Amit Kumar Yadav, 2022, 10:1
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

A Review of Mobile AD-HOC Network Attacks

M.Tech. Scholar Amit Kumar Yadav, Asst. Prof. Girish Gogate
Department of Computer Science and Engineering
Rishiraj Institute of Technology (RIT),
Indore, India
amityadav1607@gmail.com, girishgogatee@mail.com

Abstract- The routing algorithm of a Mobile Ad-hoc Network (MANET) is responsible for adapting to the random changes that may occur in the network topology during its operation. MANET is a network that consists of a large number of mobile nodes that communicate with one another without the need of an integrated framework. A MANET has a self-sorting out property as a result of which each mobile node becomes associated with one another via distant connections, resulting in an irregular topology being pursued by the network. In order to avoid being attacked by hostile nodes, the distant specifically designated network is not protected against assaults by malicious nodes. This article presents the results of a writing audit of steering conventions such as AODV, DSR, and others. In addition, the article illustrates the conduct of many levels of assaults as well as defenses against such attacks, such as Black hole attacks, Wormhole attacks, Grey hole attacks, and other similar attacks.

Keywords- AODV; DSDV; DSR; Black hole Attack; Grey hole attack; Wormhole attack.

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) as appeared in Fig 1, has become tremendous zone of research by the vast majority of the specialists now days [10].

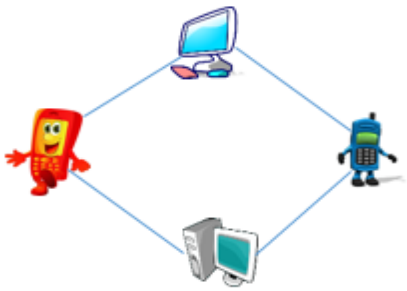

Fig 1. MANET (Mobile Ad-Hoc Network).

A MANET has a self-sorting out property because of which each portable node gets in interface with one another by remote connections, which technique an irregular topology [1]. The network topology can be changed quickly when. The MANET has gotten logically dominating in crises, for example, in war and debacles [2] [16], as it is anything but difficult to participate and effective message can be transmitted through remote connections without the need of exorbitant network framework.

Every portable node fills in as switch just as host. Every mobile node can combine and leave the network. As the portable nodes are having restricted range for the transmission, nodes transmit the parcel utilizing multi-bounce remote transmission joins.

Mobile Ad-hoc Network (MANET) has the property of set of self-designing of mobile nodes, which are furnished with a transporter sense numerous entrances with crash shirking (CSMA/CA) handset, which are allowed to move anyplace autonomously and can impart with no brought together framework support. The telecom is the activity acted in MANET for finding the course from source to goal node. The flooding networks use normally for communicate which lead to repetitive re-broadcasting and cause Broadcast Storm issue [21].

One of the significant qualities of the MANET is the asset limitations for example checked transfer speed and controlled battery handling power. MANET turns out to be all the more standing up to undertaking for the scientists because of this trademark. The quantities of investigates are centered on MANET to overpower from this issue.

International Journal of Science, Engineering and Technology

An Open Access Journal

Many steering conventions have been proposed which can be arranged based on two classes for example Receptive and Proactive routing convention. In Reactive steering convention the course is found at whatever point required. Subsequently it is otherwise called on-request steering convention. The on-request steering conventions have two significant errands: Route disclosure nodes begin course revelation on request premise and Route support when there is disappointment in the connection, upkeep is done.

In Proactive routing convention, every node keeps up the steering table and contains the data about the network topology. It is likewise called as table driven steering convention. Proactive steering conventions are not appropriate for the framework with enormous quantities of mobile nodes.

II. OVERVIEW OF ROUTING PROTOCOL

Routing Protocol plays out a significant job in MANET. Steering Protocol perceive the course from source node to the goal node. Steering Protocol can be extensively delegated: Reactive (e.g., AODV), Proactive (e.g., DSDV) and Hybrid conventions (e.g., ZRF) [2][8].

In Reactive conventions, portable nodes find the course when the source node transmits the bundles to the goal node when the course isn't known. In straightforward words the course is found at whatever point required and course support is done when the course bombs because of connection breakage and so on while in Proactive Protocol, every portable node keep up the steering table and contain the data about the network topology.

At whatever point the progressions happen, routing tables are refreshed occasionally. Proactive Protocol isn't appropriate for huge network. To keep up the route‟s right data, every portable node needs to send control messages sporadically. Every mobile node communicates routing data to their mediator nodes. Each node keeps up the steering tables that have not just the records of close by nodes and accessible nodes yet additionally the quantities of jump.

1. AODV:

Specially appointed On-Demand Distance Vector (AODV) is an overhauled type of DSDV anyway AODV is a Reactive Protocol instead of Proactive Protocol. The Reactive Protocol finds and keeps up the courses at whatever point required. It deals with separation vector routing algorithm [3] and furthermore utilizes goal succession numbers to guarantee the course freshness and the activity performed is circle free [4] [7] [22].

AODV is a steering convention for sending messages between the mobile nodes. The mobile node is permitted to transmit messages through their neighbors to which it can't have the option to associate legitimately. AODV is utilized to decide the course for transmitting the parcel and guarantee that it doesn't have the circles and attempts to find the most limited way. It can control the course changes and produce the new courses for any blunder courses.

A course to a goal can be found when a mobile node communicates route-request (RREQ) parcels to its close by nodes with the assistance of another arrangement number. Every mobile node that gets the communicate, it communicates to the nearby neighbors and the procedure proceeds till the goal gets the message. At the point when the stuck goal or a middle person node that has another course to the goal gets the RREQ, it unicasts an answer by sending a route reply (RREP) bundles forward the counter way embedded at go-between nodes during the course revelation process. What's more, the source node begins broadcasting the parcels to the goal node with the assistance of nearby neighbors that reacted with a RREP right off the bat.

A portable node can rejects a RREQ bundle that the node has recently observed and the RREQ parcel utilizes succession numbers to ensure that the courses are without circle. At the point when the parcels are communicated and the neighbor node moves alongside the bundle, it will trigger the course breakage because of the development to the neighbor nodes and transmit the route error (RERR) parcels to the each dynamic close by nodes. All the Routing data is put away in the source node, goal nodes and the close by nodes from where the information parcels are transmitted [3] [4].

This situation diminishes the memory overhead, limits the utilization of network assets, and runs well in high versatility circumstance [4] [5]. In the event that the source node moves in the past it can re-start

course revelation for transmitting the parcels to the goal and on the off chance that one of the middle person node moves from the range, at that point the close by node allows the connection to link and send the connections setback notice to the next mobile node s. The procedure is proceeding until the source re-starts the course revelation for transmitting the bundles from source to the goal.

1.1 Advantages:

One of the fundamental preferences of the AODV routing convention is that the courses are found at whatever point required and the succession numbers are utilized to know the new course from source to the goal. The course support is check by the „Hello" message.

1.2 Disadvantages:

Burden of the AODV routing convention is that the middle person node can prompt the conflicting course if the source node has the old arrangement number and the delegate nodes not having the most recent goal grouping numbers. Briefest courses can be misplaced because of traffic during way revelation.

2. DSDV Protocol:

Dynamic Destination Sequenced Distance Vector [18], is proactive steering convention that is made with the assistance of Bellmen Ford algorithm with certain changes. The Dynamic Destination Sequenced Distance Vector adds arrangement number to the course table at every portable node. In the DSDV steering convention every portable nodes have the routing table and each steering table hold the rundown of the considerable number of goals and number of bounces to each.

The update is passed on right away once any modification happens in the network. DSDV steering convention is utilized for invigorating routing table of the portable nodes to its current neighbor nodes. The commercial should be possible in the two different ways for example by communicating and by multicasting. This promotion refreshes the current neighbors about the modification in the network, which are passed on intermittently and gradually as topological changes. The primary thought of DSDV was to decrease the communicate messages and to diminish the steering overhead. Every mobile node transmits and refreshes its table sporadically in sort to keep up the dependability.

2.1 Advantages:

One of the principle points of interest of the DSDV steering convention is that it ensures the circle free courses and the check to endlessness issue was diminished. The other significant favorable position of the DSDV steering convention is that it keep up simply the best courses as opposed to keeping up the various courses from source node to the goal node.

2.2 Disadvantages:

The principle burden of the DSDV steering convention is that the multi-way routing isn't upheld. There is consumption of data transfer capacity because of pointless advancement of the routing data to every portable node regardless of whether there are no adjustments in the network and is preposterous to expect to decide the time delay.

3. DSR Protocol:

Dynamic Source Routing [24], is a responsive routing convention for portable specially appointed network. It works like AODV steering convention which is likewise a responsive convention. Receptive methods at whatever point course is required then just course is set up that is on request premise. At the point when the portable nodes demands for course then it starts for building up the courses. Like AODV, DSR doesn't keep up any steering tables; it depends on source routing.

At whatever points the portable node demands for a course then the source starts the RREQ parcel by sending it to its neighbor nodes. DSR is on request source steering convention where all routing data is kept up by every mobile node s. DSR gives network to act naturally sorted out and self-designed with no focal position. Dynamic Source Routing furnishes two instruments both work with one another to give revelation and support of courses.

These two components are: Route Discovery Phase: When the source node transmits the information bundle to the goal node, it gazes upward in the course store. On the off chance that the course reserve has the course data for goal, the source node will send the bundle. On the off chance that the course data doesn't exist in the course reserve, at that point it starts the course revelation process by transmitting the route-request RREQ parcels. The route-request bundles contain the source node and goal address with interesting ID number.

International Journal of Science, Engineering and Technology

An Open Access Journal

3.1 Course Maintenance:

The course support is started when the messed up interface is identified. At the point when the information parcels can't convey, at that point the node transmits a course mistake message to the source node. In this way the course is expelled from its reserve and retransmits the bundle. It guarantees that the way which is picked ought to be extraordinary or ideal and guarantees for circle free routing as indicated by the state of network regardless of whether some adjustment in the transmission course.

3.2 Advantages:

One of the principle focal points of the DSR is that the mediator portable nodes utilize the course store data to decrease the steering overhead and guarantees the circle free activities.

3.3 Disadvantages:

The primary detriment of the DSR steering convention is the course disclosure. At the point when the network size is less, it is anything but difficult to discover the course from source to goal however when the network size is expanded then there is plausibility for accepting various ways to goal. It can bring about the answer storm because of which blockage in the network will be expanded.

III. COMPARISON ON DIFFERENT ROUTING PROTOCOLS

The Table 1 mentioned below shows the comparison among the AODV, DSR and DSDV routing protocols.

Table 1. Comparison among routing protocols. [19]

Parameters	AODV	DSDV	DSR
Protocol	Reactive Protocol.	Proactive Protocol.	Reactive Protocol.
Routing Approach	Uses on-demand approach.	Uses table- driven approach.	Uses on- demand approach.
Type	Based on Distance Vector Routing.	Based on Distance Vector Routing.	Based on Source Routing.
Route Maintenance	Route is maintained by Route Table.	Route is maintained by Route Table.	Route is maintained by Route Cache.
Broadcast	Uses periodic broadcast.	Uses periodic broadcast.	It uses no periodic broadcast.
Loop Free Routing	It provides loop free routing.	It provides loop free routing.	It provides loop free routing.
Routing Metric	It used shortest path.	It used shortest path.	It used shortest path.
Links	It supported only bidirectional links.	It supported only bi-directional links.	It supported both unidirection al and bidirectional links.
Unicasting/M ulticasting	It supports both unicasting and multicasting.	It supports only unicasting.	It supports only unicasting.
Overhead	Message overhead is high.	Message overhead is low.	Message overhead is high.
Security	There is no security.	There is no security.	There is no security.
End to End Delay	Low	Medium	High

IV. DIFFERENT ATTACKS ON DIFFERENT LAYERS

Many different attacks are present on the different layers in the network; some of them are mentioned below Table 2:

Table 2. Different layers Attacks.

Mobile Ad-hoc Network Layers	Different types of attacks
Application Layer	Different attacks through the virus and worms.
Transport Layer	Jelly Fish attack Session Hijacking attack
Network Layer	Blackhole attack Wormhole attack Greyhole attack
Data Link Layer	Stealth attack WEP targeted attack
Physical layer	Jamming attack Malicious

V. ATTACKS ON MANET PROTOCOLS

1. Blackhole Attack:

Blackhole attacks [6][23] is the grave hazardous for the MANET, in which a malicious node sends bogus steering data, expressing that it offers the briefest way for the goal node whose bundles it needs to hinder and afterward grasp them without elevating to the goal. For instance, in AODV, the malevolent node can send counterfeit course answer (RREP) to the source nodes, asserting that it offers a most brief and the crisp course to the goal.

This enables the source node to choose the course and pass on the bundles. Because of which all the traffic are passed on through the malevolent node and accordingly the malignant node can abuse or reject the traffic.

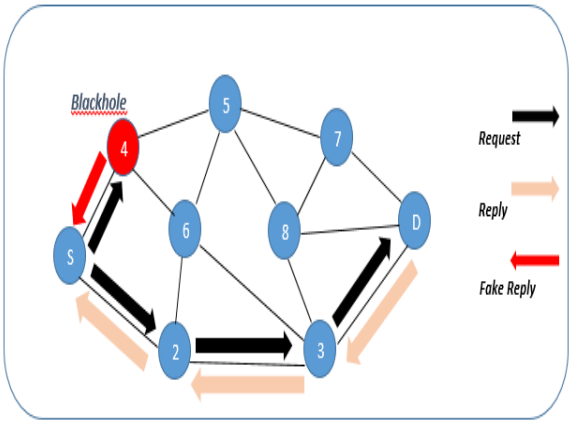

Fig 2. Blackhole Attack.

International Journal of Science, Engineering and Technology

An Open Access Journal

In the fig 2, S and D are the source and the goal nodes, though 1, 2, 3, 5, 6, 7 and 8 are the go-between nodes and 4 is the malignant node or blackhole.

The sender node "S" transmit the route-request (RREQ) to the middle person nodes yet a noxious node "4" sends bogus routing data, expressing that it offers the most limited way for the goal node "D" whose bundles it needs to hinder and afterward hold them without elevating to the goal and sends course answer (RREP) to the source node "S". The source node "S" once got the RREP; it will transmit the information bundles to the malignant node "4" as it is having the most limited course to the goal.

2. Greyhole Attack:

Greyhole attacks are the sort of dynamic attacks that prompts the dropping of the information bundles. It can likewise be called as blackhole attacks. The malignant node right off the bat licenses to transmit the bundles and afterward neglects to do as such. The fundamental distinction between both the attacks is that the undesirable node never sends the genuine control message and at first carries on accurately and react genuine message to the mobile node s that starts the route-request message.

On the off chance that the go-between nodes attempt to transmit the parcels over the attacking nodes, it loses the association with the goal, and afterward may find the course again to the goal.

Malicious nodes build up a course, sending course answer messages. The strategy goes on till the undesirable nodes succeed its point (for example assets, battery utilization and so on).

3. Wormhole Attack:

A wormhole attack [17] is likewise called as burrowing attacks. It is one of the advanced and extreme attacks in MANET. In these attacks the plotting nodes makes the passage among the two nodes for transmitting the bundles, engaging that it offers the briefest way to the goal and assume full responsibility for the node. The Wormhole can drop the parcels by short-circuiting the efficient progression of the steering bundles or it very well may be carefully transmit the parcels to maintain a strategic distance from discovery.

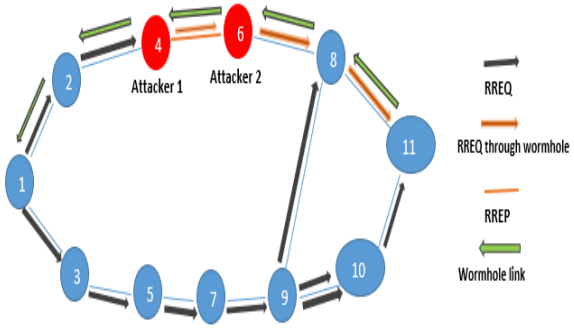

Fig 3. Wormhole Attack.

In the fig 3, we accept that the 4 and 6 nodes are the conspiring aggressors and the node 1 for example source node is imprint to be attacked. During the attacks, the source node 1 will transmit the route-request (RREQ) to the close by nodes for revelation a course to the goal node 11, its neighbor 2 and 3 forward RREQ to nearby neighbor. Anyway the node 4 will record the sent RREQ from node 4 and passages the RREQ to its conspiring accomplice 6.

At that point the node 6 will rebroadcast this RREQ to its neighbor 8.Since this RREQ is gone through rapid channel, the solicitation will reach to the goal 11 node. In this way node 11 will picked the 11-8-2-1 course to unicast the course answer (RREP) to the source node and negligence the equivalent RREQ that showed up later. Subsequently source once got the RREP will begin transmitting the parcel through 4 and 6 nodes [13].

4. Sinkhole Attack:

The sinkhole attacks are the extreme attacks in the portable specially appointed network. In the sinkhole attacks, the primary point is that the malevolent node or traded off node draw in near to all the traffic from its delegate nodes by telling that it has the briefest part for the goal node. When gotten all the traffic from the go-between nodes it makes changes in the mystery information, similar to adjustment in the bundles or drop the information parcels.

An undermined node attempts to draw in all the safe information from the encompassing mobile node s. It additionally influences the presentation of AODV, for example, augment the arrangement number or can limit bounce include while in DSR routing convention the adjustment of succession number is made in route-request (RREQ).

International Journal of Science, Engineering and Technology

An Open Access Journal

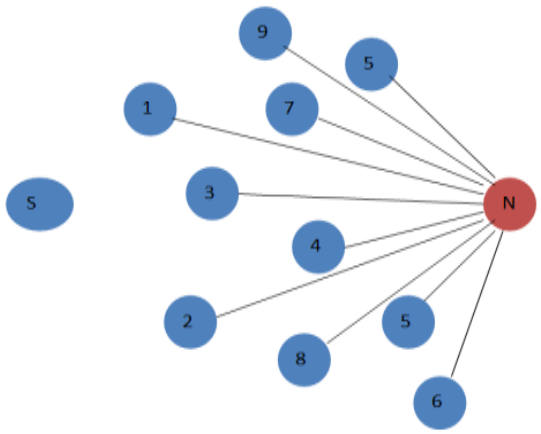

Fig 4. Sinkhole Attack.

In the fig 4, we accept that „S" is the source node and nodes 1, 2, 3, 4, 5, 6, 7, 8, 9 are the go-between nodes and node „N" is the trade off node or the sinkhole node that draws in all the traffic from the middle person nodes by disclosing to them it gives the most brief course to the goal node or base node.

VI. COUNTERMEASURES AGAINST THE ATTACKS

This part provides the related work done to protect routing protocol against the different attacks.

1. Solution to Black hole Attack:

In [9], Vimal Kumar et al. proposed an increasingly capable way out for distinguishing the black hole attacks with less correspondence cost in the network. The proposed strategy is the improvement of AODV steering convention. In this strategy, a coming course answer table (CRRT) added to the source node. A CRRT spare the course answer bundle, which have the data about the goal arrangement no., bounce check, next jump, source IP address, goal IP address and lifetime.

In [10], Kriti Patidar et al. proposed a convention that will shield portable impromptu network from blackhole attacks and wormhole attacks and improved the network soundness. Gives the interruption location framework dependent on the idea of particular based recognition framework to identify and keep from black hole attacks.

The proposed procedure utilizes the idea of counter for determining the crisp and address AODV steering conduct and the individual mobile node s will screen the routing conduct of the middle person nodes for identifying the run-time infringement of particular.

In [11], Rutvij H. Jhaveri proposed a procedure to recognize and to keep from Blackhole attacks and Greyhole attacks during the course revelation. Proposed the method Modified R-AODV.

At the point when the malevolent nodes is identified by the mediator nodes in the wake of accepting RREP, R-AODV marks the course answer as DO_NOT_CONSIDER and imprints the sending course answer as MALICIOUS_NODE in the steering table and afterward the course answer parcels is then transmitted on to the invert way to the source and updates the routing tables.

In [12], Issac Woungang et al. proposed DBA-DSR strategy for recognizing blackhole attacks in the network. This strategy distinguishes and stays away from blackhole attacks by utilizing bogus RREQ bundle before the routing is begun. DBA-DSR convention is an improved type of DSR. In this phony RREQ is instated before the genuine procedure of routing is begun to know the malignant assailants in the network.

Counterfeit RREQ message have constrained life. This message is much the same as a typical RREQ message yet with bogus goal address. Sending of information parcels are done after the affirmation is gotten. An affirmation is utilized supposing that phony RREQ process flops regardless then this affirmation conspire guarantees to distinguish the blackhole node in the network.

In [13], Jiwen CAI et al. proposed a mobile way to deal with recognize blackhole and greyhole attacks in the network. In this a way based strategy is presented which listen the exercises of the following jump. This strategy spares the assets of the node by not sending additional control bundles for identification. This move makes place in arrange layer and edge is evaluated in the MAC layer.

In [14], Saurabh Gupta et al. proposed convention to maintain a strategic distance from blackhole attacks. BAAP use Ad-hoc On-request Multipath Distance Vector that structures connect disjoint multipath through way disclosure. At the point when the middle person nodes reaction to the source node, a portion of the mobile node may have the distinctive

number of way to the goal yet it picks just a single way to goal. In BAAP every node keeps up the authenticity of their neighbor node to make the right course to the goal.

In [20], Sisily Sibichen et al. have proposed a security based methods for verifying the AODV steering convention from blackhole attacks. In this strategy, right off the bat the network recognizes for any malignant nodes and afterward the network is kept from it with the assistance of adjusted AODV. The bogus message is communicated to the mobiles nodes and if any of the nearby nodes gets the bogus routing from its middle person nodes, that implies the undesirable node is available in the network.

The mediator node advises the various mobile node s about those undesirable nodes and portable nodes can refresh their steering table. For giving greater security in the network, the creators proposed a model and that model contains RSA key trade procedures that are utilized among verified neighbors.

2. Solution to Wormhole Attack:

In [10], Kriti Patidar et al. proposed a convention that will shield portable impromptu network from blackhole attacks and wormhole attacks and improved the network dependability. The creator proposed the strategy that utilizes change in routing data between the delegate nodes to recognize wormhole. The location procedure utilized the idea of jump tally. The essential idea of this strategy was to find the elective courses to the goal.

In [15], Yudhvir Singh et al. proposed another strategy to stay away from wormhole attacks. This network is by and large for identifying getting rowdy node in the network. In this elective courses are found over and over with the assistance of course revelation process. It basically identifies the getting rowdy node and disposes of that node from the network without upsetting the general execution of the network.

3. Solution to Sinkhole Attack:

In [24], Fang-Jiao Zhang et al. proposed network to distinguish the sinkhole attacks dependent on excess instrument. The method depended on the multipath determination. The foundation of the course depends on the three stages: route-request, course answer and course foundation.

VII. CONCLUSION AND FUTURE WORK

Mobile Ad-hoc Network Network is confronting numerous issues identified with the security. A ton of conventions and the algorithmic methodologies have been produced for giving the protection from the malicious attacks; evacuate the issues related to it and to improve the presentation of an AODV steering convention.

The point is to give the one of kind algorithmic methodologies which give the protection from the attacks and subsequently improve the presentation of the AODV routing convention. The interesting algorithmic methodologies will be executed in the network test network NS2 to play out the situation and the result.

REFERENCES

[1] Alamsyah, Eko Setijadi, "Performance Comparative of AODV, AOMDV and DSDV Routing Protocols in MANET Using NS2", International Seminar on Application for Technology of Information and Communication, 2018, pp. 1-8.

[2] Aly M. El-Semary, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map", IEEE Access, Volume: 7, 2019, pp. 1-13.

[3] R. Chaudhry, S. Tapaswi, and N. Kumar, "Forwarding Zone enabled PSO routing with Network lifetime maximization in MANET," Appl. Intell., vol. 48, no. 9, pp. 3053–3080, Sep. 2018, doi: 10.1007/s10489-017-1127-5.

[4] N. Arya, U. Singh, and S. Singh, "Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm," in IEEE International Conference on Computer Communication and Control, IC4 2015, 2016, doi: 10.1109/ IC4.2015.7375649

[5] U. Singh, M. Samvatsar, A. Sharma, and A. K. Jain, "Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol," in 2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016, 2016, doi: 10.1109/CDAN.2016.7570908.

[6] S. Singh, A. Mishra, and U. Singh, "Detecting and avoiding of collaborative black hole attack on MANET using trusted AODV routing algorithm," in 2016 Symposium on Colossal Data Analysis

and Networking, CDAN 2016, 2016, doi: 10.1109/CDAN.2016.7570906.

[7] Shukla, M., Joshi, B.K. & Singh, U. Mitigate Wormhole Attack and Blackhole Attack Using Elliptic Curve Cryptography in MANET. Wireless Pers Commun 121, 503–526 (2021). https://doi.org/10.1007/s11277-021-08647-1.

[8] A. Bhawsar, Y. Pandey and U. Singh, "Detection and Prevention of Wormhole Attack using the Trust-based Routing System," 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2020, pp. 809-814, doi: 10.1109/ICESC48915.2020.9156009

[9] Vimal Kumar, Rakesh Kumar, "An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad-hoc Network", Science Direct Procedia Computer Science 48 (2015) 472 – 479.

[10] KritiPatidar and Vandana Dubey, "Modification in Routing Mechanism of AODV for Defending Blackhole and Wormhole Attacks", IEEE 2014.

[11] Rutvij H. Jhaveri, "MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs", IEEE 2013, pp.254-260.

[12] Isaac Woungang, Sanjay Kumar Dhurandher, Rajender Dheeraj Peddi and Mohammad S. Obaidat, "Detecting Blackhole Attacks on DSR-based Mobile Ad-hoc Networks", 2012 IEEE.

[13] Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG and Ning LIU, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad-hoc Network", 2010 24th IEEE International Conference on Advanced Information Networking and Applications, pp. 775-780.

[14] Saurabh Gupta, Subrat kar, S Dharmaraja, "BAAP: Blackhole Attack Avoidance Protocol for Wireless Network", International Conference on Computer & Communication Technology (ICCCT)-2011, pp.468-473.

[15] Yudhvir Singh, Avni Khatkar, Prabha Rani, Deepika and Dheer Dhwaj Barak, "Wormhole Attack Avoidance Technique in Mobile Ad-hoc Networks", 2012 Third International Conference on Advanced Computing & Communication Technologies, pp. 283-287.

[16] Muhammad Imran, Farrukh Aslam Khan, Tauseef Jamal, Muhammad HanifDurad, "Analysis of Detection Features for Wormhole Attacks in MANETs", Science Direct Procedia Computer Science 56 (2015) 384-390.

[17] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto and Nei Kato," A Survey Of Routing Attacks in Mobile Ad-hoc Networks" IEEE Wireless Communication 2007, pp.85-91.

[18] Concepts and Protocols "Wireless and Mobile Networks" book by Dr Sunilkumar S. Manvi and Mahabaleshwar S. Kakkasageri.

[19] Parma Nand, S.C. Sharma ,"Routing Load Analysis of Broadcast based Reactive Routing Protocols AODV, DSR and DYMO for MANET", International Journal of Grid and Distributed Computing, Vol. 4, No. 1, Mar 2011, pp 81-92.

[20] Sisily Sibichen, Sreela Sreedhar, "An Efficient AODV Protocol and Encryption Mechanism for Security Issues in Ad-hoc Networks", International Conference on Microelectronics, Communication and Renewable Energy (ICMiCR-2013)

[21] Parma Nand, S.C. Sharma, "Analytical Study of Broadcast in Mobile Adhoc Network", International Journal of Computer Applications (0975 – 8887), Vol 19– No.8, April 2011, pp 7-12. Impact Factor 0.845.

[22] Mohamed A. Abdelshafy, Peter J. B. King, "Analysis of Security Attacks on AODV Routing", IEEE, pp 290-295, 2013.

[23] Satria Mandala, Abdul Hanan Abdullah, Abdul Samad Ismail, Habibollah Haron, Md. Asri Ngadi, Yahaya Coulibaly, "A Review of Blackhole Attack in Mobile Ad-hoc Network", IEEE, pp. 339-344, 2013.

[24] Fang-Jiao Zhang, Li-Dong Zhai, Jin-Cui Yang and Xiang Cui, "Sinkhole attack detection based on redundancy mechanism in wireless sensor networks", Information Technology and Quantitative Management (ITQM 2014)