IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Manet Swamping And Blackhole Attack Moderation Using Machine Learning And A Protection-Based AODV Protocol

[1]R.Sivaranjani,[2]Dr.R.Shankar,[3]Dr.S.Duraisamy

[1]Research Scholar, [2]Associate Professor, [3]Assisstant Professor
[1]Department of Computer Science,
[1]Chikkanna Government Arts College ,Tirupur, India

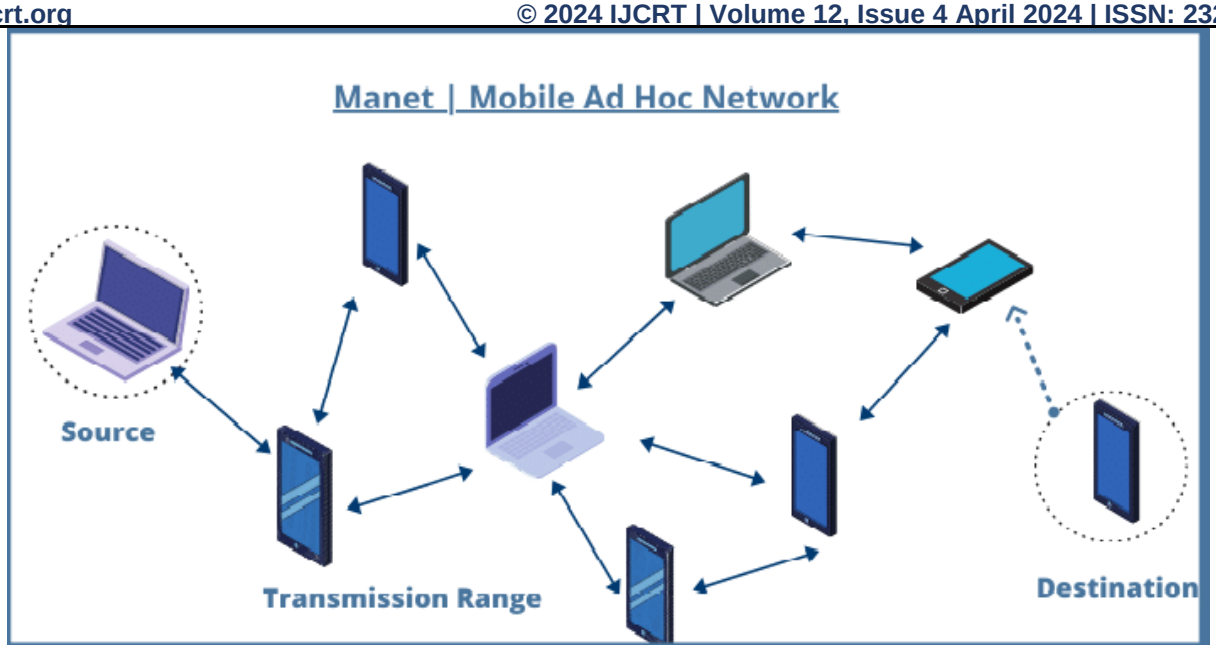
ABSTRACT

Mobile adhoc network (MANET) are one of the fastest growing areas of research.They are an attractive technology for many applications such as rescue and tactical operations,due to the flexibility provided by their dynamic infrastructure.In this paper, we provide Machine Learning approach which is used to identify the black-hole attack in manet.we are using simulator for different parameters which is delay routing overhead and packet loss ratio.

Keyword: Manet, AODV, Machine Learning

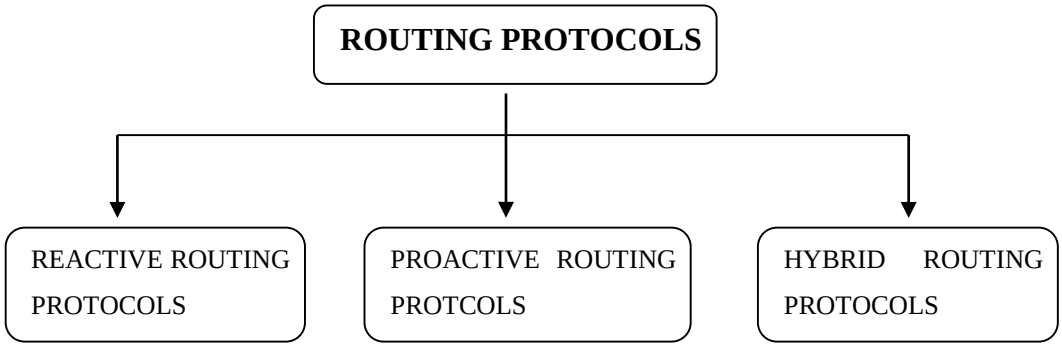
INTRODUCTION

An "infrastructure less network" (MANET) is a new, developing technology that lets users to interact without any physical infrastructure, regardless of where they are in the world (1).An ad-hoc network is adaptable and self-organizing. Devices in mobile ad hoc networks should be able to recognize other devices and set up properly to allow for communication and the exchange of data and services. Ad hoc networking enables simple device addition and removal from the network as well as connection maintenance for the devices.A MANET is typically utilized in locations where a fixed infrastructure cannot be established for a variety of reasons, such as emergency sites, conflict zones, and disaster areas. All MANET hosts may be put in vehicles, troops, ships, buses, airplanes, and emergency response teams to create temporary networks because they are all transportable (2).



1.ROUTING PROTOCOLS

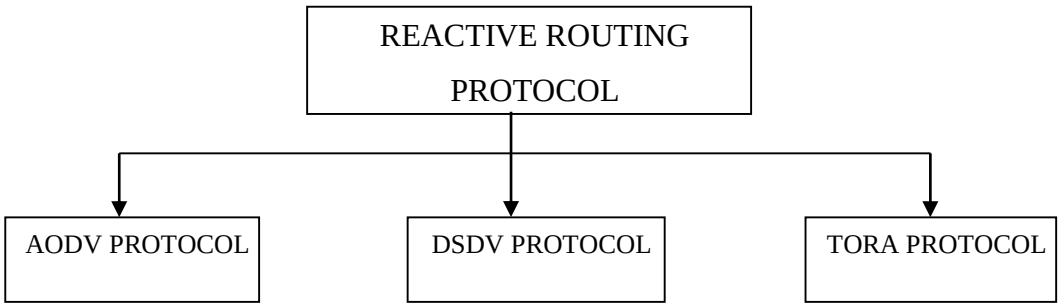
Due to the unique qualities that this network demands, the routing protocol is crucial in the design of MANETs.The path between the source and the destination is established by the routing protocols. Additionally, it is in charge of preserving the route between two nodes till the conversation is finished (3). When constructing a route, a node can face significant delays, and a broken link might force the identification of a new route. As the network grows, these additional delays and bandwidth use lead to increased network congestion (4).



1.1 REACTIVE ROUTING PROTOCOLS

The two types of reactive protocols are source routing and hop-by-hoprouting.Each data packet in source routed on-demand protocols carries the whole source to destination address. As a result, each intermediary node

transmits these packets in accordance with the data stored in each packet's header. This indicates that in order to transfer the packet to its destination,the intermediate nodes are not required to keep accurate routing informationfor each active route (4).



1.2 Ad-hoc On-demand Distance Vector (AODV) PROTOCOL

Reactive or on-demand routing protocols include AODV (Ad-hoc On-demand Distance Vector). Despite not maintaining all of the network's routes, it offers quick and effective.It allows communication between nodes with a minimum amount of control overhead via route establishment or discovery as necessary.Data packets are not subject to any additional overhead becauseAODV does not employ source routing. The AODV algorithm's key and crucial steps are as follows:**route development and maintenance** (3).Being flexible to extremely dynamic networks is an advantage of AODV. When constructing a route, a node can face significant delays, and a broken link might force the identification of a new route. As the network grows, these additional delays and bandwidth use lead to increased network congestion (4).

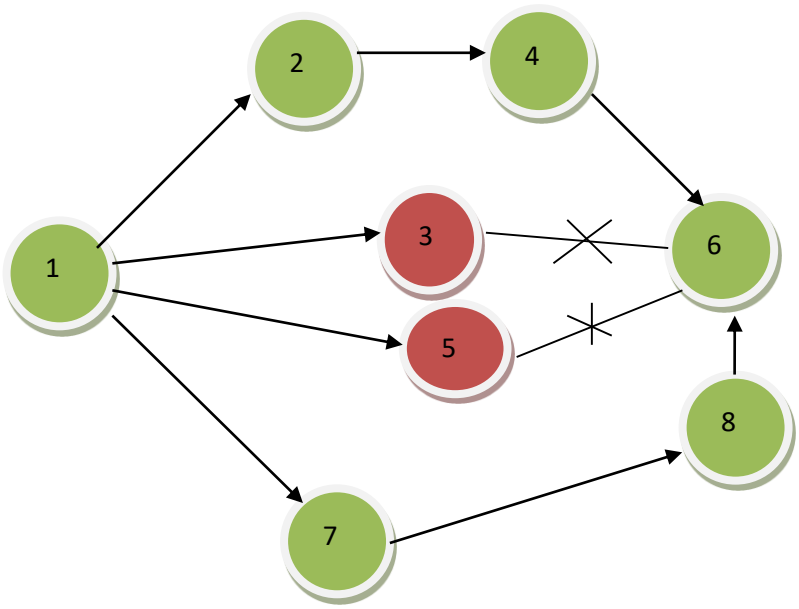
2.ATTACKS IN MANET

In MANET , two types of attack possible which are **Active** and **Passive**.An active attack is one in which the data being transferred in the network is deleted or altered by an attacker who is a certified node.While in a passive attack, an attacker node that is not permitted obtains the data without interfering with or endangering the operation of the network.Different layers attack in passive attack which is follow as shown in figure 1 (5).
Figure 1

LAYERS ATTACK ON MANET	APPLICATION LAYER	Repudiation,Data Corruption
	NETWORK LAYER	Wormhole attack,Grey hole Attack, **Black hole attack**
	TRANSPORT LAYER	TCP/UDP,Session Hijacking
	DATALINK LAYER	Monitoring ,Jamming ,Interception,Traffic analysis

2.1 BLACKHOLE ATTACK:

This kind of attack involves the attacker dropping either all control and data packets that are routed via him or just a subset of them.As a result, all packets that pass through this malicious intermediate node will experience partial or complete data loss.A malicious node employs a "blackhole attack" to trick other good nodes into believing it has the best path by sending false routing information (6).By sending fraudulent reply messages to the sender, the malicious node in a blackhole attack tries to convince the sender node that it is the true destination node.In order to make the sender node believe that the malicious node is a destination node or that it has a new node to the destination, the malicious node may respond with an extremely high sequence number (7).



3.LITERATURE REVIEW

(8) ZohaibHassan, amjadmehmood, abdulazizaldesheishem ”**Intelligent Detection of Blackhole Attacks for Secure Communication in Autonomous and Connected Vehicles**” In this paper In terms of PDR, E2E, throughput, packet loss ratio, and routing overhead, IDBA (Intelligent Detection Blackhole Attack) beats current techniques. Additionally, when the rogue node drops the packets, intimate emergency alarm.

(9) Mohammed Baqer M.Kamel,?Ibrahim Alameri, Ameer N. Onaizah“ **STAODV: a secure and trust based approach to mitigate blackhole attack on AODV based MANET**“This study outlines how the fundamentals were discovered. To determine the appropriate route response, AODV uses the sequence number in addition to NS2.

(10) Ashraf Abdelhamid, Mahmoud said Elsayed, Anca D.Jurcut , Marianne A.Azer”**A Light Weight Anomally detection system for Blackhole Attack**” This paper's primary objective is to suggest a method for identifying blackhole attacks utilizing anomaly detection based on an SVM (support Vector Machine).

(11) Abhilash Singh,Kaustav Pratim Kalita, Smriti Priya Medhi ”**Blackhole Attack On Manet and its Effects** “In this study, Manet was subjected to a blackhole assault, and the impacts of the attack were

evaluated in terms of end-to-end delay, PDR, packet loss, and throughput using a Ns2 simulator with AODV as the routing protocol.

(12) Abdulaziz Alshammari, Mohammed A.Zohdy,

Debatosh Debnath, George corser," **Real Time Vehicular Traffic Simulation for Black Hole Attack in the Greater Detroit Area**" Our *simulation's* primary objective is to use NS-2 and SUMO (simulation of Urban) to investigate the performance impact of a blackhole attack on real-time vehicle traffic in the greater Detroit area.The AODV protocol will be used for the simulation.

(13) Yasin, Adwan and Abu Zant, Mahmoud *"* **Detecting and isolating black-hole attacks in MANET using timer based baited technique**" In this study, AODV was improved by integrating a novel, simple method for identifying and isolating the network's blackhole nodes.Utilizing the simulation tool NS-2.35, the suggested technique is put into practice.

(14) Gruebler, Anna and McDonald-Maier, Klaus D and Alheeti, Khattab M Ali "**An intrusion detection system against black hole attacks on the communication network of self-driving cars**" In this paper, the authors develop an Intelligent Intrusion Detection System (IDS) for VANETs that employs a proportional overlapping scores method to cut down on the amount of features that must be collected from the trace file of VANET behavior and classified.Relevant characteristics can be used to define a vehicle's typical or anomalous behavior.The IDS detects blackhole attacks using (ANN) Artificial Neural Networks and fuzzified data.They employed anomalous and hybrid detection to find the black hole attack.The fuzzy set also aids in lowering the error rate and the quantity of false alerts.

(15) Rushdi, AH "**Protocol for Multiple Black Hole Attack Avoidance in Mobile Ad Hoc Networks**" The 'Enhanced RID-AODV' protocol, which is based on a predation mechanism, is proposed in this chapter as an improved and modified protocol.The suggested enhancement is based on the creation of a dynamic blacklist for each node, according to criteria that depend on the quantity of received packet hashvalue mismatches compared to a threshold value and sudden changes in Round-Trip Time (RTT).(RID-AODV combines RAODV and IDSAODV, two more protocols.)

(16) Malik, Abdul and Khan, Muhammad Zahid and Faisal, Mohammad and Khan, Faheem and Seo, Jung-Taek**"An efficient dynamic solution for the detection and prevention of black hole attack in vanets**" The detection and prevention of BHA (DPBHA), a unique approach, is provided in this work to safeguard and enhance the overall security performance of the VANETs by identifying BHA at an early stage of the route discovery process.The suggested remedy relies on computing a dynamic threshold value and producing a forgery of a route request (RREQ) packet.The solution is put into practice, assessed, and compared to a benchmark scheme for performance and efficiency in the NS-2 simulator.

(17) Mistry, Nital and Jinwala, Devesh C and Zaveri, Mukesh and others "**Improving AODV protocol against blackhole attacks**" They attempt to concentrate on studying and enhancing the security of one of the well-liked routing protocols for MANET, the AODV routing protocol, in this paper.They pay close attention to guaranteeing security against blackhole attacks.Additionally, suggest changes to the AODV protocol and support the changes with appropriate NS-2 simulation and implementation.

(18) Debarati Roy Choudhurya, Dr. Leena Raghab, Prof. Nilesh Marathe.b"**Implementing and improving the performance of AODV by receive reply method and securing it from Black-hole attack**" In order to lessen the Black-hole attack on the routing protocols in MANETs, this research suggests changes to the AODV protocol, which is employed in the MANET algorithm.Black-hole attacks and the AODV protocol were thwarted by the creation of wait time and request reply tables.The primary advantage of changing the AODV protocol is that the malicious node is detected at the beginning of the process and eliminated right away so that it cannot participate in subsequent steps.

(19) Samiullah Khan∗ , Faqir Usman† , Matiullah‡ , and Fahim Khan Khalil "**Enhanced Detection and elimination Mechanism from Cooperative Blackhole threats in Manet**" According to this study, there are more malicious nodes, the manets' performance suffers.The cooperative black-hole attack is thwarted by a technique that uses signatures to identify rogue nodes.The cooperative blackhole attack detection and elimination in MANETs has improved thanks to the signature-based technique.

(20) Priyanka Sonal Sao, Jageshwer Shriwas, Rohit Miri "**Performance Evaluation of Black hole Attack and prevention using AODV on MANET**" According to this study, a black hole is threatening The AODV.All data packets are absorbed by the malicious node in the blackhole.Giving each data packet a sequence number and locating multiple routes for each packet will help us avoid this issue.

(21) Ningthoujam Chidananda Singh, Avinash Sharma "**Resilience of Mobile ad hoc network to security attacks and Optimization of routing process**" This study highlights the adaptability of mobile Ad-hoc networks to different security threats and enhances the routing procedure.Ant Colony Optimization, an enhanced routing algorithm via logic, is used to address all of these issues. Distributed fuzzy logic module eliminates Ant Colony Optimization (SAFEACO) to identify the linear nodes of complexity.SAFEACO's capacity to identify linear-complexity nodes also gives it higher resistance against Sybil, inundation, and black hole assaults.

(22) Ashish Kumar Jain1 and Vrinda Tokekar "**Security Enhancement of AODV protocol using fuzzy based trust Computation in Mobile Ad-hoc Network**" To discover dangerous nodes and, as a result, safe routes in MANET, aggregated trust values are computed in this study using a fuzzy-based max-product composition approach.In this research, two different types of protocols—TFAODV (Trusted Fuzzy AODV) and TMPCF (Trusted Maximum Product Composition of Fuzzy Relations)—are used.Under every circumstance, TFAODV beat AODV in terms of network performance.

(23) Ms.Nivedita Kadam, Dr. Krovi Raja Sekhar "**Machine Learning Approach of Hybrid KSVN Algorithm to detect DDOS Attack in VANET**" In this paper, a novel Hybrid KSVM scheme, based on the KNN and SVM algorithms, is proposed. It is used to create a safe framework to identify DOS attacks, which is a component of machine learning.

(24) J.Manoranjini, A.Chandrasekar, D.Rajinigirinath "**Hybrid Detector for Detection of Black-holes in MANETs**" They suggest a brand-new methodology that, in spite of node movements, more precisely detects blackholes using a hybrid automatic detector and kalman-Bucy filters.

(25) D.Naga Tej,K V Ramana, "**MSA-SFO based Secure and Optimal energy Routing Protocol for MANET**" Modified self-adaptive sailfish optimization (MSA-SFO) is used in this paper.Even in a chaotic environment, important maps can be built.Secure key pairs are created using this procedure.Compared to other

models, MSA-SFO offers a wireless MANET network with a higher level of security.A high level of security is also provided.

(26) Safaa LAQTIB, Khalid El YASSINI, Moulay Lahcen HASNAOUI "**A Deep Learning Methods for Intrusion Detection Systemsbased Machine Learning in MANET"**The most popular deep learning models CNN, Inception-CNN, Bi-LSTM, and GRU are presented in this work, along with a systematic comparison of CNN and RNN on deep learning-based intrusion detection systems. Their goal is to provide fundamental recommendations for DNN selection in MANET.The main benefit of adopting DL-based detection systems is their high accuracy and ability to identify or classify assaults without the interference of the environment.

(27) Ajit R. Bandgar, Sandeep A. Thorat"**An Improved Location-Aware Ant Colony Optimization based routing Algorithmfor MANETs"**In this research, the author suggested the AntHocNet-LS routing method for MANET. By using the position of nodes, the proposed technique aims to decrease the overhead caused by ants and improve system performance as a whole. The simulation results have demonstrated that the suggested technique may successfully reduce the overhead produced by ants while attaining a higher packet delivery ratio. The suggested approach performed better than AntHocNet in every way, especially when there were more nodes involved.

(28) S.Murugan, S.Jeyalaksshmi, B.Mahalakshmi, G.Suseendran, T.Nusrat Jabeen, R.Manikandan **"Comparision of ACO and PSO Algorithm using Energy Comsumption and Load Balancing in emerging MANET and VANET Infrastructure"** Due to disconnections, the communication link is dangerous in VANET and MANET. By applying criteria as PDR, latency, throughput, Goodput, packet drop, and dropping ratio, particle swarm optimization (PSO) and ant colony optimization (ACO) are both simulated. Utilizing existing resources efficiently is crucial to reducing load and energy consumption as motor traffic in metropolitan areas suddenly improves. Reducing network traffic and balancing the load will help to reduce the drop. By lowering energy consumption, which makes it essential to balance energy in nodes, network lifetime may be extended. Utilizing ACO and PSO, the most dependable path is determined through evaluation, hence lowering the likelihood of connection failures.

(29) S.E. Benatia a , O. Smail , B. Meftah , M. Rebbah , B. Cousin "A reliable multipath routing protocol based on link quality and stability for MANETs in urban areas" In this study, we present the RMQS-ua (Reliable Multipath Routing Protocol based on Link Quality and Stability in Urban Areas) multipath routing protocol. To ensure dependable data transfer, we want to choose the way with the best connection quality and most stable connectivity. In order to assess network quality, we combine the signal to noise ratio (SNR), the improved packet reception ratio (PRR), and the exponential moving average (EMA). The urban environment where RMQS-ua is built has shadowing effects and background noise that degrade the connection quality. In comparison to certain current existing protocols, simulation findings demonstrate that RMQS-ua increases network performance and offers more dependability.

(30) Krzysztof Malon, Paweł Skokowski ,Jerzy Łopatka "**Optimization of the MANET Topology in Urban Area Using Redundant Relay Points** "The suggested approach offers an improvement in the throughput and dependability of mobile networks. Possible "black holes," or regions with little to no connection, are identified using a terrain model and propagation prediction, and additional, supporting nodes

are suggested. Assuming that nodes' placements during the planning phase are unknown and that only the operating area is known, the primary criterion is a maximum increase in mutual visibility of nodes. The approach can be improved by incorporating operational scenario objectives, introducing flying platforms, or specialized retransmission devices. Additionally, the study of a network with sector antenna-equipped access components will be possible with the aid of the antenna direction assessment process .

(31)Shaik Shafia , S Mounikaa , Velliangiri S "**Machine Learning and Trust Based AODV Routing Protocol to Mitigate Flooding and Blackhole Attacks in MANET**"An effective machine learning-based secure AODV routing strategy (ML-AODV) is put forth in this study for the detection of floods and blackhole attacks in MANET. For various node densities, the performance of ML-AODV has been evaluated alongside current trust-based AODV and standard AODV protocol. Additionally, the suggested ML-AODV significantly improves intrusion detection accuracy and throughput by combining an ANN with an SVM classifier. With a top speed of 20 m/s, the suggested ML-AODV is only tested for 50 nodes.

(32)Ms Shweta Pandey ,Mr Varun Singh"**Blackhole Attack Detection Using Machine Learning Approach on MANET "** The BHA in the MANET is found using the suggested methods. In this study, the suitable routing technique is described. The ANN and SVM are both used in the presented work. The mean square error is one of the metrics analyzed here.With the aid of the ANN and SVM, the model is compared between the path that is attacked as a black hole and the improved route. The suggested routing model is effective and secure. Additionally, it aids in the discovery of black holes.

(33)Gihani Jinarajadasa, Lakmal Rupasinghe, Iain Murray "**A Reinforcement Learning Approach to Enhance the Trust Level of MANETs**" They provide a method for improving confidence in a MANET based on RLTM (Reinforcement Learning confidence Manager), a collection of algorithms that uses Deep Learning and Reinforcement Learning to consider the Ad-hoc Ondemand Distance Vector (AODV) protocol as the particular protocol. A RL agent that learns to identify reliable nodes, infamous nodes, and malevolent nodes and to classify them makes up the suggested system. The developed RNN (Recurrent Neural Network) model was given the discovered parameters from the AODV simulation performed using Network Simulator-3 (NS-3), and the outcomes were assessed.

(34) Ranjita Joon , Parul Tomar"**Energy Aware Q-learning AODV (EAQ-AODV) routing for cognitive radio sensor networks "**The energy aware Q-learning AODV (EAQ-AODV) routing is a new concept that they present in this study. The proposed EAQ-AODV establishes the routing path using several factors, including Residual Energy, Common Channel, Number of Hops, Licensed Channel, Communication Range, and Trust Factor, and rewards cluster heads using a Q-learning-based method. The experimental investigation demonstrates that, when compared to the existing methodologies, the suggested EAQ-AODV routing provides a better performance in terms of average end-to-end latency, average energy consumption, and network lifespan.

(35) Cao,D.,Jiang,Y "**ARNS: Adaptive Relay-Node Selection Method for Message Broadcasting in the Internet of Vehicles"**The ARNS approach was presented in this study as a means of selecting relay nodes in complex road settings. To the best of our knowledge, this is the first time an adaptive relay-node selection technique has been developed that takes into account the road structure at each hop that is within the sender's communication range. In accordance with the layout of the road, ARNS selects the relay-node that is most advantageous. Furthermore, the impact of impediments was taken into account. Through simulation, the superiority of ARNS over approaches based on 3P3B , RTAD , and broadcast coverage over the entire method was shown. Additionally, ARNS outperforms the latter in terms of one-hop latency and PDR. We demonstrated that ARNS decreases end-to-end latency in a real-world road scenario by at least 13.8% when compared to the beacon-based method. Additionally, the broadcast coverage of ARNS was enhanced by 3.6–7% when compared to the full method.

(36) Clement Sunder ,A.J.& Shanmugam "**Black Hole Attack Detection in Healthcare Wireless Sensor Networks Using Independent Component Analysis Machine Learning Technique** "To identify the black hole attack in a healthcare wireless sensor network, Projected Independent Component Analysis (PICA), an effective machine learning technique, is presented. Mutual information is used by the PICA approach to quantify the reliance of SN behavior. The PICA technique analyzes physiological data gathered from biomedical sensors to identify black hole attacks. The mutual probability function and independent probability distribution functions are used to determine the dependence among the SN behavior. The identification of the black hole node and other normal nodes is based on the probability distribution. In order to isolate the black hole node, isolation is finally carried out. PICA is used in an experimental setting to evaluate the parameters in comparison to state-of-the-art methodologies in terms of BHADR, BHADT, FPR, PDR delay, and BHADR.

(37) Dhanaraj,R,k.krishnasamy "**Black Hole and Sink Hole Attack Detection in Wireless Body Area Networks"** Black hole and sink hole attacks are two security threats that still affect healthcare WBANs. An intrusion detection framework is suggested as a solution to these problems, with the aim of identifying attacks and notifying sensing nodes to reduce data loss. In particular, the PCS and MK-Means machine learning techniques are used in the architectural view for healthcare WBAN intrusion detection, which is implemented for classification accuracy and data reduction, respectively. By decreasing the feature size, the PCS reduces classification difficulties, improving the accuracy of assault detection.

(38) Femila ,L.,&Marsaline Beno.M "**Optimizing Transmission power and energy efficient routing protocol in Manets**"On regular line and grid line networks, the traditional shortest path routing technique achieves gains in energy savings of up to 45–75%, respectively. The EPAR algorithm reduces energy usage, extending the life of the network and enhancing performance. The EPAR technique in mobile ad hoc networks can reduce the rate of energy consumption to 80%.

(39) Khayamesh ,Y.M" **Ensuring Survivability against Blackhole attacks in MANET**" The objectives of this research were to present a technique for identifying malicious nodes, stop or restrict Black Hole Attacks on mobile ad hoc networks (MANETs), and guarantee that MANET nodes can survive black hole attacks.

(40)Pandey.S.,&Singh.V " **Blackhole Attack detection using machine learning approach on Manet**"The suggested method finds black hole attacks in the network by using an artificial neural network (ANN) and a

support vector machine (SVM). The outcomes are compared between the Secure AODV (SAODV), which we provide, and the black hole AODV. After experimenting with 100 nodes, the results showed an improvement in energy usage of 54.72%, throughput of 88.68 kbps, packet delivery ratio of 92.91%, and E to E delay of roughly 37.27 ms. The results were evaluated with varying numbers of nodes.

4.COMPLICATIONS UNDERTAKEN

The integration of machine learning components into MANET protocols introduces several challenges that must be carefully addressed. Firstly, ensuring the reliability of trust estimation is crucial, as inaccurate assessments could lead to the selection of untrustworthy relay or transmit nodes, jeopardizing routing integrity and network security.

Additionally, the increased complexity and computational overhead associated with machine learning algorithms can strain the limited resources of MANET nodes, potentially leading to higher energy consumption, latency, and degraded network performance. Moreover, machine learning-based intrusion detection mechanisms, such as Support Vector Machines (SVM), can be susceptible to adversarial attacks like black hole attacks, where attackers exploit vulnerabilities in the detection model to evade detection and compromise network security.

Furthermore, the protocol's generalization across diverse network conditions and attack scenarios poses a challenge, as variability in network characteristics and training data can impact its real-world effectiveness. Lastly, scalability concerns arise as MANETs scale in size or experience increased dynamics, requiring protocols to efficiently manage trust relationships and update machine learning models without sacrificing performance. Addressing these challenges is essential to developing robust and scalable machine learning-integrated MANET protocols capable of ensuring trust, security, and efficiency in dynamic wireless networks.

COMPARISION OF EXISTING WORK

Author	Year	Methodology	Limitation	Advantage
Abdelhamid, A. et al. (10)	2023	Anomaly detection system	Limited to black hole attacks	Lightweight and efficient anomaly detection
Cao, D. et al.(35)	2020	Adaptive relay-node selection	Focuses on Internet of Vehicles (IoV)	Addresses message broadcasting in IoV
Clement Sunder, A. J. & Shanmugam, A.(36)	2020	Independent component analysis	Limited to healthcare WSNs	Utilizes machine learning for attack detection
Dhanaraj, R. K. et al.(37)	2021	Black hole and sink hole detection	Specific to wireless body area networks	Addresses sink hole attacks
Femila, L. & Marsaline Beno, M.(38)	2019	Energy-efficient routing protocol	Limited to transmission power optimization	Optimizes energy and routing in MANETs
Jain, N. K. & Verma, A.(22)	2019	Relay node selection in WSNs	Focuses on Wireless Sensor Networks (WSNs)	Enhances relay node selection
Khamayseh, Y. M. et al.(39)	2018	Black hole attack survivability	Specific to energy efficiency in MANETs	Ensures survivability against black hole attacks
Pandey, S. & Singh, V.(40)	2020	Machine learning for attack detection	Limited to black hole attacks in MANETs	Utilizes machine learning for attack detection

CONCLUSION

In this research, we provide a machine learning method for identifying metropolitan regions black-hole attacks using current data.For many characteristics, like trust estimation, energy consumption,latency scalability and delay routing complexity and packet loss ratio, we use a network simulator.

Bibliography

1. *MANET: History, challenges and applications.* **Bang, Ankur O and Ramteke, Prabhakar L.** 9, 2013, International Journal of Application or Innovation in Engineering \& Management (IJAIEM), Vol. 2, pp. 249--251.

2. *Performance comparison and evaluation of the proactive and reactive routing protocols for MANETs.* **Bai, Yuxia and Mai, Yefa and Wang, Nan.** 2017, IEEE, pp. 1--5.

3. *A survey of reactive routing protocols in MANET.* **Patel, Daxesh N and Patel, Sejal B and Kothadiya, Hemangi R and Jethwa, Pinakin D and Jhaveri, Rutvij H.** 2014, IEEE, pp. 1--6.

4. *A review of routing protocols for mobile ad hoc networks.* **Abolhasan, Mehran and Wysocki, Tadeusz and Dutkiewicz, Eryk.** s.l. : Elsevier, 2004, Vol. 2, pp. 1--22. 1.

5. *Security Threats and Solutions in Mobile Ad Hoc Networks; A Review.* **Ichaba, Mutuma.** s.l. : Universal Journal of Communications and Network , 2018, Vol. 6, pp. 7-17.

6. *A survey of routing attacks in mobile ad hoc networks.* **Kannhavong, Bounpadith and Nakayama, Hidehisa and Nemoto, Yoshiaki and Kato, Nei and Jamalipour, Abbas.** s.l. : IEEE, 2007, Vol. 14, pp. 85--91. 5.

7. **Patel, Ankit D and Chawda, Kartik.** *Blackhole and grayhole attacks in MANET.* s.l. : IEEE, 2014. pp. 1--6.

8. *Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles.* **Hassan, Zohaib and Mehmood, Amjad and Maple, Carsten and Khan, Muhammad Altaf and Aldegheishem, Abdulaziz.** s.l. : IEEE, 2020, Vol. 8, pp. 199618--199628.

9. **Kamel, Mohammed Baqer M and Alameri, Ibrahim and Onaizah, Ameer N.** STAODV: a secure and trust based approach to mitigate blackhole attack on AODV based MANET. s.l. : IEEE, 2017, pp. 1278--1282.

10. *A Lightweight Anomaly Detection System for Black Hole Attack.* **Abdelhamid, Ashraf and Elsayed, Mahmoud Said and Jurcut, Anca D and Azer, Marianne A.** s.l. : MDPI, Electronics, Vol. 12, p. 1294.

11. **Singh, Abhilash and Kalita, Kaustav Pratim and Medhi, Smriti Priya.** Blackhole attack on MANET and its effects. *Proceedings of the 5th International Conference on Computing for Sustainable Global Development, New Delhi, India.* 2018, pp. 14--16.

12. *Real Time Vehicular Traffic Simulation for Black Hole Attack in the Greater Detroit Area.* **Alshammari, Abdulaziz and Zohdy, Mohamed A and Debnath, Debatosh and Corser, George and others.** s.l. : Scientific Research Publishing, 2019, Journal of Information Security, Vol. 11, p. 71.

13. *Detecting and isolating black-hole attacks in MANET using timer based baited technique.* **Yasin, Adwan and Abu Zant, Mahmoud.** s.l. : Hindawi, 2018, Wireless Communications and Mobile Computing, Vol. 2018.

14. **Gruebler, Anna and McDonald-Maier, Klaus D and Alheeti, Khattab M Ali.** *An intrusion detection system against black hole attacks on the communication network of self-driving cars.* s.l. : IEEE, 2015. pp. 86--91.

15. *Protocol for Multiple Black Hole Attack Avoidance in Mobile Ad Hoc Networks.* **Rushdi, AH.** 2018, Recent Advances in Cryptography and Network Security, pp. 25--41.

16. *An efficient dynamic solution for the detection and prevention of black hole attack in vanets.* **Malik, Abdul and Khan, Muhammad Zahid and Faisal, Mohammad and Khan, Faheem and Seo, Jung-Taek.** s.l. : MDPI, 2022, Sensors, Vol. 22, p. 1897.

17. *Improving AODV protocol against blackhole attacks.* **Mistry, Nital and Jinwala, Devesh C and Zaveri, Mukesh and others.** s.l. : Citeseer, 2010, Vol. 2, pp. 1--6.

18. *Implementing and improving the performance of AODV by receive reply method and securing it from Black hole attack.* **Choudhury, Debarati Roy and Ragha, Leena and Marathe, Nilesh.** s.l. : Elsevier, 2015, Procedia Computer Science, Vol. 45, pp. 564--570.

19. *Enhanced Detection and Elimination Mechanism from Cooperative Black Hole Threats in MANETs.* **Khan, Samiullah and Usman, Faqir and Khalil, Fahim Khan and others.** s.l. : Science and Information (SAI) Organization Limited, 2018, International Journal of Advanced Computer Science And Applications.

20. *Performance Evaluation of Black Hole Attack and Prevention Using AODV on MANET.* **Priyanka sonal sao, Jageshwer Shriwas,Rohit Miri.** s.l. : International Research Journal of Engineering and Technology (IRJET), 2015, Vol. 02.

21. *Resilience of mobile ad hoc networks to security attacks and optimization of routing process.* **Singh, Ningthoujam Chidananda and Sharma, Avinash.** 2020, Materials Today: Proceedings, Vol. 12, pp. 88--97.

22. *Security enhancement of AODV protocol using fuzzy based trust computation in mobile ad hoc networks.* **Jain, Ashish and Tokekar, Vrinda.** 2017, Oriental journal of computer science and technology, Vol. 10, pp. 94--102.

23. *Machine learning approach of hybrid KSVN algorithm to detect DDoS attack in VANET.* **Kadam, Nivedita and Krovi, Raja Sekhar.** s.l. : Science and Information (SAI) Organization Limited, 2021, International Journal of Advanced Computer Science and Applications, Vol. 12.

24. *Hybrid detector for detection of black holes in MANETs.* **Manoranjini, J and Chandrasekar, A and Rajinigirinath, D.** s.l. : Elsevier, IERI Procedia, Vol. 4, pp. 376--382.

25. *MSA-SFO-based Secure and Optimal Energy Routing Protocol for MANET.* **Tej, D Naga and Ramana, KV.** s.l. : Science and Information (SAI) Organization Limited, 2022, International Journal of Advanced Computer Science and Applications, Vol. 13.

26. **Laqtib, Safaa and Yassini, Khalid El and Hasnaoui, Moulay Lahcen.** A deep learning methods for intrusion detection systems based machine learning in MANET. *Proceedings of the 4th international conference on smart city applications.* 2019, pp. 1--8.

27. *An Improved Location-Aware Ant Colony Optimization based routing Algorithm.* **Ajit R. Bandgar, Sandeep A. Thorat.** s.l. : IEEE, 2013, INTERNATIONAL CONFERENCE ON COMPUTING, COMMUNICATION AND NETWORKING TECHNOLOGIES (ICCCNT).

28. *Comparison of ACO and PSO algorithm using energy consumption and load balancing in emerging MANET and VANET infrastructure.* **Murugan, S and Jeyalaksshmi, S and Mahalakshmi, B and Suseendran, G and Jabeen, T Nusrat and Manikandan, R.** 2020, Journal of Critical Reviews, Vol. 7, p. 2020.

29. *A reliable multipath routing protocol based on link quality and stability for MANETs in urban areas.* **Benatia, SE and Smail, O and Meftah, Boudjelal and Rebbah, M and Cousin, Bernard.** s.l. : Elsevier, 2021, Simulation Modelling Practice and Theory, Vol. 113, p. 102397.

30. **Malon, Krzysztof and Skokowski, Pawe and opatka, Jerzy.** Optimization of the MANET topology in urban area using redundant relay points. *2018 International Conference on Military Communications and Information Systems (ICMCIS).* s.l. : IEEE, 2018, pp. 1--4.

31. *Machine Learning and Trust Based AODV Routing Protocol to Mitigate Flooding and Blackhole Attacks in MANET.* **Shafi, Shaik and Mounika, S and Velliangiri, S.** s.l. : Elsevier, 2023, Procedia Computer Science, Vol. 218, pp. 2309--2318.

32. **Pandey, Shweta and Singh, Varun.** Blackhole attack detection using machine learning approach on MANET. *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC).* s.l. : IEEE, 2020, pp. 797--802.

33. **Jinarajadasa, Gihani and Rupasinghe, Lakmal and Murray, Iain.** A reinforcement learning approach to enhance the trust level of MANETs. *2018 National information technology conference (NITC).* s.l. : IEEE, 2018, pp. 1--7.

34. *Energy aware Q-learning AODV (EAQ-AODV) routing for cognitive radio sensor networks.* **Joon, Ranjita and Tomar, Parul.** s.l. : Elsevier, 2022, Journal of King Saud University-Computer and Information Sciences, Vol. 34, pp. 6989--7000.

35. *ARNS: Adaptive Relay-Node Selection Method for Message Broadcasting in the Internet of Vehicles.* **Dun Cao ORCID, Yuchen Jiang ORCID,Jin Wang ,*ORCID,Baofeng Ji ,Osama Alfarraj ,Amr Tolba ,ORCID,Xiaomin Ma andYonghe Liu.** s.l. : MDPI, 2020.

36. *Black Hole Attack Detection in Healthcare Wireless Sensor Networks .* **A. John Clement Sunder, and A. Shanmugam.** s.l. : BENTHAM SCIENCE, 2020, Vols. Volume 15, Issue 1, 2020, pp. [56 - 64].

37. *Black Hole and Sink Hole Attack Detection in Wireless Body Area Networks.* **Rajesh Kumar Dhanaraj, Lalitha Krishnasamy, Oana Geman, Diana Roxana Izdrui.** s.l. : Google Scholar, 2021.

38. *Optimizing transmission power and energy efficient routing protocol in MANETs.* **Femila, L.,Arsaline Beno.** s.l. : springer, 2019, pp. 1041-1056.

39. *Ensuring survivability against Black Hole Attacks in MANETS for preserving energy efficiency.* **kamayseh, Yasar.M.** s.l. : Elsivier, Vol. 18, pp. 90-100.

40. *Blackhole Attack Detection Using Machine Learning Approach on MANET.* **Shweta Pandey, Varun Singh.** s.l. : International conference on electronics and sustainable communication systems(ICESC), 2020. pp. 797-802.