Exposure and Avoidance Mechanism of Black Hole and Jamming Attack in Mobile Ad Hoc Network: A Review

Harsh Pratap Singh
PhD Scholar, SSSUTMS, Sehore (M.P.)

Rashmi Singh
AP, RITS-Bhopal (M.P.)

ABSTRACT
Mobile ad hoc network (MANETs) is an infrastructureless/self-configurable system in which every node carries on as host or router and every node can participate in the transmission of packets. Because of its dynamic behaviour such system is more susceptible against various sorts of security threats, for example, Black hole, Wormhole , Jamming , Sybil, Byzantine attack and so on which may block the transmission of the system. Black hole attack and Jamming attack is one of them which promote itself has shortest or new fresh route to the destination while jamming attack which make activity over the system. This paper introduces the thorough literature study for the Black hole attack and jamming attack of both the attack by various writers.

Keywords
Black Hole attack, Infrastructureless, Jamming, MANET, Wormhole.

1. INTRODUCTION
Rise of moveable wireless communication gadgets and rising in cell innovation has made portable mobile ad hoc network (MANET) across the board in civil and military applications. The importance for mobile ad hoc network stem from its capacity to deliver moment organizing determination in a range wherever the cell framework is either immoderate or difficult to convey. MANETs will be sent while not the need for any mounted framework like base stations. Nodes in MANET amass among themselves to decide the system progressively. They go about as a source also as switch. As an asset they produce the bundle and as a switch they forward the parcel. Parcels are transmitted from source to goal in multi-bounces. MANETs has gigantic applications each in military and civil (therapeutic, mobile processing, Disaster recuperation) [1]. Uses of MANET rely on upon the viability of steering convention. Nodes in MANET are powerful by electro-synthetic batteries whose ability is limited. Serviceor substitution these batteries won't not be conceivable. The improvement of little, less expensive and all the more capable gadgets construct MANET a quickest creating system. A specially appointed system is self-versatile and self-sorting out. Portable impromptu system gadgets ought to be skilled to decide the presence of different gadgets and perform vital set up to give correspondence and sharing of administration and information. Specially appointed systems administration allows the gadgets to oversee connections to the system and also effectively joining and disposing of gadgets to and from the system. On account of hub versatility, the system setup may change oftentimes and capriciously all through time. The system is not-incorporated, where message conveyance and system association must be performed by the nodes themselves. Steering of message is an issue in a decentralize climate where the design fluctuates. While the most brief way from a source hub to a goal hub relying upon a gave cost capacity in an altered system is regularly the ideal course, this idea is mind boggling to investigate in MANET [2][3]. The applications set for MANETs are adaptable, different, extending from expansive scale, exceedingly dynamic in nature, to little, settled systems that are controlled by force sources. Alongside, legacy applications that move from customary foundation environment into the specially appointed connection, a lot of new offices can and will be delivered for the new climate. MANET is more powerless when contrasted with wired system in view of portable nodes, assaults from bargained nodes inside the system, limited physical security, dynamic design, adaptability and inadequacy of incorporated administration. Because of these susceptibilities, MANET is more defenseless against serious threats.

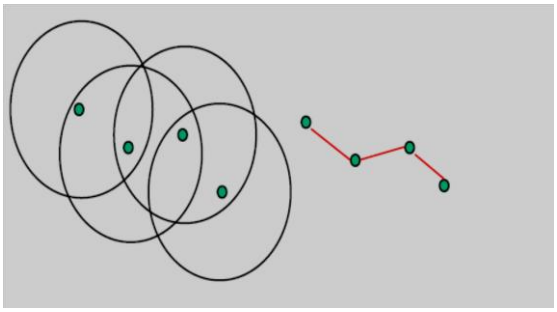

Fig 1: Architecture of Mobile Ad hoc Network

1.1 Security Goals
Security incorporates a gathering of speculations that are adequately financed. In MANET, all systems administration exercises, i.e. Directing and parcel sending are executed by nodes themselves in a self-arranging way. For these causes, ensuring a portable advertisement –hoc system is exceptionally testing. The targets to gauge if portable specially appointed system is secured or not are as per the following [12]:

i) Availability: Availability suggests the assets are open to validated gatherings at reasonable times. Accessibility applies both to administrations and to information. It guarantees the survivability of system administration notwithstanding Dos assault.

ii) Confidentiality: Confidentiality guarantees that PC related assets are gotten to just by validated gatherings i.e. just the individuals who to have entry to something ought to will truly get that entrance. To oversee privacy of some private data, we require holding them mystery from all substances that don't have benefit to get to them. Classification is some of the time known as protection or mystery.

iii) Integrity: Integrity suggests that assets can be modified just by verified gatherings or just in validated way.

Adjustment includes composing, evolving status, erasing and making. Trustworthiness guarantees that a message being transmitted is never harmed.

iv) Authentication: Authentication empowers a hub to guarantee the associate hub character it is cooperating with. Confirmation is fundamentally certification that nodes in correspondence are approved and not impersonators. Genuineness is affirmed in light of the fact that exclusive the honest to goodness sender can create a message that will unscramble appropriately with the mutual key.

v) Non denial: Non disavowal affirms that beneficiary and sender of a message can't deny that they have ever sent or acquired such a message. This is valuable when we require perceiving if a hub with some un-required capacity is traded off or not.

2. ROUTING PROTOCOLS

There are plenty and different routing protocols in MANET and kinds of investigations have been completed in recent decades [4, 5]. In this section, we introduce the famous and popular routing protocols in MANET. Before a mobile node wants to communicate with a target node, it should broadcast its present status to the neighbors due to the current routing information is unfamiliar. According to how the information is acquired, the routing protocols can be classified into proactive, reactive and hybrid routing.

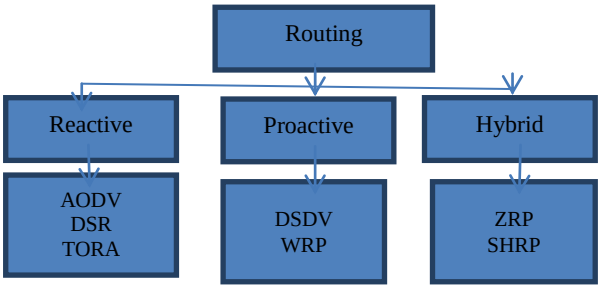

Fig. 2: Classification or Routing Protocol

2.1. Proactive (table-driven) Routing Protocol

The proactive routing is additionally called table-driven routing protocol. In this routing protocol, mobile nodes occasionally communicate their directing data to the neighbors. Every node needs to keep up their directing table which not just records the adjoining nodes and reachable nodes additionally the quantity of bounces. At the end of the day, the greater parts of the node need to assess their neighborhoods the length of the system topology has changed. Along these lines, the advantage is that the overhead ascents as the system size expands, a critical correspondence overhead inside a bigger system topology. Be that as it may, the favorable position is that system status can be instantly reflected if the noxious aggressor joins. The most well known sorts of the proactive sort are goal sequenced separation vector (DSDV) [6] directing convention and upgraded join state steering (OLSR) [7] convention.

2.2. Reactive (on-demand) Routing Protocol

The reactive routing is furnished with another appellation named on-demand routing protocol. Dissimilar to the proactive routing, the reactive routing is essentially begun when nodes yearning to transmit data packets. The quality is that the squandered data transfer capacity initiated from the consistently communicate can be lessened. By and by, this may likewise be the deadly twisted when there are any vindictive nodes in the system environment. The shortcoming is that uninvolved directing strategy prompts some bundle misfortune. Here we quickly portray two pervasive on-interest routing conventions which are impromptu on-interest separation vector (AODV) [8] and dynamic source routing (DSR) [9] convention. AODV is built taking into account DSDV routing. In AODV, every node just records the following bounce data in its directing table yet keeps up it for supporting a routing way from source to destination nodes. On the off chance that the goal node can't be come to from the source node, the course disclosure procedure will be executed instantly. In the course disclosure stage, the source node communicates the course ask for (RREQ) bundle first. At that point every single moderate node get the RREQ packet, however parts of them send the route reply (RREP) packet to the source node if the goal node data is happened in their routing table. Then again, the course support procedure is begun when the system topology has changed or the association has fizzled. The source node is educated by a course blunder (RRER) bundle first. At that point it uses the present directing data to choose another routing way or restart the course disclosure process for upgrading the data in routing table. The configuration thought of DSR depends on source directing. The source directing implies that every information packet contains the routing way from source to goal in their headers. Unlike the AODV which just records the following bounce data in the routing table, the versatile nodes in DSR keep up their course reserve from source to goal node. In terms of the above exchange, the routing way can be dictated by source node in light of the fact that the routing data is recorded in the course store at every node. Nonetheless, the execution of DSR declines with the versatility of system expands, a lower packet conveyance proportion inside the higher system portability.

2.3. Hybrid Routing Protocol

The hybrid routing protocol combines the advantages of proactive routing and reactive routing to overcome the defects of them. Most of hybrid routing protocols are designed as a hierarchical or layered network framework. In the beginning, proactive routing is employed to completely gather the unfamiliar routing information, then using the reactive routing to maintain the routing information when network topology changes. The familiar hybrid routing protocols are zone routing protocol (ZRP) [10] and temporally-ordered routing algorithm (TORA) [11].

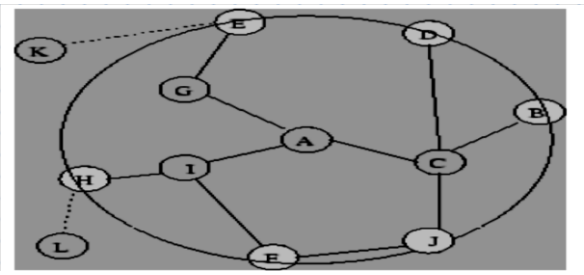

Fig. 3: Zone Routing Protocol

3. BLACK HOLE ATTACK & JAMMING ATTACK

3.1 Overview of Black Hole Attack

In a blackhole attack [13], a malicious node sends bogus routing information, claiming that it has an best route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a bogus Route Reply (including a fake destination sequence number that is made-up to be equal or higher than the one contained in the Route Request) to the source node, claiming that it has a good fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can break/abandon the traffic. There are two types of Black hole attack.

3.1.1 Single Black Hole Attack

In single black hole attack only one malicious node poach into the route and attack the MANET (see Fig. 4) by dropping the data packets to its malicious node. The malicious nodes have the routing capability and the attacker take the advantages of the lean routing protocols of MANET. The most vulnerable routing protocol is AODV, which works on the principle that the node having maximum sequence number may be consider as the fresh node that guarantees the loop free route. For the multiple routes, the node which exhibits higher sequence number and having the least hope count is considered as the fresh node with optimized route to the destination.

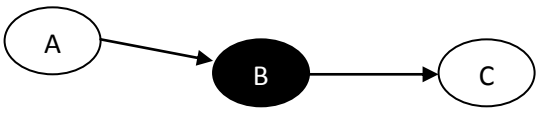

Fig.4: Single Black Hole Attack

3.1.2 Co-operative Black Hole Attack

When the malicious nodes act in a group and attack the MANET that attack is well known as Co-operative Black Hole. In the Fig. 5 the nodes 2 and 3 act as black holes. The Attack becomes complex when the multiple malicious node work in hands in gloves with each other and disrupt the complete routing of the data. In the cooperative black hole attack the packet forwarding capacity of the system shatter vigorously.

one address is needed, center all address text. For two addresses, use two centered tabs, and so on. For three authors, you may have to improvise.

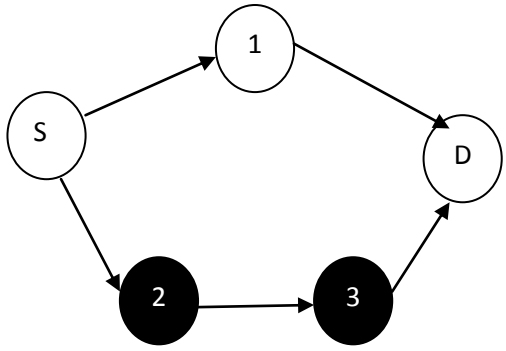

Fig.5: Cooperative Black hole Attack

3.2 Overview of Jamming Attack

Jamming Attack: - It is a type of DOS attack. There are many different attack strategies that a jammer can perform in order to interfere with other wireless communications. Some possible strategies are exposed below [14]:

• **Constant Jammer:** A constant jammer continuously emits a radio signal that represents random bits; the signal generator does not follow any MAC protocol.

• **Deceptive Jammer:** Different from the continuous jammers, deceptive jammers do not transmit random bits instead they transmit semi-valid packets. This means that the packet header is valid but the payload is useless.

• **Random Jammer:** Alternates between sleeping and jamming the channel. In the first mode the jammer jams for a random period of time (it can behave either like a constant jammer or a deceptive jammer), and in the second mode (the sleeping mode) the jammer turns its transmitters off for another random period of time. The energy efficiency is determined as the ratio of the length of the jamming period over the length of the sleeping period.

• **Reactive Jammer:** A reactive jammer tries not to waste resources by only jamming when it senses that somebody is transmitting. Its target is not the sender but the receiver, trying to input as much noise as possible in the packet to modify as many bits as possible given that only a minimum amount of power is required to modify enough bits so that when a checksum is performed over that packet at the receiver it will be classified as not valid and therefore discarded.

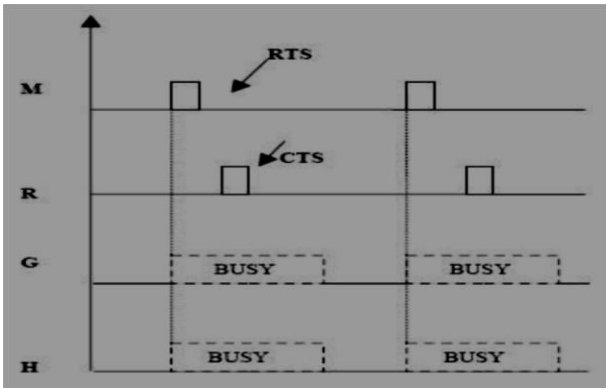

Fig.6: Jamming Attack

4. LITERATURE SURVEY

This section describes literature about the former work done in the field of black hole attack and jamming attack detection and prevention in mobile ad hoc network:

4.1 Black hole Attack Literature

Author/ Research	Literature Work
Vimal Kumar and Rakesh Kumar [15]	Presented a more proficient explanation for detecting a black hole attack with less communication cost in the MANET, which is particularly susceptible compared to infrastructure-based networks due to its mobility and shared broadcast nature. As an adversary can effectively deploy blackhole attack in the network. It can be seen that projected work is more secure than the existing solutions. They also compared its performance to standard AODV routing protocol. The experimental consequences showed that the projected approach is better than standard AODV.

Gojiya et al. [16]	Intended a solution to the black hole attack in one of the most prominent routing algorithm, ad-hoc on demand distance vector (AODV) routing, for the MANETs. The anticipated scheme uses Watchdog mechanism to detect malicious node with usage of local information of intermediate node and propagates the information of black hole node to all other node in network the simulation results show the efficiency of anticipated scheme in presences of black hole node.
Alem and Xuan [17]	Proposed a key solution Intrusion Detection using Anomaly Detection (IDAD). It uses host- based Intrusion Detection System (IDS) method to scrutinize the activities of a host. An anomaly activity is detected on the basis of inventory data which is collected and is given to the IDAD system. They compared every action of a host with the audit data on the fly and isolate a host (node) if any of its activity resembles an activity in the inventory data. However, there are several drawback of this method. It necessitates extra memory, slows down the system and is impractical to implement in some hostile scenario.
Seryvuth Tan et. Al.[18]	Anticipated a novel method for detecting and preventing these attacks and securing a route to the destination in a resourceful manner. The simulation outcomes showed. In this paper SRDAODV method significantly increases the packet delivery ratio for three types of environments with node mobility when black hole attacks are going on the network. They will progress the security mechanism for data transmissions. In this paper, the origination nodes or source node and destination node after a route has been reputable.
Apurva Jain et al.[19]	In this paper, customized AODV, which is TAODV (Trust based AODV), is a network. TAODV has numerous noteworthy features as Nodes perform trusted routing behavior mainly according to the trust relationship s among them. A node that executes black hole behavior will be detected and challenges by the whole network TAODV mollify the effect of Black Hole attack but average end-to-end delay increases in TAODV. In Indoor background Pareto traffic condition, gives the best result as far as average throughput is consider. On the other hand, Exponential traffic condition gives the best outcome for average end-to-end delay and CBR traffic condition traffic condition the best result for packet delivery ratio. In Outdoor environment, Pareto traffic condition gives the best consequence for average throughput and packet delivery ratio and Exponential traffic circumstance gives the best result for average end-to-end delay.
Rakhi Sharma and Dr D.V Gupta [20],	In this paper, blackhole attack and its different exposure techniques are presented with literature review of unusual research papers that covers black hole detection and anticipation mechanism. A blackhole node behaves maliciously in network and offers wrong data routing information or may drop the messages receives from other nodes. So it is complicated to uncover black hole attack and avoid network from them. These techniques are used in the avoidance of network from blackhole attack

.

4.2 Jamming Attack Literature

Author/ Research	Literature Work
Soneram Verma and Prof. Maya Yadav [21]	The projected protocols should be proficient in terms of Packet Delivery ratio, End-to-End Delay, normalized routing load (NRL), Outstanding Energy and Throughput. Based on the motivations to fabricate novel security measures to be incorporated in popular routing protocols AODV, the endeavor of this work has been implement secure on-demand routing (TAODV) protocols for data transmission in MANET and detect jamming node in MANET scenario using TAODV protocol. Also avoid the network from jamming attack and advance the packet delivery fraction, throughput and end-to-end delay, normalized routing load, Residual Energy even with the presence of jamming attacks. The results of both AODV and TAODV evaluate to analyze that of those 2 types of protocols offers higher performance.
Pawani Popli and Paru Raj [22]	Anticipated method used for mitigating and thwarting jamming attacks is enforced at the MAC layer that has an integration of a number of coordination techniques. These are an integration of Point Controller Functions (PCF) that are used to coordinate entire network activities at the MAC layer and RTS/CTS (Clear-To-Send) mechanisms which is a handshaking method that decreases the collisions on the wireless network. The whole network performance and technique is simulated by using OPNET modeler.
Ashwini Magardey and Dr. Tripti Arjariya [23]	Projected IDS (Intrusion Detection System) security method is recognized the attacker by their routing entry offered on other nodes routing record. The attacker has dump the whole performing of network. The Multipath

	routing protocol AOMDV is provided the multiple path if the attacker is exist in established path. The contagion from attack and performance metrics like throughput, routing load is evaluated and observe the secure anticipated security method is immobilized the routing misbehavior of jamming attacker and makes available secure AOMDV routing performance as equal to normal AOMDV performance.
Huang et al. [24]	Presented a message security method in MANETs that employs a trust based multipath AOMDV routing combined with soft encryption, yielding our so-called T-AOMDV method. Replication outcomes using ns2 exhibit that our scheme is much more secured than traditional multipath routing algorithms and a freshly proposed message security scheme for MANETs. The performance criteria used are route selection time and trust compromise. This prerequisite poses a security confront when malevolent nodes are present in the network. Indeed, the subsistence of such nodes may not simply disrupt the normal network operations, but cause sober message security issue concerns.
Aashish Mangla and Vandana [25]	Recommended a method employed for mitigating and preventing jamming attacks is implemented at the MAC layer that surrounds a combination of different coordination mechanisms. These are a combination of Point Controller Functions (PCF) that are utilized to coordinate whole network activities at the MAC layer and RTS/CTS (Clear- To-Send) strategies which is a handshaking process that reduces the collisions on the wireless network. The whole network performance and mechanism is modeled by employing OPNET simulator.
Zhu et al. [26]	In this work, they tackled the jamming attack difficulty in a systematic way. Exclusively, they designed a protocol that was capable of self-healing wireless networks under jamming attacks. The protocol identified and excluded an insider jammer and then restores normal data communications among benign nodes despite the presence of jamming by an originally unknown compromised node. The proposed scheme integrate key management, jammer identification and jammer isolation in one system. At last, they evaluated the protocol with USRP devices and GNU Radio in the context of jammer localization. The experiments demonstrated that the proposed protocol must recognize and isolate the insider jammer with high accuracy.
Kim et al. [27]	Anticipated an approach to localize a wireless node by using jamming attack as the advantage of the network. The projected localization method was divided into two steps. Primary, they ascertain the location of the jammer using power adaptation techniques. After that, they employ these properties to extrapolate the locations of jammed nodes. In addition, the author design a localization protocol using this technique, and demonstrated the feasibility of the anticipated mechanism by conducting indoor experiments based on IEEE 802.15.4 wireless nodes. The proposed consequence showed that for some situations the proposed mechanism might be used to position mobile nodes under jamming attack.

.

5. CONCLUSION

Security is a basic issue in the field of PC network. They are more helpless against attack and we have enhanced the quality and issues in Mobile Ad-hoc organize and routing protocol. In this paper, we introduce the depiction about steering convention and writing work for the introduction of black hole and jamming attack. All mechanism is great from their viewpoint yet not best from all focuses. Components clarified in this paper can offer data about security capacities and an aggregate visual check, which may be proper in a few applications. Be that as it may, there is likewise prerequisite to display a particular situation to picture the effect of with and without Jamming assault and black hole attack for the enhancing the routing protocol.

6. REFERENCE

[1] Abderrahmane Baadache and Ali Belmehdi 2014.Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks. Computer Networks, 73:173,184.

[2] Nital Mistry, Devesh C. Jinwala and Mukesh Zaveri, 2010. Improving AODV Protocol against Blackhole Attacks. International Multi conference of Engineers and Computer Scientists vol. 2,

[3] Payal N. Raj and Prashant B. Swadas 2010. DPRAODV: A dynamic learning system against black hole attack in AODV based MANET. International Journal of Computer Science Issues, Vol. 2, Issue 3 , pp: 54-59.

[4] Royer EM, Toh C-K 1999. A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. IEEE Personal Communications 6(2):46–55. DOI: 10.1109/98.760423

[5] Sanzgiri K, Dahill B 2002.A Secure Routing Protocol for Ad Hoc Networks. Paper presented at the 10th International Conference on Network Protocols, Paris, France, 12-15

[6] Perkins CE, Bhagwat P 1994. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. Paper presented at the ACM SIGCOMM'94 Conference, London, United Kingdom.

[7] acquet P, Muhlethaler P, Clausen T, Laouiti A, Qayyum A, Viennot L 2001. Optimized Link State Routing Protocol for Ad Hoc Networks. Paper presented at the IEEE International Multi Topic Conference, Lahore, Pakistan, 28-30.

[8] Perkins CE, Royer EM 1999. Ad-hoc On-Demand Distance Vector Routing. Paper presented at the Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, Louisiana.

[9] Johnson DB, Maltz DA 1996. Dynamic Source Routing in Ad Hoc Wireless Networks. In: Imielinski T, Korth H (eds) Mobile Computing, vol 353. Kluwer Academic Publishers, pp 153–181.

[10] Haas ZJ, Pearlman MR, Samar P 2002. The zone routing protocol (ZRP) for ad hoc networks. IETF Internet Draft.

[11] Park V, Corson S 1998. Temporally-Ordered Routing Algorithm (TORA) Version 1 Functional Specification. Internet Draft, Internet Engineering Task Force MANET Working Group.

[12] Kalyani Singh 1, Mamta Martolia 2016. A Review on Jamming attack in MANET. International Journal of Science, Engineering and Technology Research (IJSETR) Volume 5, Issue 8.

[13] Krishan Kumar,Taranjit Singh Aulakh 2016. Black Hole Attack in MANETs Preventions and Advancements: A Review, International Journal of Computer Applications (0975 – 8887) International Conference on Advances in Emerging Technology (ICAET 2016).

[14] Baljinder Singh, Dinesh Kumar 2015. "Jamming attack in MANET: A Selected Review" , International Journal of Advanced Research in Computer Science and Software Engineering 5(4), pp. 1264-1267.

[15] Vimal Kumar, Rakesh Kumar 2015. An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network, International Conference on Intelligent Computing, Communication &Convergence, Procedia Computer Science 48 (2015) 472 – 479.

[16] Jayshree Gojiya, Amit Nayak, Bimal Patel 2016. An Enhanced Approach of Detection and Prevention of Black Hole Attack on AODV over MANET. International Journal of Computer Applications (0975 – 8887) Volume 142 – No.13.

[17] Yibeltal Fantahun Alem and Zhao Cheng Xuan, 2010. Preventing Black Hole Attack in Mobile Ad-Hoc Networks Using Anomaly Detection, International Conference on Future Computer and Communication, pp. 672-676.

[18] Seryvuth Tan and Keecheon Kim 2013. Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs"978-0-7695-5088-6/13 © 2013 IEEE.

[19] Apurva Jain and Anshul Shrotriya 2015. Investigating the Effects of Black Hole Attack in MANET under Shadowing Model with Different Traffic conditions" IEEE International Conference on Computer, Communication and Control.

[20] Rakhi Sharma and Dr D.V Gupta 2016. Blackhole Detection and Prevention Strategies in DTN", International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 5 Issues 8, Page No. 17386-17391.

[21] Soneram verma1, Prof. Maya Yadav 2016 "Detection and Prevention for Jamming Attack in MANET using TAODV Protocol", International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 05.

[22] Pawani Popli1, Paru Raj 2016. Mitigation of Jamming Attack in Mobile Ad Hoc Networks", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 6.

[23] Ashwini Magardey, Dr. Tripti Arjariya 2013. Secure Detection and Prevention Scheme for Jamming Attack in MANET, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064.

[24] Jing-Wei Huang, Isaac Woungang, Han-Chieh Chao, Mohammad S. Obaidat 2011. Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks, Publication in the IEEE Globecom.

[25] Ashish Mangla ,Vandana 2015. Prevention of Jamming Attack in MANET, International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 7, July 2015.

[26] Longquan Li, Sencun Zhu, Don Torrieriy, Sushil Jajodia 2014.Self-Healing Wireless Networks under Insider Jamming Attacks", IEEE-2014.

[27] Yu Seung Kim, Frank Mokaya, Eric Chen, and Patrick Tague 2012. All Your Jammers Belong To Us - Localization of Wireless Sensors Under Jamming Attack, IEEE-2012.