Mitigating the Effect of Wormhole Attack on MANET with AODV Routing Protocol

Abhipriya Singhal[1] Mrs. Reshu Grover[2]
[1,2]Department of Computer Science and Engineering
[1,2]Laxmi Devi Institute of Engineering & Technology (LIET), Alwar, India

Abstract— As MANET (Mobile Ad-hoc Network) applications are deployed, security emerges as a central requirement. We introduce the wormhole attack, an excessive attack in ad hoc networks that is in particular tough to guard against. The wormhole assault is possible despite the fact that the intruder has not damage any hosts or even if all communiqué gives authenticity and confidentiality. In the wormhole assault, intruder statistics packets (bits) at one location within the community, tunnels them (possibly selectively) to any other region, and retransmits them there into the network. The wormhole assault can form a serious hazard in MANET, mainly against many Mobile Ad-hoc Network routing protocols and region primarily based security structures. For example, most existing MANET routing protocols, without some mechanism to defend against the wormhole attack, would be unable to find routes longer than one or two hops, severely interrupt communication. Here is a general mechanism, called packet watchdog, for detecting and protecting against wormhole attacks, and a specific protocol that implements watchdog. In this performance of Mobile Ad-hoc Networks (MANET) under wormhole attack is analyzed. Multiple QoS parameters had been taken into consideration right here together with throughput, postpone, packet shipping ratio, and node power and node density. The NS3 community simulator has been used and the reference point organization mobility model is taken into consideration to observe the effect of node density and the preliminary power at the throughput.

Keywords: MANET, Routing, AODV, Worm Hole, NS3

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a fixed of Wi-Fi cell nodes which also can shape a brief community, without using any consistent infrastructure or centralized management. Nodes calculate on multi-hop routing protocols to forward statistics packets sent from a source node to a vacation spot node that is out of its transmission variety. Every node can also function as each a records supply and a router that forward facts for other nodes.

Mobile networking is one of the maximum important eras helping pervasive computing [1]. During the final decade, advances in each hardware and software program strategies had resulted in mobile hosts and Wi-Fi networking not unusual and miscellaneous. Generally there are two super techniques for permissive Wi-Fi cell gadgets to talk with every other:

A. Infrastructure:

Wireless cellular networks have historically been based totally on the cellular idea and relied on actual infrastructure stay, wherein cell gadgets communicate with access points like base stations related to the regular network infrastructure. Typical examples of these kinds of Wi-Fi networks are WLL, WLAN, GSM, UMTS, and lots of others.

B. Infrastructure-less:

As to infrastructure much less method, the mobile wireless network is generally referred to as a cell advert hoc community (MANET). A MANET is a set of Wi-Fi nodes which can dynamically layout a community to change records without using any pre-gift regular community infrastructure. This is a very critical a part of communiqué era that helps virtually common computing, because of the truth in many contexts facts exchange among cell units can't rely on any fixed network infrastructure, however on rapid configuration of a wireless network on-the-fly. Wireless advert hoc networks themselves are an unbiased, huge region of studies and programs, in area of being most effective just a complement of the cellular machine. In this dissertation, the fundamental issues of advert hoc networking is described with the aid of giving its associated studies historical past together with the idea, capabilities, status, and packages of MANET. Some of the technical challenges MANET poses also are conferred. Some of the important thing studies troubles for ad hoc networking generation are discussed in detail which might be predicted to promote the development and accelerate the industrial packages of the MANET era.

The easy characteristic of those networks is the whole loss of any type of infrastructure, and consequently the absence of committed nodes that offer community management operations just like the traditional routers in fixed networks. In order to maintain connectivity in a cell ad hoc community, all of the players' nodes must carry out routing of community visitors. The cooperation of nodes cannot be enforced by using manner of a centralized administration authority as it does no longer exist. Therefore, a network layer protocol designed for such self-worried networks have to put into effect connectivity and security requirements which will guarantee the undisrupted operation of the higher layer protocols. [2]

II. MANET CHALLENGES

Independent of the appealing bundles, the capacities of MANET present SEVERA requesting circumstances that should be considered cautiously ahead of time than an immense business endeavor sending might be normal. These epitomize:

A. Routing:

Because the topology of the system is ceaselessly changing, the inconvenience of directing parcels among any pair of hubs transforms into a troublesome assignment. Most conventions should be fundamentally founded on receptive directing instead of proactive. Multicast steering is each other test on account of the reality the multicast tree is once static because of the irregular movement of hubs inside the system. Courses among hubs can likewise involve more than one bounces, this

is more perplexing than the single jump discussion a couple of the hubs [9].

B. Security and Reliability:

Further to the not uncommon vulnerabilities of Wi-Fi association, a specially appointed system has its one of a kind security issues on account of e.g. Frightful neighbor communicate bundles. The normal for circulated activity calls for explicit plans of validation and key control. Further, remote connection qualities report besides dependability issues, because of the limited Wi-Fi transmission run, the distributed idea of the remote medium (e.g. Shrouded terminal problem), portability accelerated bundle misfortunes, and insights report botches.

C. Quality of Service (QoS):

Quality of Service (QoS) providing one-of-a-type momentous of backer ranges in a consistently changing condition is likely an endeavor. The innate stochastic component of interchanges top notch in a MANET makes it intense to offer standard guarantees at the contributions outfitted to a gadget. A versatile QoS ought to be connected over the conventional advantageous guide reservation to manual the media contributions [10].

D. Power Consumption:

For the vast majority of the gentle weight versatile terminals, the discussion related skills should be enhanced for lean vitality utilization. Wellbeing of power and vitality cognizant directing should be considered [11][12].

III. Problem Statement

The problem of all the current ad hoc routing protocols is that they trust all nodes and assume that they behave properly; therefore they are vulnerable to attacks launched by fool around nodes. The resource limitation of nodes used in MANET, along with the multi-hop nature of this network may cause a new phenomenon which does not exist in classical networks. To save its resources, nodes may behave selfishly and uses the services of other nodes without correctly participate in system. Watchdog method is a reputation based method used for the disclosure of selfish nodes and worm holes in MANETS. Standard Watchdog Implementation, along with Bayesian Filtering [5], provides a much more improved estimation for disclosure of selfish nodes in MANETs. This Bayesian Watchdog can be further improved by collaborative message passing so that local information from each node can be utilized to get global information for proper routing. The objective of the research is to improve the estimation of probability of packet delivery to the destination, as computed on every hop node on the path, using Bayesian Filtering and Probability Distribution. Feasibility of any node being selfish or not is computed using a set of observations witnessed by nodes on the path under consideration.

IV. Scope of Research

The presence of node misbehaviors and multiple failures yields new challenges to the survivability of wireless ad hoc networks and provide motivation to reveal their fundamental impacts on network survivability. Also, optimum utilization of network resources is possible only when there is some mechanism which ensures the survivability of the network under malicious or selfish nodes. Current research is important in the sense that it improves the probability estimate at every node regarding successful packet delivery to the destination. An overall cumulative probability estimate can be computed from these observations giving an impact of selfishness on the network and the survivability of Ad hoc network.

V. Literature Survey

A. A Novel Taxonomy of MANET Attacks [13]:

The vulnerabilities of Mobile Ad hoc Networks (MANETs) make it subject to a large number of attacks. In order to understand the nature and behavior of such attacks, many classification schemes and taxonomies to MANET attacks have been proposed. This paper proposes a new taxonomy to MANETs attacks. The taxonomy is aimed to provide a consistent means of classifying attacks, as well as allowing previous knowledge to be applied to new attacks and providing a structured way to view such attacks. The taxonomy is based on attack attributes. Every attack is characterized by a unique vector of attribute values, where each attribute defines a specific attack property which may have different values. The taxonomy uses six attributes; the legitimacy of attacking node/s, the number of nodes participating in the attack, MANETs vulnerabilities utilized by the attack, the network resources exploited by the attacking node/s, the targeted victim and finally, the network security service compromised by the attack. The analysis of some well-known attacks shows the capability of the proposed taxonomy in describing and categorizing these attacks as taxonomy vectors.

B. Impact of Wormhole Attacks on MANETs [14]:

A mobile ad hoc networks (MANETs) includes a set of Wi-Fi cell nodes which are able to speaking with every different. MANETs is infrastructure-much less, loss of centralized monitoring and dynamic changing community topology. So, this community is fairly susceptible to attacks because of the open medium. In this paper, we talk about the effect of wormhole ambush in MANETs. The wormhole assault is difficult to distinguish with the guide of utilizing any cryptographic measures since they do now not make any different parcels. In this work, a few strategies of wormhole location like guard dog, hubs with directional radio wire and group essentially put together strategy thus with respect to. Some counteractive action methods comprehensive of bundle rope, time-of-flight, Delphi convention, way rater procedure, etc. Are additionally displayed. The outcome assessment demonstrates the impact of wormhole assault on MANETs in expressions of throughput varieties.

C. A Study on Wormhole Attacks in MANET [20]:

An Ad-hoc system is a self-composed network, without a significant facilitator, and which frequently changes its topology. In this paper, we've broke down the exhibition of Mobile Ad-hoc Networks (MANET) underneath wormhole assault. Different QoS parameters have been mulled over here

which incorporate throughput, put off, parcel shipping proportion, hub vitality and hub thickness. The NS2 organize test system has been utilized and the reference factor bunch versatility adaptation (RPGM) is considered to ponder the impact of hub thickness and the fundamental vitality on the throughput.

D. Survey on Security Issues in MANET [21]:

A survey of various issues (mainly wormhole attack) in MANET regarding security is done considering all major aspects. In the proposed MANET architecture, the network is formed with two types nodes, namely trusted mobile nodes and trusted mobile nodes. The trusted and trusted mobile nodes resemble with specialized and non-specialized responders respectively at the disaster site. In the proposed trust management scheme, the trust derivation is through reputation, recommendation and context. Reputation of a node, as evaluated by another node, is through comparing of monitored traffic with each other. Suggested through neighbouring nodes leads to truthfulness of a node. A node with truth value less than a threshold is treated as malicious. To discover a trustworthy path in the MANET, the trust management scheme has been incorporated in the routing protocol.

E. A Result Paper of Wormhole Attack Detection and Prevention in MANET using Bait Scheme [22]:

The nodes in mobile ad hoc networks communicate wirelessly with each other. The wireless nature of the communication makes nodes susceptible to various kinds of attacks such as black hole attack, worm hole attacks, denial of service attacks etc. In present work, the paper aims at detection and prevention of the wormhole attack. In wormhole attack, the attacker nodes form a tunnel. As a result, the length of the path between source and destination is shortened in terms of the hop count. The source node has to select the path containing lowest hop count, and when the data is received by the wormhole nodes on the path the nodes drop the packets coming to them. This hampers the performance of the network in terms of packet drops, packet delivery ratio and throughput. This paper is an extension to the bait scheme which was earlier used to detect the black hole attacks. The performance of the network has been considered under wormhole attack and then after its detection and prevention.

F. Security Assessment of AODV Protocol under Wormhole and DOS Attacks [23]:

A MANET a is ready of Wi-Fi mobile nodes that share a not unusual Wi-Fi channel without any centralized unit. In latest years many routing protocols were proposed for application of MANETs in authorities, commercial and military area. MANETs have a few features inclusive of dynamic nature, decentralized support and infrastructure-much less which make it extraordinarily susceptible to assaults. Security becomes a primary issue in the layout of routing protocols in MANETs. In this paper, we gift protection evaluation of routing protocol in trendy and Ad-hoc on demand Distance Vector especially beneath exceptional type of attacks.

G. Analysis and Prevention of Wormhole Attack Using Trust and Reputation Management Scheme in MANET [24]:

MANETs operates without fixed framework and all nodes in network perform like a router in sequence to forward information next receiver. Since the pivotal point rein lack, MANETs are additionally pregnable routing attacks as against various grids. Routing is one of the most serious attacks of wormhole attacks that are easier to be implemented nevertheless harder detection. Generally, it operates in two phases; in the first phase, wormhole channel nodes tend to draw more and more traffic route, and by other phase, they loss the grid by altering or dropping the grid traffic. In MANETs, numerous writers have implemented diverse results to prevent attacks. In this paper, we proposed a trust and reputation management scheme for find out the trusted location in MANET environment.

VI. WORMHOLES AND ITS VARIANTS

This content is makes a specialty of the wormhole attack, where two colluding nodes which are some distance aside are connected by using a tunnel giving an illusion that they're pals. Each of these nodes advantage course request and topology control messages from the network and send it to the opposite colluding node thru tunnel so that you can then replay it into the community from there. By the usage of this additional drift, these nodes are able to market it that they've the shortest direction via them. Once this hyperlink is set up, the attackers may additionally pick out every different as multipoint relays (MPRs), which then result in an transaction of some topology manipulate (TC) messages and information packets thru the wormhole tunnel. Since those MPRs forward improper topology records, it consequences in spreading of incorrect topology information during the community [8]. On receiving this false statistics, different nodes might also send their messages through them for immediate delivery. Thus, it prevents actual intermediate nodes from organizing links between the supply and the vacation spot [11]. Sometimes, due to this, even a wormhole attacker may fall sufferer to its mine achievement.

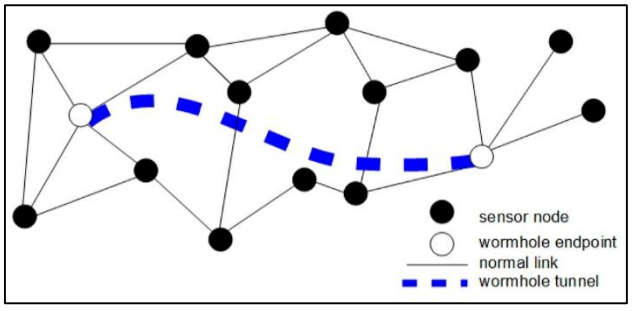

Fig. 1: Wormholes and Its Variants

In [9], a specific type of wormhole attack we find “in-band wormhole attack”. A sport theoretic technique has been accompanied to hit upon intrusion in the community. Presence of a government is affected for monitoring the network. This is a drawback in Wi-Fi situation along with military or emergency rescue. No experimental end result is stated in [9].

In [14] the wormhole attacks are categorized as 1) In-band wormhole attack, which require a covert overlay over the existing wireless medium and 2) Out-of-band wormhole

assault, which require a hardware channel which join two colluding nodes. The in-band wormhole assaults are in addition divided in [14] as 1.1) Self-enough wormhole assault, in which the assault is constrained to the colluding nodes and 1.2) Extended wormhole assault, where the beyond the colluding nodes assault is extended. The colluding nodes attack some of its neighboring nodes and appeal to all of the traffic acquired by its neighbor to bypass through them.
In the kind second of wormhole assaults [15], the intrusions are outstanding between a) hidden attack, in which the community is ignorant of the life of malicious nodes and b) exposed attack, where the community is aware about the presence of nodes however cannot pick out malicious nodes among them.

VII. PREVENTION OF WORMHOLE ATTACK

Choi et al. In [16] considered that each one the nodes will reveal the behavior of its buddies. Each node will ship RREQ messages to destination through the use of its neighbor list. If the source does now not get hold of again the RREP message within a assure time, it detects the presence of wormhole and provides the route to its wormhole list. Each node continues a neighbor node desk which encloses a sending time and receiving time of the RREQ, RREQ collection wide variety, neighbor node ID and matter. Here the source node sets the Wormhole Prevention Timer (WPT) after sending RREQ packet and wait until it listen in its neighbor's retransmission. According to the writer, the most amount of time required for a packet to tour one-hop distance is WPT/2. Hence, the postpone according to hop price should no longer beat expected WPT. However, the proposed approach does no longer completely aid DSR as its miles based on quit-to-cease signature authentication of routing packets.

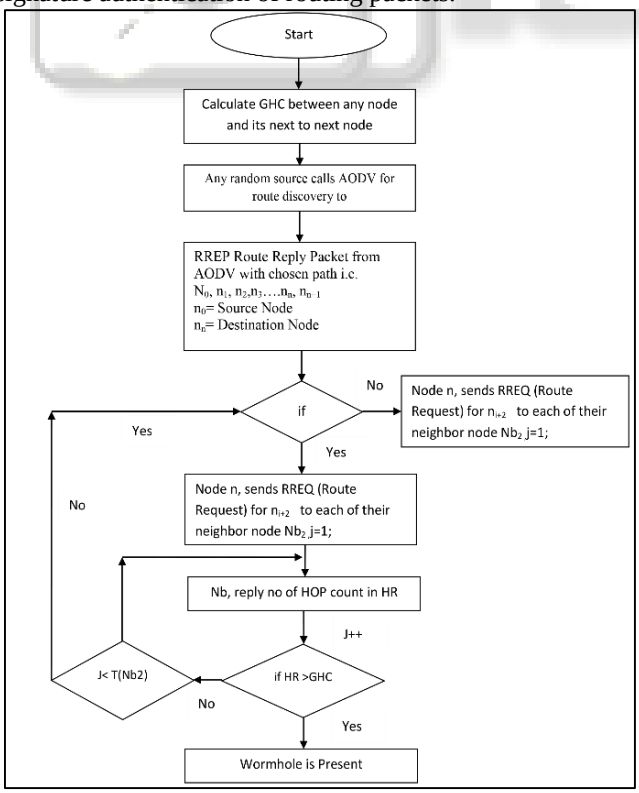

Fig. 5.2: Flow chart of Technique to detect Wormhole Detection

Some proposals to stumble on wormhole assaults like:

1) The abrupt lower inside the course lengths can be used as a likely symptom of the wormhole assault.
2) With the possible displayed course statistics, if the give up-to-end route put off for a course cannot be defined by the sum of hop delays of the hops present on its marketed direction, presence of wormhole may be suspected.
3) Some of the paths may not observe the displayed fake link, yet they'll use a few nodes worried within the wormhole attack. This will lead to a upward push in hop stoppage due to wormhole site visitors and sooner or later an boom in cease-to-end postpone at the path. An abrupt increase ultimately-to-end postpone and the hop queuing delay values that can't be interpreted with the aid of the site visitors supposedly flowing thru those nodes can lead us to suspect the presence of wormhole.

VIII. SIMULATION SETUP

Simulations had been finished so that you can examine routing protocol. We focused our attention at the evaluation of community overall performance in phrases of routing overhead, throughput, packet transport ratio and normalized routing load of a cellular advert hoc network in which some of nodes are varying.

Number of Nodes	10,20,30,40,50
Topology	Dynamic
Simulation Time	1000 Sec
MAC Layer	802.11
Range	200 meters
Simulation Area	1000 x 1000 meter2
Routing Protocol	AODV
Traffic Model	Constant Bit Rate
Packet Size	512 Bytes
Interval	1 Sec

Table 1: Simulation Parameter

IX. SIMULATION RESULTS

A. Throughput:

Network throughput is the slight cost of effective message conveyance over a report channel. This measurements might be included over a physical or legitimate hyperlink, or go through a definite network hub.

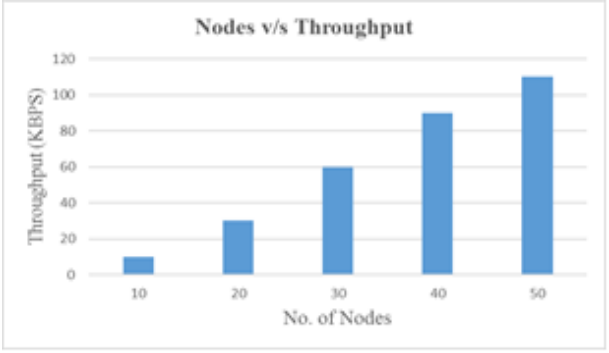

Fig. 2: Nodes Vs Throughput

The throughput is regularly determined in bits with regards to second (piece/s or bps), and periodically in records parcels in venture with second or realities bundles in accordance with vacancy.

B. Packet Delivery Ratio:

Packet transport ratio can be identifying by way of the ratio between the number of information packets which are dispatched by the source and the variety of information packets which can be obtained via the sink. Graph suggests because the number of node growth it receives higher due to the fact chance of direction breakage decrease.

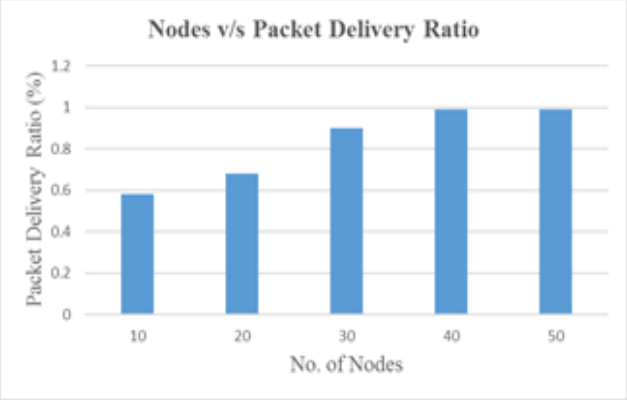

Fig. 3: Nodes Vs Packet Delivery Ratio

C. Normalized Routing Load (NRL):

It's the range of routing packets transmitted in keeping with records packet sent to the destination. Also every forwarded packet is counted as one transportation. This metric is likewise surprisingly correlated with the variety of direction adjustments befell within the simulation.

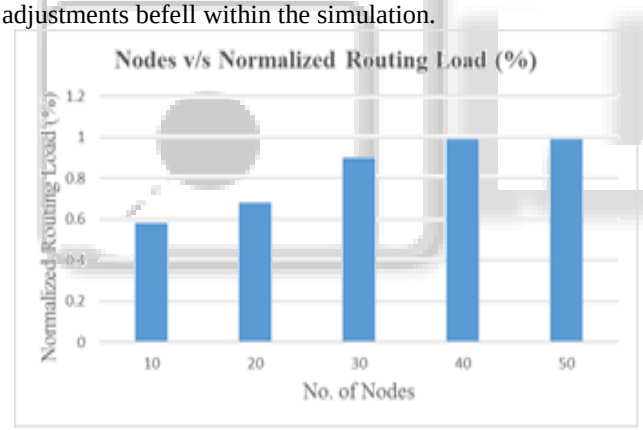

Fig. 4: Nodes Vs NRL

D. Average end-to-end delay of data packets:

There are possible deferrals realized by buffering during course divulgence latency, lining at the interface line, retransmission delays at the MAC, and expansion and relocation times. When the time distinction between every CBR bundle dispatched and got become recorded, isolating the absolute time contrast over the general scope of CBR parcels procured give the basic offer up-to-stop delay for the obtained parcels. This measurement depicts the bundle transportation time: the decline the stop to-stop put off the better the product in general execution.

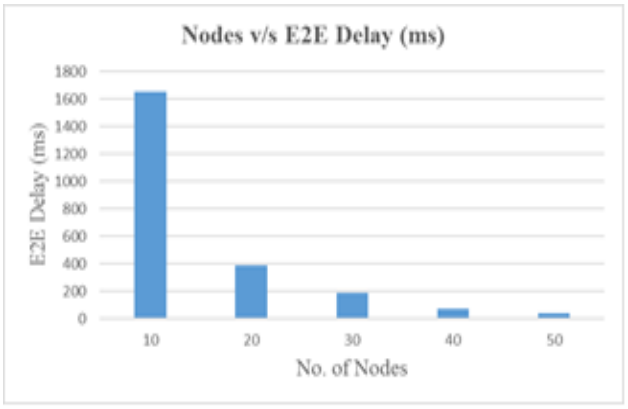

Fig. 6.4: Nodes Vs E2E-delay

X. CONCLUSION & FUTURE WORK

Portable Ad-Hoc Networks can possibly introduce a network wherein a customary system framework environment can't most likely be conveyed. With the criticalness of MANET similar to its sizable ability it has in any case numerous upsetting circumstances left so as to triumph over. Security of MANET is one of the indispensable capabilities for its organization. In our postulation, we've were given have been given dissected the conduct and difficulties of insurance dangers in cell advert-hoc systems with arrangement finding strategy. Dark gap strike is recreated and its impact at the MANETS is dissected with three acting lattices for example offer up-to - stop disposes of, organize burden and throughput. The impacts gained from reproduction are examined profoundly a decent method to draw in the absolute last avert. Distinctive moderation plans are contemplated in detail and we concoct relief plan that suits best to evacuate Black Hole assault.

A. Conclusion

Addressing the essential research question, in our exploration we broke down that dark empty ambush with four astonishing circumstances with perceive to the exhibition parameters of quit-to - give up put off, throughput and network load. in a system it is critical for a convention to be excess and green in term of wellbeing. we have dissected the defenselessness of conventions OLSR and AODV have increasingly radical impact while there might be better style of hubs and further course demands. The level of severances in postponement underneath assault is to five rate and if there should arise an occurrence of OLSR, in which as it's miles five to ten rate for AODV. The throughput of AODV is influenced through multiple times as analyze of OLSR. In the event of network load be that as it may, there can be sway on AODV through method for the noxious hub is less as see to OLSR. tending to the subsequent research inquiry, from the impact of dark gap assault on the MANETS we saw that AODV is significantly all the more experiencing the assault rather than OLSR. From our examination we stop that AODV convention is more prominent powerless against dark empty attack than that of OLSR convention. Responding to the zero.33 examinations question, numerous answers have been considered through sizable writing analyze. A significant number of the proposed answer professed to be the fine answer be that as it may in spite of the fact that those arrangements are not impeccable

as far as viability and execution. On the off chance that any answer works pleasantly within the sight of unmarried malignant hub, it can't be significant in the event of different malevolent hubs. The middle of the road react messages whenever crippled outcomes in the delivery of message to the goal hub will never again best enhance the exhibition of network, however it'll furthermore quiet the system from Black Hole attack. In view of our exploration and assessment of recreation stop final product we draw the conviction that AODV is extra in danger of Black Hole ambush than OLSR.

B. Future Work

Responding to the essential research question, in our exploration we investigated that dark empty attack with four awe inspiring circumstances with perceive to the presentation parameters of quit-to - give up put off, throughput and network load. In a system it is essential for a convention to be repetitive and green in term of security.

REFERENCES

[1] Shrivastava, S.P. Singh, "A Survey on Wormhole Attack Detection in Wireless Network", International Journal of Computer Science and Information Technologies, Vol. 7 (3), 2016, 1273-1276.
[2] N. Devi, S. Deswal, "A review: wormhole attack detection in MANET", International Journal of Science, Engineering and Technology Research (IJSETR) Volume 5, Issue 6, June 2016.
[3] Neema Soliyal , H.S. Bhadauria , Preventing Packet Dropping Attack on AODV Based Routing in Mobile Ad-Hoc MANET, International Conference on Advances in Computing, Communications and Informatics (ICACCI), Sept. 21-24, 2016.
[4] L. Prashar and R. K. Kapur, "Performance analysis of routing protocols under different types of attacks in MANETs," 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, 2016, pp. 405-408.
[5] ALshahrani, Abdullah Saad, "Rushing Attack in Mobile Ad Hoc Networks", International Conference on Intelligent Networking and Collaborative Systems, 2011.
[6] Sukiswo and M. R. Rifquddin, "Performance of AOMDV routing protocol under rushing and flooding attacks in MANET," 2015 2nd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Semarang, 2015, pp. 386-390.
[7] K. Rajkumar , S. Prasanna , "Complete analysis of various attacks in MANET", International Journal of Pure and Applied Mathematics, Volume 119 No. 15 2018.
[8] Anshika Garg, Shweta Sharma, "A Study on Wormhole Attack in MANET", International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882211, Volume 3 Issue 2, May 2014.
[9] Aakanksha Kadam1, Niravkumar Patel2, Vaishali Gaikwad3, Detection and Prevention of Wormhole attack in MANET" International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 03 | Mar-2016.
[10] Tiruvakadu, Divya sai & Venkatarm, Pallapa. (2018). Confirmation of wormhole attack in MANETs using honeypot. Computers & Security. 76. 10.1016/j.cose.2018.02.004.
[11] Upadhyay, Saurabh and Chaurasia, Brijesh Kumar, "Detecting and Avoiding Wormhole Attack in MANET Using Statistical Analysis Approach", Advances in Computer Science and Information Technology. Networks and Communications, PP. 402—408, 2012.
[12] Ranjeeta Siwach1, Vanditaa Kaul2 , "A Study of Manet and Wormhole Attack in Mobile Adhoc Network", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 2, Issue. 6, June 2013, pg.413 – 420.
[13] N. A. Noureldien, "A novel taxonomy of MANET attacks," 2015 International Conference on Electrical and Information Technologies (ICEIT), Marrakech, 2015, pp. 109-113.
[14] Sharma and R. Kumar, "Reviewing the impact of wormhole attack in MANET," 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Noida, 2016, pp. 336-341.
[15] 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," 2015 International Conference on Computer, Communication and Control (IC4), Indore, 2015, pp. 1-5.
[16] Jhaveri, Dr Rutvij. (2010)."MANET Routing Protocols and Wormhole Attack against AODV" International Journal of Computer Science and Network Security. 10. 12-18.
[17] A. Grewal, G. Singh, 'Detection and Prevention of Grayhole, Blackhole and Wormhole Attacks in MANET Using IIRD" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 9, September 2017.
[18] S. Singh, R. Kansal, "Novel Technique for Detection of Wormhole Attack in MANET", International Journal of Computer Sciences and Engineering, Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693.
[19] Ghayvat, S. Pandya, S. Shah, S. C. Mukhopadhyay, M. H. Yap and K. H. Wandra, "Advanced AODV approach for efficient detection and mitigation of wormhole attack in MANET," 2016 10th International Conference on Sensing Technology (ICST), Nanjing, 2016, pp. 1-6.
[20] Maulik, Reshmi & Chaki, Nabendu. (2011). "A study on wormhole attacks in MANET". International Journal of Computer Information Systems and Industrial Management Applications. 3.
[21] P. K. Sharma and V. Sharma, "Survey on security issues in MANET: Wormhole detection and prevention," 2016 International Conference on Computing, Communication and Automation (ICCCA), Noida, 2016, pp. 637-640.
[22] Harjinder Kaur1, Sukhjit Singh2, "A Result Paper of Wormhole Attack Detection and Prevention in MANET using Bait Scheme", International Journal of

Engineering Science and Computing, May 2017, Volume 7 Issue No.5.

[23] K. Joshi and M. Soni, "Security assessment of AODV protocol under Wormhole and DOS attacks," 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), Noida, 2016, pp. 173-177.

[24] S. Parbin and L. Mahor, "Analysis and prevention of wormhole attack using trust and reputation management scheme in MANET," 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Bangalore, 2016, pp. 225-228.

[25] S. Upadhyay and B.K. Chaurasia, "Detecting and Avoiding Wormhole Attack in MANET Using Statistical Analysis Approach", International conference on Computer Science and Information Technology (CCSIT), 2012.

[26] Roy, R. Chaki, N. Chaki "A New Cluster-Based Wormhole Intrusion Detection Algorithm For Mobile Ad-Hoc Networks", International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 1, April 2009.

