Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

A Technique for Detecting Wormhole and Jellyfish Attack in MANET

SVD Anil Kumar [1], Neelam Sunda [2], Babita Jain [3], Shruti Thapar [4]

[1]Professor, EEE Dept, St.Ann's college of Engineering and Technology, Chirala, Andhra Pradesh, India, eee.dranil@sacet.ac.in

[2]Computer Science Application, (Asst. Prof.), Kanoria PG Mahila Mahavidyalaya, (Jaipur), Rajasthan, India,, research.neelam@gmail.com

[3] Electrical Engineering, (Prof.), St. Ann's College of Engineering and Technology, Chirala, Andhra Pradesh, India, jain.babita@gmail.com

[4]Electronics and Communication, (Asst. Prof.), PIET, Jaipur, (RTU, KOTA), Jaipur, Rajasthan ,India, shruti.thapar@poornima.org

Article Info
Page Number: 1529-1539
Publication Issue:
Vol. 71 No. 4 (2022)

Article History
Article Received: 25 March 2022
Revised: 30 April 2022
Accepted: 15 June 2022
Publication: 19 August 2022

Abstract

Ad hoc networks are conniving or leaned to interrupt by remote connection methodology. In this manner the information from these associations can be taken successfully by presenting the aggressor place focuses in the construction. The straight course still up in the air with the help of node count metric. Due to this, it wants to defeat conventions. From various assaults, the wormhole assault is viewed as the unsafe one. This interference is begun with the assistance of couple aggressor focus focuses. These middle focuses make a channel by setting two or three sensor habitats among transmitter and collector. The open structure regards the wormhole interferences without center individual sensor center points amidst target. This part is enormous for the area where the course distance in the midst of transmitter and finder is two stages fundamentally. This part isn't reasonable for those conditions where multi hubs are introduced in the midst of transmitter and beneficiary. In the projected review, another strategy is finished for the confirmation and division of attacker sensor focus focuses from the affiliation. The wormhole obstructions are set off by these assailant communities in the climate. The projected game plan is used in NS2 and it is portrayed by the duplication results that the projected course of action shows better execution regarding existing systems.

Keywords: MANET, AODV, Wormhole, Direct Trust Based Detection Technique.

1. Introduction

In this day and age of digitalization, innovation is essentially worried on effective controlling and overseeing force of the framework. For this appropriate directing conventions and secure correspondence climate are must to support some remote detecting applications like Military region, Commercial Sector, Personal use, Bluetooth and neighborhood level etc[4][9][25][13]. MANET has shown huge development in arising remote detecting networks in light of the exceptionally expanding requests and various assumptions in the space [5]. It includes absence of foundation, channel sharing for remote correspondence,

lesser number of hubs, dynamic geography and moderate sources. There is no focal infrastructural in the middle of between the organization for the checking the information development between the hubs [13][11]. Any hub in the organization can go about as shipper, collector and switch also. There is no data to any hub in the climate about its transitional hubs. Steering conventions assume an essential part in MANET like introducing new courses; moderating and change of new courses inside the organization geography are the vital jobs to it [10][14][20][24].

Because of absence of infrastructural arrangement and portable hubs, security and keeping up with effective steering of hubs, is turning into the significant test in MANET [19]. The significant damages which influence the organization arrangement are moment evolving geography, no incorporated control, limited assets and absence of data about halfway nodes[18]. Because of this, MANET is particularly inclined to the digital assaults due to self getting sorted out and arrangement property. As this assault will straightforwardly hurt the significant nature of administration figure the organization arrangement like battery reinforcement, execution estimation, manageability and the main security of the network[15][12].

In MANET, two various types of assaults are there which can cause the causality in the organization arrangement for example outside and inner assaults [19]

1.1 External Attack: These going after hubs are absent in the climate arrangement and can hurt the organization from outside. Blockage, sending incorrectly directing data and causing inaccessibility of organization administrations are the significant impact of this assault [2].

1.2 Internal Attack: These going after hubs are available as a certified hub in the organization. This bogus hub in the arrangement will acquire unapproved control hurt the organization in numerous ways [7]. It is again characterized into two sections for example

1.2.1 PASSIVE ATTACKS: The information is just gathered from the client location and not modified at any rate. By and large programmer utilizes this sort to go after to get the information and utilize the results [6] [12].

1.2.2 ACTIVE ATTACKS: In this assault, aggressor gets the information and does a modification in it to acquire the entrance and break the protection in the organization [11]. This sort of assault is entirely versatile and useful in quality as they continue to change their geography habitually. Due to these attacks MANET is becoming less secure and less effective because of dynamic changing structure and open medium access control. Some of the attack forms in MANET are Wormhole attack, black hole attack, gray hole attack, flooding, replay attack, DoS (Denial of Service) attack, Man-in-middle attack and eavesdropping attack etc. which are able to harm the network topology and upper layer Applications[3][8][21][12][16][17]. This research paper we will try to analyze the MANET's execution under wormhole attack. Detection and prevention mechanism will be discussed and analyzed under suitable network environment.

2. Wormhole Attack In MANET

It is the most severe and serious sort of assault in MANET climate is wormhole assault [17]. Wormhole is a Denial of Service kind of assault which is persuading on network layer. It is idle kind of attack so; it makes an easy route to the objective by acquiring information from starting phase of the organization and broadcast it to another end. It can undoubtedly upset the entire organization, because of solid malignant aims assault and the partnership of two bogus hubs with legitimate data about the organization geography. It is begun by several associate center points [9]. In wormhole assault a part is shaped between the bogus focuses to dump the traffic and complete horrendous positions in the affiliation. It requires less investment to send the information on finishing hub of the course then the ordinary time stretch. This is because of the less measures of in the middle of between the way in examination with different way courses [15] [11]. Figure 1 is having ordinary focus focuses and typical relationship with unsafe focus focuses (S2, S9) will get information and elaborate the course lengths by utilizing private redirect known as wormhole in the middle between. Vindictive focus point will draw in the information bundle towards itself by showing lesser number of jumps and less development time. In this passage, a misleading hub possesses the information envelopes and moves it to next halfway hub on the last mark of the passage through a confidential channel, which will retransmit the information parcel commonly. Due to having better natural elements for centers in the wormhole network i.e., barely any leaps or less time, in relationship with data sent on commonplace courses, that is the reason course among source and objective is chosen through confidential channel. It regularly starts in two sections [14]. The aggressor hub, first and foremost, includes themselves in numerous ways and also, these misleading hubs the opening shot their naughty movement on the parcels they get. Because of this the worth of the affiliation will be hurt in different ways moreover, making jumble between the focuses, develops the traffic rate, above issues and the essential it will debilitate the battery utilization of the system[19]. It advances the information through off channel joins, so figuring out the misleading focus focuses in the structure is bothersome. One line definition for Wormhole will be that it can delay, drop, change and move pack to cloud focus with deluding suppositions.

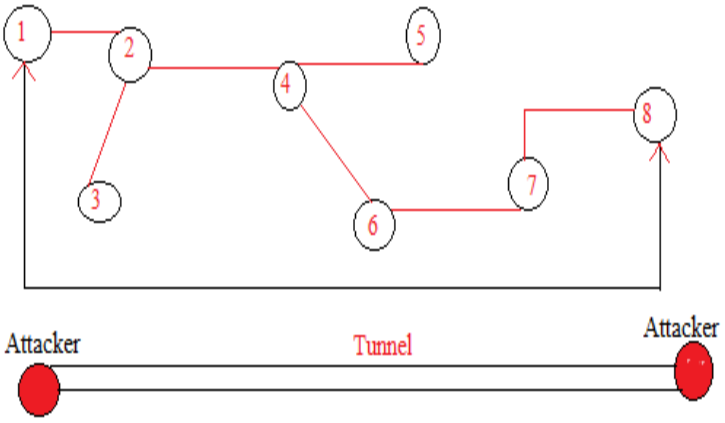

Figure 1: Wormhole Attack.

2.1 Out-of-band wormhole: It comes from external hubs. Misleading hubs can without much of a stretch make an association in the organization. Exceptional infrastructural arrangement is expected for correspondence between the hubs [22]. It gives quicker conveyance rates then, at that point, in-band wormhole assault**.**

2.2 In-band wormhole: Their no outer association is expected in the framework hubs. Likewise there is no requirement of equipment arrangement and steering conventions to convey information parcels starting with one hub then onto the next [16]. In the two types of assaults, the going after hubs are absent at exceptionally close to one another however appear to be the nearby nodes.

3. Literature Review

In this assessment paper [1], creator zeroed in on multi rate Delphi process for wormhole region, as regular Delphi plot doesn't work completely on factor cycle rate traffic in distant affiliation climate furthermore follows are not completely seen by it. As such, multi rate Delphi is utilized for flourishing redesign with three undeniable cases for example multi rate transmission, taking care of deferral and abutting process. That's what creator recommended in the event that these three circumstances are recognized cautiously, 90% of the identification part is overseen and refreshed in the organization. Creator hit on the point that none of the strategy can permit discovery and counteraction from assault at the same time for wellbeing and security. Creator additionally recommended that identification pace of any malevolent hub can be expanded utilizing such variant of plans which will straightforwardly build the PDR and great put calculate the framework by decreasing the postpone rates. In this [15], study and examination over different techniques for distinguishing and keeping from wormhole assault is been finished. Specialist executed a bounce count verification conspire for recognition and cryptography for counteraction instrument. The recommended technique requires no sort of equipment in it. In this system, toxic center can be finding out by using number of bobs and deferment of each and every center point present in the structure. Communicating hub can without much of a stretch ready to follow wormhole assaults. Using this acknowledgment methodology on multipath coordinating show, in case skip count is more than the typical edge limit, the way is malicious and it will be killed and relentless bad habit a versa. Resulting to recognizing misleading focus point cryptographic models were finished on the focuses in the relationship for security reason. Producer has mulled over that PDR and throughput part can be broadened or more issues can be controlled cleverly with close to no pursuing center point in the association. In [16], creator dealt with discovery and counteraction approaches of wormhole assault. Burrowing technique is been utilized for location and hash capability and advanced marks are utilized avoidance plans in the organization brought about by misleading hubs. Here, recognition strategy will give the specific area and current status of the malignant hubs. The proposed technique utilizes burrowing time estimation utilized by passage to notice the idea of the wormhole. It, first and foremost, will examine the time consumed by the passage to track down the assault and as indicated by that limit level will be dissected. After that assumption system will be applied on it. Producer expected that utilizing such techniques defer will be decreased; but lifetime and throughput will be reached out in the framework. Paper [17], presents a detail depiction about

trust spread out methodologies to find and settle the assaults in MANET. Here, producer utilized strong and honor based philosophy to isolate the dependable part and trustful focus focuses inside seeing wormhole assaults in the affiliation. Producer utilized base stations and greater part mining method to convey the confidence in the affiliation and additionally to track down the sensible area of focuses in the affiliation. They remained mindful of the base for information unwavering quality. Hence, that wormhole assault may not hurt the affiliation any longer. Finally, results showed that this strategy will prepared to work out the got packs, drop speed of the packages and sent groups on a reliable region gainfully. The delayed consequences of the proposed work show that the recommended plot is superior to the nonstop one. Like as of late referred to explore papers, here producer directs multi way controlling show with trust based plot and cryptographic models for divulgence and countering structure for wormhole assault in the affiliation. This plan chips away at various courses to figure out the best course or way in the organization. After consistent checking on courses, the way which will pass as far as possible will have a vindictive hub on it. In the event that the multipath steering in the organization gangs time more prominent than 0.5 edge limits, then, at that point, framework is reliable and bad habit a versa after cap cryptographic plan is applied on the organization for counteraction benefits. Specialist inferred that the organization climate is thoroughly relies upon limit esteem, the more noteworthy the edge esteem nature of administration will increment viceversa. Eventual outcomes of the situation show that Packet drop rate and defer can be limited, but throughput might benefit from outside input utilizing such multipath coordinating plans. In [14], confirmation based plot is utilized for dull opening assault recognizing verification and skip count for wormhole assault region. As it utilizes no area care, time sync and intend plan for any evaluation. The examination paper comparatively gives a short graph on bounce count revelation philosophy to track down joke community focuses in the affiliation. Examiner oversaw various advances including five controlling shows for example AODV, faint opening ODV, IDS-AODV, wormhole AODV and changed AODV. As per these strategies, each of the procedures have shown higher PDR and throughput rates in any case as count of focus focuses raises, delay likewise expands in the framework. At last, producer came on the outcomes that IDS - AODV has shown tremendous outcomes with lesser yield rates when separated from changed AODV thinking about the way that in AODV, as the count of focus will develop, it will accordingly raise the group transport degree and throughput in the affiliation. Be that as it may, it will raise the speed of postponement with expanding number of focuses. The help behind this, assuming focus point count gathers, traffic will develop which is the fundamental driver of crash in the climate for course age process obtaining higher delay at any rate utilizing IDS system with it gives striking outcomes. The paper [17], dealt with another procedure to find the wormhole assault in the framework utilizing further developed bunching strategy. It, right off the bat, manages bounce count and time sync technique which will really take a look at the presence and area of the vindictive hubs in the climate. Subsequently bunching procedure is applied all around the organization for appropriate anticipation of the organization. The entire organization is segmented into groups which will have individual Cluster Head and can ready to control the whole communities nearby for controlling development in MANET. Specialist saw that the proposed strategy can give a great deal of progress in PDR and throughput

factors because of innocuous climate arrangement as grouping method will give the best counteraction strategies to a protected organization arrangement. In paper [21], creator manages AOMDV steering convention with jump count and RTT (Round Trip Time) estimation for the tracking down the misleading hubs in the framework. AOMDV directing convention will assist with laying out another course in the organization, on the off chance that any adjoining hub is in the middle of between the steering systems. It will assist the organization with keeping up with and work out the legitimate jump count and RTT around the organization. The outcomes in the organization show that in the event that RTT is more prominent than ordinary course foundation, than vindictive hubs is available in the organization and bad habit a versa. That is the means by which bogus hub will be recognized for an enormous scope and framework can be made blunder free. At last, creator declared that an expanded throughput element will be shown utilizing this changed AOMDV.

4. Result

The wormhole assault is defer knowing it will manufacture the yield in the affiliation. The briefest way between sources to true depends upon the sway count and strategy number. Course which has less bounce count and most crazy arrangement number is best reasonable for information transmission from source to objective. The dangerous center point exits in the picked manner which could augment at any point concede in the environment. The deceptive center makes tunnel beginning with one end then onto the following which prompts increase concedes over the association. The edge based strategy is arranged in this assessment paper for the disclosure of false center points from the association. The typical not set in stone before data transmission in the association. The expected not set in stone from the association and center point which has more deferral than the typical deferral is separate as pernicious. The outcomes are broke down on boundaries like normal start to finish postponement and bundles conveyance proportion relates to various arrangements of versatile hubs. It is been seen that proposed system will find the malignant hubs proficiently and contrasted with different strategies.

Table 2: Simulation Parameters

Parameters	Values
Simulator	NS2-2.35
Area	700 * 700
Number of nodes	50
Antenna type	Omi-directional
Queue type	Priority queue
Queue length	50
Propagation model	Two ray

For this, we have taken 50 numbers of nodes, just to clarify the situations that what will happen to the network when we increase the number of nodes or what increases the load on the network. We will check the quality of service i.e. throughput, end to end delay and packet

delivery ratio with the increasing number of nodes that it may increase, decrease or stays constant with increasing number of nodes simultaneously.

Here, in the graph three colored lines are used, which indicates the functioning of the attack individually.

• **Blue line:** It defines the packet delivery rate before the entry of the attack in the network.

• **Red line**: It defines the packet delivery rate during the functioning of attack in network.

• **Green line**: It defines the packet delivery rate after the removal of the harmful attack present in the network.

In figure 3, graph is related to the 50 nodes setup for wormhole attack. After analysis, the 50 nodes setup environment does not decrease the packet delivery rate and throughput. As, it is on higher risk factor because we have increased the number of nodes in the network and automatically load will increased on the setup but this DTD detection and prevention scheme proves that it will not decrease the throughput and will also maintain or decrease the delay rate accordingly.

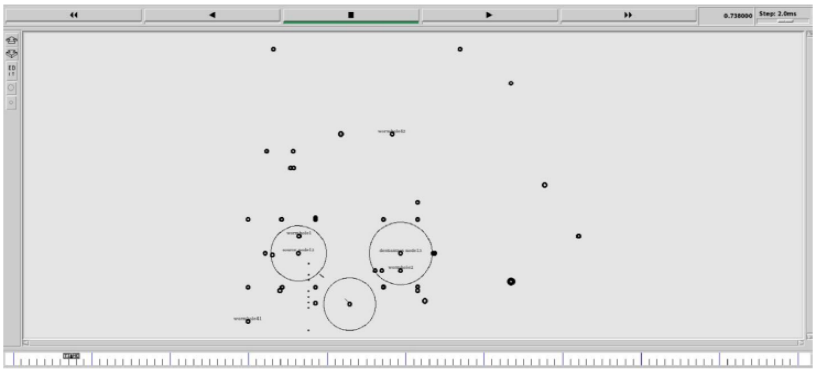

Figure 2: 50 nodes setup for Wormhole Attack Detection in the Network.

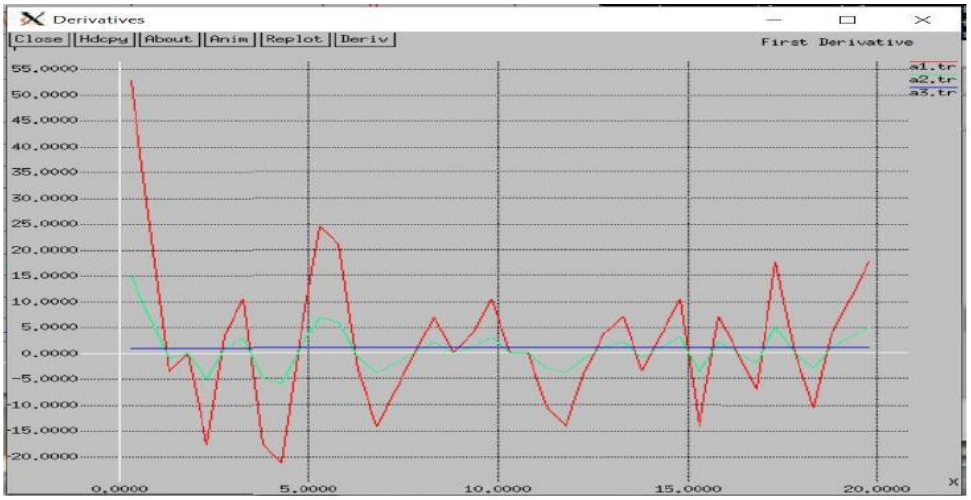

Figure 3: For 50 Nodes setup, Packet Transfer rate before (blue), during (red) and after (green) for Wormhole Attack.

In figure 4, average end to end delays for with and without wormhole attack present in the network is showcasing two color lines. One line is for attack (green) and another line for without attack (red). We can see in the graph that as number of nodes will increase delay will be increased in the network, if attacker nodes are present in the network and if attacking nodes are not present then red line is showing the constant delay rates in the network and hence proved that detection and prevention policy which we have chosen is working efficiently in the network. And with constant delay rates, Packet delivery rates also increases as we can see in figure 5, which is showing the packet delivery ratio for with and without wormhole attack in the environment. Here, in figure 5, blue line goes for without attack PDR and red line shows the with attack conditions. As we can see that as attacker's nodes are successfully removed packet delivery ratio is increased in the network and vice versa.

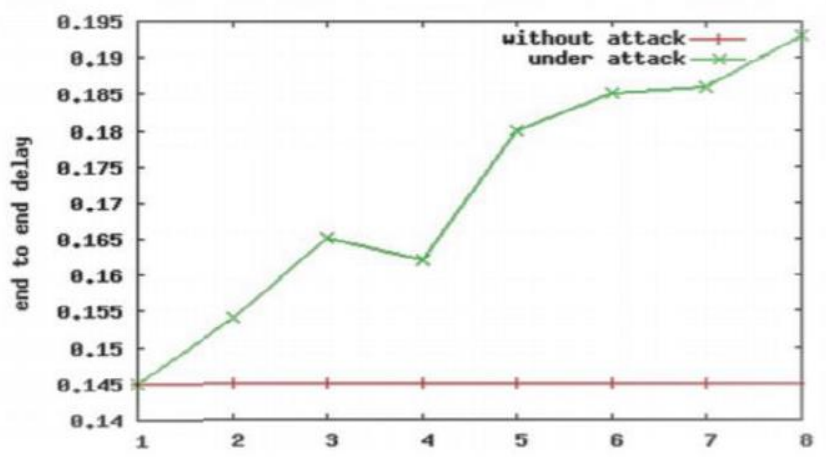

Figure 4: Average End to End Delay with and without wormhole attack in the Network

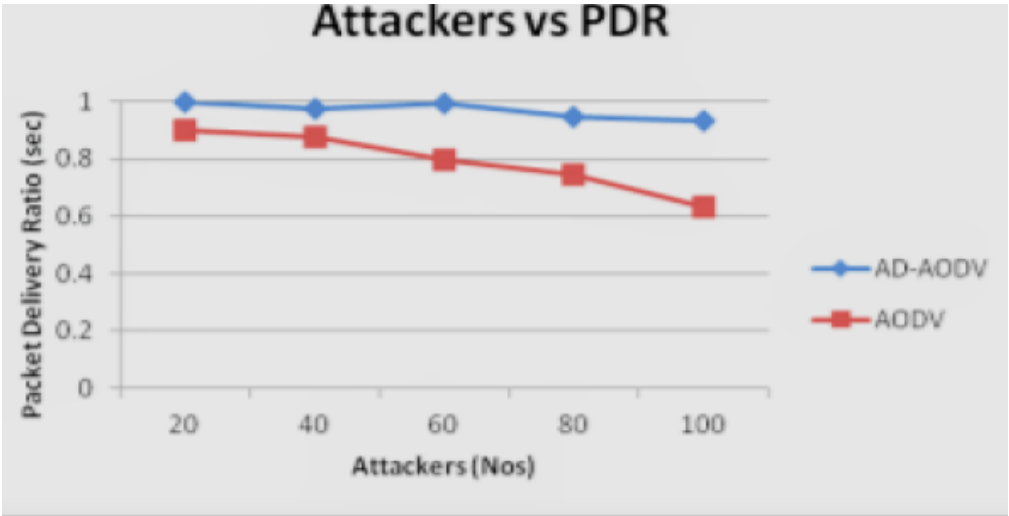

Figure 5: Packet Delivery Ratio with and without wormhole attack in the Network.

Conclusion

It is seen that the far off remarkably assigned frameworks are scattered sort of relationship in which sensor focus focuses can combine or leave the design as per them. No center controller is introduced in the far off uncommonly chosen frameworks. On account of the opportunity character of the framework success, heading finding and association quality are the chief issues related with this construction. A functioning sort of assault named wormhole impedance might be the explanation of the entering of assailant focuses in the framework and as a result of this surrender increment. In the introduced research, DTD conspire is used. For the confirmation of assailant sensor focus focuses, this plan shows less accuracy and colossal execution times. The normal and available methods are applied in NS2 and the age results portray progress in power use, all around, and bunch whipping.

References

1. Shruti Thapar, "A Review: Study about Routing Protocol of MANET", International Conference on "Smart Innovations for Society" (ICISC-2022) on 6-7 May 2022, in Scopus Proceedings.
2. Shruti Thapar and Sudhir Kumar Sharma, "An Integrated Approach for Detecting Wormhole and Jellyfish Attack in MANET", International Conference on Engineering & Design (ICED) 25-26 June-2021 ISBN: 978-81-954037-0-7, pp.51- 63.
3. Shruti Thapar and Sudhir Kumar Sharma, "Detection and Prevention Policies of Attack in MANET" Proceedings of International Conference on Innovative Advancement in Science and Technology (IAET 2020), India, https://dx.doi.org/10.2139/ssrn.3548382.
4. S.Thapar and S.K.Sharma, "Direct Trust-based Detection Algorithm for Preventing Jellyfish Attack in MANET", 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), IEEE, DOI: 10.1109/ICECA49313.2020.9297601, ISBN: 978-1-7281-6387-1, pp. 749-753, 2020.
5. Shruti Thapar and Sudhir Kumar Sharm, "Attack and Security Issues of Mobile Ad Hoc Networks", Proceeding of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM 2019), India, https://dx.doi.org/10.2139/ssrn.3356214.
6. International conference on role of computer science in the field of networking security and privacy "Survey report on Mobile AD-HOC Networks" (April'2013).
7. National conference on advances in wireless and optical communication on "Security Protocol and Sensor Network" (March'2012).
8. National conference on role of electronics and instrumentation engineering for rural development on "Under water Acoustic Network and Communication" (Feb'2012).
9. International conference on recent cognizance in wireless communication & image processing "A Review on Performance Evaluation of Routing Protocols in MANET" (December'2014), *PUBLISHED IN SPRINGER 2015 EDITION*.
10. Shruti Thapar and Sudhir Kumar Sharma, "Analysis of Isolation access of Wormhole Attack in Mobile Ad hoc Network using Delay Prediction Technique", International journal of Advanced Science and Technology (IJAST), ISSN: 2005-4238 IJAST, volume-29 issue-6, 2020, page no.- 9401-9411.

11. Shruti Thapar and Sudhir Kumar Sharma, "Study of Direct Trust Based Detection Algorithm for Prohibiting Jellyfish Attack in MANET", ILKOGRETIM Online, doi: 10.17051/ ilkoline.2021.04.234, volume 20 issue 4, 2021, page no. -2052-2057.

12. Shruti Thapar, M Venu Gopala Rao, Babita Jain, Rohan Sharma , "Research Article on Routing Protocols for MANET: A Review", International Journal of Early Childhood Special Education (INT-JECSE)DOI:10.9756/INTJECSE/V14I5.305 ISSN: 1308-5581 Vol 14, Issue 05 2022, pp 2939-2949.

13. Shruti Thapar, M Venu Gopala Rao, Babita Jain, Rajkumar Kaushik, "A Secure Routing for MANET using Internet of Things", International Journal of Early Childhood Special Education (INT-JECSE)DOI:10.9756/INTJECSE/V14I5.305 ISSN: 1308-5581 Vol 14, Issue 05 2022, pp. 2957-2965.

14. Shruti Thapar, M Venu Gopala Rao, Babita Jain, Rohan Sharma , "A Review on Routing Protocol of MANET with its Characteristics, Applications and Issues", International Journal of Early Childhood Special Education (INT-JECSE) DOI:10.9756/INTJECSE/V14I5.305 ISSN: 1308-5581 Vol 14, Issue 05 2022, pp. 2950-2956.

15. Shams Qazi, Raad Raad, Yi Mu and Willy Susilo ,"Multirate DelPHI to secure multirate ad hoc networks against wormhole attacks", Journal of Information Security and Applications 39 (2018) 31–40, 2018.

16. Mr.Shaubham N.Ghormare, Prof.Swati Sorte and Dr.S.S.Dorle," Detection and Prevention of Wormhole Attack inWiMAX Based Mobile Adhoc Network", International conference on Electronics, Communication and Aerospace Technology (ICECA 2018), ISBN: 978-1-5386-0965-1, IEEE 2018.

17. M. Anand and T. Sasikala," Efficient energy optimization in mobile ad hoc network (MANET) using better-quality AODV protocol", springer publications, doi.org/10.1007/s10586-018-1721-2, 2018.

18. Tu T. Vo, Ngoc T. Luong and Doan Hoang,'' MLAMAN: a novel multi-level authentication model and protocol for preventing wormhole attack in mobile ad hoc network", springer publication, doi.org/10.1007/s11276-018-1734-z, 2018.

19. Rubal Sagwal and A. K. Singh," A Power Efficient Solution to Counter Blackhole and Wormhole Attacks in MANET Multicast Routing", ICAICR, CCIS 956, doi.org/10.1007/978-981-13-3143-5_45, Springer Nature, 2019.

20. Kai Dong, Ding Zhu and A. Daniel Hill," Mechanism of wormholing and its optimal conditions: A fundamental explanation", Journal of Petroleum Science and Engineering 169-126–134,doi.org/10.1016/j.petrol.2018.05.060, Elsevier 2018.

21. Jegan Govindasamy and Samundiswary Punniakody," A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack",

Journal of Electrical Systems and Information Technology 5 (2018) 735–744, Elsevier 2018.

22. M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi and A. Mammeri." Graph-Based Wormhole Attack Detection in Mobile Ad hoc Networks (MANETs)", International Conference on Mobile and Secure Services (MobiSecServ).doi:10.1109/mobisecserv.2018.8311439, 2018.

23. Sayan Majumder and Prof. Dr. Debika Bhattacharyya," Mitigating Wormhole Attack in MANET Using Absolute Deviation Statistical Approach", 978-1-5386-4649-6/18/$31.00, IEEE 2018.

24. Anusha K & Sathiyamoorthy E," A new trust-based mechanism for detecting intrusions in MANET",dx.doi.org/10.1080/19393555.2017.1328544, Taylor & Francis 2018.

25. Roshani Verma, PROF. Roopesh Sharma and Upendra Singh," New Approach through Detection and Prevention of Wormhole Attack in MANET", International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 978-1-5090-5686-6/17, IEEE, 2017.

26. Shahram Jamali and Reza Fotohi," DAWA: Defending against wormhole attack in MANETs by using fuzzy logic and artificial immune system", DOI 10.1007/s11227-017-2075-x, Springer Science 2017.

27. Parvinder Kaur, Dalveer Kaur and Rajiv Mahajan," Simulation Based Comparative Study of Routing Protocols under Wormhole Attack in Manet", DOI 10.1007/s11277-017-4150-2, Springer 2017.