Global Scientific Review
A Peer Reviewed, Open Access, International Journal
www.scienticreview.com
Volume 7, September 2022 ISSN (E): 2795-4951

Improving The Performance of Ad-Hoc Networks

Haroon Rashid Hammood Al Dallal
Bachelor's degree, Department Engineering in Communication Techniques, Al-Furat Al-Awsat Technical University, Najaf, Iraq.
Master's degree, Department Infocommunication Technologies and Communication Systems, Saratov State Technical University, Saratov, Russia.
haroonra1994@gmail.com
Noor J. Mahdi
Ass.Lec.
Department of Civil Engineering, Al-Maaref University College, Ramadi, Iraq.
noor.jabbar@uoa.edu.iq

Abstract: Ad-hoc networks (A-h-N) are wireless networks of individuals for usually a short period of time. The use of mobile phones, laptops, and computers combined with network services has fuelled the use of A-h-N in the 21st century. In this global world, the demand for cost-effective and technically efficient Ad-hoc networks is rising rapidly. The review of literature clarifies how various factors largely affect the ad-hoc network's performance. Keeping in view the significance of Ad-hoc network performance, I have given a deep analysis of improving its performance in this study. The factors affecting the ad-hoc network's performance are challenging for technical experts, network companies, and individual users. My paper is of significance to all the stakeholders. The model approach is a precondition to improving the performance of an A-h-N. The use of malicious node detectors' ineffective devices is bound to disallow harmful nodes. The increase in signal strength is a factor preventing link failures. It is equally important to ensure minimum packet losses in an ad-hoc network. Hence, improving the performance of an ad-hoc network is the core idea of this study indeed.

Keywords: Ad-Hoc network, Malicious node detector, Signal strength, Packet loss, Link failure

1. Introduction

As a network of communication, an ad-hoc network formed temporarily without a fixed infrastructure [1]. This temporary nature makes it vulnerable to issues that include the security and performance-however not limited to, of an A-h-N [2]. The issue of the performance of ad-hoc networks has gathered a lot of attention in academia in recent years [3]. There are commendable efforts made by other research scholars to improve security concerns [4]. Sun et al., used an innovative method to enhance the security of A-h-N as a strategy. It was developed in a way to pave the way for a node to evaluate the efficiency or authenticity of other nodes. In the detection of bad nodes and enhancing the performance, the method worked well and good nodes were protected from the bad ones [5]. There is no iota of doubt that security improvements also result in efficient ad-hoc network communication.

Generally, the increasing globalization is triggering the use of ad-hoc networks as well as impacting its security [6]. The expansion of mobile markets has brought a revolutionary change commonly stated as Mobile A-h-N (MANET) in the 21st century.

Volume 7, September 2022 ISSN (E): 2795-4951

Mobile communication has narrowed the distance based on national boundaries. It knows no country, government, race, ethnicity, gender, and religion. There is almost uniform use of Mobile A-h-N across the world; from children to elders, everyone is equally connected with this expanding network [7]. Given the importance of Mobile ad-hoc networks besides other ad-hoc networks, the improvement in the performance of an Ad-Hoc network is indispensable.

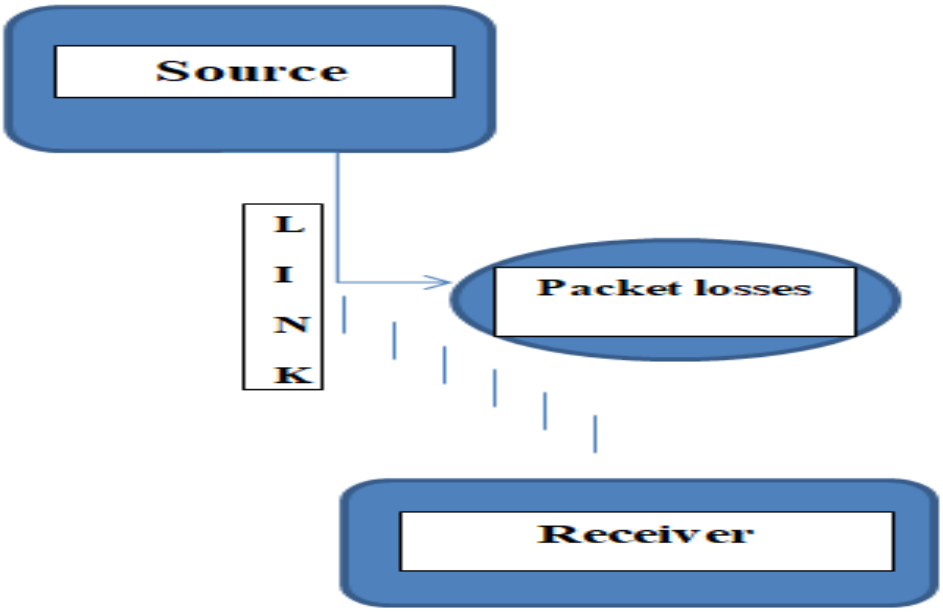
Technically, the performance of an Ad-Hoc network is highly dependent on multifarious variables [8]. Link layer, node mobility, signal strength, and device capacity are the major indicators of improvement in the performance of an Ad-Hoc network. The role of nodes is much worth sending and receiving the data [9]. A-h-Ns were negatively affected by a slight disruption in the nodes and their performance as well. The defective ad-hoc network becomes less cost-effective. The performance of an Ad-Hoc network is crucial to establishing strong communications and data sharing [10]. Therefore, this study is designed to improve the performance of A-h-Ns. The focus is much and much on the novelty of the work to come up with an effective model in this regard. Our idea in this paper is that reducing the rate of packet losses, strengthening signals, using technology-efficient devices, managing network size, and high node speed, and using malicious node detectors can significantly enhance the performance of an Ad-Hoc network.

2. Review of literature: Factors leading to improving the performance of A-h-Ns

The performance of ad-hoc networks can be understood in the context of the efficiency and effectiveness of the parameters. For this purpose, a review of existing literature on the parameters of ad-hoc networks is sought. The notable parameters of ad-hoc networks are packet processing, nodes mobility and security, network size, and signal strength [1]. Following related works offer a reasonable insight into these parameters were for A-h-Ns' better performance.

2.1Packet losses

The sharing of data from source to destination is done through packets in ad-hoc networks [11]. Individual networks receive and forward these to one another these packets for maintain the flow of messages. Packets are the segments of data sharing from one or more sources to other. For example, an email sent is divided into segments called packets. The device leads them to their destiny by making a number of bytes existing in the packets re-associated. It becomes difficult for a node to go ahead to route's next hop which get them out because if it does not work properly then Packets drop them off that the. In a shared medium, congestion is another reason for packet loss. It is when same time is the occasion that the channel is accessed by some nodes which are working; it happens for the second reason. The mess consequently cause s single node to capture the medium [12]. Unquestionably, the loss of packets has massive effect on the ad-hoc network's performance. Node mobility increases the prospect of link failures in ad-hoc networks. The routing layer receives this link-failure message whereby then manages to re-compute it to another destination. This relationship is illustrated in the following diagram;



Figure(1): The packet loss causes drop-out connection links from the source to a receiver.

2.2 Malicious nodes

A node is malicious when it denies or suspends the service to other nodes in a network [13]. The source and destination are subject to the nodes' normal functioning. Any deviation in the security of nodes is termed malicious nodes. The question may raise the reason behind a change of mode from normal to malicious. The answer lies in nodes. As it is movable and may join one or other networks, it makes it vulnerable. The malicious nodes are found to be affecting the performance of an A-h-N. A close examination of malicious nodes reveals that they are harmful to the functional ad-hoc network. Its effect is multidimensional that considerably impacts the response time of the network [14]. It is an increasing area of research to identify the poor performance of ad-hoc networks caused by various kinds of malicious nodes. The prominent of these types are false data injection, challenge collapsar, distributed denial of service, and other attacks troubling the ad-hoc networks [15]. Other malicious nodes are a drop of Packet, draining the battery, overflow of buffer, consumption of bandwidth, packets staled, break of link, tampering of messages, Denying from Sending Message, Fake Routing, Stealing Information, and Session Capturing, [16]. Regardless of type, malicious nodes intervene in the smooth functioning of an A-h-N. It reduces the likelihood that a message could deliver to its destination at an optimum time. These malicious nodes are not only responsible for delaying the message, but also carry huge potential risks to security and privacy in the worst-case scenario indeed.

2.3 Speed of Node and Size of Network

The node speed determines the frequency of data sharing each time. A simulation study focused on the factors caused or led to the functioning of A-h-N. They found in the number of traffic sources followed by node speed and network size had strongly impacted the performance of the ad-hoc network [17]. The free space model helps identify the role of node transmission and signal strength. This model predicts the

signal strength when there is an uninterrupted and clear line of a path between receiver and transmitter. Somewhere in this process, node speed affects the performance of an ad-hoc network. Similarly, the increase in size of network has to do with the functioning of an A-h-N. The larger the network size, the more interruptions to it [18]. Although large ad-hoc networks have become the necessity for the globalization of the mobile community, its negative effects cannot be ruled out. Perkin's study has shown that the large size of an ad-hoc network increases the pause time and frequency of node transmission. This leads to issues in routing and processing the flow of messages in an ad-hoc network.

2.4 Signal weakness

It is quite obvious in ad-hoc networks the nodes work through a medium of air. Unlike the medium of wire, an ad-hoc network requires signal reach to continue to function. In a study, the signal threshold model was drawn to illustrate the role of strengths in ad-hoc networks. According to it, a source initiates the packet and awaits the destination response. They denote it as A and B. However, the threshold of signals determines the connection. For example, if B is out of reach the threshold, then it forwards the packets to another C making possible the connection [19]. The strength of the signal is primarily dependent on the proximity of the nodes along with inhomogeneity of the magnetic field [20], the strength of the device, and general weather conditions as well. On top of that, mobile ad-hoc networks are among the most affected by signal strengths. They are portable ad-hoc networks that increase the issue nodes' mobility and ultimately packet losses. Signal weakness is one of the foremost predictors of the performance of ad-hoc networks [21].

3. Good performance of the A-h-N: considering the important factors

There is a variety of factors that influence the performance of ad-hoc networks as discussed above in detail. Mobile ad-hoc networks and laptops A-h-N are the fastest growing industry in the age of globalization. I have a model-like argument in this study extracted from the depth of literary analysis. I focus on the efficiency of nodes in relation to other factors. Nodes' speed is to improve the flow of data between and among sources and destinations. What reduces the speed and exchange of nodes is the malicious nodes [22]. A malicious node detector is when used minimizes the disruptions while maximizing the sharing and receiving of data in an ad-hoc network [23]. Developed the malicious nodes identification routing mechanism; AODV routing algorithms ensures the transmission of packets safe in the network [24]. They developed this experimental model on a vehicular ad-hoc network (VANET). Yet it can be expanded for other ad-hoc networks such as mobile ad-hoc networks. Some factors need to be considered while analyzing these kinds of ad-hoc networks; the battery of the device [25], the capacity of receivers and transmitters, and more importantly the reach of signals causing variation in nodes speed.

A. Use of Malicious Nodes Detector

There are differences of opinion to address the issue of malicious nodes. Pareek and Sharm recommend the use of MAC addresses to counter the Sybil attacks [26]. Sathya and Rathod are of the view an algorithm can not only detect the wormhole attacks in mobile ad-hoc networks but also it can recover wormhole attacks [27]. I have observed in my model that malicious nodes detector positively contributes to the performance

of ad-hoc networks. Malware is harmful to the nodes transferred from one to another in a network. The invasions of a malicious node not only slow the pace of data sharing but also completely suspend the functional capacity of the entire ad-hoc networks. Use of an effective malicious nodes detector improves the performance of ad-hoc networks in multifarious ways. In the early phase the malicious nodes detectors warn a system to prepare itself. It becomes hard for malicious nodes to negatively impact the performance of ad-hoc networks. The nodes speed and functioning remain intact from the malicious nodes. This way an ad-hoc network performs significantly. In the outcome, malicious nodes detectors save from any invasion of privacy the security of those connected in networks somewhere in the connection.

B. Minimizing packets loss in data exchange

The packet loss is a true indicator of the poor performance of an ad-hoc network. Rana. & Kumar concludes when nodes are under attack the AODV performance is a matter of grave concern. For network simulation, they set a menu value in their experimental design. The study has shown that packet drops were much more during node attacks than that during normal conditions. The ad-hoc networks (including mobile ad-hoc networks) are more prone to these attacks in ordinary situations than wired networks [28]. The malicious node attack is thus reducing the efficiency of packets. It causes a considerable packet loss [29]. In a study, a comparison was made between DBR and AODV. The performance of the former was observed better than the latter in packet dropped and packet delivery ratio. The DBR was also very effective in case of link failures than AODV. Eventually, it was concluded that failure of the route was associated with packet losses. As soon as route failure happens, it restarts from the beginning and makes the loss of packets unavoidable [30]. The route reestablishment's relationship with packet loss is yet another critical factor in maximizing packet loss.

My idea is that minimizing packet loss is a strong indicator to improve the performance of an ad-hoc network. Abdulsaheb. et al. used a clustering technique in the network to counter the routing traffic. What they did is splitting the networks into small pieces of clusters and their head. The small clusters were then developed into a clustering algorithm for node selection within each cluster. As a result, the desired outcomes were achieved in terms of packet delivery rate, minimizing routing traffic minimized, and ultimately packet loss was reduced to a desirable level [31]. These techniques work smoothly in even large network sizes [32]. I argue that packet losses can be minimized in manners like these renowned scholars have done so. Packet loss is an outcome of link failure. What I argue is that there should not be a large network size enough to allow the packet losses. The network size can be taken into while forming the clustering models for routing efficiency and routing establishments. Why I am emphasizing network size and network clusters is due to the fact of link failure. It is, therefore, necessary to condense a large number of individuals into segments that are close in distance but fast in packet sharing.

C. Signal strength and clustering networks

The ad-hoc networks are unexpectedly connected for short time [33]. The signal works as a medium to maintain the connection between sources and destination [34]. There is no denying the fact that signal strength paves the way to make better the functioning of an A-h-N. Routes in node discovery is impacted not only differences in

protocols but also by the signals affect its performance [2]. Dr. Reem undertook a study to analyze the impacts of signal strength over routing protocols in wireless networks. He recognized the importance of signal strength in two ways; one way it improves route optimization and the other is routing metrics [35]. Undoubtedly, signal strength enables routing to select nodes of quality, or what I should call them free from link failures. In another study, a practical approach was employed by the scholar. By the measurement of fluctuations in signal strength in neighboring nodes [36]. These nodes were not selected as route nodes due to the potential risk of link failures [37]. For this reason, I have placed a great emphasis on signal strengths. Signal strength enables the nodes' speed while eliminating the malicious nodes in an ad-hoc network. To the extent the strength of signal rises, it is positively followed by the good performance of A-h-N.

D. Models utility and other models

I have come up with a design that is not only feasible but also cost-effective to improve the performance of an ad-hoc network. My model idea is based on the arguments that malicious node detectors, minimum packet losses, link failure, and strong signals are reliable indicators for improving the performance of an ad-hoc network. In addition, sustained battery and device efficiency cannot be ruled out [38]. I have argued that all these are essential components to improving the performance of an ad-hoc network. This model can be utilized with the correspondence of other models. Trust models and probability-based models are paramount to making my idea realistic and fruitful. The algorithm models can make the aim of this study achievable. The use of ad-hoc networks is fuelling concerns about its efficiency and effectiveness[39]. The performance of ad-hoc networks is subject to multiple variables [40]. I have tried some of them the most critical and urgently needed to improve the performance of an ad-hoc network. Nevertheless, there is always a ground for future research studies and techniques to explore further innovations in this regard.

4. Conclusion

The improvement of an ad-hoc network is a matter of great value in wireless technology. The world has become a global village that is physically distanced but spiritually closed. The rising trend of ad-hoc networks has even eased the burdensome physical visits within the cities besides out-of-borders. The increasing demand for wireless communication and data sharing has underlined the importance of efficient ad-hoc networks. Therefore, I conclude the use of smart technology can significantly enhance the performance of an ad-hoc network. I suggest the use of malicious node detectors; for minimizing the harmful nodes in routing. For positive responses among the individual's only nodes of meaningful data be transmitted and received through the use of malicious node detectors. As link failures further diminish the performance of an ad-hoc network, strong signals can help to address the concern. Signal strength accelerates the speed of nodes besides retaining the connection in an ad-hoc network. I am highly convinced that we cannot make the ad-hoc network more efficient unless packet loss is tackled. I have given in this paper the idea that packet loss can be reduced to the desired level. The use of effective and speedy devices coupled with strong batteries blocks the ways leading to the loss of packets in an ad-hoc network. Hence, my paper is a blueprint for securing the performance and outcome of ad-hoc networks.

References

[1] R. Ramanathan and J. Redi, "A brief overview of ad hoc networks: challenges and directions," *IEEE Commun. Mag.*, vol. 40, no. 5, pp. 20–22, Apr. 2005, doi: 10.1109/MCOM.2002.1006968.

[2] C. E. Perkins, E. M. Royer, S. R. Das, and M. K. Marina, "Performance comparison of two on-demand routing protocols for ad hoc networks," *IEEE Pers. Commun.*, vol. 8, no. 1, pp. 16–28, Feb. 2001, doi: 10.1109/98.904895.

[3] J. Z. Sun, "Mobile ad hoc networking: An essential technology for pervasive computing," *2001 Int. Conf. Info-Tech Info-Net A Key to Better Life, ICII 2001 - Proc.*, vol. 3, pp. 316–321, 2001, doi: 10.1109/ICII.2001.983076.

[4] F. Klemm, Z. Ye, S. V. Krishnamurthy, and S. K. Tripathi, "Improving TCP performance in ad hoc networks using signal strength based link management," *Ad Hoc Networks*, vol. 3, no. 2, pp. 175–191, Mar. 2005, doi: 10.1016/J.ADHOC.2004.07.005.

[5] Y. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Trust modeling and evaluation in ad hoc networks," *GLOBECOM - IEEE Glob. Telecommun. Conf.*, vol. 3, pp. 1862–1867, 2005, doi: 10.1109/GLOCOM.2005.1577971.

[6] R. S. Chauhan, K. Taneja, R. Khanduja, V. Kamra, and R. Rattan, "Evolutionary Computation with Intelligent Systems," *Evol. Comput. with Intell. Syst.*, Feb. 2022, doi: 10.1201/9781003158165.

[7] S. Dixit, T. Ojanpera, R. van Nee, and R. Prasad, "Introduction to Globalization of Mobile and Wireless Communications: Today and in 2020," pp. 1–8, 2011, doi: 10.1007/978-94-007-0107-6_1.

[8] S. P. Weber, X. Yang, J. G. Andrews, and G. de Veciana, "Transmission capacity of wireless ad hoc networks with outage constraints," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4091–4102, Dec. 2005, doi: 10.1109/TIT.2005.858939.

[9] "Helen, D., & Arivazhagan, D. (2014). Applications, advantages and challenges of ad hoc networks. Journal of Academia and Industrial Research (JAIR), 2(8), 453-457. - Google Search." https://www.google.com/search?q=Helen%2C+D.%2C+%26+Arivazhagan%2C+D.+%282014%29.+Applications%2C+advantages+and+challenges+of+ad+hoc+networks.+Journal+of+Academia+and+Industrial+Research+%28JAIR%29%2C+2%288%29%2C+453-457.&sxsrf=ALiCzsZScswjpV9O3kB1Gx6pxinmVIquyA%3A1657375136375&ei=oInJYqmwFqOPlwTAyLmAAg&ved=0ahUKEwipgI3C--v4AhWjx4UKHUBkDiAQ4dUDCA4&uact=5&oq=Helen%2C+D.%2C+%26+Arivazhagan%2C+D.+%282014%29.+Applications%2C+advantages+and+challenges+of+ad+hoc+networks.+Journal+of+Academia+and+Industrial+Research+%28JAIR%29%2C+2%288%29%2C+453-457.&gs_lcp=Cgdnd3Mtd2l6EAMyBwgjEOoCECcyBwgjEOoCECcyBwgjEOoCECcyBwgjEOoCECcyBwgjEOoCECcyBwgjEOoCECcyBwgjEOoCECcyBwgjEOoCECcyBwgjEOoCECdKBAhBGAFKBAhGGABQ9QlYnxFg1RdoAnAAeACAAQCIAQCSAQCYAQCgAQGgAQKwAQrAAQE&sclient=gws-wiz (accessed Jul. 09, 2022).

[10] A. Nasipuri, R. Castañeda, and S. R. Das, "Performance of Multipath Routing for On-Demand Protocols in Mobile Ad Hoc Networks," *Mob. Networks Appl. 2001 64*, vol. 6, no. 4, pp. 339–349, Aug. 2001, doi: 10.1023/A:1011426611520.

[11] Y. C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure On-Demand Routing

Protocol for Ad Hoc Networks," *Wirel. Networks 2005 111*, vol. 11, no. 1, pp. 21–38, Jan. 2005, doi: 10.1007/S11276-004-4744-Y.

[12] S. Xu and T. Saadawi, "Performance evaluation of TCP algorithms in multi-hop wireless packet networks," *Wirel. Commun. Mob. Comput.*, vol. 2, no. 1, pp. 85–100, Feb. 2002, doi: 10.1002/WCM.35.

[13] "What is Malicious Node | IGI Global." https://www.igi-global.com/dictionary/a-novel-secure-routing-protocol-in-manet/33926 (accessed Jun. 23, 2022).

[14] M. Dhingra, S. C. Jain, and R. Singh Jadon, "Malicious node detection based on clustering techniques in network," *Mater. Today Proc.*, vol. 47, pp. 6676–6678, Jan. 2021, doi: 10.1016/J.MATPR.2021.05.111.

[15] Y. Lai *et al.*, "Identifying malicious nodes in wireless sensor networks based on correlation detection," *Comput. Secur.*, vol. 113, p. 102540, Feb. 2022, doi: 10.1016/J.COSE.2021.102540.

[16] R. Saini and M. Khari, "Defining Malicious Behavior of a Node and its Defensive Methods in Ad Hoc Network," *Int. J. Comput. Appl.*, vol. 20, no. 4, 2011.

[17] D. D. Perkins., H. D. Hughes., and C. B. Owen, "Factors Affecting the Performance of Ad Hoc Networks".

[18] RajaramanRajmohan, "Topology control and routing in ad hoc networks," *ACM SIGACT News*, vol. 33, no. 2, pp. 60–73, Jun. 2002, doi: 10.1145/564585.564602.

[19] B. Ramachandran and S. Shanmugavel, "Received signal strength-based cross-layer designs for mobile ad hoc networks," *IETE Tech. Rev. (Institution Electron. Telecommun. Eng. India)*, vol. 25, no. 4, pp. 192–200, Jul. 2008, doi: 10.4103/0256-4602.42811.

[20] I. I. Er and W. K. G. Seah, "Mobility-based d-hop clustering algorithm for mobile ad hoc networks," *2004 IEEE Wirel. Commun. Netw. Conf. WCNC 2004*, vol. 4, pp. 2359–2364, 2004, doi: 10.1109/WCNC.2004.1311457.

[21] I. F. Akyildiz, W. Y. Lee, and K. R. Chowdhury, "CRAHNs: Cognitive radio ad hoc networks," *Ad Hoc Networks*, vol. 7, no. 5, pp. 810–836, Jul. 2009, doi: 10.1016/J.ADHOC.2009.01.001.

[22] S. Desilva and R. V. Boppana, "Mitigating malicious control packet floods in ad hoc networks," *IEEE Wirel. Commun. Netw. Conf. WCNC*, vol. 4, pp. 2112–2117, 2005, doi: 10.1109/WCNC.2005.1424844.

[23] F. Kargl, A. Klenk, S. Schlott, and M. Weber, "Advanced detection of selfish or malicious nodes in ad hoc networks," *Lect. Notes Comput. Sci.*, vol. 3313, pp. 152–165, 2005, doi: 10.1007/978-3-540-30496-8_13/COVER/.

[24] S. Ahmed *et al.*, "Measuring the efficiency of health systems in Asia: a data envelopment analysis," *BMJ Open*, vol. 9, no. 3, p. e022155, Mar. 2019, doi: 10.1136/BMJOPEN-2018-022155.

[25] R. Zheng and R. Kravets, "On-demand power management for ad hoc networks," *Proc. - IEEE INFOCOM*, vol. 1, pp. 481–491, 2003, doi: 10.1109/INFCOM.2003.1208699.

[26] A. Pareek and M. Sharma, "Detection and Prevention of Sybil Attack in MANET using MAC Address," *IJCA*, vol. 122, no. 21, pp. 20–23, Jul. 2015, doi: 10.5120/21849-5167.

[27] D. Sorathiya, "Algorithm to Detect and Recover Wormhole Attack in MANETs," *Artic. Int. J. Comput. Appl.*, vol. 124, no. 14, pp. 975–8887, 2015, doi:

10.5120/ijca2015905754.
[28] R. Rana. and R. Kumar, "PERFORMANCE ANALYSIS OF AODV IN PRESENCE OF MALICIOUS NODE," *Acta Electron. Malaysia*, 2019.
[29] D. A. Maltz, J. Broch, J. Jetcheva, and D. B. Johnson, "Effects of on-demand behavior in routing protocols for multihop wireless ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 17, no. 8, pp. 1439–1453, Aug. 1999, doi: 10.1109/49.779925.
[30] P. K. Ga. and A. Unnikrishnana, "Improving the Routing Performance of Mobile Ad hoc Networks Using Domination Set," *ScienceDirect*, 2014.
[31] Abdulsaheb., G. O. I. K. Muttasher, N. Sulaiman., H. F. Zmezm., and Harith Zmezm, "Improving Ad Hoc Network Performance by using an Efficient Cluster Based Routing Algorithm," *Indian J. Sci. Technol.*, vol. 8, no. 30, 2015.
[32] A. D. Amis and R. Prakash, "Load-balancing clusters in wireless ad hoc networks," *Proc. - 3rd IEEE Symp. Appl. Syst. Softw. Eng. Technol.*, pp. 25–32, 2000, doi: 10.1109/ASSET.2000.888028.
[33] R. Roy Choudhury and N. H. Vaidya, "MAC-layer anycasting in ad hoc networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 1, pp. 75–80, Jan. 2004, doi: 10.1145/972374.972388.
[34] S. L. Wu, Y. C. Tseng, and J. P. Sheu, "Intelligent medium access for mobile ad hoc networks with busy tones and power control," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 9, pp. 1647–1657, Sep. 2000, doi: 10.1109/49.872953.
[35] D. R. J. Ismail, "The Impact of Signal Strength over Routing Protocols in Wireless Networks," *Int. J. Eng. Manag. Res.*, vol. 8, no. 4, pp. 126–130, 2018.
[36] M. Chatterjee, S. K. Das, and D. Turgut, "On-demand weighted clustering algorithm (WCA) for ad hoc networks," *Conf. Rec. / IEEE Glob. Telecommun. Conf.*, vol. 3, pp. 1697–1701, 2000, doi: 10.1109/GLOCOM.2000.891926.
[37] Y. Taj. and K. Faez, "Signal strength based reliability: A novel routing metric in MANETs," 2010.
[38] C. Funai, C. Tapparello, H. Ba, B. Karaoglu, and W. Heinzelman, "Extending volunteer computing through mobile ad hoc networking," *2014 IEEE Glob. Commun. Conf. GLOBECOM 2014*, pp. 32–38, Feb. 2014, doi: 10.1109/GLOCOM.2014.7036780.
[39] Q. Xue and A. Ganz, "Ad hoc QoS on-demand routing (AQOR) in mobile ad hoc networks," *J. Parallel Distrib. Comput.*, vol. 63, no. 2, pp. 154–165, Feb. 2003, doi: 10.1016/S0743-7315(02)00061-8.
[40] J. Kong and X. Hong, "ANODR," p. 291, 2003, doi: 10.1145/778415.778449.