Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 7, No.1, July : 2024

AN EFFECTIVE ANALYSIS OF BLACKHOLE ATTACK IN MANET: A COMPREHENSIVE ANALYSIS

Dr. B. Arivazhagan, Assistant Professor, Department of Computer Science, VET Institution of Arts & Science (Co- Ed) College, Erode. Email: arivazhaganpsgcas92@gmail.com.
Mr. K. Mohanraj, Research Scholar, Department of Computer Science, VET Institution of Arts & Science (Co- Ed) College, Erode. Email: kmohamca@gmail.com.

ABSTRACT:
Mobile Ad Hoc Networks (MANETs) are particularly vulnerable to blackhole attacks, where malicious nodes falsely advertise optimal paths to intercept and discard data packets. This research investigates the impact of blackhole attacks on MANET performance and explores countermeasures to mitigate their effects. Blackhole attacks can significantly degrade network performance by increasing packet loss, reducing throughput, and elevating latency. The study evaluates existing detection and prevention techniques, including trust-based mechanisms, cryptographic methods, and machine learning approaches, to identify the most effective solutions. In Mobile Ad Hoc Networks (MANETs), nodes cooperate to relay data without centralized authority, creating vulnerabilities to various attacks. This survey explores three trust-enforcing mechanisms designed to mitigate the impact of malicious nodes on routing protocols. The dynamic nature of MANETs makes them susceptible to attacks like denial of service, black-hole, and grey-hole, which exploit network resources. Ensuring secure routing in MANETs involves maintaining data confidentiality, integrity, and service availability. The study highlights the significance of trust mechanisms in enhancing network performance by mitigating malicious behaviors. By analyzing different routing attacks and their impact, the research underscores the necessity of robust security measures.
Keywords:MANET, attack, routing, packet drop, blackhole, sinkhole, network and security threats.

INTRODUCTION :

In Mobile Ad Hoc Networks (MANETs), the cooperative network operation among nodes is required due to the absence of a centralized authority during communication process. The mobile nodes cooperating in MANETs may introduce malicious behaviors that disturb the functionality of the routing protocol during the process of route discovery or data communication. The mobile nodes play an anchor role as a router that forwards the packets from the source to the destination with extended support during the transmission of data packets for the objective of ensuring the data availability in MANET. MANETs has the potentiality of being established anywhere at anytime due to its nature of dynamicity [1].This dynamic nature of ad hoc network makes it highly vulnerable to several number of security threats that exploits the resources of the network. The specific attacks that exploit the nature of ad hoc network includes denial of service attacks (DoS), black-hole attacks and grey-hole attacks on par with the traditional counterpart. The security facilitation in MANETs completely concentrates on the process of guaranteeing and maintaining confidentiality and integrity of data exchanged in the network. This provision of security also concentrates on the process of facilitating network service provider availability and legitimate use of network nodes as per the requirements of Quality of Service (QoS). Thus the existence ofMANET completely depends on the reliability of mobile nodes that actively interact between one another during the process of route discovery that genuinely forwards the data packets to the other nodes in the network. Each mobile nodes in the network need to forward packets of other nodes that exist with the radio range to attain optimal network performance. However, energy is required for routing or forwarding the data packets depending on the requirements of each mobile nodes interacting in the network with necessitating any benefits from its own actions. In this context, trust mechanisms are required for

enforcing maximized trust which aids in better collaboration among the mobile nodes of the network for attaining optimal network performance. In this thesis, three different trust-enforcing mechanisms are proposed for handling the impact of malicious nodes in the network [2].A Mobile Ad-hoc Network (MANET) comprises of a huge amount of mobile devices that form a network deprived of support from internet infrastructure or any type of fixed stations. It is an autonomous system that includes nodes or Mobile Stations (MSs) acting as routers coupled by wireless links, unification of which establishes a network exhibited as a graph. In a single hop cellular network, wireless communication amid mobile nodes is established trusting on a wired backbone and fixed Base Stations (BSs). On the other hand, a MANET is an infrastructure-less network with a dynamic topology. It supports anytime/anywhere computing. The nodes move freely, and every node has restrictive transmitting power and constrained admittance to nodes only in the adjoining range. They are essentially peer-to-peer, multihop networks wherein packets are stored and forwarded from a source to a random destination through intermediary nodes. With node mobility, the connectivity changes with the comparative positions of other nodes.The subsequent topology change at the local level is propagated to other nodes and the topology based information is updated.The communication links between the nodes may be symmetric and asymmetric supporting bi-directional and unidirectional communication respectively. Routing in asymmetric networks is challenging. Excluding asymmetric links leads to want of links to establish a reverse path. Ensuring efficient routing is a challenge faced in a MANET. The second challenge is that the mobility forms of nodes vary. Some nodes may be highly mobile, while others may be motionless. It is hard to predict a node's motion with the direction. Several studies are carried out to assess the performance using diverse simulators [3].

Routing in MANET :

With the dynamic nature of nodes, topology changes frequently and randomly causing an increase in the routing overhead. Routing is challenging as finding effectual paths to the destination is based on diverse factors like Residual Energy, Received Signal Strength (RSS) of the neighboring node, topology, position of request creator and so on., The routing protocols are classified into different categories based on topology, location and energy. It is essential to evaluate the importance of a routing protocol, both qualitatively and quantitatively to determine the appropriateness as well as performance [4, 5]. The metrics are independent of any routing protocol.Following are the necessary qualitative properties of routing protocols:

- Distributed: It is essential that the routing protocol is distributed in nature.
- Freedom from Loops: Some packets may spin about in the network for random time periods. Time To Live (TTL) values can deal with the problem. Yet an organized and well-formed method is necessary as it typically leads to improved complete performance.
- Demand-based Function: Rather than assuming uniform traffic distribution in a network with routes maintained among nodes, the routing algorithm adjusts to the traffic pattern on demand. If done sensitively, network energy and bandwidth will be used more competently with increase in delay involved in route discovery.
- Proactive Functioning: Demand-based function with increased latency may be intolerable. In case the bandwidth and energy accept latency, proactive operation is anticipated.
- Security: Without network or link-layer security, a routing protocol is susceptible to several attacks like snooping network traffic, replaying transmissions, handling packet headers and redirecting messages within a network without suitable security provisions. Preserving security of transmission media is tough. Suitable mechanisms to ensure security by prohibiting disruption or change of protocol function are demanded. This is orthogonal to any specific protocol.

- Sleep Period: To conserve energy, some nodes are inactive, stop transmitting and receiving for random time periods. The routing protocols should be capable of accommodating these sleep periods without any adverse effects. There should be a close linking with the protocol in the link-layer through a consistent interface.
- Unidirectional Link Support: Bi-directional links are considered, as several algorithms are inefficient in functioning over uni-directional links. Unidirectional links are of restricted added value. A pair of uni-directional links forms a bidirectional connection amid two regions, but the capability of using them is valuable.

Routing Attacks in MANET :

Several attacks prevalent in the network layer of MANET are detailed below [6-10].

- Wormhole Attack: The attacker gets packets from any point in the network and tunnels those packets to another point from where they are replayed. Routing gets disturbed when control messages are tunneled. The tunnel is established amid 2 colluding attackers. It is hazardous for a node that hears a transmission from another node to consider itself to be in the range of the node.
- Blackhole Attack: The assailant node publicizes as having shortest paths to nodes whose packets it wants to capture. The node listens to the RREQs using a flooding based routing protocol. On receiving a RREQ to a node of attention, it generates a Route Reply (RREP) including the shortest route. If malevolent reply reaches the origin node before getting a RREP from the real node, a bogus path is established. Once a malevolent node inserts itself amid the collaborating nodes, it intercepts the packets transmitted among them.
- Rushing Attack: It results in Denial of Service (DoS) exploiting identical suppression by rapidly forwarding RREQ packets so as to access the forwarding group. When a RREQ packet is received by an assailant node, it accepts and forwards it to its neighbors rapidly in contrast to other nodes. As this RREQ reaches the destination before the original one, the destination accepts it and discards the other ensuing requests. The first non-duplicate RREQ is considered and a path is established between the sender and the receiver. The path so formed is considered as a valid one and is used for further communication.
- Neighboring Attack: On getting a packet, the intermediate nodes store the packet ID before sending it to the neighboring node. An intruder, on the other hand, simply sends the packet without storing the packet ID so as to make nodes which are not within the range of communication to trust that they are adjacent to each other leading to an interrupted route.
- Jellyfish Attack: A malevolent node that launches this attack is active during route discovery as well as packet forwarding so as to prevent it from being detected. The attacker intervenes into the multicast forwarding group. It attacks the traffic by reordering packets, intermittently dropping packets or increasing jitter. It is particularly hazardous to TCP traffic in compromised nodes, as it is tedious to distinguish the attacks from congestion. The data packets are delayed needlessly for some quantity of time before sending them. This increases the delay and worsens performance. The malevolent nodes use abuse directional antenna and dynamic power methodsto evade upstream nodes to identify misbehaviors of dropping packets.
- Sybil Attack: An entity can take control of a considerable portion of the system by offering several identities. It has different forms: (a) Presenting several IDs concurrently and completely (b) Formulating new IDs or replicating the prevailing IDs (c) Localized/ globalized attack. The attack may be executed either from the network or application layer with IP address and node ID considered as identifiers. These attacks do not support uniform resource allocation, distributed storage, voting, routing, misbehavior identification etc., As

there is no centralized control and a trusted authority to guarantee one-to-one correspondence amid entity and identity, there are chances for an unaccustomed entity to represent itself with duplicate entities. By masquerading with manifold IDs, the opponent takes control of the network considerably.

- Blackmail attack: The malevolent nodes consider an authentic node to make other nodes to trust that routing through that genuine node is unsafe. These attacks prevent senders from selecting the finest path to the destination thus reducing efficiency as well as throughput.
- Byzamite Attack: An intermediary node or a collection of compromised nodes works in conspiracy, creates routing loops, sends packets on paths that are non-optimal and particularly drops packets resulting in disruption as well as degradation of services. Though the network seems to be functioning normally in nodes' perspective, it may show Byzantine behavior.
- Gray hole attack: It is an extension of black-hole attack, wherein the nodes perform selective packet dropping but act as honest node. It is challenging to identify this attack when compared to black hole attack in which the malevolent node drops packets. The malevolent nodes partake in route discovery and update routing tables advertising themselves as having the shortest paths. Malevolent nodes capture the incoming packets and arbitrarily drop them. In another type, the node behaves malevolently for a particular period by dropping packets but might change to standard behavior after sometime. The behavior may be an amalgamation of both, thus making the identification even more tedious. This attack includes 2 phases. Initially, a malevolent node uses protocol to publicize itself of having the correct path to the destination for capturing packets although the path is bogus. In the second stage, the node drops captured packets with a particular likelihood.
- Resource Consumption Attack: A malevolent node intentionally tries to devour resources including battery power, bandwidth etc., Unnecessary RREQ control messages may be generated, beacon packets may be frequently produced or stale information may be forwarded to nodes.
- Location Disclosure Attack: An attacker may disclose information concerning node positions or network structure. It collects the location based information including route map and decides the attack scenarios. Traffic analysis is an understated security attack in MANET which remains unsolved. Adversaries determine the IDs of thecommunicating parties and examine the traffic to study the pattern and handle modifications in the design of traffic. Seeping of such information is overwhelming in securitybased scenarios.
- Sinkhole Attacks: A cooperated node attracts data to itself from all adjoining nodes. As this node becomes a repository of data, it is the source of all attacks which include eavesdropping or data modification. These loopholes present themselves to be smart in multi-hop communication. These effects of these attacks are more at the application level, where nodes have diverse roles. The influence of these attacks may be particularly severe. By impersonating the centralized node or its adjacent nodes, the opponent gains access to the main portion of data flowing in the network. Multi-path protocols aid in reducing the impact of these attacks as data is sent redundantly, not trusting one path alone. On the other hand, the probabilistic protocols measure the message reliability depending on the likelihood of the packet from a particular source.
- Sleep Deprivation Attack: The services offered by a particular node are requested repeatedly so that the node stays active without going into an idle or power conservation state. This is devastating in networks comprising of nodes with inadequate resources like battery power. This hinders other nodes from reasonably requesting services, data or information from the affected entity. It is hard to avoid such attacks, but the impact can be reduced by ranking the functions of the node in such a way that request for low-priority services do not affect high-

priority ones. Resources may be shared unevenly amid diverse kinds of services. More amounts of resources may be given to particular nodes than others with reduced priority

- Flooding Attack: The network resources including bandwidth, computational as well as battery power are exhausted that affects routing causing severe performance degradation. A malevolent node may send more amounts of RREQs in a small duration to the destination which is not present. As no replies are generated to the RREQs, they flood the network leading to Denial of Service (DoS).
- Link Withholding Attack: A malevolent node disregards the demand to publicize the links of particular nodes or a collection of nodes resulting in link loss. It is predominant in OLSR protocol.
- Link Spoofing Attack: Malevolent nodes present bogus links with nodes that are not neighbors to disturb routing functions. This makes the target node to choose the malevolent node as its Multi-Point Relay (MPR). The malicious node may handle data or routing traffic by altering, dropping traffic or executing other DoS attacks.
- Colluding Misrelay Attack: Several assailants work in conspiracy to alter or drop packets to interrupt routing function. It is hard to identify by using conventional schemes like watchdog as well as path rater.
- Message Tampering: It is propelled by opponents acting as compromised nodes. The data packets are taken and modified. The information may be related to network topology, paths etc., Additional data may be added or prevailing bytes may be removed. An insignificant change in data may perceptibly cause irregularities in the network.
- Routing Attacks: Several routing attacks are mounted on routing protocols which disrupt the appropriate network functions. Following are some of the routing attacks:
- Routing Table Overflow: The assailant generates paths to nonexistent nodes. The main aim is to produce sufficient number of routes to evade new routes from being produced or overload protocol implementation. In proactive routing, it is essential to find routing information even before it is essential. In reactive algorithms, a path is found only on demand. This attack causes overflow of routing tables which prevents entries conforming to paths to approved nodes from being included.
- Routing Table Poisoning: The compromised nodes forward false updates related to routing or alter genuine route update packets forwarded to other authorized nodes. It results in suboptimal routing, congestion or inaccessibility in some portions of the network.
- Packet Replication: An attacker duplicates an old packet which consumes more bandwidth as well as battery power that are available to nodes, causing unwanted confusion in routing
- Route Cache Poisoning: In on-demand routing protocols, every node conserves a route cache that holds information concerning paths which is recently known to the node.

RELATED WORKS :

Wireless networks are becoming increasingly popular. Mobile ad hoc networks (MANETs) are a type of wireless network that transmits packets from the sender node to the receiver node without using a base station or infrastructure. In MANETs, nodes act as both hosts and routers, making the network highly adaptable and mobile. However, this mobility and lack of fixed infrastructure make MANETs vulnerable to various attacks, such as Blackhole attacks, where malicious nodes misroute data packets. Existing solutions to combat these attacks often result in increased memory space consumption and overhead. To address these issues, Olanrewaju et al. (2023) propose an Enhanced On-demand Distance Vector (AODV) routing protocol to prevent Blackhole attacks using a combination of Diffie Hellman and Message Digest 5 (DHMD). This protocol was implemented

using Network Simulator 2 (NS2). The performance of the proposed protocol was evaluated using several metrics: Packet Delivery Ratio, throughput, End-to-End (E2E) Delay, and routing overhead. The results showed that DHMD significantly reduced network overhead to 23%, compared to AODV's 38%. Additionally, memory consumption for DHMD was lower at 0.52ms, compared to AODV's 0.81ms, due to the prevention of Blackhole attacks. This research highlights the potential of DHMD in enhancing network performance by reducing overhead and memory consumption, thereby mitigating the impact of Blackhole attacks [11].

Mobile ad hoc networks (MANETs) are increasingly crucial in scenarios requiring rapid network formation without pre-existing infrastructure or human intervention. These networks have various applications, such as in battlefields, education, and rescue missions, characterized by high mobility and limited resources (power, storage, and processing). MANETs rely on a hopping mechanism where each node communicates through intermediate nodes within its range. Unlike standard networks with dedicated routing and communication equipment, MANET nodes perform multiple functions, making them more susceptible to attacks. To address this, Abdelhamid et al. (2023) propose a solution for detecting Blackhole attacks using anomaly detection based on a support vector machine (SVM). This system analyzes network traffic to identify anomalies and distinguish between normal and malicious node behaviors. Using the OMNET++ simulator, the proposed solution demonstrated high accuracy in detecting Blackhole attacks, effectively identifying malicious nodes by analyzing traffic patterns under attack conditions[12].Recent advancements in wireless communication have spurred research into expanding Mobile Ad hoc Networks (MANETs), which provide real-time infotainment services through node-to-node communication. Despite their benefits, the decentralized architecture and wireless connectivity of MANETs pose significant security challenges, particularly in constructing secure routing protocols. Shafi et al. (2023) propose a Machine Learning and Trust-Based AODV Routing Protocol (ML-AODV) to mitigate Flooding and Blackhole attacks. This protocol uses trust estimation to select cooperative intermediate nodes, avoiding the unnecessary transmission of routing packets to nonexistent destinations. Key metrics for trust estimation include Hop Count (HC), Residual Energy (RE), and Link Expiration Time (LET). The ML-AODV protocol further optimizes packet transmission paths using an Artificial Neural Network (ANN) combined with a Support Vector Machine (SVM) classifier to detect intruders. Performance evaluation using NS-2 showed that ML-AODV improved throughput by 4% and reliability by 44% compared to existing approaches. Additionally, it reduced delay, routing overhead, and packet loss ratio by 12%, 15%, and 10%, respectively[13]. Mobile Ad-hoc Networks (MANETs) consist of autonomous mobile nodes that interact without fixed infrastructure, relying on intermediate nodes to relay packets. However, malicious nodes can disrupt this process by falsely advertising optimal paths, leading to packet drops—an attack known as a Blackhole attack. Mankotia et al. (2023) propose a Dynamic Threshold-Ad-hoc On-Demand Distance Vector (DT-AODV) protocol, which adjusts thresholds dynamically to improve network performance under Blackhole attacks. Evaluations using the NS-2 simulator demonstrated that DT-AODV outperforms the MBDP-AODV protocol, achieving a 99.10% packet delivery rate, 20.01 kbps throughput, 1750 routing overhead, and a 0.51 normalized routing load. This approach shows promise in enhancing MANET performance by effectively mitigating the impact of Blackhole attacks[14]. The presence of malevolent as well as selfish nodes highly worsens the performance of the network. Identification and segregation of such nodes is challenging. Fayaz et al. (2022) have proposed a reputation-based mechanism that is based on consumption as well as contribution based information for identification of selfish node and co-operation implementation. Nodes that do not cooperate are disconnected from the network to conserve resources with respectable repute. The proposed mechanism offers better Normalized Routing Load (NRL) and PDR involvingreduced packet drop for malevolent as well as selfish attacks. Selfish nodes are identified rapidly and precisely when compared to other

schemes[15]. Participating nodes may act selfishly and cause huge loss of network performance due to restricted resources or fitting to a varying administrative domain. Reputation-dependent solutions are extensively used for mitigating selfishness. These solutions may be contingent on the feedback of any node obtained from contributing nodes for safe exchange of information in an adversarial setting. A safe opinion distribution depending on network coding that guarantees effectiveness of reputation against selfishness in a hostile setting is proposed by Sangi et al. (2020). The mechanism handles the risk of opinion interchange in reputation-dependent solution with slight modifications. Further, it can be used for exchanging data safely in a hostile setting. It is seen that the mechanism offers better opinion exchange ratio, reasonable delay and per cycle overhead. Ponnusamy (2021) has applied node repute and energy-efficient model for reducing the embarrassment produced by selfish nodes and eliminates them from thesystem during routing. Reputed and energy-efficient nodes are found and data transmission follows consistent paths. Nevertheless in this reputation mechanism, the malevolent nodes are non-co-operative in nature. The nodes with good reputation are identified by analysing the communication ratio amid nodes[16 and 17]. The malevolent nodes consider the intrinsic reliability to be comfortable and execute distrustful activities. In case of attacks in unreceptive environments, fresh challenges emerge to prevent routing attacks comprising of gray hole attack that unfavourably reduces the availability as well as accuracy in the network by dropping data packets. Ourouss et al. (2021) have focussed on this attack by observing the nature of partaking nodes using a bio-inspired trust managing model. This non-centralised reliability assessment model depends on beta reputation with Ant Colony Optimization (ACO)metaheuristic. The chief emphasis of beta repute system is the evaluation of nodes based on effective tasks and consumed energy, while ACO sustains the reputation during discovery and computes the preference of every traversed route to choose the secure path. The propounded model enhances the conventional Dynamic Source Routing (DSR) by stopping the malevolent nodes from taking part in packet transmission[18]. In a unified or complete environment, some nodes do not offer actual data to find the ideal path to the destination. This is owing to the greedy nature of the nodes that demands traffic over times. The nodes that offer wrong data do not send the data packets but drop the packets. Black hole attack strictly disturbs the network performance. Kowsigan et al. (2021) has proposed an IDS called Alleviating the effects of Black hole throughIdentification and Protection (ABIP). ABIP depends on the non-static threshold of Receiver Succession Number (RSN), where the nodes generating wrong data produce high RSN. This work offers better PDR and reduces the impact of black hole attacks[19]. Shukla et al. (2021) have focussed on black hole as well as wormhole attacks. SWBAODV and scalable-dynamic elliptic curve cryptography are used. Prime numbers are chosen arbitrarily. A particular prime number is used. The level of security is not dependent on the key size. A 2-Dimensional vector function is formed involving wormhole and black hole. The network is assessed with and without attacks. SWBAODV is applied to the network in case of the presence of attacks. The network involves less delay, energy and routing overhead with increased PDR[20]. The selfish nodes conserve energy and remain active by not forwarding. Skellam Distribution Inspired Trust Factor-based Selfish Node Detection Technique (SDITF-SNDT) is propounded by Deva Priya et al. (2021) for imposing efficient detection and removal of selfish nodes. The mean packet variation is determined through which Standard Deviation (SD) long with Variance are used for calculating the SDITF. Reliability is estimated so as to classify them into selfish as well as co-operative nodes. The proposed scheme offers improved PDR with reduced energy for varying amount of mobile nodes[21]. Shajin & Rajesh (2020) guarantees to assess the Direct Trust Value (DTV) for every node and computes the node trust sustaining the condition and updating the trust and update interval for safe and efficient communication amid the sender as well as destination. A Trusted Secure Geographic Routing Protocol (TSGRP) is propounded for identifying attackers by taking the trust of a node formed by including the position and direct trust information. It outperforms conventional

protocols for identifying attacks. A trust-based safe communication is established amid the sender and the destination. The assessed DTV is used after sending Route-REQuest (RREQ) and RouteREPly (RREP) packets to assess the DTV of every node and safe route is established amid the sender and the destination. The efficiency of the propounded scheme is assessed and compared with the PRISM scheme[22]. Mukhedkar & Kolekar (2020) have proposed a routing scheme called Encrypted Trust-based Dolphin Glowworm Optimization (E-TDGO) using Advanced Encryption Standard-128 (AES-128) as well as trustdependent optimization model for safe routing. The propounded protocolcomprises of 3 stages namely, discovering k-paths, choosing optimum path and communication. Initially, 'k' paths are found depending on distance as well as trust of nodes. From 'k' paths identified, ideal path is chosen using DGO that is designed by combining Glowworm Swarm Optimization (GSO) algorithm and Dolphin Echolocation Algorithm (DEA). Once an optimum route is chosen, communication commences such that the protocol guarantees security. The messages involved in routing are encoded using AES-128 with shared code as well as key to ensure security[23]. Trust based secure AODV routing is proposed by Keerthika & Malarvizhi (2019) to safeguard a network from black hole attack. Hybrid Weighted Trust based Artificial Bee Colony 2-Opt (HWTABC 2-Opt) algorithm is propounded. Ideal safe paths are identified using ABC algorithm. Algorithm hybridisation is performed using 2-opt which acts as local search. The algorithm's efficacy is improved using the present solution based on the fitness for producing new solutions. The proposed scheme improves PDR, hops to sink including end-to-end delay. Rani et al. (2020) have dealt with black hole and grey hole attacks using Artificial Neural Network (ANN) along with Swarm-based Artificial Bee Colony (SABC) optimization. The system performance is increased by choosing appropriate and finest nodes for packet transmission. The proposed model is implemented using MATLAB with communication and NN toolboxes. The proposed protocol offers better results when compared to the prevailing works[24 and 25]. Majumder & Bhattacharyya (2020) have assessed the proportion of the amount of packets dropped to those sent in a network that is prone to Wormhole attack by using regression analysis, Method of Least Square (MLS) and Least Absolute Deviation (LAD). The performance of these schemes is compared. The linearity amid packets forwarded and dropped due to Wormhole attack along with the form of dropped packets is obtained by using MLS as well as LAD regression. As fake tunnels involve less time, the path related to the tunnel is also time consuming. It is essential to compute the time taken for estimating the relationship between the dropped and sent packets. Linear regression for pattern assessment offers better results[26].

CONCLUSION :

The dynamic and decentralized nature of Mobile Ad Hoc Networks (MANETs) makes them susceptible to a variety of security threats, including black-hole, grey-hole, and denial-of-service (DoS) attacks. Trust mechanisms are essential to enhancing cooperation among nodes and ensuring optimal network performance. Recent research has focused on developing trust-based protocols and anomaly detection systems to mitigate these threats. For instance, an Enhanced AODV protocol using Diffie Hellman and MD5 has been introduced to reduce network overhead and memory consumption, significantly improving robustness against black-hole attacks. Similarly, support vector machines have been leveraged for anomaly detection, demonstrating high accuracy in identifying malicious nodes. Additionally, a Machine Learning and Trust-Based AODV protocol has been proposed, which improved throughput and reliability while reducing delay, routing overhead, and packet loss. These advancements underscore the potential of integrating machine learning and trust mechanisms to bolster the security and performance of MANETs in dynamic environments.

REFERENCE :

1. Bharanidharan, C., Malathi, S., & Manoharan, H. (2024). Detection of black hole attacks in vehicle-to-vehicle communications using ad hoc networks and on demand protocols. *International Journal of Intelligent Unmanned Systems*.
2. Arunmozhi, S. A., Rajeswari, S., & Venkataramani, Y. (2023). Swarm Intelligence Based Routing with Black Hole Attack Detection inMANET. *Computer Systems Science & Engineering*, *44*(3).
3. Kumari, A., Dutta, S., & Chakraborty, S. (2023). Detection and Prevention of Black Hole Attack in MANET using Node Credibility and Andrews Plot.
4. Alkanhel, R., El-kenawy, E. S. M., Abdelhamid, A. A., Ibrahim, A., Abotaleb, M., & Khafaga, D. S. (2023). Dipper Throated Optimization for Detecting Black-Hole Attacks inMANETs. *Computers, Materials & Continua*, *75*(1).
5. Murty, K., & Rajalakshmi, M. V. D. S. (2023). Secure and light weight Aodv (SLW-AODV) routing protocol for resilience against blackhole attack in manets. *Int J Soft Comput Eng (IJSCE)*, *13*(1), 2231-2307.
6. Ramesh, R., & Seshikala, G. (2023, June). Link Aware Multipath Routing to Defend Against Black Hole Attacks for MANETs. In *2023 3rd International Conference on Intelligent Technologies (CONIT)* (pp. 1-6). IEEE.
7. Esaid, A., & Agoyi, M. (2023). Avoid Suspicious Route of Blackhole Nodes in MANET's: Using A Cooperative Trapping. *Computer Systems Science & Engineering*, *45*(2).
8. Kaushik, S., Tripathi, K., Gupta, R., & Mahajan, P. (2024). Enhancing Reliability in Mobile Ad Hoc Networks (MANETs) Through the K-AOMDV Routing Protocol to Mitigate Black Hole Attacks. *SN Computer Science*, *5*(2), 263.
9. Ryu, J., & Kim, S. (2023). Reputation-based opportunistic routing protocol using q-learning for manet attacked by malicious nodes. *IEEE Access*.
10. Rajeshkumar, G., Kumar, M. V., Kumar, K. S., Bhatia, S., Mashat, A., & Dadheech, P. (2023). An Improved Multi-Objective Particle Swarm Optimization Routing on MANET. *Computer Systems Science & Engineering*, *44*(2).
11. Olanrewaju, O. M., Abdulwasiu, A. A. A., & Nuhu, A. (2023). Enhanced On-demand Distance Vector Routing Protocol to prevent Blackhole Attack in MANET. *International Journal of Software Engineering and Computer Systems*, *9*(1), 68-75.
12. Abdelhamid, A., Elsayed, M. S., Jurcut, A. D., & Azer, M. A. (2023). A lightweight anomaly detection system for black hole attack. *Electronics*, *12*(6), 1294.
13. Shafi, S., Mounika, S., & Velliangiri, S. J. P. C. S. (2023). Machine learning and trust based AODV routing protocol to mitigate flooding and blackhole attacks in MANET. *Procedia Computer Science*, *218*, 2309-2318.
14. Mankotia, V., Sunkaria, R. K., & Gurung, S. (2023). DT-AODV: A dynamic threshold protocol against black-hole attack in MANET. *Sādhanā*, *48*(4), 190.
15. Fayaz, M., Mehmood, G., Khan, A., Abbas, S., Fayaz, M., & Gwak, J. (2022). Counteracting Selfish Nodes Using Reputation Based System in Mobile Ad Hoc Networks. Electronics 2022, 11, 185.
16. Sangi, A. R., Liu, J., Alkatheiri, M. S., & Anamalamudi, S. (2020). Secure opinion sharing for reputation-based systems in mobile ad hoc networks. *Measurement and Control*, *53*(3-4), 748-756.
17. Ponnusamy, M. (2021). Detection of selfish nodes through reputation model in mobile adhoc network-MANET. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(9), 2404-2410.

18. Ourouss, K., Naja, N., & Jamali, A. (2021). Defending against smart grayhole attack within MANETs: A reputation-based ant colony optimization approach for secure route discovery in DSR protocol. *Wireless Personal Communications*, *116*, 207-226.
19. Kowsigan, M., Rajeshkumar, J., Baranidharan, B., Prasath, N., Nalini, S., & Venkatachalam, K. (2022). RETRACTED ARTICLE: A Novel Intrusion Detection System to Alleviate the Black Hole Attacks to Improve the Security and Performance of the MANET. *Wireless Personal Communications*, *127*(Suppl 1), 3-3.
20. Shukla, M., Joshi, B. K., & Singh, U. (2021). Mitigate wormhole attack and blackhole attack using elliptic curve cryptography in MANET. *Wireless Personal Communications*, *121*, 503-526.
21. Deva Priya, M., Christy Jeba Malar, A., Sengathir, J., & Akash, T. (2021). A Skellam Distribution Inspired Trust Factor-Based Selfish Node Detection Technique in MANETs. In *Proceedings of 6th International Conference on Recent Trends in Computing: ICRTC 2020* (pp. 357-368). Springer Singapore.
22. Shajin, F. H., & Rajesh, P. (2022). Trusted secure geographic routing protocol: outsider attack detection in mobile ad hoc networks by adopting trusted secure geographic routing protocol. *International Journal of Pervasive Computing and Communications*, *18*(5), 603-621.
23. Mukhedkar, M. M., & Kolekar, U. (2020). E-TDGO: An encrypted trust-based dolphin glowworm optimization for secure routing in mobile ad hoc network. *International Journal of Communication Systems*, *33*(7), e4252.
24. Keerthika, V., & Malarvizhi, N. (2019). Mitigate black hole attack using hybrid bee optimized weighted trust with 2-Opt AODV in MANET. *Wireless Personal Communications*, *106*, 621-632.
25. Rani, P., Kavita, Verma, S., Kaur, N., Wozniak, M., Shafi, J., & Ijaz, M. F. (2021). Robust and secure data transmission using artificial intelligence techniques in ad-hoc networks. *Sensors*, *22*(1), 251.
26. Majumder, S., & Bhattacharyya, D. (2020). Improvement of packet delivery fraction due to discrete attacks in MANET using MAD statistical approach. In *Proceedings of the Global AI Congress 2019* (pp. 187-196). Springer Singapore.