IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Evolution Of Security Mechanisms In Mobile Ad-Hoc Networks

[1]**K. Sivapriya,** [2]**Dr. N. Revathy,**
[1]Research Scholar, [2] Professor,
[1, 2]Department of Computer Applications (PG),
[1, 2]Hindusthan College of Arts & Science, Sowripalayam,
[1, 2] Coimbatore, Tamil Nadu, India.

Abstract

This explores the evolutionary trajectory of security mechanisms in Mobile Ad-hoc Networks (MANETs), charting the progress from traditional solutions to contemporary approaches. The review encompasses the challenges posed by the dynamic and decentralized nature of MANETs, emphasizing the need for robust security protocols. It delves into early encryption techniques and authentication methods, highlighting their limitations in addressing modern threats. The abstract then navigates through the emergence of intrusion detection systems and cryptographic advancements, outlining their contributions to enhancing network security. Furthermore, it explores recent innovations such as machine learning and fuzzy logic integration, illustrating their potential in mitigating complex security challenges. By examining the historical development and current state of security mechanisms in MANETs, this abstract provides insights into the evolving strategies that researchers employ to fortify these networks against a spectrum of threats, fostering a deeper understanding of the dynamic field of mobile ad-hoc network security.

Keywords: Security protocols, Intrusion detection, Trust management, Routing security, Key management.

1.Introduction

The rapid proliferation of Mobile Ad-hoc Networks (MANETs) in recent years has been accompanied by a surge in security challenges, necessitating a constant evolution of security mechanisms. MANETs characterized by their dynamic and decentralized nature, present a unique set of vulnerabilities that traditional wired networks do not encounter. These networks are particularly susceptible to various security threats, including but not limited to, malicious attacks, data breaches, and unauthorized access due to their open and self-configuring nature.The evolution of security mechanisms in MANETs has been a direct response to the escalating sophistication of cyber threats and the need for robust protective measures. Early MANETs predominantly relied on traditional security mechanisms, which were often insufficient to address the distinctive challenges posed by the network's characteristics. As MANETs operate without a fixed infrastructure and depend on cooperative nodes for routing and communication, the vulnerabilities extend beyond the conventional concerns of wired networks. The applications of Adhoc network are showed in the below [Figure 1].

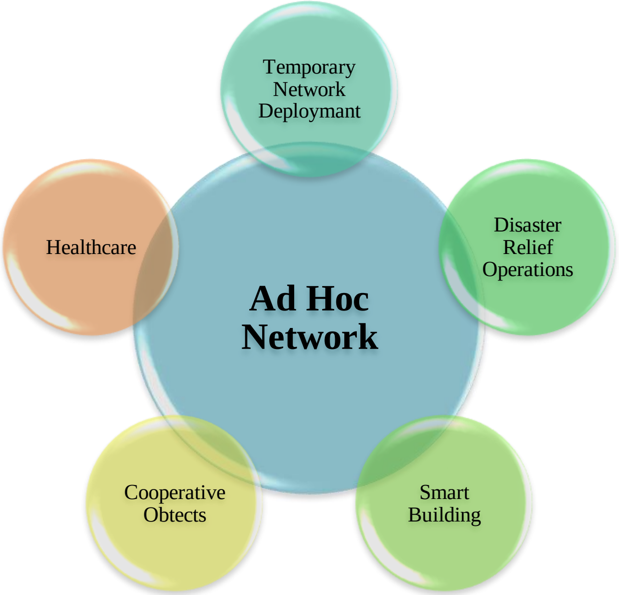

Figure 1. Application of ad hoc network

The security in MANETs primarily focused on securing the routing protocols, given their crucial role in facilitating communication among nodes. However, as attacks became more sophisticated, the scope expanded to encompass various layers of the network stack. The emergence of encryption techniques, intrusion detection systems, and secure key management protocols marked a pivotal shift towards a holistic approach to MANET security.The introduction of adaptive and self-healing security mechanisms became imperative to counteract the dynamic nature of MANETs. Research efforts started incorporating machine learning algorithms to enhance threat detection and response capabilities. Fuzzy logic, with its ability to handle uncertainties and imprecise information, found applications in mitigating security threats by dynamically adapting to changing network conditions.

Furthermore, the evolution of security mechanisms in MANETs extends to the integration of advanced cryptographic techniques, biometric authentication, and anomaly detection. These innovations aim to fortify the network against diverse attacks, including black hole attacks, Sybil attacks, and other malicious activities that compromise the integrity, confidentiality, and availability of communication within the MANET.In this dynamic landscape, this research explores the chronological development and current state of security mechanisms in MANETs, shedding light on the transformative transition from conventional methods to the incorporation of state-of-the-art technologies. Understanding this evolution is vital for comprehending the challenges that persist and for paving the way toward more resilient and secure mobile ad-hoc communication networks.

2. Literature Survey

1.Dhanke J (2024) et.al proposed an Efficient Approach for Prevention of Blackhole Attack in MANET[1]. In the realm of Mobile Ad-Hoc Networks (MANETs), the absence of a fixed infrastructure and central monitoring authority defines its dynamic and decentralized nature, making it widely applicable across various domains. However, this openness introduces security challenges, and one prevalent issue is the Packet Drop Attack, particularly the Blackhole Attack, where an intruder falsely claims to possess the shortest route and drops all packets without forwarding them. This research addresses the mitigation of this security concern, focusing on an optimal solution for the Blackhole Attack. Various techniques, including Opinion-based, Trust-based, Intrusion Detection, Crypto-based, and Destination Sequence Number (DSN) based methods, have been explored by researchers. The proposed method uniquely employs DSN, where the attacker lures packets by sending a forged RREP message to the source node. The suggested solution allows for the rejection of counterfeit RREP messages by comparing the DSN to a threshold value. This innovative approach enhances the security of MANETs, particularly in thwarting Blackhole Attacks. The significance of MANETs in various sectors, ranging from finance to healthcare, underscores the importance of addressing security challenges to ensure the integrity and reliability of communication. The proposed method, through its use of DSN and threshold comparisons, offers a robust solution, demonstrating superior performance in simulations compared to existing approaches. The results showcase a high Packet Delivery Ratio, throughput, and reduced end-to-end delay, reinforcing the efficacy of the proposed scheme in enhancing the security of MANETs against Blackhole Attacks.

Merits

1. The proposed scheme not only thwarts single Blackhole attacks but also cooperative Blackhole attacks.

Demerits

1. Security vulnerabilities, potential data breaches, and increased susceptibility to attacks.

2. Pandian E (2024) et.al proposed Fuzzy Heuristics for Detecting and Preventing Black Hole Attack[2]. This research addresses security concerns in Mobile Ad-hoc Networks (MANETs), where the lack of fixed infrastructure and dynamic topology pose challenges, especially in relation to attacks by black holes. For the purpose of detecting black hole attacks, a novel fuzzy inference approach is put forth that prioritizes node authentication, Certificate Authority (CA), energy levels, and trust value, and message integrity. The focus is on node authentication before initiating the route discovery process in MANETs, crucial for preventing black hole attacks. Through simulations in the Network Simulator (NS2), the fuzzy inference system demonstrates superior performance by providing certificates only to trusted nodes, aiding in the detection and prevention of malicious nodes. The results show enhanced Packet Delivery Ratio (PDR), throughput, and reduced end-to-end delay, indicating the reliability and suitability of the proposed system. The research recognizes the importance of secure communication in MANETs, particularly in military applications, and the proposed methodology presents a comprehensive solution by combining CA and fuzzy-based analysis for improved security and robust detection of black hole attacks. The proposed approach exhibits a 20% improvement in identification ratios compared to existing techniques, emphasizing its efficacy in enhancing the security of MANETs.

Merits

1. The proposed fuzzy inference system enhances MANET security by prioritizing node authentication, CA, energy levels, trust, and message integrity.

Demerits

1. The fuzzy inference system's computational complexity and resource requirements may pose challenges in resource-constrained MANET environments.

3. Reshi IA (2024) et.al proposed mitigating Black Hole Attacks with an Innovative Defense Algorithm[3]. A new era of interconnected possibilities and creativity has been brought about by the Internet of Things' (IoT) and Wireless Sensor Networks' (WSNs) rapid spread. The transition from IPv4 to IPv6, facilitated by advancements in networking technology and nano devices, has further improved connectivity, allowing a broader range of devices to connect to servers. However, this increased interconnectivity poses challenges in efficiently managing and analyzing the vast amount of data generated across all levels of the IoT. Security management is particularly critical for IoT devices, given their large quantity and small size. Within the layered architecture of IoT, the network layer plays a pivotal role in ensuring security, responsible for storing routing information and executing corresponding decisions. The Black Hole attack emerges as a significant concern among security threats, prompting a comprehensive examination of its consequences on IoT networks and the development of a novel mitigation algorithm. Simulations using NS2 and SimuLink evaluate the proposed algorithm's effectiveness, showcasing a substantial improvement in throughput and a Packet Delivery Ratio (PDR) of 98.21%. This demonstrates how well the algorithm worked to lessen the negative consequences of the Black Hole attack on IoT networks, offering insightful information for improving network security in complex IoT deployments.

Merits

1. Improved connectivity with IPv6 enhances the range of devices in IoT.

Demerits

1. Security challenges, especially the Black Hole attack, pose threats to IoT networks' integrity and performance.

4. Mankotia V (2023) et.al proposed (DT-AODV) a Dynamic threshold protocol against black-hole attack in MANET[4]. Mobile Ad-hoc Networks (MANETs) represent a dynamic and decentralized wireless technology where autonomous mobile nodes can freely join or leave the network. In this environment, nodes interact through intermediaries without relying on a fixed infrastructure. However, the presence of dishonest nodes can compromise the network's integrity, particularly through black-hole attacks, where malicious nodes provide false route replies, leading to packet drops and performance degradation. The research uses dynamic threshold values to propose a Dynamic Threshold-Ad-hoc On-Demand Distance Vector (DT-AODV) protocol in order to overcome this. Using the NS-2 simulator, the proposed protocol is evaluated against the MBDP-AODV protocol under black-hole attacks. The results showcase the effectiveness of DT-AODV, achieving a 99.10% packet delivery rate, 20.01 kbps throughput, 1750 routing overhead, and 0.51 normalized routing loads. The security concern of black-hole attacks in MANETs is crucial, and DT-AODV proves to be a promising solution, outperforming existing protocols and demonstrating its robustness in ensuring reliable communication in the face of such malicious threats.

Merit

1. DT-AODV enhances MANET security with dynamic threshold values, achieving high packet delivery rates, throughput, and routing efficiency under black-hole attacks.

Demerit

1. Protocol complexity may pose implementation challenges, and the dynamic nature could introduce overhead in certain scenarios.

5. Shafi S (2023) et.al proposed Machine Learning and Trust Based AODV Routing Protocol to Mitigate Flooding and Blackhole Attacks in MANET[5]. In the realm of wireless networks, Mobile Ad-hoc Networks (MANETs) have emerged as a dynamic and pervasive technology, comprising autonomous mobile nodes capable of freely joining or leaving the network. In this decentralized network, mobile nodes interact through intermediate nodes without relying on a fixed infrastructure. However, the inherent openness of MANETs exposes them to security challenges, notably the black-hole attack—an active attack where a dishonest node provides false route replies, claiming to have the shortest path for destination nodes with maximum destination sequence numbers. This malicious activity attracts data traffic, leading to packet dropping and degradation of network performance. To address this security concern, this research proposes the Dynamic Threshold-Ad-hoc On-Demand Distance Vector (DT-AODV) protocol, which incorporates a dynamic threshold value for destination sequence numbers. The NS-2 simulator is employed to evaluate the protocol's performance, demonstrating its effectiveness under black-hole attacks with a 99.10%20.01 kbps throughput, 0.51 normalized routing load, 1750 routing overhead, and packet delivery rate. MANETs, being temporary networks with movable nodes, face security challenges, and the proposed DT-AODV protocol proves to be a robust solution against black-hole attacks, showcasing superior performance compared to existing protocols. The dynamic threshold mechanism contributes to enhanced security, making DT-AODV a promising approach for securing MANETs against active attacks.

Merits

1. DT-AODV enhances MANET security with dynamic thresholds, achieving high packet delivery, throughput, and reduced routing overhead.

Demerits

1. Potential complexity in dynamic threshold adjustment may require careful tuning for optimal performance.

6. Kanaparthi VM (2024) et.al analyzed Greyhole attack in mobile ad-hoc network mitigation and protection[6]. Mobile ad-hoc systems operate as transient, infrastructure-fewer networks where identification base stations are connected using a cable design. In this dynamic networking paradigm, devices have the autonomy to travel or migrate freely, with every gadget serving as both a traffic mover and a router. Mobile ad-hoc networks (MANETs) exhibit characteristics like self-organization, router functionality, and high mobility, but they are vulnerable to service denial threats. Limited resources, including throughput, power consumption, and storage, add to the challenges in MANETs. The grayhole attack emerges as a disruptive force in this context, intentionally disrupting the entire platform's functionality. This article proposes a method to combat grayhole attacks and enhance network system parameters such as throughput, drop incidence, delivery ratio, and normalization expense transportation. MANETs, characterized by their absence of centralized management and dispersed collaboration, have various applications, spanning from emergency personnel to industrial settings. The proposed method efficiently addresses the challenges posed by grayhole attacks in AODV values, employing improved blacklisting judgments and tracking behavioral intentions. The approach integrates a high-speed Intrusion Detection System (IDS) to identify and prevent grayhole attacks, demonstrating promising detection rates and packet delivery ratios in numerical simulations. Future work aims to enhance recognition accuracy in high network congestion scenarios. Overall, the proposed method contributes to the resilience and security of MANETs against grayhole attacks, ensuring their reliability in diverse environments.

Merit

1. The proposed method enhances network security, throughput, and delivery ratio, effectively combating greyhole attacks in MANETs.

Demerit

1. Potential drawbacks include increased computational overhead and reliance on behavioral analysis for attack identification.

7. Alabdulatif A (2024) et.al developedBlockchain Based Smart Contractsfor mitigating blackhole and greyhole routing Attacks in Vehicular Ad Hoc Networks[7]. The escalating vehicular traffic in modern societies necessitates innovative solutions to alleviate congestion and enhance traffic management efficiency. Intelligent Transportation Systems (ITS) have emerged as a revolutionary technology, providing real-time information on vehicle traffic and transportation systems. However, the utilization of Vehicular Ad Hoc Networks (VANETs) in IT'S introduces routing challenges at the network layer, leading to complex communication networks and vulnerabilities to routing attacks. Addressing these issues, this research proposes a Blockchain-based smart contracts model to bolster security in VANETs, specifically focusing on routing in ITS. The model employs Self-Classification Blockchain-Based Contracts (SCBC) and Voting-Classification Blockchain-Based Contracts (VCBC). Results indicate that VCBC outperforms SCBC in Packet Delivery Ratio (PDR) and Throughput (TP) performance, even in the face of Blackhole and Grayhole attacks. The robustness of the proposed model lies in its dual smart contract approach, with SCBC offering a baseline and VCBC leveraging blockchain-stored miner votes for enhanced source car awareness. This heightened awareness in VCBC contributes to superior PDR performance, showcasing its efficacy in mitigating routing issues. The encouraging findings suggest potential applications in other Ad Hoc Networks, and future research could further validate and refine these results, potentially incorporating machine learning methods for a more comprehensive evaluation.

Merits

1. Blockchain-based smart contracts enhance VANET security, mitigate routing attacks, and improve trust among vehicles, ensuring reliable data relay.

Demerits

1. Increased routing overhead in SCBC, potential complexity in implementation, and the need for further research to validate findings.

8.Mankotia EV (2023) et.al proposed aDual Security Based Protocol against Gray-Hole Attack in MANET[8]. In this research, the focus is on addressing security concerns in Mobile Ad-hoc Networks (MANETs), particularly in the context of gray-hole attacks, where malicious nodes intentionally drop data packets, posing a threat to communication within the network. Two security methods are proposed by the suggested approach, Dual Security Ad-hoc On-Demand Distance Vector (DS-AODV), to counter both sequence number-based gray-hole attacks during the path discovery stage and smart gray-hole attacks during the data transmission phase. The efficacy of DS-AODV is evaluated using the NS-2.35 simulator, showcasing superior performance compared to existing approaches. With a 98.20% packet delivery rate and a throughput of 19.73 kbps, DS-AODV, augmented with four Intrusion Detection System (IDS) nodes, demonstrates its effectiveness in securing MANETs. The research also highlights the evolving nature of gray-hole attacks and emphasizes the importance of dual security mechanisms to address both types of threats. As a forward-looking perspective, the authors suggest exploring innovative technologies such as blockchain, machine learning, deep reinforcement learning, or distributed ledger technology for achieving secure and efficient network operations in the future. This comprehensive approach reflects the commitment to advancing the security of MANETs through a dual-layered defense strategy and integrating cutting-edge technologies for enhanced protection.

Merits

1. DS-AODV enhances MANET security against both gray-hole attacks during route discovery and data transmission stages, ensuring robust protection.

Demerits

1. Implementing dual security mechanisms may incur higher computational overhead and resource utilization in the network.

9. Khosa TN (2023) et.al proposed A Model to Prevent Gray Hole Attack in Mobile Ad-Hoc Networks[1]. In recent years, the significance of Mobile Ad-hoc Networks (MANET) has surged due to their ability to operate in decentralized, infrastructure-independent environments with dynamic topologies, making them ideal for ubiquitous networks. However, this very flexibility exposes MANETs to various network attacks, particularly Denial of Service (DoS) attacks like black hole and grayhole attacks. While existing secured routing protocols have been proposed, the often fall short in guaranteeing security against these sophisticated threats. This research introduces the Gray Hole Prevention (GRAY-HP) algorithm, a novel approach that enhances node classification accuracy in detecting malicious nodes. Utilizing a proactive plan and the Secure Detection Prevention and Elimination Gray Hole (SDPEGH) approach, GRAY-HP performs better than other algorithms like Genetic Algorithm to Bacterial Foraging Optimization (GA-BFO) and Rough Set Theory (RSetTheory) in terms of throughput, routing overhead, and delivery ratio, as demonstrated via simulations using Network Simulator 2 (NS2). The integration of SDPEGH and the proactive scheme ensures not only the successful elimination of grayhole nodes but also avoids false exclusion of legitimate nodes. The simulation results reveal a significant improvement in network throughput, delivery ratio, and routing overhead, showcasing the effectiveness of the proposed GRAY-HP algorithm in securing MANETs without compromising Quality of Service (QoS). This research lays the groundwork for future investigations into addressing other types of attacks on MANET, such as Black hole, Selfish, Wormhole, and Jellyfish attacks, opening avenues for further algorithmic enhancements and network security advancements.

Merits

1. GRAY-HP algorithm significantly improves MANET security with high throughput, delivery ratio, and reduced routing overhead, enhancing overall performance.

Demerits

1. Integration of multiple algorithms may lead to increased complexity and resource utilization in the proposed GRAY-HP solution.

10. Tropea M (2023) et.al proposed an (SecGPSR) secure GPSR protocol for FANET against Sybil and Gray Hole Attacks[10]. In recent years, the exponential rise of drones in diverse applications has underscored the need for robust communication within Fly Ad-hoc Networks (FANETs). Unfortunately, many existing routing protocols in these networks lack built-in security measures, posing significant vulnerabilities. This research addresses two formidable routing attacks, Sybil and Gray Hole, and proposes mitigating techniques within the context of the Greedy Perimeter Stateless Routing Protocol (GPSR). The resulting solution, secGPSR, enhances the GPSR by introducing security measures to thwart malicious activities. The security challenges inherent in FANETs are particularly pronounced due to the high mobility of Unmanned Aerial Vehicles (UAVs). The research emphasizes the necessity of dynamic connectivity and adaptive routing protocols to contend with the rapid node changes in the network topology. Notably, secGPSR tackles the Sybil threat by extending the GPSR's beacon packet with a digital signature, employing the ECDSA for drone authentication. Simultaneously, the Gray Hole attack is combated by introducing trustworthiness metric to identify and neutralize drones behaving maliciously. The effectiveness of secGPSR is validated through simulations using Omnet++, demonstrating its efficacy in countering Sybil and Gray Hole attacks without imposing undue overhead on the drones. This research contributes significantly to the development of secure FANET routing protocols, paving the way for the deployment of drones in critical applications with heightened confidence in their communication integrity.

Merits

1. SecGPSR enhances FANET security against Gray Hole and Sybil attacks, maintaining efficiency without imposing significant overhead on drones.

Demerits

1. Implementation complexity may increase, requiring thorough integration and potential resource implications for drones in certain scenarios.

11. Ryu J (2024) et.al proposed Trust System-and Multiple Verification Technique-based Method for Detecting Wormhole Attacks in MANETs[11]. The surge in wireless mobile devices has fueled the prominence of Mobile Ad Hoc Networks (MANETs), where networks form without infrastructure assistance. However, this technological advancement has led to an array of attacks, with routing attacks like wormhole attacks exploiting MANET vulnerabilities. Detecting such attacks is challenging as don't directly damage networks. In response, it suggests a brand-new, trust-system-based technique for multiple verification-based wormhole attack detection. Nodes' credits are measured based on trust levels, reduced for suspicious nodes during routing, and those below a threshold are deemed malicious. The trust system is implemented using reinforcement learning, enhancing accuracy over time. Simulation experiments in densely populated environments showed a significant reduction in traffic passing through paths with malicious nodes. MANETs' vulnerability lies in their handling of node failures, making them susceptible to routing attacks like wormholes. The proposed Q-learning-based algorithm dynamically adjusts Q-values during routing suspicion, identifying and excluding malicious nodes for stable routing. Notably, this method is adaptable to various routing protocols, making it suitable for general MANETs and sensitive networks like underwater sensor networks. Despite successful avoidance of wormhole tunnels in simulations, practical challenges remain in notifying all nodes simultaneously. Future efforts will focus on efficient dissemination of threat data, leveraging relay nodes, broadcast mechanisms, or clustering techniques to enhance the method's effectiveness in securing MANETs against wormhole attacks.

Merits

1. Novel Q-learning-based method enhances MANET security, adaptable to various routing protocols, reduces traffic through wormhole paths effectively.

Demerits

1. Challenges in disseminating threat data to all nodes simultaneously, limited success in restricting nodes passing through the tunnel below 10%.

12. Majumder S (2024) et.al proposed Cryptic-AODV for Mitigation of Wormhole attack in MANET[12]. This research addresses the security concerns inherent in Mobile Ad-hoc Networks (MANETs), focusing on the dynamic topology and vulnerability to security threats.It proposes CRYPTIC-AODV, a novel cryptographic Ad-Hoc on Demand Distance Vector (AODV) routing protocol. Utilizing Dijkstra's algorithm for path calculation, the protocol employs a hash function technique to safeguard data packets within network nodes. Through decryption and validation, secure data packets traverse nodes until reaching the destination. Comparative analysis against existing protocols (DSR, DSDV, and ZRP) demonstrates that CRYPTIC-AODV enhances security and efficiency, showing improved throughput, reduced end-to-end delay, and increased data transfer success rates, particularly in the presence of Wormhole attacks. In the broader context of MANET security challenges, this research introduces a comprehensive security scheme addressing attack prevention and classification. Within the AODV network, Cryptic-AODV uses Elliptic Curve Cryptography (ECC) for data encryption and decryption. A dual approach, rooted in transductive learning, is employed for both preventing and detecting attacks through k-centroids and hyper-alerts. Thorough evaluation of the Cryptic-AODV scheme focuses on attack detection and classification, achieving an impressive 98% overall accuracy rate within the Software-Defined Networking (SDN) framework. The proposed model showcases the effectiveness of cryptography-based security measures, contributing to the robustness and resilience of MANETs in dynamic and challenging environments.

Merits

1. CRYPTIC-AODV enhances MANET security with ECC, achieving improved throughput and high attack detection accuracy in SDN environments.

Demerits

1. Potential complexity in implementing cryptographic measures, requiring careful consideration of computational resources and deployment challenges.

13. Reji M (2023) et.al proposed Genetic-based Fuzzy IDS for Feature Set Reduction and Worm Hole Attack Detection[13]. This research addresses the security challenges in wireless ad-hoc networks, particularly focusing on the serious threat of Wormhole attacks. The decentralized and dynamic nature of these networks amplifies security concerns, requiring effective intrusion detection systems (IDS). Traditional preventive measures rely solely on signatures, while reactive measures, including IDS, detect various threats across network layers. However, the calculation of extensive feature sets from ad-hoc networks poses a challenge. This research introduces a genetic algorithm (GA)-based feature reduction approach for IDS, aiming to minimize the wireless feature sets needed to identify Wormhole attacks. The proposed model combines GA-based feature selection with a fuzzy logic system (FLS) for attack detection. Comparative analysis with principal component analysis (PCA) and statistical parametric mapping (SPM) showcases the effectiveness of the genetic approach. Network performance metrics and IDS parameters, such as detection ratio, accuracy, and false alarm rate, are evaluated. The proposed model achieves a notable 95.5% detection ratio with 96.8% accuracy and a minimal false alarm rate of 14%, outperforming existing techniques. The primary focus lies in developing a GA-based feature selection algorithm to identify and select relevant features, reducing the feature set for efficient intrusion detection. This approach yields promising results, with high accuracy and detection rates. Future implementations could extend the model to Internet of Things (IoT) networks, enhancing attack detection capabilities in IoT environments using this IDS model.

Merits

1. Genetic algorithm enhances IDS efficiency, achieving high detection rates and accuracy in minimizing feature sets for wireless ad-hoc network security.

Demerits

1. Potential complexity in implementing and tuning the genetic algorithm, requiring expertise; limited discussion on scalability to IoT networks.

14. Thapar S (2023) et.al proposed An Approach to Detect Wormhole Attack in Mobile Ad Hoc Networks Using Direct Trust Based Detection Approach[14]. Mobile ad hoc networks (MANETs) find widespread use in various applications, from strategic projects to everyday device connectivity. Their popularity stems from easy setup, dynamic adaptability, and the lack of a formal infrastructure requirement. However, this flexibility comes at the cost of increased vulnerability to cyber-attacks. Wormhole and jellyfish attacks are identified as significant threats to MANETs. This research proposes an integrated approach capable of detecting and mitigating both types of attacks using the same parameters. During a wormhole attack, attackers create a topological deception within the network by establishing a tunnel between malicious nodes. The proposed approach addresses both wormhole and jellyfish attacks simultaneously, offering a unified solution to the challenges posed by these threats. The authors introduce a coordinated strategy that detects and prevents these attacks, leveraging common parameters for both. The research emphasizes the vulnerability of MANETs to various attacks and highlights the need for comprehensive prevention methods. While existing literature proposes individual approaches for wormhole and jellyfish attacks, this research bridges the gap by presenting a combined algorithm capable of addressing both threats simultaneously. The proposed approach is simulated using the NS2 simulator, evaluating its performance with 100 nodes based on end-to-end delay and throughput. The results indicate the effectiveness of the proposed algorithm in detecting and preventing both wormhole and jellyfish attacks, showcasing its robustness across an expanding network.

Merits

1. The integrated approach provides a unified solution for detecting and mitigating both wormhole and jellyfish attacks in MANETs.

Demerits

1. Simulating with 100 nodes may not fully represent real-world scalability, potentially limiting generalization of findings.

15. Rajkumar K (2023) et.al proposed Boomerang packet testing to mitigate wormhole attack in MANET[15]. Mobile Ad-hoc Networks (MANETs) play a crucial role in critical infrastructure areas such as military operations and disaster management, which it is susceptible to security breaches, with the wormhole attack being a notable threat. Wormhole attackers can cause significant harm by dropping data packets, manipulating data, and disrupting routing. This research introduces a novel wormhole mitigation security framework designed to detect and prevent active wormhole attacks in MANET. The main component of the system is choosing an admin node from a list of reliable nodes, which then sends out boomerang packets on a regular basis, the packets ending up back at the admin node. By analyzing the state of the returning boomerang packet, the admin node determines whether a wormhole attack has occurred and implements preventive measures if needed. Extensive experiments conducted in the NS-3.26 simulator demonstrate the effectiveness of the proposed strategy, achieving 97% accuracy in detecting wormhole nodes and minimizing packet loss rates compared to cutting-edge defenses against wormhole attacks. This security framework addresses the challenges posed by wormhole attacks in MANETs, providing a promising solution through early and accurate detection, showcasing its superiority over existing approaches in the literature survey.

Merits

1. Efficient wormhole detection (97% accuracy) and reduced packet loss, enhancing MANET security with a novel admin-node-based boomerang packet approach.

Demerits

1. Dependency on trusted admin nodes may create a single point of failure, and simulation-based results may not fully represent real-world scenarios.

Here's a table comparing the proposed approaches based on their protection against different types of attacks:

Table 1. Comparison of proposed approaches

Researcher & Year	Protocol Name	Blackhole Attack	Greyhole Attack	Wormhole Attack	Sybil Attack	Jellyfish Attack
Dhanke J (2024)	Efficient Approach for Prevention of Blackhole Attack	Yes	No	No	No	No
Pandian E (2024)	Fuzzy Heuristics for Detecting and Preventing Black Hole Attack	Yes	No	No	No	No
Mankotia V (2023)	Dynamic Threshold Protocol (DT-AODV)	Yes	No	No	No	No
Shafi S (2023)	Machine Learning and Trust-Based AODV Routing Protocol	Yes	No	No	No	Yes
Majumder S (2024)	Cryptic-AODV	No	No	Yes	No	No
Ryu J (2024)	Trust System-and Multiple Verification Technique-based Method	No	No	Yes	No	No
Reji M (2023)	Genetic-based Fuzzy IDS	No	No	Yes	No	No
Thapar S (2023)	Direct Trust-Based Detection Approach	Yes	Yes	No	Yes	Yes
Rajkumar K (2023)	Boomerang Packet Testing	Yes	No	Yes	No	No

Here’s a comparison focusing specifically on the machine learning-based approaches proposed in the provided research:

Table 2. Proposed Methods, Merits and Demerits

Researcher & Year	Protocol Name	Attack Mitigated	Machine Learning Method	Performance Metrics
Shafi S (2023)	Machine Learning and Trust-Based AODV Routing Protocol	Blackhole Attack	Utilizes machine learning for trust-based routing, incorporating dynamic thresholds for destination sequence numbers.	High packet delivery rate, throughput, reduced routing overhead, and normalized routing load
Reji M (2023)	Genetic-Based Fuzzy IDS	Wormhole Attack	Introduces genetic algorithm-based IDS for feature set reduction, combining GA-based feature selection with a fuzzy logic system for attack detection.	Achieves high detection rates and accuracy in minimizing feature sets for wireless ad-hoc network security
Ryu J (2024)	Trust System-Based Wormhole Detection	Wormhole Attack	Introduces a trust-system-based technique for detecting wormhole attacks, leveraging node trust levels and reinforcement learning for attack detection.	Adaptable to various routing protocols, reduces traffic through wormhole paths effectively

3. Conclusion

The exploration of the evolution of security mechanisms in Mobile Ad-hoc Networks (MANETs) underscores the continuous efforts to fortify these dynamic and decentralized networks against emerging threats. From traditional cryptographic approaches to more sophisticated intrusion detection systems, the landscape has witnessed a significant transformation. The adaptation of machine learning and fuzzy logic in enhancing security showcases a promising direction, providing dynamic and context-aware defense mechanisms. However, challenges such as scalability, resource constraints, and the need for real-time threat detection persist. The pursuit of innovative solutions must navigate the delicate balance between robust protection and minimizing overhead. As MANETs continue to play a crucial role in modern communication paradigms, the evolution of security mechanisms remains a dynamic process, calling for ongoing research and collaborative efforts to ensure the resilience and reliability of these networks in the face of evolving cyber threats.

4.References

1. Dhanke J, Rastogi S, Singh K, Saxena K, Kumar K, Mishra P. An Efficient Approach for Prevention of Blackhole Attack in MANET. *International Journal of Intelligent Systems and Applications in Engineering*. 2024 Jan 12; 12(12s):743-52.
2. Pandian E, Soundar R, Gunasekaran S, Anantharajan S. Fuzzy Heuristics for Detecting and Preventing Black Hole Attack.
3. Reshi IA, Sholla S, Najar ZA. Safeguarding IoT Networks: Mitigating Black Hole Attacks with an Innovative Defence Algorithm. *Journal of Engineering Research*. 2024 Jan 20.
4. Mankotia V, Sunkaria RK, Gurung S. DT-AODV: A dynamic threshold protocol against black-hole attack in MANET. *Sādhanā*. 2023 Sep 8; 48(4):190.

5. Shafi S, Mounika S, Velliangiri S. Machine Learning and Trust Based AODV Routing Protocol to Mitigate Flooding and Blackhole Attacks in MANET. *Procedia Computer Science*. 2023 Jan 1; 218:2309-18.
6. Kanaparthi VM, Vempati K. Greyhole attack in mobile ad-hoc network mitigation and protection. *InAIP Conference Proceedings* 2024 Jan 25 (Vol. 2802, No. 1). AIP Publishing.
7. Alabdulatif A, Alharbi M, Mchergui A, Moulahi T. Mitigating Blackhole and Greyhole Routing Attacks in Vehicular Ad Hoc Networks Using Blockchain Based Smart Contracts. CMES-Computer Modeling in Engineering & Sciences. 2024 Feb 1; 138(2).
8. Mankotia EV, Sunkaria RK, Gurung S. Dual Security Based Protocol against Gray-Hole Attack in MANET. Adhoc & Sensor Wireless Networks. 2023 Sep 1; 56.
9. Khosa TN, Mathonsi TE, Du Plessis DP. A Model to Prevent Gray Hole Attack in Mobile Ad-Hoc Networks. *Journal of Advances in Information Technology*. 2023; 14(3).
10. Tropea M, Spina MG, Lakas A, Sarigiannidis P, De Rango F. SecGPSR: A secure GPSR protocol for FANET against Sybil and Gray Hole Attacks.
11. Ryu J, Kim S. Trust System-and Multiple Verification Technique-based Method for Detecting Wormhole Attacks in MANETs. *IEEE Access*. 2024 Jan 18.
12. Majumder S, Bhattacharyya D, Chakraborty S. Mitigation of Wormhole attack in MANET Using Cryptic-AODV: A Modified Routing Protocol. *International Journal of Intelligent Systems and Applications in Engineering*. 2024; 12(1):619-27.
13. Reji M, Joseph C, Thaiyalnayaki K, Lathamanju R. Genetic-based Fuzzy IDS for Feature Set Reduction and Worm Hole Attack Detection. *Computer Systems Science & Engineering*. 2023 May 1; 45(2).
14. Thapar S, Purohit A, Kanwer B, Jaiman A, Mounika A, Madhumala VS. An Approach to Detect Wormhole Attack in Mobile Ad Hoc Networks Using Direct Trust Based Detection Approach. *International Journal of Intelligent Systems and Applications in Engineering*. 2023 May 17;11(6s):276-83.
15. Rajkumar K, mercy Shalinie S. Boomerang packet testing to mitigate wormhole attack in MANET.