Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
May 2024 5(5), 650–657

COMPARATIVE ANALYSIS OF EXISTING ALGORITHMS WITH A NEW APPROACH FOR ELIMINATE THE BLACKHOLE AND WORMHOLE ATTACK TO FIND THE BEST PATH FOR ROUTING

Prajeet Sharma[1], Pratima Gautam[2]

[1]Research Scholar, Rabindranath Tagore University Bhopal M.P
[2]Professor, Rabindranath Tagore University Bhopal M.P

Corresponding Author
Prajeet Sharma,
prajeetsharma09@gmail.com

DOI
10.29121/shodhkosh.v5.i5.2024.2106

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Effective routing algorithms are crucial for optimizing network communication in various domains, including telecommunications, computer networks, and transportation systems. This research paper proposes a novel routing algorithm and compares its performance with existing algorithms to identify the most efficient solution. By evaluating factors such as latency, throughput, scalability, and resource utilization, this study aims to provide insights into improving network routing for enhanced performance and reliability. These algorithms have go through the important role in networks and in suggesting the best path for data transmission. In this study, we propose a novel routing algorithm and conduct a comprehensive comparison with established algorithms to identify the best path for routing in various network scenarios with the removal of blackhole and wormhole attack. The proposed algorithm is designed to optimize path selection based on key metrics such as packet delivery ratio, end-to-end delay, throughput and robustness. To evaluate its performance, we implement the proposed algorithm alongside well-known routing algorithms, and prominent routing protocol such as AODV. In this research we found that it the packet delivery ratio and throughput become higher than this is the proof that the data packet has been follows the best path to the destination. Using a simulated environment, we generate diverse test cases representing different network topologies, traffic patterns, and failure scenarios. Through extensive experimentation, we collect and analyzed performance metrics for each algorithm, enabling a thorough comparison of their strengths and weaknesses. Our findings provide valuable insights into the effectiveness of the proposed algorithm relative to existing approaches. Research highlights its unique advantages and areas for improvement, offering valuable guidance for network engineers and researchers seeking optimal routing solutions. This study contributes to the ongoing evolution of routing algorithms, facilitating more efficient and reliable network communication in diverse environments.

Keywords: RREQ, RREP, AODV, Block hole, wormhole attack, ,SAODV, MSAODV.

1. INTRODUCTION

This work encompasses all the scenarios of the standard "AODV" protocol without any kind of attack. When the system functions according to its intended design, it operates normally. However, there is another situation where there are attacker nodes either it is the combination of the blackhole and wormhole attack or single blackhole, wormhole attack. In this justification, we apply our newly developed "AODV" algorithm to these nodes and compare the outcomes with the previous scenario. The proposed AODV method broadcast as same as the standard AODV protocol. However, our approach comes into action when nodes begin sending replays. [1]

The value is regarded as indicating a sudden or questionable rise in the series number that represents the paths involving the M-Nodes. The proposed approach aims to utilize the unique properties of a black hole and wormhole node. It suggests a technique where a S- node verifies the legitimacy of an intermediary node by examining the" RREP packet" when

How to cite this article (APA): Sharma, P., and Gautam, P. (2024). Comparative Analysis of Existing Algorithms with a New Approach for Eliminate the Blackhole and Wormhole Attack to Find the Best Path for Routing. *ShodhKosh: Journal of Visual and Performing Arts, 5*(5), 650–657. doi: 10.29121/shodhkosh.v5.i5.2024.2106

destination sequence number is high as compare to the threshold value then, it apply our proposed algorithms and eliminate the attacker node and finds the best route for routing the packet to the destination. [2].

1.1 STATEMENT OF THE RESEARCH PROBLEM.

Elimination of the attacker nodes from the network is the crucial task for the every algorithm and the most important task is to find the best route in the network and for the given increasing complexity and demands of modern networks, there is a pressing need to identify the best routing algorithm that can optimize network performance while considering factors such as latency, throughput, scalability, and resource utilization. This research aims to find the optimal routing algorithm by proposing a novel algorithm and comparing its performance with existing algorithms.[3]

1.2 OBJECTIVES OF THE STUDY.

1. Develop a novel routing algorithm that addresses the limitations of existing algorithms and improves overall network performance and also eliminate the attacker nodes from the network.
2. Evaluate the proposed algorithm's effectiveness in terms of latency, throughput, scalability, and resource utilization.

2. LITERATURE REVIEW

H.R. Sharma et al. [2] examined the impacts of Blackhole Attacks on the performance of MANETs using the Qualnet network simulator. The experimental findings demonstrate that the conventional “AODV” exhibits greater “throughput”, packet delivery rate, and end-to-end latency compared to Blackhole Attacks.

Sridhar Iyer et al. [5] using the NS2 network simulator to examine the effects of Blackhole Attacks on MANET. They conducted 100 simulations and quantified the packet loss in the system under two conditions: with and wanting Blackhole nodes.

Donatas Sumyla [6] employed the NS3 network simulator to build a network scenario consisting of 25 nodes, which were subjected to attacks from 0, 1, 3, and 5 Blackhole nodes. The researchers conducted a comparison and assessment of both normal and attack situations, focusing on performance measures such as end-to-end latency, packet loss rate, and “throughput”. The investigational results indicate that as the amount of Blackhole nodes increases, the system packet loss rate rises, the end-to-end latency remains relatively stable, and the “throughput” falls.

Panagiotis et al. [9] suggested that when an S- node receives an” RREP packet” with a destination sequence number that is immense than the source sequence number by more than the assumed Arbt, it will rebroadcast the “RREQ packet”. At this time the sequence number received by the reply message is set as destination sequence number in the next broadcast. now if this time reply from same node's packet contains unusually high destination sequence number, then the path is eliminated from the trusted routes.

Johnson et al. [10] may go through all possible attacks which are against “Ad hoc On-Demand Distance Vector” protocol. They provided a comprehensive summary of each attack that might potentially disrupt the functioning of this protocol. Specifically, their investigation has been on assaults that specifically aim to disrupt the routing flow, including flooding, black hole, wormholes, and rushing attacks.

Muhannad Tahboush and Mary Agoyi [15] have proposed a hybrid algorithm to detect wormhole attack and name it as HWAD (hybrid wormhole attack detection) algorithm. The algorithm is capable to detect both type of worm hole attack i.e in band and out of band worm hole attack by taking the parameters like round trip time based on hup count and PDR.

Mr. Aditya Bhawsar and Dr. Yogadhar Pandey [16] have presented a technique to identify and mitigate warm hole attacks using the “AODV” protocol, which relies on trust calculation. Yulong Fu also contributed to this work.

3. PROCEDURE FOR PROPOSED ALGORITHM

3.1 SAODV (SECURE AODV) PROTOCOL: - The initial detection approach, known as "Detective, “AODV” based on Maximum Sequence Number" (D”AODV”_MSN), relies on the detection of attacks constructed on series numbers. The second detection approach, known as "Detective, “AODV” based on Neighbor Awareness Count" (D”AODV”_NAC), relies on the process of neighbor awareness counting. The third detection approach, known as "Detective, “AODV” based on Trusted Path" (D”AODV”_TP), primarily relies on the development of a trusted path [17]. The combine approach for these three are named as secure adhoc distance vector protocol (SAODV Protocol.) This is used for Blackhole attack detection and elimination of the attacker node.

3.2 MSAODV (MODIFY SECURE AODV) PROTOCOL -: The initial identification technique, known as " Identification, “AODV” based on Maximum Sequence Number" (I”AODV”_MSN), relies on the detection and enhancement of attacks based on sequence numbers [18]. The second identification strategy, known as " Identification, “AODV” based on neighbor Awareness Count" (I”AODV”_NAC), relies on the counting of neighbors awareness. The third preventative strategy, known as " Identification, “AODV” based on Trusted Path" (I”AODV”_TP), primarily relies on establishing a trustworthy path. If a particular delivery ratio is identified, a choice will be made to manage the trusted path. The following notation is consistent with the one listed in section [44]. Modified Secure AODV Protocol (MS”AODV”) will be suggested as the collaboration of these three methods.

3.3 CALCULATION OF THE THRESHOLD VALUE

Step I - The Mobile “ad-hoc network” has been established and the S-node is prepared to transmit data to the destination.

Step II - The S- node intends to communicate data to the End Node. To fulfill this requirement, the S- node should implement the “AODV” protocol. The “AODV” protocol operates by broadcasting the route discovery or route request message to all nodes in the system to locate the shortest and most optimal path.

Step III- the S- node begins to receive replay packets from other nodes in the system. These packets provide information about the destination path. The replay packet, also known as the replay message (RREP), primarily includes the sequence number and hop count. A higher sequence number indicates a more recent message, while a lower hop count indicates the quickest route to the destination. The sender collects RREP for the specified time (t).

Step IV, the S- node calculates the “threshold value” (T) by summing all the sequence numbers (seqn) or the parameter which algo wants to calculate the value for the respective method, received from distinct RREP messages and dividing the result by the number of RREP messages (n). Assign the value of i to the total count of RREP messages received by the S- node.

Step V - Next, compare the ”RREP packet” by considering the greatest sequence number and the lowest hop count with the specified “threshold value” (T). If the value of the sequence number (seqi) exceeds the “threshold value” (T)

Step VI - Next, eliminate the RREP and remove the RREP node from the routing table, designating it as a suspicious node. Now, subtract one from the value. Repeat Step V. During this process, if the sequence number (seqi) is less than the “threshold value” (T).

Step VII - After reception of the reply then acknowledge is done” with sequence number 'seqi' and start the transmission of data from this node.

Step VIII – Terminate the operation upon successful completion of data transmission.

A Black hole and wormhole node strive to present themselves as the most advantageous next hop node for the S- node to reach the End Node. The mechanism operates by responding with an ”RREP packet” containing inaccurate data regarding the lowest number of hops and the highest sequence number. To identify the freshness of the route it will find the highest sequence number and hup count represents the nodes in between sender and receiver. Therefore, in this approach, we assume that the attacker node would increment the sequence number in the “RREQ packet” by a maximum value of 100 when responding.

4. EXPERIMENTAL AND RESULTS FOR MULTIPLE BLACK HOLE AND WORMHOLE ATTACKS

4.1 COMPARISON OF AVERAGE “THROUGHPUT

Table 1. Comparison of Average “Throughput” Kilobits Per Second (Kbps)”

Protocol	Average “throughput”
“AODV”	1185.49
“Wormhole and black hole”, “AODV”	187.98
“Proposed algorithm (SAODV, MSAODV)”	199.91
“Proposed algorithm” compare with attack “AODV” (%)	6.35% (improved)

This study shows a comparison of “AODV”, “wormhole and black hole” “AODV”, and “proposed algorithm’s” protocols based on the average throughput, which serves as solution. The “proposed algorithm (SAODV, MSAODV)” demonstrates a 6.35% improvement compared to “wormhole and black hole” “AODV”, and a higher performance than regular “AODV”.

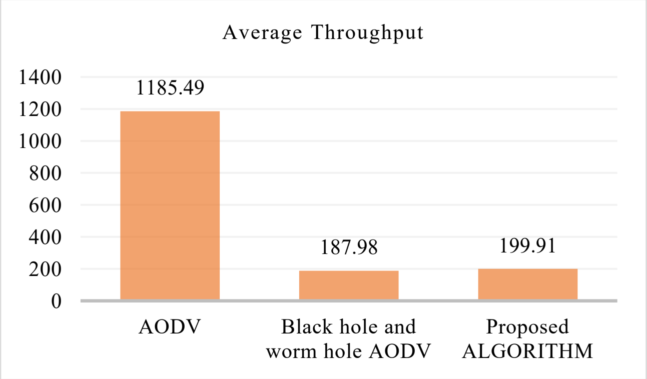

Figure 1: Displays the average “throughput” in kilobits per second (kbps).

This study shows a comparison of “AODV”, “wormhole and black hole” “AODV”, and “proposed algorithm’s” protocols based on the average throughput, which serves as solution. The “proposed algorithm (SAODV, MSAODV)” demonstrates a 6.35% improvement compared to “wormhole and black hole” “AODV”, and a higher performance than regular “AODV”.

4.2 AVERAGE END-TO-END LATENCY

Table 2 Displays the average end-to-end latency, measured in milliseconds

Protocol	End to End delay (MS)
“AODV”	478.61
“Wormhole and black hole” “AODV”	631.02
“Proposed algorithms”	595.10
Proposed Algo. compare with attack “AODV” (%)	5.69 % (reduced)

This study shows a comparison of “AODV”, “wormhole and black hole” “AODV”, and “proposed algorithm’s” protocols based on the average end-to-end latency, which serves as solution. The “proposed algorithm (SAODV, MSAODV)” demonstrates a 5.65% improvement compared to “wormhole and black hole” “AODV”, and a higher performance than regular “AODV”. All the combine results are of average of the data

5. PERFORMANCE EVALUATION

To validate the given technique, a sequence of simulations was conducted using NS-2. The performance of the proposed method is evaluated by comparing it with the normal AODV with SAODV and MSAODV protocols, specifically in the presence of “wormhole and black hole” nodes. This comparison is based on 100 simulations conducted on the NS-2 platform. Additionally, the “simulation” settings are modified based on the number of nodes in the system. The experimental parameter is “throughput” and “packet delivery ratio”. Only a single pair of source and End Nodes is evaluated throughout the series of simulations [10]. The simulations are conducted on two distinct network setups as outlined below:

- The system consists of a variable number of M-Nodes ranging from 10 to 50, with a permanent presence of 5 black hole and worm hole nodes.
- With varying the number of black hole and worm hole nodes from 1 to 10 while M-Nodes are fixed at 30

The findings given are derived from the average value of the fluctuating data associated with the performance indicators gained through simulations. The fluctuations in the data following each “simulation” are a result of the stochastic movement of the nodes inside the system and the ever-changing network structure.

Table 3 Presents the simulation parameters.

Parameters	Details
Simulation Dimension	500*500
Simulation Duration	100 second
Node density	10*15 nodes

“Malicious node”	1to 10 “wormhole and black hole” nodes
Movement/ Position	Random
“Routing protocol”	“AODV”, “SAODV”, “MSAODV”
MAC	MAC 802 11 Ext (IEEE 802.11p)
PHY	PHY Wireless 802 11 Ext (IEEE 802.11p)
Propagation Model	Two Ray Ground
Antenna Type	Omni directional
Transport Layer	UDP

5.1 THROUGHPUT

Throughput is calculated in the all three scenarios like with normal AODV with attack, SAODV with attack and MSAODV with Attack

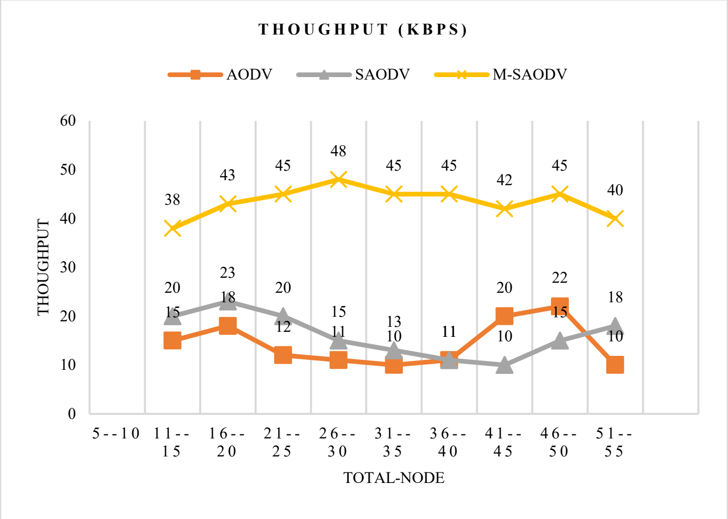

Figure 2 Throughput execution in five wormhole and black hole nodes present.

Figure 2 depicts the system’s “throughput” execution when there are 5 black hole and worm hole nodes consistently present in a network with a fluctuating number of M-Nodes. Given that the number of black hole and worm hole nodes remains constant in this set of simulations, it appears that the “throughput” is growing as the overall number of M-Nodes grows. Nevertheless, when the quantity of nodes grows, there is a threshold at which the “throughput” achieves its maximum capacity and then begins to decline. The suggested approach (“SAODV” & “MSAODV”) consistently outperforms the existing techniques in all scenarios.

5.2 PACKET DELIVERY RATIO– Packet Delivery Ratio is calculated in the all three scenario like with normal AODV with attack, SAODV with attack and MSAODV with Attack.

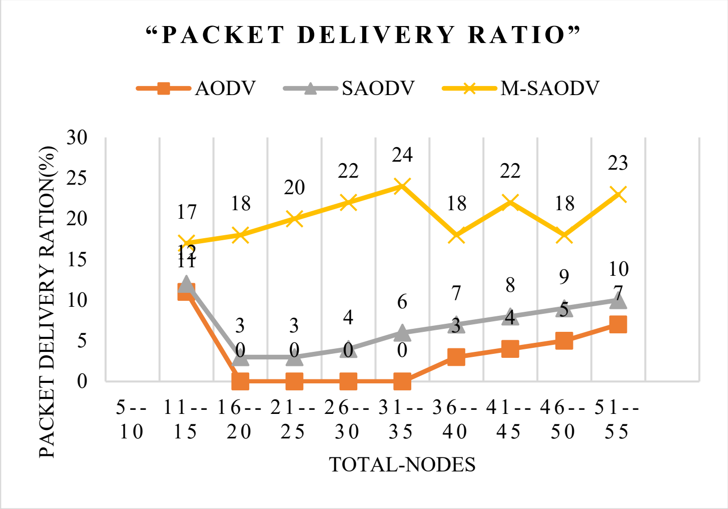

Figure 3 illustrates the Probability of Detection and Ranging (PDR) in the presence of five nodes that are either Black holes or worm holes.

According to Figure 3 shows that, when the network participating nodes has to be increases so it will effect the packet delivery ratio, means PDR is increases Additionally, the suggested method ("SAODV" & "MSAODV") shows higher performance in terms of results. Where our suggest algorithm MSAODV gives higher result.

6. COMPARATIVE ANALYSIS OF VARIOUS TECHNIQUES

The term "ADHOC" describes a class of multi-hop networks in which each node has a wireless transceiver device rather than a cable one. Military operations, disaster relief, commercial enterprises, healthcare, and personal area networks are just a few of the industries that use "ADHOC" networks. The technology of network emerged from battlefield communication networks and is mostly used in military command operations and tactical battlefield communication networks [12]. After testing all the perameters with the simple AODV protocol, AODV protocol with attack and proposed algorithm, Research found that all the results of proposed algorithm are satisfactory and now its time to compare the proposed work with the various existing algorithms, for this we have to summarised all the result of different existing algorithms in the form of average. Because it is hard to compare all together separately.

6.1 Investigational Assessment and Comparison of previous algorithms on "packet delivery ratio"

In Table 4, the "packet delivery ratio" of the "AODV" protocol is presented in relation to the "wormhole and black hole" assault utilizing the current projected technique, the suggested strategy, and the "previous algorithm." When compared to an existing technique, the proposed method shows a greater PDR in both attack scenarios.

Table 4 : Comparison of PDR

Simulation Time	Normal AODV with attack	Proposed algorithm	Previous algo	Proposed alg.-related with Normal AODV with attack (%)	Previous algo with. Normal AODV with attack (%)
200	92.58	99.94	95.15	7.95	2.78
400	87.05	99.97	97.57	14.84	12.09
600	86.68	99.98	98.39	15.34	13.51
800	86.85	100	98.79	15.14	13.75
1000	86.83	100	99.03	15.17	14.05
Average:				13.69% (increased)	11.23% (increased)

6.2 EXPERIMENTAL ANALYSIS, COMPARISON, AND Discussion ON "Throughput"

The "throughput" results of the "AODV" protocol utilizing the current Normal AODV with attack, the proposed method, and the previous technique for the "wormhole and black hole" attack are shown in Table 5. The "throughput" of the proposed approach for both attacks is similar to that of the current algorithm. The outcomes demonstrate that the "proposed algorithm" performs less well than the existing method. The system's dynamic structure and the node's mobility are blamed for the "throughput" decrease. PDR, or "packet delivery ratio," showed excellent performance for both approaches. Throughput (kbps) is represented graphically by a graph utilizing the numerical values from the table.

Table 5: Comparison of "Throughput" (Kbps)

Simulation Time	Normal AODV with attack	Proposed algorithm	Previous algo	Proposed alg.-related with Normal AODV with attack (%)	Previous algo with. Normal AODV with attack (%)
200	1431.64	1627.21	1141.07	13.66	29.88
400	3542.17	3530.64	2306.12	0.33	34.68
600	5583.17	5435.92	3464.94	2.64	36.26
800	8531.23	7341.15	4622.87	13.95	37.03
1000	11474.6	9247.71	5780.58	19.41	37.49
Average				**10% (reduced)**	**35% (reduced)**

For varying "simulation" timeframes, the three scenarios' "throughput" (kbps) was measured. The table and analysis indicates that, under the defined "simulation" settings, the "throughput" of the suggested technique for both attacks is either slightly lower or similar to that of the suggested approach for a length of less than 1000 seconds. The suggested method's performance for both assaults become more similar to the current strategy as the "simulation" length increases. The statistical analysis of "throughput" shows that the recommended strategy, on average, reduced the "throughput" by 10% in comparison to the previous methodology as the "simulation" time increased in the system. Taking into account "wormhole and black hole" assaults, the recommended approach has an average "throughput" loss of 35% when compared to the standard case.

7. CONCLUSION

The Proposed model covers the examination of a security issue named “wormhole and black hole” in “ADHOC”s and examines its influence on the system. Also, the existing solutions to the issue are researched, assessed, and based on that a new method is presented. The suggested approach is basic and can perform well in contrast to the traditional techniques. The validity of the suggested technique is also confirmed by network “simulation” The Existing model handles effectively for the finding and avoidance of blackhole and “wormhole attack” in Mobile “ADHOC” network. The system out to be made safe against numerous threats for sustaining data integrity that are obvious. It was found that the performance of the system is improved by the implemented technique which produces better outputs.

The Existing effort is greater to the existing work. In this suggested study, the tool applied for “simulation” is NS-2, which offers a better analysis of the task. It may be stated that utilizing the provided approach the “throughput” and container dip ratio increased. The algorithm priorities security as several of the primary factors to be looked upon. When compared with the scenario, loss ratio is lessened when algorithm was not utilized. How the effort has been done to beat the show of assault is the proof of “simulation” results? First the analysis is summarized and then it may be employed for attack mitigation. The “simulation” results reveal that the suggested technique has good accuracy in categorizing and predicting dangerous nodes in the system. In this research we found that it the packet delivery ratio and throughput become higher then this is the proof that the data packet has been follows the best path to the destination.

CONFLICT OF INTERESTS

None

ACKNOWLEDGMENTS

None

REFERENCES

S. Zeadally E. Yaprak1 Y. Li X. Che , “A Survey of Network Performance Tools For Computer Networks Classes” , Division of Engineering Technology, 2001

Asha Ambaikar, H.R. Sharma, V. K. Mohabey , “ Improved AODV for Solving Link Failure In Manet” , International Journal of Scientific & Engineering Research, Volume 3, Issue 10, October-2012 1 ISSN 2229-5518 2012

Sunil Kumar and Pankaj Negi , “A Link Failure Solution in Mobile Adhoc Network through Backward AODV (B-AODV)”, IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011 ISSN (Online): 2230-7893, 2011

Ravindra .E, VinayaDatt V Kohir and V. D Mytri , “A Local Route Repair Algorithm Based On Link Failure Prediction In Mobile Adhoc Network”, World Journal of Science and Technology 2011, 1(8): 64-67 ISSN: 2231 –2587, 2011

Srinath Perur, Abhilash P. and Sridhar Iyer , “Router Handoff: A Preemptive Route Repair Strategy for AODV” IEEE, 2003

Donatas Sumyla, “ Mobile Adhoc Networks” , IEEE Personal Communications Magazine, April 2003, pp. 46-55

Charles, E.P., Elizabeth, M.R.: Ad hoc On-Demand Distance Vector Routing. In: Proc. of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, pp. 90–100 (1999)

Refik, M., Pietro, M.: Security in ad hoc networks. In: Conti, M., Giordano, S., Gregori, E., Olariu, S. (eds.) PWC 2003. LNCS, vol. 2775, pp. 756–775. Springer, Heidelberg (2003)

Panagiotis, P., Zygmunt, J.H.: Secure Routing for Mobile Ad hoc Networks. In: SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX (2002)

Johnson, D., Maltz, D.: Dynamic source routing in ad hoc wireless networks. In: Imielinski, T., Korth, H. (eds.) Mobile computing. Kluwer Academic Publ., Dordrecht (1996)

M.F. Khan, K.-L.A. Yau, Route Selection in 5G-based Flying Ad-hoc Networks using Reinforcement Learning, in: Int. Conf. on Control Sys., Comp. and Eng., ICCSCE, 2020, pp. 23–28.

Y. Wang, Y. Tang, BRLR: A Routing Strategy for MANET Based on Reinforcement Learning, in: 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom, 2021, pp. 1412–1417.

Tsvetan Marinov and Borislava Petkova, "Comparative Analysis of AODV and MTP Routing Protocols in VANET", 2023 58th International Scientific Conference on Information Communication and Energy Systems and Technologies (ICEST) Nis Serbia, 29 June 2023 – 01 July 2024

Salam, T. and Hossen, M., 2020. Performance analysis on homogeneous LEACH and EAMMH protocols in wireless sensor network. Wireless Personal Communications, 113(1), pp.189-222.

Muhannad Tahboush 1 And Mary Agoyi "A Hybrid Wormhole Attack Detection In Mobile Ad-Hoc Network (MANET) " January 11, 2021, Date Of Publication January 13, 2021 Digital Object Identifier 10.1109/ACCESS.2021.3051491

Aditya Bhawsar; Yogadhar Pandey; Upendra Singh" Detection And Prevention Of Wormhole Attack Using The Trust-Based Routing System", IEEE Electronics And Sustainable Communication Systems (ICESC), 2020 International Conference.

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.

Sudhir Kumar Sharma And Shruti Thapar , "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.