Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 4 (2023)

Reputation-Based Opportunistic Routing Protocol Using Q-Learning For Manet Attacked By Malicious Nodes: A Survey

[1]P. Saranya, [2]Dr. A. Nithya

[1]Research Scholar, Department of Computer Science, Park's College, Chinnakarai, Palladam Main Road, Tirupur, Tamilnadu
[2]Professor & Head, Department of Computer Science, AMC BU College, Bangalore, India

Abstract: Mobile Ad-hoc Networks (MANETs) have emerged as a viable paradigm for creating dynamic communication between mobile nodes in the absence of a permanent infrastructure. However, since MANETs are inherently decentralized and self-organizing, they are vulnerable to a variety of security concerns, especially when hostile nodes seek to interrupt communication and undermine network operations. As a consequence, developing efficient and robust routing protocols is critical to ensuring dependable and secure data transmission in MANETs. This review study gives an in-depth look into Reputation-Based Opportunistic Routing Protocols (RORPs), which use Q-Learning methods to improve MANET resistance against malicious node assaults. We provide a thorough study of current RORPs, delving into their core design ideas, underlying processes, and comparative performance evaluations. We begin with a comprehensive introduction to the fundamental concepts, issues, and security risks associated with MANETs. Following that, we explore the concepts of reputation-based routing, emphasizing the need of reputation management in discriminating between malicious and genuine nodes. The review then goes into further detail on the incorporation of Q-Learning methods into RORPs, emphasizing on how reinforcement learning mechanisms may adaptively change routing choices depending on the developing network state and the dynamic reputations of participating nodes. This article reviews 38 research papers of opportunistic routing protocol and explores the potential of computer-assisted methods for MANET. We next divide the studied RORPs into categories depending on their approach to reputation computation, learning algorithms, and cooperative enforcement methods. Furthermore, we analyze their strengths and weaknesses in terms of resilience to different sorts of attacks, as well as their influence on network performance measures including packet delivery ratio, end-to-end latency, and throughput.
Keywords: Black Hole Attack, Gray Hole Attack, Malicious Nodes**,** Mobile Ad-Hoc Networks, Q-Learning

1. Introduction

MANETs have evolved as a flexible and self-organizing communication paradigm, allowing nodes to build dynamic, ad-hoc connections without depending on any permanent infrastructure [1-3]. These networks find use in a variety of contexts, including military operations, disaster response, distant places, and IoT installations, when standard network infrastructure is prohibitive or impossible to create [4-9]. However, since MANETs are decentralized and open, they are exposed to a variety of security risks and issues [10]. The existence of malicious nodes, which may purposefully disrupt network operations, jeopardize data integrity, and degrade network performance, is one of the main difficulties that MANETs confront [11]. Malicious nodes may drop, change, or forge packets, execute denial-of-service (DoS) attacks, and impersonate genuine nodes. Such malicious conduct may have a significant impact on overall network stability, resulting in communication failures and decreased efficiency [12-15].

MANETs have developed as a flexible and efficient communication paradigm, enabling nodes to construct dynamic, self-configuring, and transitory networks without the requirement for a permanent infrastructure [16-19]. These networks are used in a variety of settings, including disaster recovery, military deployments, vehicle networks, and IoT environments [20]. However, the decentralized structure of MANETs makes them subject to security risks and assaults, particularly when rogue nodes intentionally disrupt communication and affect network performance [21-25]. Malicious nodes in MANETs may use a variety of disruptive strategies to intercept, alter, or discard data packets, such as blackhole attacks, wormhole assaults, Sybil attacks, and selective forwarding [26-27]. These assaults may have serious effects, such as a breakdown in

communication, data loss, and the interruption of key services. To provide efficient and reliable communication in the presence of hostile nodes, strong and secure routing protocols must be designed [28-31].

Reputation-based routing has emerged as a viable strategy for improving MANET resistance against such assaults. Reputation-based routing algorithms may identify trustworthy nodes for data forwarding while avoiding hostile or uncooperative nodes by preserving and assessing the reputation of individual nodes based on their prior behavior [32-35]. This idea of "trustworthiness" is critical for encouraging network node cooperation and self-regulation. This study presents a new Reputation-Based Opportunistic Routing Protocol (RORP) that uses Q-Learning methods to improve the efficiency and flexibility of reputation-based routing in the setting of MANETs targeted by malicious nodes [36]. Q-Learning is a reinforcement learning method that allows nodes to learn from their prior experiences and alter their routing choices depending on the observed rewards and penalties for various activities [37]. RORP aims to provide an intelligent and adaptive routing system capable of dynamically determining the optimum routes while protecting against malicious entities by integrating reputation management with Q-Learning [38].

2. Background Study

2.1 Survey on opportunistic routing protocol

A.Afdhal et al. (2022) the method used by these writers makes advantage of a traffic model's freedom of movement, maximum speed, and junction rules. This method provides the attack detection rate in relation to traffic density in an ITS-V2X deployment zone by comparing the prevalent speed with the estimated approximation speed of a realistic traffic model. The ability to identify attackers may improve if models at different scales are combined.

A.U. Khan et al. (2021) AODV protocols were overwhelmed by network layer routing assaults. AODV has a smaller energy footprint when under attack since it utilizes fewer control packets and only involves chosen nodes. The disruption produced by network layer attacks reduces AODV's packet delivery capabilities. It was critical to safeguard the network against intrusion in order to deliver the best communication services available. AODV needs a security method to secure critical information and applications. To build a secure system, the author must first investigate how the network reacts to attacks.

B. S. Rani and K. Shyamala et al. (2023) the trust-based Secure EELB-AOMDV protocol may identify an ongoing Blackhole attack and redirect traffic around a compromised node. The protocol utilizes all accessible paths and distributes traffic among them equally. As additional nodes were added, performance parameters like as PDR, throughput, routing overhead, and energy use all increase by double digit percentages. When compared to the AOMDV protocol, it achieves a 35.71% increase in PDR, a 40.48% increase in throughput, a 26.32% rise in routing overhead, and a 0.0016% increase in energy use as packet count increases. However, EED increases as a consequence, since calculating the TV of surrounding nodes during packet forwarding and reception adds time and energy consumption.

B. V. Sherif and P. Salini et al. (2021) a mobile ad hoc network (MANET) was a wirelessly connected network of autonomous mobile nodes that configure and function independently of any centralized authority. MANET has become more viable as a result of the growth of high-powered mobile devices and advancements in wireless technology. Because of their mobile nature, MANETs were particularly vulnerable to attacks, which may have a severe influence on network efficiency. To improve MANET performance, researchers must concentrate on developing novel methods for detecting and mitigating threats. As a result, while developing attack detection algorithms, environment adaptive features should be combined with machine learning.

C. Shang et al. (2021) This study makes a theoretical contribution by using privacy computing and privacy concern theory to build a conceptual model of the variables influencing students' openness to adopting online learning platforms. This model offers a fresh perspective and theoretical grounding for online learning platforms to attract more users and increase user stickiness by beginning with the privacy cognitive and analyzing the impact of learners' privacy concerns, trust, perceived risks, and perceived benefits on the willingness to adopt these platforms. The conceptual model was validated using empirical research and structural equation modeling in this study. According to the results, learners' motivation to embrace online learning platforms was strongly influenced by their views of benefits and trust, and adversely influenced by their perceptions of danger.

C. Sharma and R. Vaid (2021) The security of data was critical in WSNs. Data transfer via the allegedly unprotected wireless connection puts attackers at danger of unwanted access. Man-in-the-middle attacks may damage DH because to its lack of node authentication. In this work, the author used a DH-based approach to detect and block WSN Sybil assaults. The results reveal that when compared to the state-of-the-art techniques RPC, CAM-PVM, and MAP, the recommended algorithm DH-SAM obtains a better detection rate. According to the research and simulation results, DH-SAM has lower AE2E latency and higher throughput than ECC.

2.2 Survey on black hole attack

D. Cui et al. (2022) The LINDDUN threat modeling framework was used in this research to show privacy threats related with DCTP. The privacy issues that have been discovered were then coupled with viable countermeasures. While these authors' previous studies looked at DCT at the application layer, this one looks at it at the protocol layer. This page has been updated with new material, such as the categories of privacy issues raised by the EU's GDPR and EPR, protocol classification criteria, a DFD mapping, and mitigating techniques.

D. J. Richter and R. A. Calix (2022) This paper presents a way for using DDQN agents to regulate the attitude of fixed-wing aircraft. Using the QPlane toolbox, experiments were run in JSBSim. After being trained in one environment (JSBSim), the agent was put through its paces in two other, completely different settings (X-Plane-11 and JSBSim) that it had never encountered before. This demonstrates that DDQN may get desirable outcomes even in very complicated settings, provided that the trials were properly designed.

D. Rastogi et al. (2023) to overcome the drawbacks of standard Q-learning, this study introduces IQ-CRL, a revolutionary approach that incorporates artificial neural networks (ANNs) into the learning process. The proposed IQ-CRL method was used to operate a mobile robot, and the results were compared to those achieved using a proportional-integral-derivative (PID) controller and classical Q-learning. The IQ-CRL approach was designed for scalability and adaptation in big continuous systems with changing surroundings and impediments. IQCRL's value was shown by point-to-point navigation with obstacle avoidance.

D. Zala et al. (2021) In this research, the writer proposes a theoretical technique for protecting against blackhole assaults in UWSN by making use of the coordinator node. Now, let's take a look at the limitations this method imposes. There were many options available: Repeatedly broadcasting an Authentication Packet over a large cluster of nodes may deplete battery life, which was an issue for submerged nodes. This time, the issue was a failed connection or a crashed legitimate node. Because the author haven't heard back from the node, there's a risk that the algorithm has mistakenly labeled a valid node as a blackhole.

E. D. Benedetto and A. Cucchi (2022) there were several limitations to this research. To begin, the nature of search engines imposes limits. Because Google Scholar does not have its own API, the author utilized the Publish or Perish tool to query it; this yielded a maximum of 980 results per query. Scopus has the equivalent of 200 searches..

G. Kaur et al. (2022) VANETs must be preserved since they play such an important role in keeping cars and pedestrians safe. VANET was subject to numerous types of attacks. Malicious nodes disturbing the network may make it more difficult to send trustworthy data to nodes. By acquiring and analyzing data from adjacent nodes, the author offer a technique for identifying gray hole attacks in a VANET environment. Several metrics were monitored before and after the bogus node was found and removed, including PDR and throughput. These findings show that the proposed strategy for avoiding gray holes improves PDR by almost 60% and throughput by 45%.

2.3 Survey on gray hole attack

H. Hamann and A. Reina (2022) The author provide a new general paradigm for exploring the scalability of parallel systems composed of many individual components (for example, a supercomputer composed of individual central processing units or an artificial swarm composed of individual robots). They account for non-contention-limited systems, declining returns, and ideal parallel processing in their approach. The authors' model relied on a detailed description of the state changes occurring inside the individual building blocks of the system at the microscopic level. As they interact with one another, the units cycle through three

distinct phases. To represent the typical actions of a single unit, the model may be described as a probabilistic state machine (Microscopic Model).

I.R and A. R. K. P (2021) these authors research proposes a Secured OLSR protocol for identifying and avoiding gray-hole attacks on VANET. Overhead was also reduced, and timing parameters from the original OLSR protocol were optimized. The recommended approach may identify the attacker within 30-50 seconds of starting the experiment.

J. Ryu and S. Kim (2023) the author introduced a unique kind of opportunistic routing in this study as a method of improving on the existing form of MANET routing, which was vulnerable to assaults from malicious nodes. The author calculates the node's reputation based on its forwarding performance and uses it to restrict the pool of prospective forwarding nodes. Effective routing was therefore conceivable on MANETs when hostile nodes were vulnerable to blackhole and grayhole attacks. Since Q-learning is a kind of reinforcement learning, the suggested method is particularly well-suited to a dynamic MANET situation. Several experimental metrics, including packet loss ratio, average end-to-end delay, and energy consumption, showed that the proposed method outperformed both traditional Q-routing and state-of-the-art routing protocols like BTOR, SAQ, and QMCR in networks containing malicious nodes.

K. A. Awan et al. (2023) these authors research ensemble learning approach may detect rogue nodes in an IoT ecosystem by using knowledge, reputation, and experience as trust management components. To identify whether or not a node was hostile, the proposed technique uses an ANN as a fundamental model. The Keras tuner will be used to discover the optimal values for the ANN's hyperparameters, which include the number of hidden layers, the size of each layer's neurons, the activation function, the learning rate, and the optimizer. The suggested architecture has three major components: a data collection component, a trust management component, and a decision-making component.

2.4 Survey on MANET Attack

K. Bala et al. (2023) these authors research applies a fuzzy logic method inside the Intrusion Detection System (IDS) to detect gray hole attacks in MANET. As a result, the author were able to identify the network's bad actors by following down instances of packet loss and failure. Fuzzy logic was used to detect potentially dangerous nodes and repair them before they impair network traffic. As a consequence, the rogue node may be repaired or ignored, and network connection and data transfer can resume normally.

L. Darwish et al. (2023) when malicious nodes were let into a network, security was compromised, and network performance and reliability decrease. This article proposes a strategy for detecting the existence of malicious nodes in sensor networks. This technique compares performance metrics when a malicious node was present against when it was not. The findings of the empirical inquiry show that there was a difference in network characteristics with and without the malicious node. Knowing if a malicious node exists in a sensor network was critical for safeguarding the network.

L. E. Buck and B. Bodenheimer (2021) When it comes to data availability and privacy, users' allocation and maintenance of personal space in immersive virtual worlds increases both. This talk seeks to increase awareness of these issues and to initiate a discussion on how academics and the VR community may put this knowledge to good use.

M. Bashir et al. (2023) the author provide a machine learning strategy based on the SVM-GA classifier for predicting network nodes and MANET attacks while taking node properties into account. It can prepare ahead for route invasions by discriminating between benign and harmful nodes.

M. D. Chawhan et al. (2023) Because of their theoretical invulnerability in actuality, updated encryption algorithms were unequaled in terms of speed and security. The Modified Encryption Algorithm takes longer to encrypt data but less time to decode than AES, 3DES, and RSA. This metric, according to previous research, demonstrates that these authors encryption was both faster and more secure.

M. D. Chawhan et al. (2022) these authors research examines the MANET, the AODV routing protocol, and the attack in detail in order to block the Grayhole attack and protect the network. In the proposed approach, twenty-five mobile nodes, including two malicious nodes and two intrusion detection system nodes, were combined into a network established using the AODV routing protocol. IDS nodes serve as the foundation

of a detection and prevention system. The simulation results demonstrate that the desired increases in key performance metrics, such as packet delivery ratio (PDR) and throughput (67.8 Mbps), were realized.

M. Knaj et al. (2023) When MANETs are attacked by wormholes, their Throughput and Packet Delivery Ratio both suffer. This causes an overall average delay to grow. All performance indicators decline as the number of attacking nodes and the rate of network nodes rise. Hop count analysis might help MANETs that were attacked through wormholes. Both the network performance and the packet delivery ratio are excellent. The value of Average End-to-End Delay rises due to the Hop Count Analysis Method, although it may be lowered with the use of additional secret tunnels and faster node movement.

M. M. Gaber and M. A. Azer (2022) Mobile ad hoc networks (MANETs) were infrastructure-free, decentralized networks. Because of their unique nature, they were vulnerable to a broad range of attacks, especially at the network level. The author investigate how the Blackhole assault impacts AODV-based MANETs in this study. Author compares AODV routing protocol without Blackhole assault to AODV routing protocol with Blackhole assault and finds it has negative effect on single and multiple connections in random mobility. The following metrics were used to assess the network's performance: It was important to measure things like throughput, packet dropping ratio, routing cost, and packet delivery success rate.

2.5 Survey on Malicious Nodes

N. Panda and M. Supriya (2022) This article's experimental study paints a credible picture of how IPv6-based IoT networks react to a blackhole assault. There will be a drop in performance throughout the assault, as measured by PDR, average latency, control overhead, and total energy consumption. Nodes attacking from higher positions in the network will suffer more severe routing failure and data loss if the subnet was big. The negative impacts of such an attack on a network's overall performance only worsen as its size grows. The security flaws in the 6LoWPAN RPL protocol have various network-wide consequences. To boost resilience in the face of an adversary node, the OFs alternate between a fixed and a mobile network.

Q. Li (2022) Finally, a prediction link in the controller structure was necessary when employing a neural network for energy saving control due to the characteristics of too complex variables during operation. This was done to guarantee that the central air-conditioning system of buildings can understand the characteristics of environmental changes in real time and adjust the parameters accordingly. In addition, a plan was presented for controlling VAV HVAC units. Fuzzy neural network based predictor with nonlinear parameter connections for electrical energy savings control purpose. This predictor may autonomously adapt the system's stability in response to variations in the degree of disturbance in the environment.

S. Haider (2020) Human error may be discovered, avoided, and managed by designing aircraft systems carefully. To assure a new aircraft's safety in the dynamic aviation environment, more consideration of the multiple failure scenarios that may develop over the course of its prolonged life cycle was required. It was possible to utilize systems in ways that were not intended. Because intended safety barriers may fail or lose efficiency throughout the course of a system's lifespan, designers must account for possible vulnerabilities that may jeopardize safety.

S. Ibrahimy et al. (2022) This study looked at the impact of Blackhole attacks and mobility on RPL-based networks. Multiple simulations were done to evaluate which routing parameters in a mobile network were most influenced by rogue nodes. The data analysis shows that the blackhole attack has a detrimental influence on network performance in a mobile scenario.

S. Kumar et al. (2022) Safe and secure travel in ITS relied heavily on the security of VANETs. Threats to the VANETs' availability, confidentiality, integrity, and privacy came from both within and outside the network. As many VANET processes are disrupted by Sybil attacks, they might be deadly. Sybil attacks may take three forms: identities, communication, and involvement. To identify these many forms of Sybil vulnerabilities, several approaches such as central authentication, cryptography-based, trust-based, resource testing, and localization-based have been suggested. However, none of them were successful in detecting all Sybil versions.

Table 1: Comparison table for existing work

Author	Year	Methodology	Advantage	Limitation
A.U. Khan et al.	2021	Absence of security mechanism	The paper's design and analysis of critical network layer attacks, such as black-hole (BH), gray-hole (GH), and worm-hole (WH) assaults, provide the area of Mobile Adhoc Network (MANET) security a substantial edge.	One major shortcoming of the article was the lack of a complete assessment of additional potential network layer assaults that might endanger the AODV protocol.
C. Sharma and R. Vaid	2021	Elliptic curve Cryptography	The use of multipath routing using the AOMDV protocol improves network resilience and data availability even more. DH-SAM increases the robustness of the communication infrastructure in WSNs by offering numerous alternative pathways to transmit data packets to the destination.	The DH-SAM algorithm's dependence on the Diffie-Hellman key exchange for secure communication between sensor nodes was one possible shortcoming.
D. J. Richter and R. A. Calix	2022	Double Deep Q-Learning	The use of DRL in aircraft attitude control might lead to more efficient and adaptable flight control systems.	Aviation was a safety-critical area, and any use of DRL for flight control had to provide the greatest standards of safety and dependability.
K. A. Awan et al.	2023	federated learning	FedTrust provides a less computationally demanding approach to trust management than previous cryptographic approaches.	The FedTrust approach's dependence on the availability and quality of the trust dataset was one possible weakness. Because trust management is primarily reliant on data, the FedTrust model's efficacy is strongly reliant on the quality and reliability of the data used for training.
N. Panda and M. Supriya	2022	Low Power Lossy Networks	The assessment of blackhole assaults was carried out in both static and mobile contexts, resulting in a thorough knowledge of the attack's impacts under various network scenarios.	One major weakness of the report was its emphasis on blackhole attacks, which were just one of several potential security concerns in IoT networks. While the examination of blackhole attacks proved useful, the larger landscape of security concerns in LLNs should also be taken into account.

S. Radhika et al. (2023) In most circumstances, the efficiency of a WSN was degraded because a gray hole attacker node discards data packets indiscriminately. Using more traditional approaches, it was difficult to

discover gray hole attacker nodes in WSN. In order to strengthen data integrity and make gray hole attack detection easier, the author of this research proposes a hash signature technique. In this scenario, a hash signature approach was utilized to look for the gray hole attack on the network. The destination node received the transmission and validated the sensor node's signature. Whether or not the signature matches affected how the receiving node would react to the message. The packet's size and PCC are checked at the receiving node.

2.6 Survey on Q-Learning

S. -W. Lin and C. -C. Chu (2023) Distributed control in isolated MGs using a model-free data-driven Q-learning approach for autonomous voltage restoration under saturated input signals was presented.

Y. Elnadi et al. (2021) Because of the Internet of Things and other technological breakthroughs, the internal environmental parameters of a smart greenhouse may be monitored, managed, and controlled. A Networked Control System (NCS) enables for both on-site and off-site (remote) control, boosting the production and efficiency of the smart greenhouse. The author investigates a Greenhouse NCS made of Wi-Fi sensors and access points that can gather data on a variety of environmental stimuli. Switched Ethernet was used to provide sensor data to a controller, which then connects with wired actuators to carry out the controller's actuation decisions. The model also includes a number of security cameras that transmit data to the controller through the Internet.

Y. Wang and M. Tan (2023) This study delves into the potential drawbacks of blockchain technology to sybil attacks, examines the shortcomings of current security techniques against sybil attacks, and suggests a revised PBFT algorithm to counter them. By including the assessment findings with the voting weight in the PBFT algorithm, this technique increases the system's reliability and security by accurately identifying Sybil nodes. In order to assess and rank the nodes in the network, it makes use of the reputation evaluation method established by the Proof of Stake. Based on our experiments, we can conclude that the strategy is very effective, scalable, and resistant to Sybil attacks. As a result, this method might be a valuable tool for safeguarding distributed systems against Sybil attacks.

Z. Bai et al. (2022) This study proposes a revolutionary MQ-FPA for route planning that effectively overcomes the issue of Q-Learning's slow convergence rate. In the simulation results, the derived Q-value from the FPA was demonstrated to be a good starting point for the mobile robot's training. In the same context, the proposed MQ-FPA was 55.21% and 71.80% more efficient in terms of computation time than Q-Learning. Meanwhile, when compared to Q-Learning, these authors proposed MQ-FPA decreases the driving distance of the optimum route by about 6.21% and 6.96%, respectively.

Z. S. Li et al. (2022) Eliciting requirements now entails frequently evaluating user activities on social media networks. The authors analyzed posts from software-related message boards to learn more about consumers' privacy concerns and the evolution of these issues over time. The author collected this information from several software-related communities on Reddit. The authors' method of categorizing privacy-related postings and grouping them into nine major sections greatly facilitated our ability to locate the many debates pertaining to privacy. The author found that people's attitudes about privacy were influenced by stories.

3. Discussion

For MANETs targeted by hostile nodes, the Reputation-Based Opportunistic Routing Protocol (RORP) with Q-Learning improves network resilience and dependability. RORP uses reputation-based routing to let nodes to make educated judgments about which neighbors to trust for data forwarding, thereby isolating hostile nodes and preventing their disruptive behaviors. The addition of Q-Learning to the protocol provides flexibility and intelligence, enabling nodes to dynamically alter their routing choices depending on observable rewards and penalties. RORP can learn and optimize its routing algorithms over time thanks to this reinforcement learning mechanism, which improves the network's capacity to adapt to changing circumstances and adversarial assaults. However, the efficiency of RORP is dependent on the accuracy of reputation evaluations and the proper choice of Q-Learning parameters, which may pose difficulties in real-world deployments. Nonetheless, the protocol's ability to drastically reduce the effect of rogue nodes while also improving MANET overall performance makes it a viable route for safeguarding mobile ad hoc networks against dynamic threats.

4. Conclusion

Finally, the Reputation-Based Opportunistic Routing Protocol (RORP) with Q-Learning marks an important step forward in protecting MANETs against malicious node assaults. Its reputation-based approach and reinforcement learning mechanism enable the protocol to adapt and react to constantly changing network dynamics. As mobile ad-hoc networks continue to play an important role in a variety of applications, RORP provides a viable path toward developing more secure and reliable communication frameworks in the face of growing security issues. RORP has the potential to greatly improve the trustworthiness and efficiency of MANETs with continuous study and development, opening the door for more secure and robust communication in dynamic and difficult contexts. While RORP shows considerable potential, its actual implementation confronts difficulties such as accurate reputation assessments, balancing reputation updates, and optimizing Q-Learning settings. More study and testing are required to fine-tune the technique and evaluate its efficacy in a variety of real-world circumstances.

References

[1] A.Afdhal, A. Ahmadiar and R. Adriman, "Sybil Attack Detection on ITS-V2X System using a Realistic Traffic Model-based Approach," 2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT), Solo, Indonesia, 2022, pp. 333-338, doi: 10.1109/COMNETSAT56033.2022.9994541.

[2] A.U. Khan, M. D. Chawhan, M. M. Mushrif and B. Neole, "Performance Analysis of Adhoc On-demand Distance Vector Protocol under the influence of Black-Hole, Gray-Hole and Worm-Hole Attacks in Mobile Adhoc Network," 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2021, pp. 238-243, doi: 10.1109/ICICCS51141.2021.9432072.

[3] B. S. Rani and K. Shyamala, "Secure EELB-AOMDV Protocol to Mitigate Blackhole Attack," 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2023, pp. 589-592, doi: 10.1109/ICACCS57279.2023.10112747.

[4] B. V. Sherif and P. Salini, "Effective and Prominent Approaches for Malicious Node Detection in MANET," 2021 International Conference on Computational Intelligence and Computing Applications (ICCICA), Nagpur, India, 2021, pp. 1-6, doi: 10.1109/ICCICA52458.2021.9697234.

[5] C. Shang, L. Zhao, Y. Zheng and L. Liu, "Study on the Influence of Learners' Trust and Privacy Concerns on the Willingness to Use Online Learning Platforms," 2021 International Conference on Big Data, Artificial Intelligence and Risk Management (ICBAR), Shanghai, China, 2021, pp. 163-167, doi: 10.1109/ICBAR55169.2021.00041.

[6] C. Sharma and R. Vaid, "A Novel Sybil Attack Detection and Prevention Mechanism for Wireless Sensor Networks," 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 2021, pp. 340-345, doi: 10.1109/ISPCC53510.2021.9609450.

[7] D. Cui, Z. Quan and Y. Piao, "An Effective Method for Privacy Concerns on Digital Contact Tracing Protocols," 2022 5th International Conference on Pattern Recognition and Artificial Intelligence (PRAI), Chengdu, China, 2022, pp. 1125-1129, doi: 10.1109/PRAI55851.2022.9904273.

[8] D. J. Richter and R. A. Calix, "Using Double Deep Q-Learning to learn Attitude Control of Fixed-Wing Aircraft," 2022 16th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), Dijon, France, 2022, pp. 646-651, doi: 10.1109/SITIS57111.2022.00102.

[9] D. Rastogi, M. Jain, M. M. Rayguru and S. K. Valluru, "Intelligent Control of Mobile Robots with ANN Assisted Improved Q-learning: IQ-CRL Algorithm," 2023 IEEE IAS Global Conference on Emerging Technologies (GlobConET), London, United Kingdom, 2023, pp. 1-6, doi: 10.1109/GlobConET56651.2023.10150049.

[10] D. Zala, D. Thummar and B. R. Chandavarkar, "Mitigating Blackhole attack of Underwater Sensor Networks," 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2021, pp. 1-8, doi: 10.1109/ICCCNT51525.2021.9579473.

[11] E. D. Benedetto and A. Cucchi, "A bibliometric analysis of privacy concerns," 2022 3rd International Conference on Next Generation Computing Applications (NextComp), Flic-en-Flac, Mauritius, 2022, pp. 1-7, doi: 10.1109/NextComp55567.2022.9932220.

[12] G. Kaur, M. Khurana and A. Kaur, "Gray Hole Attack Detection and Prevention System in Vehicular Adhoc Network (VANET)," 2022 3rd International Conference on Computing, Analytics and Networks (ICAN), Rajpura, Punjab, India, 2022, pp. 1-6, doi: 10.1109/ICAN56228.2022.10007192.

[13] H. Hamann and A. Reina, "Scalability in Computing and Robotics," in IEEE Transactions on Computers, vol. 71, no. 6, pp. 1453-1465, 1 June 2022, doi: 10.1109/TC.2021.3089044.

[14] I.R and A. R. K. P, "SOLSR: Secure OLSR with denial contradiction rules to detect and prevent gray hole attack in VANET," 2021 International Conference on Communication, Control and Information Sciences (ICCISc), Idukki, India, 2021, pp. 1-7, doi: 10.1109/ICCISc52257.2021.9484993.

[15] J. Ryu and S. Kim, "Reputation-Based Opportunistic Routing Protocol Using Q-Learning for MANET Attacked by Malicious Nodes," in IEEE Access, vol. 11, pp. 47701-47711, 2023, doi: 10.1109/ACCESS.2023.3242608.

[16] K. A. Awan, I. Ud Din, M. Zareei, A. Almogren, B. Seo-Kim and J. A. Pérez-Díaz, "Securing IoT With Deep Federated Learning: A Trust-Based Malicious Node Identification Approach," in IEEE Access, vol. 11, pp. 58901-58914, 2023, doi: 10.1109/ACCESS.2023.3284677.

[17] K. Bala, J. Paramesh, K. J. Elma and S. T. Santhanalakshmi, "An Intrusion Detection System for MANET to Detect Gray Hole Attack using Fuzzy Logic System," 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2023, pp. 941-945, doi: 10.1109/IDCIoT56793.2023.10053550.

[18] L. Darwish, M. Nassr, F. Ghosna, H. M. Fardoun, D. K. Voronkova and M. Anbar, "Malicious Node Detection in Wireless Sensor Networks: Comparative Study," 2023 5th International Youth Conference on Radio Electronics, Electrical and Power Engineering (REEPE), Moscow, Russian Federation, 2023, pp. 1-5, doi: 10.1109/REEPE57272.2023.10086790.

[19] L. E. Buck and B. Bodenheimer, "Privacy and Personal Space: Addressing Interactions and Interaction Data as a Privacy Concern," 2021 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Lisbon, Portugal, 2021, pp. 399-400, doi: 10.1109/VRW52623.2021.00086.

[20] M. Bashir, S. Tahir, M. F. Almufareh, B. Hamid and F. Qamar, "Wormhole Attack Detection Technques In MANET," 2023 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 2023, pp. 1-7, doi: 10.1109/ICBATS57792.2023.10111269.

[21] M. D. Chawhan et al., "Prevention of Jamming Attacks in MANET," 2023 11th International Conference on Emerging Trends in Engineering & Technology - Signal and Information Processing (ICETET - SIP), Nagpur, India, 2023, pp. 1-5, doi: 10.1109/ICETET-SIP58143.2023.10151635.

[22] M. D. Chawhan, K. Karmarkar, G. Almelkar, D. Borkar, K. D. Kulat and B. Neole, "Identification and prevention of Gray hole attack using IDS mechanism in MANET," 2022 10th International Conference on Emerging Trends in Engineering and Technology - Signal and Information Processing (ICETET-SIP-22), Nagpur, India, 2022, pp. 1-6, doi: 10.1109/ICETET-SIP-2254415.2022.9791594.

[23] M. Knaj, M. Anbar, F. Ghosna, M. Nassr and D. K. Voronkova, "Detecting and Mitigating Wormhole Attack Effect in MANETs Based on Hop Count Technique," 2023 5th International Youth Conference on Radio Electronics, Electrical and Power Engineering (REEPE), Moscow, Russian Federation, 2023, pp. 1-5, doi: 10.1109/REEPE57272.2023.10086929.

[24] M. M. Gaber and M. A. Azer, "Blackhole Attack effect on MANETs' Performance," 2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC), Cairo, Egypt, 2022, pp. 397-401, doi: 10.1109/MIUCC55081.2022.9781680.

[25] N. Panda and M. Supriya, "Blackhole Attack Impact Analysis on Low Power Lossy Networks," 2022 IEEE 3rd Global Conference for Advancement in Technology (GCAT), Bangalore, India, 2022, pp. 1-5, doi: 10.1109/GCAT55367.2022.9971814.

[26] Q. Li, "Research on Energy Saving Control of Building Central Air Conditioning Based on Neural Network," 2022 International Conference on Machine Learning, Computer Systems and Security (MLCSS), Bhubaneswar, India, 2022, pp. 59-62, doi: 10.1109/MLCSS57186.2022.00019.

[27] R. Zhao, S. Wang and H. Wen, "A Scheme for Detecting Malicious Nodes in UAV Clusters Based on Community Division," 2022 8th Annual International Conference on Network and Information Systems for Computers (ICNISC), Hangzhou, China, 2022, pp. 222-226, doi: 10.1109/ICNISC57059.2022.00053.

[28] S. Haider, "Ensuring Aircraft Safety In Single Point Failures, Automation and Human Factors," 2020 Annual Reliability and Maintainability Symposium (RAMS), Palm Springs, CA, USA, 2020, pp. 1-6, doi: 10.1109/RAMS48030.2020.9153682.

[29] S. Ibrahimy, H. Lamaazi and N. Benamar, "Mobility-Aware RPL Network Assessment under a Blackhole Attack," 2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sakheer, Bahrain, 2022, pp. 541-546, doi: 10.1109/3ICT56508.2022.9990638.

[30] S. Kumar, A. Vasudeva and M. Sood, "Sybil Attack Countermeasures in Vehicular Ad Hoc Networks," 2022 International Conference on Communications, Information, Electronic and Energy Systems (CIEES), Veliko Tarnovo, Bulgaria, 2022, pp. 1-6, doi: 10.1109/CIEES55704.2022.9990799.

[31] S. Radhika, M. Srikanth, K. Anand, K. Saravanan and S. Sree Southry, "Improving Data Integrity for Gray Hole Attack Detection by using a Hash Signature Algorithm in WSN," 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2023, pp. 619-623, doi: 10.1109/ICSSIT55814.2023.10061102.

[32] S. -W. Lin and C. -C. Chu, "Distributed Q-Learning Secondary Voltage Control of Isolated AC Microgrids with Saturated Input," 2023 IEEE/IAS 59th Industrial and Commercial Power Systems Technical Conference (I&CPS), Las Vegas, NV, USA, 2023, pp. 1-5, doi: 10.1109/ICPS57144.2023.10142088.

[33] T. N. Tran, T. -V. Nguyen, K. Shim and B. An, "An Optimal QoS Multicast Routing Protocol in IoT Enabling Cognitive Radio MANETs: A Deep Q-Learning Approach," 2021 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Jeju Island, Korea (South), 2021, pp. 279-283, doi: 10.1109/ICAIIC51459.2021.9415188.

[34] Y. Elnadi, T. Refaat, R. Daoud and H. Amer, "Fault Tolerance for Access Point Failures in Smart Greenhouse Networked Control Systems," IEEE EUROCON 2021 - 19th International Conference on Smart Technologies, Lviv, Ukraine, 2021, pp. 290-295, doi: 10.1109/EUROCON52738.2021.9535545.

[35] Y. Wang and M. Tan, "Defense against sybil attack in blockchain based on improved consensus algorithm," 2023 IEEE International Conference on Control, Electronics and Computer Technology (ICCECT), Jilin, China, 2023, pp. 986-989, doi: 10.1109/ICCECT57938.2023.10140278.

[36] Z. Bai, H. Pang, M. Liu and M. Wang, "An improved Q-Learning algorithm and its application to the optimized path planning for unmanned ground robot with obstacle avoidance," 2022 6th CAA International Conference on Vehicular Control and Intelligence (CVCI), Nanjing, China, 2022, pp. 1-6, doi: 10.1109/CVCI56766.2022.9964859.

[37] Z. Liu, M. Yu and R. Li, "A Fake Message and Malicious Node Detection Method Using Machine Learning in V-NDN," 2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Rio de Janeiro, Brazil, 2023, pp. 772-777, doi: 10.1109/CSCWD57460.2023.10152557.

[38] Z. S. Li et al., "Narratives: the Unforeseen Influencer of Privacy Concerns," 2022 IEEE 30th International Requirements Engineering Conference (RE), Melbourne, Australia, 2022, pp. 127-139, doi: 10.1109/RE54965.2022.00018.