ISSN (ONLINE) 2583-2506
http://publications.rayatbahrauniversity.edu.in
RBIJMR-Rayat Bahra International Journal of Multidisciplinary Research, Vol. 02, Issue 01, June 2022

A Review on Detection and Prevention of Attacks in MANET

Nishi Goyal and Pooja Rani*

Department of Computer Science & Applications, RayatBahra University, Mohali-140104

Abstract: *MANET (Mobile Ad-hoc Network) is a combination of wireless mobile devices which interacts with each other through radio communication. There is no centralized control in MANET. Due to no centralized control, the mobile nodes are vulnerable to various attacks. This work presents a review on various mechanisms proposed by various researchers on detection and prevention of attacks in MANET. The main objective of this paper is to give an overview on introduction to MANET, Various types of attacks and detection and prevention techniques. The research work of different researchers is presented here to find out the facts and will be helpful in further developments in the network security field.*

Keywords: MANET, Detection, Prevention, Network layer attacks, routing, IDS, Security Mechanism, AODV

*Corresponding author: Dr. Pooja Rani
e-mail: pooja.sharma@rayatbahrauniversity.edu.in

1. Introduction

MANET (Mobile Ad-hoc Network) is a combination of wireless mobile devices which interacts with each other through radio communication. There is no centralized control in MANET. Nodes of Mobile Ad-hoc Network functions like a router and host as well. A dynamic topology is used in MANET and there is no static topology like in other networks. This network is independent of any fixed infrastructure or centralized system, so every node has to decide at its own and they are independent of each other. MANET is used in defence, disaster management and Vehicle computing and many other applications where installation of infrastructure-based network is not feasible.

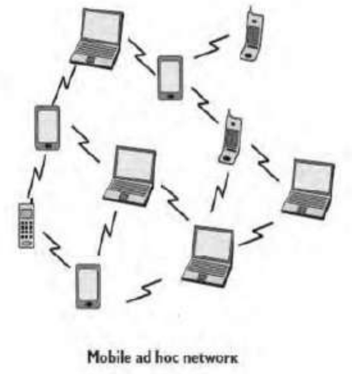

Fig. 1: MANET Architecture

2. Attacks in MANET

Due to no centralized control, the mobile nodes are vulnerable to various attacks. Shortcomings of MANET include Energy constraints of nodes, security attacks, scalability problems, security vulnerabilities and threats. Various network layer attacks in MANET are Black hole, Gray Hole, Worm hole, flooding and sink hole attack. The attacks disrupt the routing of packets and degrade networks performance. Various routing protocols are AODV, DSR, DSDV and ZRP.

Table 1: Types of attacks

MANET Security Layer	**Attacks**
Application Layer	Malicious code, Repudiation
Transport Layer	Session hijacking, SYN Flooding
Network Layer	Black Hole, Grey Hole, Worm Hole, Flooding,
Data Link Layer	Traffic analysis and monitoring
Physical Layer	Traffic Jamming, Eavesdropping

3. Detection and Prevention of Attacks in MANET

There are various security mechanisms which are proposed by various researchers to detect and prevent the attacks in MANET; some of them are summarized as below.

A. U. Khan, *et al.* proposed a mechanism to analyse the performance of Adhoc on-demand Distance Vector Protocol (AODV), a reactive routing protocol under the influence of Black hole, Gray hole and Worm hole attacks in MANET. He proposed a security mechanism as two techniques i.e., cryptography based, and trust based. Cryptography technique is more accurate but consumes more energy and takes more time for detection and prevention of attacks as compared to trust based. Trust based technique consumes less energy and time but sometimes doesn't provide accurate detection. This technique is not efficient for multiple attacks and can be used for particular type of attacks [1].

Pooja Rani (2020) proposed a mechanism for the protection against dual attacks for BHA (Black Hole Attack) and GHA (Gray Hole Attack) by using the concept of Artificial Neural Network (ANN) as a deep learning algorithm along with the swarm-based Artificial Bee Colony (ABC) optimization technique. ABC optimization technique utilized the intelligent behaviour of honeybees, which had been used to segregates the nodes based on their properties, such as into two lists named healthy and affected nodes lists. The attacker nodes list is subdivided into BHA nodes and the GHA nodes list. Using these properties, ANN trained the network. The performance of the network has been analysed based on PDR, throughput, and delay parameters. Hence, the improvement against PDR, throughput, and delay has been attained with the swarm-based Artificial Bee Colony (ABC) optimization technique [2].

M. M. Khalifa, *et al.* proposed a new Intrusion detection system using three Machine Learning (ML) techniques. These techniques were Random Forest (RF), support vector machines (SVM), and Naive Bayes (NB) and these were used to classify nodes in MANET. The routing protocol was used is Dynamic Source Routing (DSR). The type of IDS used is a Network Intrusion Detection System (NIDS). The **Random Forest (RF)** supervised machine learning classification algorithm creates a forest out of individual trees to analyse each new entry and this algorithm was found to be the most accurate through experimental research. The **Support Vector Machines (SVM)** is a supervised learning technique that uses related learning methods to look for patterns in classification and regression activities to improve predictive performance and reduce data. The **Naive Bayes (NB)** is a probability classifier model, which means it can guess for multiple classes simultaneously. Instead of one algorithm, this model uses a group of techniques that all share a familiar concept. In this concept, each attribute is assumed to contribute equally to the outcome. Unlike other models, this one requires very little data to train [3].

D. Regassa, *et al.* designed and implemented an OLSR (Optimized Link State Routing) protocol used with an Intrusion Detection System (IDS) mechanism that accurately detects misbehaviour node(s) using few additional messages on the existing messages on the transmission path. It validates the path and attacker detection message which isolates the attacker using an alternative path for End-to-End (E2E) communication between the source and the destination nodes in a typical MANET. This study adds a significantly small data to the existing packet used for detection and isolation to the OLSR message, so it increases the network overhead. If there is no attacker in the communication line, the overhead of this mechanism is expected slightly higher, and this is relatively higher when the attacker is smarter than a normal attacker node. Even though overhead is introduced, it was rewarded by the achievement of this mechanism as it contributed to the security of the network. A number of future research directions were also suggested which needs a more extensive investigation like: Evaluating the routing protocol, the developed mechanism for minimization of the overhead introduced to the network traffic and instead of reviewing the routing table of the neighbouring node [4].

H. A. Ibrahim, *et al.* presented the rushing attack, in the Ad Hoc On-Demand Multipath Vector (AOMDV) multicast routing protocol and examine the impact of the rushing attack on MANET. The result of this study shows that rushing attack degrades MANET network performances. Furthermore, a rushing attack prevention mechanism based on time threshold value and random route selection techniques is implemented. **Rushing attack** highly transmits route request with higher transmission power than the genuine nodes and become participate between source and destination nodes, after that, it delays or drop actual data pass through it. Based on the time RREQ arrives, a node takes a decision, if the RREQ packet arrives before threshold value, the RREQ packet consider as came from an attacker and discarded else RREQ packet received then randomly select RREQ to forward. Routing performance was studied using performance metrics like throughput, delay, and packet delivery ratio under Normal AOMDV (N-AOMDV), Attacked AOMDV (AAOMDV) and Prevented AOMDV (P-AOMDV) routing protocols. At the end results show that the A-AOMDV had the lowest throughput, packet delivery ratio and highest end to end delay of the network than the N-AOMDV & P-AOMDV. This shows the rushing attack prevention mechanism can protect the network from rushing attack and its works correctly without requires external resource because Mobile Ad hoc Network had the smallest amount of resource [5].

A. Pathania, *et al*. presented a hybrid model for IDS (Intrusion Detection System) using ANN and data mining approaches. In this research while starting the transmission, source node and destination node is defined and then using IDS and AODV protocol route is created between destination and source node. If network's performance decreases, then it needs to apply cuckoo search as an optimization algorithm. **Cuckoo search algorithm** extracts the properties and observes the energy been consumed by each node. Optimized properties are being used as an input to the decision tree classifier and then system is prepared according to these properties. If there is a chance for existence of intruder in the network, then it will be classified using decision tree algorithm. At the end, QOS parameters like energy consumption is evaluated using cuckoo search optimization algorithm. The detected intruder is prevented using decision tree and removed from the MANET network. For further study fuzzy logic can also be used along with the ANN model for achieving higher accuracy in the detection of attackers and malicious activities [6].

B. V. Sherif, *et al.* proposed a selfish node detection technique known as Chimp-CoCoWa-AODV to improve the performance of MANET. To eliminate the drawbacks of existing approaches in selfish node detection, this technique integrates both Ad-hoc On-Demand Distance Vector (AODV) protocol incorporated with chimp optimization algorithm and Collaborative Contact based Watchdog. The main role of chimp optimization algorithm in AODV is to undergo optimal route selection process. The performance of the proposed Chimp-CoCoWa-AODV approach is compared with existing approaches in terms of average routing load, Average Packet Delivery Fraction (PDF), Average End-to-end Delay (EED), Average Throughput, Total packet drop in the application layer, and maliciously dropped packet in the routing layer. The selfish node is detected by the local watchdog in the CoCoWa. The information about this selfish node is transmitted to all nodes. Then the selfish node is isolated from the packet transmission [7].

S. Devi, *et al.* implemented a trust based security protocol. This dynamic protocol picks a dynamic IDS node based on trust criteria. The trust parameters, derived from two factors: Current Energy and Packed Drop Count of a node, are used to choose IDS. The selected IDS node assists the source node in selecting a data transmission path and then monitoring that route until the transmission is complete. The impact of each scenario is computed using PDR, NRO, and PLR, and the performance of this proposed protocol is tested using three distinct scenarios with varied numbers of attackers, mobility, and nodes. In order to assess the effectiveness of this work, a grey hole attack is used. The results of the proposed protocol are better than the existing AGHA and AODV protocols. In this work, a comparison is conducted for each scenario, and it is noticed that increasing the number of attackers and mobility decreases performance, but increasing the number of nodes increases the possibility of more alternative path ways [8].

R. Abassi, *et al*. proposed a trust based security scheme for message exchange in vehicular Ad hoc networks. An intrusion detection system (IDS) was developed to preserve network efficiency and prevent and detect grey hole attacks. The proposed grayhole attack method eliminates the unusual differences between the router packs in the ad hoc on demand distance vector (AODV) route protocol, in addition to establishing security. An appropriate clustering technique dubbed VANET Grouping Algorithm (VGA) organizes the network into groups with elected Group-Heads. Second, they established a trust management strategy for vehicle reputations based on the VGA. This technique uses blockchain to increase ad hoc network security and prevent malicious activity during communication. The support learning approach was also used to assist route nodes in selecting increasingly reliable and productive routing connections. With a system of reliable and trustworthy nodes, the proposed study identifies a Trust-Based Efficient Blockchain Linked Routing Method (TbEBCLRM) [9].

R. Prasad, *et al.* proposed and developed a Secure Energy Routing (SER) protocol for MANETs. His basic vision was to further enhance the security of Intrusion Detection System (IDS) in order to prevent different kinds of active and passive network attacks that are available in the mobile ad-hoc networks. In his security algorithm, the shortest routing paths have been used and the routing protocol utilized less consumption of energy while transmitting information. To safeguards the network nodes from various attacks the S-IDS algorithm used for SER protocol regularly updates the node information. To maintain the redundancy, the proposed protocol used multiple routes to transmit the information to the destination. The comparison of SER protocol has been evaluated with existing DSR, AODV and DSDV protocols for PDR and end-to-end delay respectively and the final simulation results validated SER protocol’s performance on different industry parameters. [10].

A. Vasudeva, *et al.* proposes a transmission power-controlled approach by which a Sybil attack is capable of violating the functioning of the mobility-based clustering algorithm in MANETs. An algorithm was introduced by which a Sybil attacker can increase its chances of becoming the cluster head during the head election process. In the proposed Sybil attack algorithm, one of the Sybil nodes is randomly picked as the candidate Sybil node. A candidate Sybil node participates in the cluster head election process for winning. The rest of the Sybil nodes also participate in the election process, but not for becoming the cluster head. They only support the candidate Sybil node to enhance further its chances of winning the election.It is demonstrated that a Sybil attacker is capable of deceiving the cluster head election process in MOBIC to fabricate the result in its favor. A Sybil assault can utilize its various ghost identities to raise the aggregated relative mobility of its reputable neighboring nodes and reduce its personal aggregated relative mobility. It indeed raises the likelihood of the Sybil attacker node becoming the cluster representative. To achieve this, a Sybil attacker broadcasts two successive signals through each of its Sybil nodes with deviation in their transmission powers within the specified limits. The deviations in the transmission powers of two consecutive signals can be altered to increase the aggregated relative mobility of the legitimate neighbors [11].

P. B. Reddy, analysis of blackhole attack on AODV routing protocol and the proposed routing protocol AODV-BS is carried out with respect to different performance parameters such as Packet Delivery Ratio, Average End to end delay, Normalized Routing overhead and Throughput. A deliberate attempt to detect and counter the blackhole nodes is made by deploying threshold evaluation and cryptographic verification in MANETs. This investigation is aimed to analyze the vulnerability of two protocols AODV and AODV-BS under different network scenarios and traffic patterns against Blackhole attack. The Simulation results showed that AODV-BS performs better than AODV in terms of all quality of Service (QoS) parameters in the presence of blackhole attack. In this paper attempt is made only to counter the internal attacks so further research can be performed by considering some cryptography security framework to defend the external attacks [12].

M. Chatzidakis, *et al.* introduced a mechanism to identify malicious nodes and promptly alerting the network. In addition, the same mechanism is used to restore the trust of a malicious node, in case it resumes healthy operation or it was a misclassification issue. The mechanism can be fine-tuned to balance the sensitivity of the reaction and the timely detection of a status change, as required. A complete MANET transaction protocol along with a trust management/restoration mechanism has been introduced. The mechanism increases the lifespan of a cluster, minimizes the malicious transactions and efficiently restores the trust of nodes that either were wrongfully categorized as malicious, or converted from a malicious to healthy state. A scheme was proposed which can efficiently identify the change in the trust status of the node, thus improving the security status of the MANET. The energy impact on a MANET network lifespan was also evaluated when malicious nodes are present and found that the network energy is drastically decreased when such nodes are present and not detected [13].

I. Ali Shah, *et al.* proposed to deploy DPS (Detection and Prevention System) nodes in the network that uninterruptedly monitor the RREQs advertised by all other nodes in the networks. DPS nodes sense the mischievous nodes by detecting the activities of their immediate neighbour. When a node demonstrates some peculiar manners, DPS node states that particular distrustful node as black hole node by propagation of a threat message to all the remaining nodes in the network. A protocol with a clustering approach in AODV routing protocol is used to sense and prevent the black hole attack in the network. Then the black hole node is abandoned and prohibited from the whole system and is not allowed any data transfer from any node thereafter. The main objective of the DPS node is to monitor the request and reply in the network and also to manage the suspected nodes. When the suspicious node is found, the suspected value of the network is reached to its threshold and then that particular node is considered as black hole node [14].

S. Barai, *et al.*, presented a technique to identify the Blackhole nodes in the network. It is very challenging when the attack is in an Opportunistic network as there is no predefined path between source and destination and it's difficult to differentiate adversary node behaviour from normal packet drops. The proposed technique provides a way to identify a potential list of Blackhole nodes. When incorporated with standard routing protocols, namely Spray-and-Wait, Epidemic, and Prophet Protocols, it was observed that the effect of Blackhole attacks on Opportunistic networks by avoiding the paths containing these blacklisted nodes was mitigated. It was possible to reduce the number of dropped packets compared to the scenario where blackhole nodes could not be avoided. Moreover, the message overhead is not significantly high to affect the network efficiency [15].

S. Kaushik *et al.* presented the performance analysis of two protocols which are AODV and SAODV where AODV stands for Adhoc-on-Demand Distance Vector and SAODV stands for Secure Ad-hoc-on-Demand Distance Vector (SAODV) protocol for packets transfer and communication among the nodes using Support Vector Machine (SVM) technique. The comparative analysis of SAODV and AODV protocol is presented against black hole attack for the parameters energy consumption, throughput the packet delivery ratio and end-to-end delay in ad hoc networks.

Table 2.: Tabular representation of some of reviews of carried out earlier work

Detection and prevention Technique used	**Type of attack**	**Simulation Tool used**	**Year**
Cryptography and trust based	Black hole, Gray hole, Worm Hole	NetSim	2021
ANN with Swarm based Artificial Bee Colony	Black hole, Gray hole	MATLAB	2020
ML Techniques- Random Forest, SVM Support Vector Machines, Naive Bayes	DDoS	NS-2	2022
OLSR protocol with IDS	IDS	NS-2	2022
Random route selection technique	Rushing attack	NS-2	2021
ANN - Cuckoo search algorithm	IDS	MATLAB	2021
Chimp CoCoWa-AODV	Selfish nodes	NS-2	2021
Dynamic Trust based security protocol	Gray hole	NS-2	2021
VANET Grouping Algorithm using clustering technique- Blockchain linked routing method	Gray hole	NS-2	2020
Secure Energy Routing Protocol	Active and passive attacks	NS-2	2021
Mobile based clustering- MOBIC algorithm	Sybil attack	Java Simulation	2022
AODV-BS routing protocol	Black hole attack	NS-2	2021
Trust change detection mechanism by clustering	Malicious nodes	Java Simulation	2022
Detection and prevention system (DPS)	Black hole	NS-2	2021
Spray and wait, Epidemic, Prophet Protocols	Black hole	ONE Simulator	2021
AODV and SAODV protocol using SVM	Black hole	NS-2 and Python	2022
On demand distance vector routing protocol	Black hole	NS-2	2021

AODV is on demand distance vector routing protocol while **SAODV** refers to secure AODV routing protocols for pa cket transfer in any network. The secure AODV consist secure algorithms and authentication mechanism for routing. The secure algorithms are generated with the help of encryption policies. The hashing techniques can also be used to convert multivalued functions into single point data which makes AODV more secure. A methodology is designed which lays rules based on learnings from the computations and estimations made at the time of packet transfer. The comparative analysis shows that secure AODV using SVM technique performed much better and can be used for further scenario in any networks for different parameters of MANET [16]. V. Bibhu *et al.* proposed a modified AODV protocol to prevent the black hole attack in MANET. In the proposed mechanism, two different Route Reply with sequence numbers are compared separately. When the message comes from nearby nodes with half of the value of maximum value of 32 bit sequence number. If the message sequence number of received Route Reply message is equal or less than half of the maximum value of sequence number then it is considered that the Route Reply comes from genuine node not from the black hole node. On Demand Distance Vector Routing protocol is very common and implemented with Mobile Ad Hoc Network nodes to handle the operations of packet routing from by any node as a source node to destination node. The sequence number and On demand Distance Vector Routing protocol are integrated with a mechanism to find the Request Reply of message containing routing information from source to destination node in Mobile Ad Hoc Network [17].

4. Conclusion

This review work has presented various mechanisms implemented by various researchers to prevent and detect attacks in MANET. From this review work, we can conclude that though a very large amount of work has been done on this; detection and prevention of attacks is still a concern in MANET and further research is required to detect and prevent multiple attacks using one technique. Most of the research has been done on handling one type of attack at a time and it is not sufficient to provide a secure communication in the networks for multiple types of attacks. The security can be more maximized and network overhead can be minimized by implementing more optimization techniques. Many Artificial Intelligent based techniques are used with intrusion detection technique to give more efficient results but more techniques for detection and prevention of multiple attacks needs to be explored. It is expected that this literature review work will enable researchers to obtain a detailed overview of various techniques for detection and prevention of attacks in MANET and will be helpful in future research.

References

[1] A. U. Khan, M. D. Chawhan, M. M. Mushrif, B. Neole, (2021), "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," Proceedings of the Fifth Int. Conf. on Intelligent Computing and Control Systems (ICICCS 2021) IEEE Xplore Part Number: CFP21K74-ART; ISBN: 978-0-7381-1327-2.

[2] Pooja Rani, Kavita, Sahil Verma and Gia Nhu Nguyen, (2020), Mitigation of Black Hole and Gray Hole Attack Using Swarm Inspired Algorithm with Artificial Neural Network, IEEE.

[3] M. M. Khalifa, O. Nuri, K. M. Ali Alheeti, (2021), "New Intrusion Detection System to Protect MANET Networks Employing Machine Learning Techniques," Int. Conf. of Modern Trends in Information and Communication Tech. Industry (MTICTI) IEEE.

[4] D. Regassa, H. Y. Yeom, Y. Son, (2022), Efficient Attacker Node(s) Detection and Isolation Schemes in MANETs OLSR Protocol, Int. Conf. on Information Networking (ICOIN) IEEE.

[5] H. A. Ibrahim, A. S. Ahmed, B. B. Sundaram, P. Karthika, (2021), Prevention of Rushing Attack in AOMDV using Random Route Selection Technique in Mobile Adhoc Network, Proceedings of Fifth Int. Conf. on Electronics, Communication and Aerospace Tech. (ICECA-2021) IEEE.

[6] A. Pathania, V. Ghai, (2021), A Hybrid Approach for Intrusion Detection System using Data Mining and Artificial Neural Network, 3rd Int. Conf. on Advances in Computing, Communication Control and Networking (ICACCCN) IEEE.

[7] B. V. Sherif, P. Salini, (2021), Effective and Prominent Approaches for Malicious Node Detection in MANET, Int. Conf. on Computational Intelligence and Computing Applications (ICCICA) IEEE.

[8] S. Devi, M. Kumar, S. Bhardwaj, (2021), Dynamic Trust based IDS to Mitigate Gray Hole Attacks in Mobile Adhoc Networks, 2nd Int. Conf. on Computational Methods in Science & Technology (ICCMST) IEEE.

[9] R. Abassi, B. C. Douss and D. Sauveron, (2020), TSME: A trust based security scheme for message exchange in Vehicular Ad hoc Networks, Human-centric Computational Inf. Sci. **10 (1)**.

[10] R. Prasad and Shivashankar, Secure intrusion detection system routing protocol for Mobile Ad-hoc Network, *Global Transitions Proceed.* (2021), doi: https://doi.org/10.1016/j.gltp.2021.10.003.

[11] Amol Vasudeva and Manu Sood, (2022) On the vulnerability of the mobile ad hoc network to transmission power controlled Sybil attack: Adopting the mobility-based clustering, Journal of King Saud Univ. Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2022.04.020.

[12] P. Reddy, B. B. Reddy, B. Dhananjaya, (2021), The AODV routing protocol with built-in security to counter black hole attack in

MANET, Elsevier https://doi.org/10.1016/j.matpr.2021.08.039.

[13] M. Chatzidakis, S. Hadjiefthymiades, (2022), A Trust Change Detection Mechanism in mobile ad-hoc networks, Elsevier https://doi.org/10.1016/j.comcom.2022.02.007.

[14] I. Ali Shah, N. Kapoor, (2021), To Detect and Prevent Black Hole Attack in Mobile Ad Hoc Network, 2nd Global Conference for Advancement in Technology (GCAT).

[15] S. Barai, P. Bhaumik, (2021), ”Detection and Mitigation of Black hole Attack Effect in Opportunistic Networks”, 19th OITS Int. Conf. on Info. Tech. (OCIT).

[16] S. Kaushik, K. Tripathi, R. Gupta, P. Mahajan, (2022), “Performance Analysis of AODV and SAODV Routing Protocol using SVM against Black Hole Attack,” 2nd Int. Conf. on Innovative Practices in Technology and Management (ICIPTM).

[17] V. Bibhu, A. Kumar, B. P. Lohani, (2021), Black Hole Attack in Mobile Ad Hoc Network and its Avoidance, Int. Conf. on Innovative Practices in Tech. and Management (ICIPTM).