al. [18] proposed a counterattack detection method based on the timestamped method. In this method, the authors used a time stamp to detect anomalies in a two-step counterattack detection method. In the first step, the transmission time of each hop is extracted from the RREQ. If the attacker creates an early time of the RREQ to bypass the detection system, it will be detected in the next (i.e., second) step. This is because the created transmission time is shorter than the actual time.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1551

Upadhyay et al. [19] proposed a numerical method for WHA detection using the main parameters such as time delay, number of input packets, number of output packets, and average route discovery time. Monitoring is done using the above parameters, if any anomaly is detected then detection of attack algorithms is activated.

Chen et al [20] give a label-based DV positioning method. A self-positioning node is used as a node to locate long-distance hops in the area of no packet loss in the network. And the transmission radius is the same for all network nodes.

Sundararajan et al [21] gives a biological system based on artificial intrusion detection (BAIDS). It is robust compared to the hybrid negative selection algorithm. This method is expected to provide satisfactory performance for anomaly detection in terms of FAR and PDR, but suffers from high computational complexity due to insufficient path information.

Karlsson et al. [22] gives a WHAD method called hop count and Traversal count analysis, which is based on parameters like RTT(Round Trip Time) and hope count (HC). This method provides 75% detection rate with less overhead.

The problem of generating the initial RREQ cycle was studied by Karlsson et al. [23] who proposed a method for timing spoofing in transmission time analysis and hop counting (TTHCA for worm detection). In addition to the Time Stamp, they also include a hop count parameter to solve this problem. Limitations of this method: Low FPR when used to detect various attacks.

Gianetos and Dimitrieu [24] proposed a Localized decentralized algorithm for countering (LDAC) to deal with WHA. Connection information is used to work in mobile nodes network. This algorithm apply on the connectivity graph to detect malicious nodes. As many algorithm required some special hardware but in this algorithm there is no need of any special kind of hardware and GPS coordinates, clock synchronization or any other special statistical methods. Only the ID of the node in the network is used. The short startup time interval for partial neighborhood assembly is the only limitation of this method.

Qazi et al. [25] proposed a routing method called DSR routing method for network security from Wormhole attack in a multi-rate environment using two messages called RREP and RREQ messages.

Xia et al [26] presented a prediction model based on fuzzy logic and dynamic trust. The proposed model uses the past actions of nodes to predict the future. This example further illustrates a trust-based source routing approach to select the safest and fastest route. The proposed model simplifies route discovery by using a special type of request message called FLOW-REQ message. Furthermore, it also supports methods based on reliability prediction algorithms.

M. Anand and T. Shasikala [27] The main limitation of the MANET routing scheme is that nodes have the right to exchange packets in transit. This privilege often leads to security breaches. Changing the sequence number in the packet header is a common way to modify a packet. Moreover, it is always difficult to know which malicious node made the changes. An effective way to prevent such attacks is to require each node to be authentic to the MANET before sending data. Many researchers have adopted this approach.

Table 3 Summarization of Technique in Wormhole Attack

Author	Technique	Algorithm	Strength	Weakness	Rate of Detection
Kim et al. [18]	TS[Timestamp]	Algo for Time stamp counterattack detection	Quickly detect WHA with counterattack of attacker	Only 2 nodes are used in Simulation	FPR = 7.78% and DR = 96.3 %
Upadhyay and Chaurasia [19]	DA	SAA	Lightweight	Increases time in the Route discovery	Valuable
Chen et al. [20]	Technique of Node localization	DV-hop localization	Decrease the value of Localization error	Parameter like Packet loss should include, transmission radii of nodes must be identical	BSR = 50% and DR = 95.6%
Sundararajan et al. [21]	Technique HNSA is used	Algorithm BAIDS implemented	Information is more accurate	Due to algorithm computational cost is increased	less FPR and High PDR
Karlson et al. [22]	Algorithm HC and RTT is used	Algorithm TTHCA is used	Computationally Less overhead	Time measurement is typical because nodes can	75%

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1551

Author	Technique	Algorithm	Strength	Weakness	Rate of Detection
				alter the time mesurement	
Karlson Dimitriou [23]	Algorithm TS, HC, and TTHCA are used	TTHCA	Increases the power of TTHCA approach and enhanced security	Complexity is very high	Less FPR
Giannetsos and Dimitriou [24]	Algorithm NB and CB are used	LDAC	Apply in both dynamic and static network. Less overhead, and no special hardware is Required.	Requires small initial time interval for partial neighbourhood establishment	DR = 100%
Qazi et al. [25]	RTT algorithm is used,	Securing DSR from WHA in multi-rate ad-hoc network	Security against packet encapsulation wormhole, out of band wormhole, high power transmission wormhole, packet relay wormhole	Extra 18 bytes for data added to RREP message proposed for DSR can be extended for AODV	Efficient
M. Anand and T. Shasikala [27]	HC, Sequence Number	Authentication method	Each Node is a non malicious	Apply only on AODV	High Throughput

VII. CONCLUSION

Black hole attacks and wormhole attack have been a big problem for ad hoc networks for many years. Over time, different algorithms have been created to stop these kinds of attacks. This paper thoroughly examines the methods used to detect and prevent these attacks. The methods are based on various factors like Throughput, packet delivery rate, end-to-end delay, trust, acknowledgement, and fake packets. The paper also discusses the results and issues of these methods, which should be considered when creating a new protocol. Based on the survey, one can identify which algorithms are better at reducing these two attacks. In the future, efforts to prevent These two attacks can focus more on removing harmful nodes in hybrid protocols and detecting smart wormhole and black hole nodes. These solutions might use more complex and effective algorithms to come up with new ways to stop these attacks. Saurabh et al. [9] suggest the best scheme for blackhole detection with the division of nodes into clusters and each cluster have the cluster's master head to check activities within the network. Among to all the papers on the wormhole attack Giannetsos and Dimitriou [24] gives algorithm NB and CB in which detection rate is 100% as per their simulation scenario and parameters.

REFERENCES

[1]. Rakesh Kumar Singh, Rajesh Joshi and Mayank Singhal "Analysis of Security Threats and Vulnerabilities in Mobile Ad Hoc Network (MANET)" International Journal of Computer Applications (0975 – 8887 Volume 68– No.4, April 2013.

[2]. Attacks Finding and Prevention Techniques in MANET: A Survey - Advances in Wireless and Mobile Communications. ISSN 0973-6972 Volume 10, Number 5 (2017), pp. 1185-1195 © Research India Publications http://www.ripublication.com

[3]. Rupali Sharma, Gray-hole Attack in Mobile Ad-hoc Networks : A Survey, ISSN: 0975-9646, International Journal of Computer Science and Information Technologies, Vol. 7 (3) , 2016, 1457-1460

[4]. The Impact of Resource Consumption Attack on Mobile Adhoc Network Routing" - International Journal of Network Security, Vol.16, No.4, PP.399-404, July 2014- ,

[5]. Network Security and Types of Attacks in Network, Mohan V. Pawar1 , Anuradha J2, - "International Conference on Intelligent Computing, Communication & Convergence 2015" -, 1877-0509 © 2015.

[6]. Mohamed Elboukhari , Mostafa Azizi and Abdelmalek Azizi "Impact Analysis of Blackhole attack on Mobile Adhoc Network Performance" International Journal of Grid Computing & Applications (IJGCA) Vol.6,No.1/2, June 2015 DOI:10.5121/ijgca.2015.6201

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

[8]. T. Noguchi, and M. Hayakawa, "Black hole Attack Prevention Method Using Multiple reps in Mobile Ad Hoc Networks," IEEE, 2018, pp. 539-544.

[9]. V.K. Saurabh, R. Sharma, R. Itare, and U. Singh, "Cluster-based technique for detection and prevention of black-hole attack in manets," International conference of Electronics, Communication and Aerospace Technology (ICECA) IEEE, April 2017, pp. 489-494

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1551

[10]. M.B.M. Kame, I. Alameri, and A.N. Onaizah. "STADOV: a secure and trust based approach to mitigate blackhole attack on AODV based MANET," IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), March2017, pp.1278- 1282.
[11]. M. Shivare and P.K. Gautam, "Prevention of black hole attack in MANET using indexing algorithm" IJESC,7(6), 2017, pp. 12603- 12606.
[12]. A. Dorri, "An EDRI- based approach for detecting and eliminating cooperative black hole nodes in MANET," Springer, 23(6), 2017, pp. 1767-1778.
[13]. P. Tamilselvi and C.G. Babu, " An efficient approach to circumvent black hole nodes in manet," Cluster Computing, Springer, 22(5), 2017, pp. 11401-11409.
[14]. P.R. Jasmine Jeni, Vimala Juliet, R. Parthasarathy, A. Messiah Bose. "Performance analysis of DOA and AODV routing protocols with black hole attack in MANET" Conference: Smart Structures and Systems (ICSSS), 2013 IEEE International Conference.
[15]. Shikha Sharma, Manish Mahajan, Security Mechanisms for Mitigating Multiple Black Hole Attack in Manets IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 11, November 2015. Www.ijiset.com ISSN 2348 – 7968.
[16]. Semih et al. Active networking: one view of the past, present, and future, Ieee Transactions On Systems, Man, And Cybernetics—Part C: Applications And Reviews, Vol. 34, No. 1, February 2004
[17]. Deepika Kancharakuntla and Hosam El-Ocla "EBR: Routing Protocol to Detect Blackhole Attacks in Mobile Ad Hoc Networks "Ad Hoc Networks. Electronics 2022, 11, 3480.
[18]. Kim, H. Kim, G. Kim, and S. Kim, "A counterattack-detection scheme in transmission time-based wormhole detection methods," Hindawi Publ. Corporation, Int. J. Distrib. Sens. Netw., vol. 9, no. 3. P.
[19]. S. Upadhyay, and B. K. Chaurasia, "Detecting and avoiding wormhole attack in MANET using statistical analysis approach," Advances in Computer Science and Information Technology. Networks and Communications, CCSIT, 84, Springer, 2012.
[20]. H. Chen, W. Lou, Z. Wang, J. Wu, Z. Wang, and A. Xia, "Securing DV-Hop localization against wormhole attacks in wireless sensor networks," Pervasive Mob. Comput., vol. 16, pp. 22–35, 2015.
[21]. T. V. P. Sundararajan, S. M. Ramesh, R. Maheswar, and K. R. Deepak, "Biologically inspired artificial intrusion detection system for detecting wormhole attack in MANET," Springer Science Business Media New York, Wireless Network, 2013.
[22]. J. Karlsson, L. S. Dooley, and G. Pulkkis, "A new MANET wormhole detection algorithm based on traversal time and hop count analysis," Sensors, vol. 11, pp. 11122–11140, 2011.
[23]. J. Karlsson, L. S. Dooley, and G. Pulkkis, "Identifying time measurement tampering in the traversal time and hop count analysis (TTHCA), wormhole detection algorithm," Sensors, vol. 13, no. 5. Pp. 6651–6668, 2013.
[24]. T. Giannetsos and T. Dimitriou, "LDAC: A localized and decentralized algorithm for efficiently countering wormholes in mobile wireless networks," J. Computer Syst. Sci., vol. 80, no. 3. Pp. 618–643, 2014.
[25]. S. Qazi, R. Raad, Y. Mu, and W. Susilo, "Securing DSR against wormhole attacks in multirate ad hoc networks," J. Netw. Computer Appl., vol. 36, no. 2, pp. 582–592, 2013.
[26]. Xia et al., Trust prediction and trust-based source routing in mobile ad hoc networks September 2013 ,Ad Hoc Networks 11(7):2096-2114 ,DOI:10.1016/j.adhoc.2012.02.009
[27]. M. Anand and T. Sasikala," Efficient energy optimization in mobile ad hoc network (MANET) using better-quality AODV protocol", springer publications, 2018.