International Journal of Emerging Science and Engineering (IJESE)
ISSN: 2319–6378 (Online), Volume-10 Issue-6, May 2022

Detecting Malicious Nodes in Mobile Ad-hoc Networks - A Review

Imran Khan, Pratik Gite

Abstract*: *Every new innovation brings its own set of challenges. Manet, or mobile ad-hoc networks, have the ability to form proxy networks without requiring any standard devices or central administration. The network is wireless and can communicate with each other. First and foremost, a reliable and effective network intrusion detection system (NIDS) must be installed and maintained. A system's data should be protected against access by anyone without authorization. Structures that have interruption detection procedures may be able to estimate future interrupts as well as current interruptions with a high degree of accuracy. There have been artificial intelligence approaches for organizing interruption locations for more than two decades, and there are numerous approaches. A reliable interruption detection system will probably remain a subject of debate for some time. The number of digital assaults and the volume of system information continue to grow at an alarming rate, forcing companies to devise better methods for keeping their systems and information secure.

Keywords*: *Portability; Signatures.

I. INTRODUCTION

This Due to their dynamic topology, distributed channel sharing, open wireless medium, and constraints on power and computation, MANETs are more susceptible to security attacks than traditional wired networks. Because each device in a MANET is free to move in any direction, it will regularly change its links with other devices. The key problem in constructing a MANET is supplying each device with the necessary information to appropriately route traffic, these networks can be self-contained or connected to the larger Internet. An intrusion detection system (IDS) is a hardware or software programme that monitors network or system activity for malicious activity or policy breaches and generates reports for a Management Station. Intrusion Detection Systems (IDS for short) are designed to catch what might have gotten past the firewall. They can either be designed to catch an active break-in attempt in progress, or to detect a successful break-in after the fact. In the latter case, it is too late to prevent any damage, but at least we have early awareness of a problem.

Multi-hoc network pathways can be constructed in a mobile ad Hoc community (MANET), in which each node serves as a router, without the requirement for a telecommunications backbone. Whilst a wireless network is utilized in area of a stressed network, it is ideal for navy and emergency rescue operations, in addition to for brief-time period lecture room or conference events. The security of such a community should be given high significance. The openness of the wireless medium lets in outsiders to observe and interfere with network interest as a consequence of its use with the aid of criminals. Such considerations may expose sensors to a broad variety of assaults [1] as a result of their implementation. These malicious nodes are able to launching both passive and competitive assaults at the community from their positions. However, energetic attacks may additionally require the rogue node to spoof or reject real messages further to simply listening in on them. Wormhole assaults are a commonplace form of energetic security attack that has the capacity to do massive harm. An attacker collects packets from one website online in a community and provides them to some other malicious node, which then repeats the packets in its very own community, thereby inflicting the community to crash. This lively assault poses a danger to wireless security systems and routing protocols, as well as aggregated and clustered data storage systems. MANET Communication and Intrusion Mobile ad hoc network (MANET) comprises of wireless devices to move in random directions for communicating with one another without infrastructure. Other nodes act as routers communication through multiple intermediate nodes between source and destination. MANETs susceptible to security attacks.

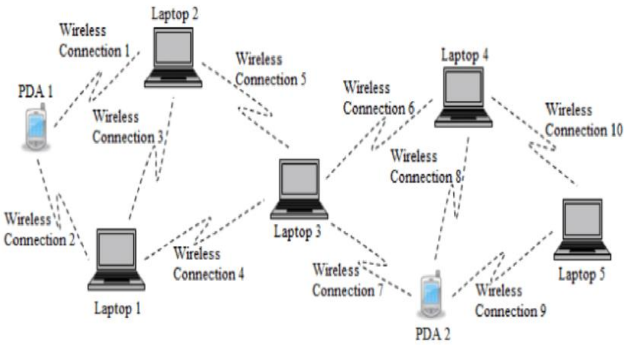

Fig. 1. Example of mobile ad-hoc Network [2]

A. Applications of MANET

Versatility and adaptability of MANET makes it an extreme key for an expansive assortment of uses.

Manuscript received on 21 February 2022
Revised Manuscript received on 16 April 2022
Manuscript published on 30 May 2022
***** Correspondence Author

Imran Khan*, Research Scholar, Department of Computer Science and Engineering, IPSA IES, Indore (M.P), India. E-mail: imran.khanikik@gmail.com

Dr. Pratik Gite, Associate Professor, Department of Computer Science and Engineering, IPSA IES, Indore (M.P), India. E-mail: pratikgite@ipsacademy.org

- The most basic use of MANET is gathering correspondence amid meetings.
- Prior, military vital operations were the main applications in which MANETs were habitually sent.
- MANETs are generally utilized for correspondences at areas where there is no accessibility of system framework, either in light of the fact that the foundation has been annihilated or the cost of its establishment does not allow the organization of a system. For instance, military units included troopers and tanks together frame a specially appointed system while meandering in a combat zone.
- Quick and simple organization of MANET makes it reasonable for use in circumstances, for example, surge, fire blast, earth tremor and the ranges of fiasco and common cataclysms. These systems likewise assume a crucial part in safeguard missions, swarm control and observations.

B. Characteristics of MANET

- Manet's dynamic nature makes it incredibly dependable; nodes can move about freely without relying on permanent infrastructure, allowing Manet to perform in a larger range.
- Routing is the backbone of Manet; it allows the network to respond quickly and reliably. Because all of the devices connected to this network are mobile, Manet must ensure that its network is available to all users to its maximum capacity while also maintaining security.
- Manet is made up of dozens of protocols that are classified as proactive, reactive, or hybrid, such as AODV, DSR, and DREAM.
- Manet ensures that security is one of the most important features for us, since it does not allow any unauthorised nodes to communicate or participate in any network function. It acknowledges its all transmission to ensure this, also cryptography method is also introduced in the Manet to increase the layer in a security.

II. LITERATURE REVIEW

In this [3] paper the author used triangle encryption to prevent fraudulent reply packets (TE). When a sender sends a plain text RREQ packet to a node that knows the route to the destination, the node simply forwards the RREQ packet to the destination.

The encryption text is sent back to the source by the destination node. When a source receives a response, it verifies its legitimacy by examining the cypher text. Because he doesn't have encrypted text, a malicious node sends a reply without examining the routing table. In [4] here by counting RREP packets, the author was able to detect a black hole attack. If a node sends one RREP, it is regarded a legitimate destination. If it receives multiple RREPs, one of them is from a legal destination, while the others are generated by the malicious node. The author also keeps a Route Reply Table (RRT), which keeps track of the RRRP message's sequence number and arrival time. The author detected black hole attack in [5] by comparing its sequence number to a dynamically updated threshold value within the time interval. The black hole attack is identified and the node is declared a malicious node if sequence no is more than the threshold value. The malicious node is notified of this by sending an alert packet, and the malicious node's response is destroyed. When adjacent nodes become aware of a malicious node, they begin to ignore and eliminate packets from that node.

In [6] the author detected a black hole attack by giving the node two IP addresses, one real and the other invalid. Without the attacker's environment, all nodes would ordinarily relay packets received from nodes, but the attacker's node would respond to an invalid address. Amish Parmar and co-authors. WSN wormhole attack frameworks are examined and a strategy for acknowledging wormhole strike and evading it is provided in this study. In this tactic, the AOMDV (Ad hoc on intrigue Multipath Distance Vector) legacy is blended with RTT (Round Trip Time) framework and wormhole ambush's various properties. In writing, the recommended strategy seems to be comforting when it stands out from the rest of the options. All entertainment is played out using the NS2 test framework [9]. In [7], The authors suggested a secure routing protocol based on fuzzy logic that computes a secure path from the sending host to the destination host based on the trust, energy, and dependability levels. During the path discovery process, a node calculates the trust and energy levels and stores them in the Route Request (RREQ) packet. The destination node uses the reliability value to select the best path. To increase both network security and node energy consumption in MANETs, an energy consumption model [8] that calculates the energy and trust levels of nodes is presented. The Honorable G. Vijaya Lakshmi The queuing technique introduced by Dr. C. Shoba Bindhu, thereby increases the network metrics such as total network throughput, decreases the route time, overhead, and traffic blocking likelihood. An ad hoc network's routing strategy is used to construct the method [10]. In [11], a clustering solution using a public-key cryptosystem is proposed, with a cluster leader in each cluster network. Every node has a public key that is visible to all nodes in the network and a private key that is only visible to a single node. The cluster leader holds all of the public keys for all nodes in their network, as well as its own private key portions, which it retains to itself and uses to decode and encrypt messages for transmission.

III. RESEARCH SCOPE

Because of its dynamic nature Manet, it doesn't follow a pre-determined path but rather monitors the current situation and acts accordingly. For example, as network traffic increases, it initiates the multipath mechanism, causing incoming packets to be dropped at the router's bottleneck. Excess packets arrive at the network, causing the network to retransmit the packets, increasing the strain on it.

All of these conditions reduce the overall network performance. It is important to highlight that any of the algorithms, techniques, or mechanisms that we are providing or that any author is providing are not an ultimate answer because the freedom in the structure of the Manet might generate very large changes in the entire network. The routing architecture is meant to achieve its aim, and in the future, better algorithms and formulae can be implemented in terms of earlier congestion detection, allowing for more precise values to be calculated, boosting the Manet's performance.

When a multiple route is being identified, not only one but many paths are discovered, but only one of them is chosen to transmit the packets; the other paths are kept in reserve in case the primary path fails to complete its mission.

IV. CONCLUSION

Due to progress of Ad-hoc Networks and are used in many areas, Mobile Ad-hoc Network has gotten a lot of attention in recent years from academics. The detection of Malicious Nodes and detection of previously unknown problems through Deep learning and Machine learning algorithms serve critical role in identification of such malicious elements in a wide range of fundamental implementation across a broad range of application areas and they are becoming popular. However there are number of more techniques and still a number of hurdles to overcome the issue of MANET securities.

REFERENCES

1. Mohd Zaki and H. Rosilah, “The implementation of Internet of Things using test bed in the UKMnet environment,” AsiaPacific Journal of Information Technology and Multimedia, vol. 8, no. 2, pp. 1–17, 2019
2. R. Almaharmah, "Multi-Aware Cluster Head Maintenance for Mobile Ad Hoc Networks with Wireless Power Transfer Capabilities", Ph.D, Universität Duisburg-Essen, 2016
3. Nabarun Chatterjeea , Jyotsna Kumar Mandalb, “ Detection of Blackhole Behaviour using Triangular Encryption in NS2”,elsevier, Procedia Technology 10 (2013), pp-524 – 529
4. Tarek M. Mahmoud, Abdelmgeid A. Aly, Omar Makram M, “ A Modified AODV Routing Protocol to Avoid Black Hole Attack in MANETs", International Journal of Computer Applications (0975 – 8887) Volume 109 – No. 6, January 2015,pp-27-33
5. Reza Amiri, Marjan Kuchaki Rafsanjani and Ehsan Khosravi ,“Black Hole Attacks Detection by Invalid IP Addresses in MobileAd Hoc Networks”, Indian Journal of Science and Technology, Vol 7(4), April 2014,pp.401–408.
6. C. Karlof and D. Wagner, Secure routing in wireless sensor networks: attacks and counter measures, University of California at Berkeley, 2003.
7. yal N. Raj, Prashant B. Swadas. “DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV Based 3 MANET”, IJCSI International Journal of Computer Science Issues,2009, pp.54-59
8. S. Sahraoui1 and S. Bouam, Secure Routing Optimization in Hierarchical Cluster-Based Wireless Sensor Networks, International Journal of Communication Networks and Information Security (IJCNIS), 5, 3(2013), pp. 178-185.
9. Amish Parmar, V.B.Vaghela, “Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol”, Science Direct, 7th International Conference on Communication, Computing and Virtualization 2016, Page No. 700-701.
10. G.Vijaya Lakshmi Dr. C.Shoba Bindhu, “ Congestion Control Avoidance in Ad hoc network using queuing model”, International Journal of Computer Technology and Applications, pp 750-760, vol 2, Issue 4, 2011.
11. T. S. Bharati and R. Kumar, Secure Intrusion Detection System for Mobile Adhoc Networks, 2nd International Conference on Computing for Sustainable Global Development (INDIACom), 2015, pp. 1257–1261

AUTHORS PROFILE

Imran Khan has received B.E (C.S.E) from Jawaharlal Institute of Technology Borawan, Khargone in year 2019 and M.E.(C.S.E) from IES, IPS Academy Indore in year 2022. His areas of interests are Mobile Ad-hoc Network, Software Testing, Software Engineering, Computer Network. He has published 2 paper in various international and national conferences. Research Scholar, Department of Computer Science Engineering, IPSA IES, Indore India. E-mail: imran.khanikik@gmail.com

Dr. Pratik Gite has completed his B.E. and M.E. from RGPV University Bhopal (M.P). He holds a PhD in wireless Mobile Ad-hoc Network from Pacific Academy of Higher Education & Research University, Udaipur Rajasthan. He started his academics at LKCT Indore (MP). Associate Professor, Department of Computer Science Engineering, IPSA IES, Indore India. E-mail: pratikgite@ipsacademy.org