IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Security Approach to Detect and Isolate Routing Attacks in MANET

[1]Er. Rachna Rajput, [2]Er. Harmandeep Kaur
[1]Assistant Professor & H.O.D, [2]Assistant Professor
Department of Computer Science & Engineering
Guru Kashi University, Bathinda, India

Abstract: *Secure routing is of utmost importance in protecting mobile devices from external threats. However, the dynamic characteristics of Mobile Ad hoc Networks (MANETs) pose significant challenges in achieving a secure routing path. MANET is prone to attacks and hence security considerations are required to secure highly confidential data communicated through these network most of the time. Energy constraints and bandwidth limitation of this network make it more sensitive to routing attacks. Various routing protocols have been extended and some protocols with new features have been proposed to ensure the secure routing scheme. Mobile ad hoc network (MANET) is an infrastructure-less network where mobile nodes can share information through wireless links without dedicated hardware that handles the network routing. MANETs' nodes create on-the-fly connections with each other to share information, and they frequently join and leave MANET during run time.The greatest imperative attacks in Manet are wormhole attack and jellyfish assault.*

***Keywords*-MANET, Secure Routing, Rushing Attacks, Blackhole Attacks, AntHocNet.**

I. INTRODUCTION

Introduction A collection of network nodes that interact outside of a fixed physical structure make up a mobile ad hoc network (MANET). MANETs include a variety of noteworthy characteristics, including variable topology, quick deployment, and multi-hop wireless transmission [1]. MANET is appropriate for various time-sensitive tasks thanks to all these qualities. In cases when it is challenging to construct basic infrastructure, ad hoc networks offer a viable communication facility. Additionally, with MANETs, mobile nodes communicate without requiring a physical infrastructure and without engaging in administrative tasks. As a result, these systems are flexible, self-organizing, and automatically created, enabling nodes to move at will while interacting [2-4]. These systems can be expanded and merged to create intelligent solutions for addressing industrial demands with cutting-edge technology like cloud computing, the IoT, and machine learning methods. Figure 1 shows MANET's organizational structure. Given the changeable topology of the MANET, implementing a secure routing protocol while assuring the quality of service is challenging.

As the traditional routing techniques for these networks presuppose collaborative, trusting settings among mobile devices, secure routing in ad-hoc networks was one of the main challenges for researchers. Attackers can readily hack authorized corporate mobile nodes to cause a variety of packet transmission errors and launch DoS assaults. Sequence number assaults are a typical denial-of-service attack against traditional MANET routing protocols, and they can drop data packets during the transmission process after violating protocol requirements during the route-finding phase. As a result, it is challenging to provide secure and trustworthy routing in such a network. According to their architecture and routing method, routing protocols in MANETs can typically be divided into three categories: proactive routing protocols, reactive routing protocols, and hybrid routing protocols.

By developing a secure attack detection and recognition that takes into account issues like a safe path to endpoints for transmission of data, negligible node energy usage, and the innovation of protection schemes that really can come to terms with egoistic and harmful attacks on the entire network, the security concerns in MANET can be resolved [10-15]. The assault detection mechanism for the MANET has not yet been implemented completely. The Secure attack gesture recognition algorithm has a distinct structure and design compared to wired and wireless networks. Because MANET lacks a system, node assaults on the networks are unaffected. To illustrate the situations for the needs of the safe assault detection method, Fig. 1 shows the MANET topology with the source and destination nodes, connections in a network, and malicious nodes.

Ad hoc On-Demand Distance Vector is highly vulnerable to numerous assaults, including wormholes, denial of service, and black hole assaults [13] It is vital to develop a new strategy to address these security vulnerabilities Numerous scholars have suggested various variations of the AODV protocol to address the abovementioned problems. However, there are currently no AODV protocols that address all the above mentioned problems as a solitary framework.

The most recent research findings based on the Mobile Ad-Hoc Network (MANET) security aspect have offered various elements [11]. To ensure a high level of safety in packet forwarding, current research has focused on specific attacks and some approaches that significantly increase communication costs. Based on the findings of the latest analysis, the primary goals were

set for creating the proposed methodology with the overarching goal of offering a high level of protection to the content in the MANET.

- To develop a reliable and secure navigation system that tackles issues with creating a secure path among MANET nodes.
- To manage and minimize packet losses.
- To provide a system that allows nodes to interact with one another about data securely.
- Finding and ultimately stopping the threats in MANET.
- Improving MANET's level of service quality.

II. ROUTING ATTACKS IN MANETS

Routing attacks in MANETs can be categorized into several types:

1. **Black Hole Attack**: A malicious node advertises itself as having the shortest path to the destination but drops the intercepted packets.
2. **Wormhole Attack**: Two or more colluding attackers create a shortcut in the network, disrupting the routing process.
3. **Sybil Attack**: A single node presents multiple identities to other nodes, confusing the routing mechanism.
4. **Gray Hole Attack**: Similar to a black hole attack, but the malicious node selectively drops packets.
5. **Routing Table Overflow Attack**: An attacker tries to create routes to non-existent nodes to overwhelm the routing table.
6. **Blackmail:** This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodesand propagate messages that try to blacklist the offender.
7. **Denial of Service:** Denial of service attacks aim at the complete disruption of the routing function and therefore the entireoperation of the ad hoc network. Specific instances of denial of service attacks include the routing table overflow and thesleep deprivationtorture. In a routing table overflow attack the malicious node floods the network with bogus routecreation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate
8. **Routing Table Poisoning:** Routing protocols maintain tables that hold information regarding routes of the network. Inpoisoning attacks, the malicious nodes generate and send fabricated signaling traffic, or modify legitimate messages fromother nodes, in order to create false entries in the tables of the participating nodes. For example, an attacker cans sendrouting updates that do not correspond to actual changes in the topology of the ad hoc network. Routing table poisoningattacks can result in the selection of non-optimal routes, the creation of routing loops, bottlenecks, and even partitioningcertain parts of the network.

III. SECURE MANET ROUTING PROTOCOLS

The types of attacks that we reviewed in the previous Section cannot be ignored, since it will give rise to the vulnerability in the network and might highly affect the efficiency of the system. Security mechanisms are therefore necessary to mitigate against these eventualities. This section reviews some of the routing security schemes which have been proposed to address the security shortcomings of these protocols.

3.1. Classification of Secure MANET Routing Protocols

Secure Position Aided Ad hoc Routing. The SPAAR protocol was developed with the classical managed-hostile environment in mind, thus meant to provide a very high level of security, and sometimes at the cost of performance. Among other things, SPAAR also requires that each device to use a GPS locator to determine its position, although some leeway is given to nodes using a so-called ―locator-proxy‖ if absolute security is not required. In SPAAR packets are only accepted between neighboring nodes one hop away from each other, this is to avoid the ―invisible node-attack‖. The basic transmission procedure is quite similar to ARAN, although the group neighborhood key is used for encryption in order to ensure one-hop communication only. Since all nodes also have information on their location they only forwardRREQs if their position is closer to the destination The only real security disadvantage currently discovered in SPAAR is that the usage of the certificate server and the extreme need to keep this server uncompromised.

IV. RELATED WORK

Due to its transparency, the changing topology of the network, and the absence of centralized control and monitoring, wireless communication is more vulnerable to attacks than wired ones. In wireless connections, security concerns are becoming ever more crucial. Some considerations should be made when creating an attack node detection mechanism for MANETs. The assault node detection techniques for MANETs will function differently from their wired equivalents. Some issues must be resolved while creating attack node detection techniques for MANETs.

The characteristics of privacy have been covered in several wireless security studies. Numerous studies on protected transit in Mobile Ad-Hoc Networks have been done throughout the last few generations. Since energy constraints and unforeseen events in network activity frequently and unpredictably lead to topological changes, the task of locating and conditioning will lead to WSNs is challenging. The biggest obstacle is figuring out where the agents are while the nodes move. Similarly, the nodes housing the intrusion-detecting agents need more computing power, connectivity, and battery life.

4.1. Implementation Challenges

Implementing a robust security solution in MANETs involves several challenges:

- **Resource Constraints**: Nodes in MANETs typically have limited processing power, memory, and battery life, making it essential to develop lightweight security solutions.
- **Dynamic Topology**: The constantly changing network topology requires adaptive security mechanisms.
- **Scalability**: The solution must scale efficiently with the size of the network.

- **False Positives/Negatives**: Balancing the detection accuracy to minimize false positives and negatives is crucial for effective security.

V. CRYPTOGRAPHY TECHNIQUES

Cryptography is the study of mathematical techniques concerned with protecting information or data from adversaries. Cryptography provides security of information such as Availability, Authenticity, data confidentiality, Data integrity and Non repudiation. Also it provides secure routing in MANETs. Several Cryptographic primitives of functions have been designed in order to achieve the objectives. These primitives can be divided as: 1. Symmetric Key Cryptography: It involves the use of single key. 2. Asymmetric Key cryptography: It involves the use of two keys 3. Message digest: It does not involve use of any keys. Conventional symmetric key cryptography makes use of one key that is shared by both sender and receiver. In this scheme distribution of key must be taken into consideration. Disclosure of this key will result in compromise of communication hence we make use of Asymmetric key cryptography or Public key cryptosystems. Asymmetric key cryptography suits for providing security in MANETs since it makes use of 2 keys such as Public key and private key. Public key defines encryption method while private key defines decryption method. Public key may be known anyone in the network while private key is supposed to be known only to one creating a message. These 2 keys are not same but related by mathematical values. Also it is infeasible to obtain private key knowing only public key and algorithm. Public Key encryption does not require secure channel instead it requires authenticated channel for ensuring genuineness of the public key of other party. Some of the examples are RSA algorithm, ELGAMAL Algorithm and Rabin Algorithm.

REFERENCES

[1] G. Li, F. Liu, A. Sharma, O. I. Khalaf, Y. Alotaibi, A. Alsufyani and S. Alghamdi, "Research on the Natural Language Recognition Method Based on Cluster Analysis using Neural Network," Mathematical Problems in Engineering, vol. 2021, 2021. Crossref, https://doi.org/10.1155/2021/9982305.

[2] H. Xiong, "On the Design of Blockchain-Based ECDSA with Fault-Tolerant Batch Verification Protocol for Blockchain-Enabled Iomt," IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 5 2022. Crossref, https://doi.org/10.1109/JBHI.2021.3112693.

[3] UdhayaSankar S.M, Ganesan R, JeevaaKatiravan, Ramakrishnan M and RuhinKouser R, "Mobile Application Based Speech and Voice Analysis for COVID-19 Detection Using Computational Audit Techniques," International Journal of Pervasive Computing and Communications, vol. 18, no. 5 2020. Crossref, https://doi.org/10.1108/IJPCC-09-2020-0150.

[4] D. Dhinakaran, D. A. Kumar, S. Dinesh, D. Selvaraj and K. Srikanth, "Recommendation System for Research Studies Based on GCR," International Mobile and Embedded Technology Conference (MECON), Noida, India, pp. 61-65, 2022. Crossref,https://doi.org/10.1109/MECON53876.2022.9751920.

[5] Jena Catherine Bel D, Esther C, Zionna Sen G B,Tamizhmalar D, Dhinakaran D and Anish T. P, "Trustworthy Cloud Storage Data Protection based on Blockchain Technology," International Conference on Edge Computing and Applications (ICECAA), pp. 538-543, 2022. . Crossref, https://doi.org/10.1109/ICECAA55415.2022.9936299.

[6] UdhayaSankar S.M, Christo M.S and Uma Priyadarsini P.S, "Secure and Energy Concise Route Revamp Technique in Wireless Sensor Networks," Intelligent Automation and Soft Computing, vol. 35, no. 2, pp. 2337-2351, 2023. Crossref, https://doi.org/10.32604/iasc.2023.030278.

[7] D. Dhinakaran, and P. M. Joe Prathap, "Preserving Data Confidentiality in Association Rule Mining using Data Share Allocator Algorithm," Intelligent Automation & Soft Computing, vol. 33, no. 3, pp. 1877-1892, 2022. Crossref,https://doi.org/10.32604/iasc.2022.024509.

[8] M. M. Mukhedkar and U. Kolekar, "E-TDGO: An Encrypted Trust-Based Dolphin Glowworm Optimization for Secure Routing in Mobile Ad Hoc Network," International Journal of Communication Systems, vol. 33, no. 9, pp. e4252, 2020.

[9] M.Supriya and T.Adilakshmi, "Secure Routing using ISMO for Wireless Sensor Networks," SSRG International Journal of Computer Science and Engineering, vol. 8, no. 12, pp. 14-20, 2021. Crossref, https://doi.org/10.14445/23488387/IJCSE-V8I12P103.

[10] Sharma and L. Tharani, "Ant Colony, Based Node Disjoint Local Repair in Multipath Routing in MANET Network," Wireless Personal Communications, pp. 1–28, 2021.

[11] Sankar, S.M, ChamundeeswariVijaya and KatiravanJeevaa, "Identity-Based Attack Detection and Manifold Adversaries Localization in Wireless Networks," Journal of Theoretical and Applied Information Technology, vol. 67, no. 2, pp. 513-518, 2014.

[12] G. Suryanarayana, K. Chandran, O. I. Khalaf, Y. Alotaibi, A. Alsufyani, and S. A. Alghamdi, "Accurate Magnetic Resonance Image Super Resolution Using Deep Networks and Gaussian Filtering in the Stationary Wavelet Domain," IEEE Access, vol. 9, pp. 71406–71417, 2021. Crossref, https://doi.org/10.1109/ACCESS.2021.3077611.

[13] Velusamy, K. Karunanithy, D. Sauveron, R. N. Akram, and J. Cho, "Multi-Objective Function-Based Node-Disjoint Multipath Routing for Mobile Ad Hoc Networks," Electronics, vol. 10, no. 15, pp. 1781, 2021. Crossref, https://doi.org/10.3390/electronics10151781.

[14] K. Sudharson, A. M. Sermakani, V. Parthipan, D. Dhinakaran, G. EswariPetchiammal and N. S. Usha, "Hybrid Deep Learning Neural System for Brain Tumor Detection," 2022 2nd International Conference on Intelligent Technologies (CONIT), pp. 1-6, 2022. Crossref, https://doi.org/10.1109/CONIT55038.2022.9847708.