A Review Paper to Improve The Security of Mobile Ad HOC Networks For Energy-Saving System on Wormhole Detection and Prevention

Md. Imran Ansari
MTech Scholar
Sagar, Institute of Research & Technology
Bhopal, Madhya Pradesh, India
imraininfo70@gmail.com

Ashish Chourey
Assistant Professor
Sagar, Institute of Research & Technology
Bhopal, Madhya Pradesh, India

Abstract An overview of mobile ad hoc networks, security issues, and various attack types is provided in this study. Additionally, wormholes are linked by MANET as a serious thread that has been successfully separated from the network in question. Wormhole attacks are seen as a major risk to multi-hop ad hoc networks' security. Wormhole attacks include the attacker creating a tunnel from one network end to another, with nodes at either end assuming the role of genuine neighbors and gaining access to the discussion through the wormhole link. Worm hole attacks, in contrast to many other ad hoc routing attacks, cannot be stopped by cryptographic methods since hackers modify or generate new packages before they are discovered. This paper proposes a straightforward method for efficiently detecting wormhole attacks without the need for specialized hardware, location, or timing of the strict requirements. The suggested method offered a hybrid model that combined location-assisted route analysis with route redundancy using a graphical-based system. In order to identify whether a wormhole is present, this technique uses routing variation between neighbors. Simulations for various wormhole node distributions and connection models have been used to test the method

Keywords:- MANET, Attack Over MANET, Wormhole Attack, AODV, LAR Protocol.

I. INTRODUCTION

On the of network architecture wireless network can be divided in two categories infrastructure-based network and infrastructure-less network. In the infrastructure-based networks, all the devices are connected with a pre-constructed infrastructure and make fixed network architecture. Through these pre-constructed infrastructures, services are delivered in the network. For example, cellular mobile networks are infrastructure-based networks that are made from (PSTN) public-switched telephone network mainstay controls, mobile switching centers (MSCs), base locations, and mobile hosts. The role of each node of the network is specific for routing the data, and a stringent signaling structure among the nodes is followed by the connection establishment. Wireless local area networks are another example of infrastructure-based network.

In Infrastructure-less networks an arbitrary set of self-regulating wireless devices are formed dynamically through the co-operation, and make a network that is called an infrastructure-less network. The explicit role of each node is not predefined. Typically apiece node is expected to be clever to forward the packets for any different node if it is requested to do so. Built on network condition all node can freely make its own decision. Mobile ad-hoc network and wireless sensor networks are the examples of infrastructure- less network.

Properties of Wireless Ad hoc Network

Ad hoc networks have certain characteristics [8] that set them apart from conventional networks and help them accomplish the objective of delivering connectivity anywhere. Because ad-hoc networks are established to accomplish a specific objective then disband once that objective is accomplished, they are transient networks. On ad hoc networks, mobile devices have a dynamic architecture and can join or leave the network at any time. The majority of mobile gadgets communicate via wireless or infrared frequencies, which results in an extremely short transmission range. Multi-hop routing pathways are generally used to improve the transmission range. The ability of ad hoc networks to self-organize is its most notable characteristic. Without a trustworthy third party (TTP), all network connections—including those that establish a secure channel between nodes and initialize recently joined nodes—should be able to be executed. As a result, ad hoc networks are not dependent on a fixed infrastructure or the availability of a TTP like wireless networks are. Ad hoc networks have the self-organization trait, which makes it challenging to design security procedures.

II. MOBILE AD HOC NETWORK

With the necessity for a fixed network or infrastructure, the mobile ad hoc network [6] is a type of centralized management that inadvertently sets itself up from a number of mobile nodes. Each node in this type contains a wireless transmitter and receiver, so you can link to other nodes. It is preferable to resend a packet to a node that is outside the radio's range and is supported by other network nodes; this is referred to as a multi-hop version. Consequently, each node must serve as both a host and a router. Network topology frequently changes as a result of mobile nodes' involuntary movement throughout the network. Because the nodes are dispersed over a battlefield and lack the infrastructure necessary to build a network, MANET was primarily developed for military applications. Due to its ability to be constructed without the need for "an infrastructure or interaction with a human being," MANETs are rapidly expanding and being used in a variety of fields, including commercial, military, and civilian ones. Examples include data collecting, virtual classes, search and rescue, and conferences where laptops, PDAs, or other mobile devices interact and share wireless resources. The security issue has grown to be one of the main issues due to the widespread usage of MANET. For instance, the majority of MANET's routing protocols assume that all network nodes are compliant and not malicious. As a result, mistakes can spread throughout the network from a single hacked node.

III. CERTAINTY PROBLEMS WITH THE MOBILE AD HOC NETWORK

MANET is vulnerable to many kinds of assaults. Some of the assaults are specific to MANET, while others impact the wireless network and the worldwide network. For instance, there are a number of factors that can be used to differentiate security threats, assaults or methods of attack. The following categories can be used to broadly classify security attacks from MANETs and all other networks: Cryptographic or non-cryptographic, active or process, internal or external, distinct, and private.

Passive vs. active attacks

Internal vs. external attacks

Eavesdropping

Interference and Jamming

Blackhole attack

Byzantine attack

Rushing attack

Malicious code attacks

Denial of service

Impersonation attacks

Man-in-the-middle attacks

Wormhole attacks

IV. LITERATURE REVIEW

By Muhannad Tahboush and Mary Agoyi "A Hybrid Wormhole Attack Detection in Mobile Ad-Hoc Network (MANET)" in IEEE, 2021. Decentralized wireless networks known as Mobile Ad-hoc Networks (MANET) can interact without the need for pre-existing infrastructure. Manets are susceptible to the most common threats and attacks, including wormhole attacks. Wormhole attacks are extremely difficult problems that record packets from one part of the network and tunnel them to another part of the network. This degrades the wireless network's performance and messes with the routing protocol the most.

By Rajendra Prasad P, Shivashankar "Enhanced Energy Efficient Secure Routing Protocol for Mobile Ad-Hoc Network" ScienceDirect Global Transitions Proceedings 3 (2022). Wireless networks are seen to be the most effective networks, and Mobile Ad-hoc NETworks (MANETs) in particular have found numerous uses for their ability to transmit data in real-time. The present routing protocols employed specifically in MANETs are limited by the concomitant issues. The network's design challenges include limiting energy consumption during information transmission and ensuring node security. In the current routing protocols, a route originates from a source node that uses energy to send messages to its neighboring nodes in an attempt to find a path to the target node. Enhancing energy efficiency and ensuring routing protocol security are problems for mobile ad hoc networks.

By Saad Al-Ahmadi "A Novel Energy-efficient Wormhole Attack Prevention Protocol for WSN based on Trust and Reputation Factors" (SENSORNETS 2022). Although the Internet of Things (IoT) benefits greatly from the implementation of Wireless Sensor Networks (WSNs), there are certain security concerns. The Wormhole assault is one of the many threats that Wireless Sensor Networks (WSNs) are susceptible to. Even when the transmission is genuine and the sensors are unhacked, the Wormhole assault is one of the most serious and difficult to protect against on WSNs.

By Y. C. Hu, A. Perrig, and D. B. Johnson, *"Packet leashes: a defense beside wormhole attacks in wireless networks",* in *Proc. of IEEE INFOCOM,* 2003. A defense against network worms: As mobile applications for mobile applications are organized, security is a key requirement. The author presents the pyramid attack; A serious problem in an ad hoc network is a solid foundation to defend. The wormhole attack is possible even if the attacker has not cooperated with the hosts and even if all communications provide authenticity and confidentiality.

By P. Papadimitratos and Z. J. Haas, *"Secure routing for mobile adhoc networks",* in *Proc. of CNDS,* 2002. Writers discover a path that reduces adverse effects that lead to bad behavior, to provide adequate link information. Their protocol is compromised, or response responses are deactivated or the keyword button will never return. The only need for the proposed scheme is the existence of an initiated keyword search and destination safety link. In particular, there is no mid note hypothesis to show arbitrary and malicious behavior [10]. The protocol offers a number of features, such as checking the order to the destination.

By K. Sanzgiri, B. Dahill, E. M. Belding- Royer B. N. Levine, C. Shields, and, *"A secure routing protocol of ad hoc networks",* in *Proc. Of IEEE ICNP,* 2002. With a focus on AODV and DSR, the author has described the security risks associated with ad hoc routing protocols in depth. A solution for a controlled, open scenario where no network infrastructure has been installed previously but some pre-security coordination is needed is developed in light of these dangers. They define three distinct settings with varying security requirements. Its certificate-based ARAN protocol effectively thwarts every known attack. [11].

V. OBJECTIVE OF WORK

Ad hoc networks are vulnerable to a variety of security threats and usually function in an unsecure, open, and nervous environment. The wormhole attack has gained a lot of attention lately and is a blitz on ad hoc systems. Wormhole attacks occur when a hacker intercepts packets from a specific spot inside the system and tunnels to a distant location where they replicate, typically unaltered. Consequently, wormhole detection is a critical network.

A wormhole attack must draw a lot of network traffic in order to have a significant effect on the network, and this is accomplished by providing a quicker path to the target network. As a result, the wormhole's passageways must be smaller than its alternatives. using legitimate network nodes.

Furthermore, it is evident that the majority of the wormhole detection techniques mentioned above perform poorly and are comparatively more complicated. Since mobile nodes run on a little amount of battery power, it is imperative to create a method that can effectively fend off wormhole attacks while retaining simplicity.This work's goal is to develop a novel approach that can effectively fend off wormhole attacks.

VI. PROPOSED METHODOLOGY

The wormhole attacks pose a seriousi threat to ani ad hoc network for mobile phones. And it cannot easily be registered. A technique has been proposed for detecting the wormhole attacks in MANET. In a wormhole attack, two attack nodes come together. A hacker button receives packets at ai given time and "tunnels" to another attack node via ai private network connection and then repeats them to the network. The wormhole holds the nodesi attacked in a dominant position compared to other nodes on the network ini the immediate AODV routing protocols as the attackers in each query packet, route to another attacker close to the node of destiny thei tunnel could. When the neighbors on the destination listen to this RREQ, they return this RREQ, and then delete all other RREQs received in the same route search process. This type of attack prevents other routes from being detected instead of the wormhole, I thus eliminating ai permanent refusal of service attacks for datai or specific packages to be removedi selectively or a change is required [19].

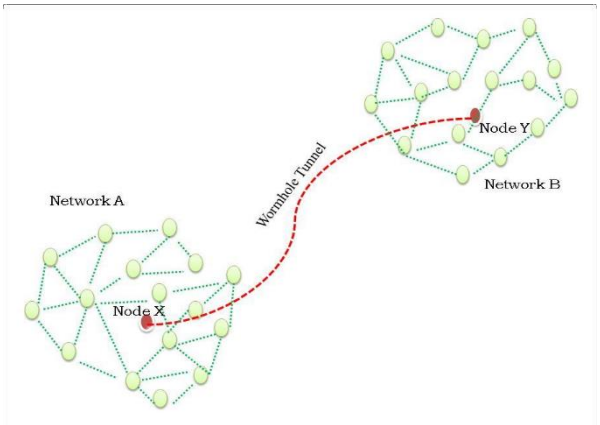

Figure 5.1 Wormhole attack

VII. PROPOSED FRAMEWORK

The proposed framework is shown ini figure 5.8. There arei six major component of this framework. Staringi with selecting target node wherei the destinationi node will decide. In next sectioni hello packet will send to other nodes. After thati neighbor nodei will count. This will help to calculate the number of hopes togeti the destination node. This hope count willi compare with the threshold which was already calculated. If thisi hope count will grater theni the thresholdi value so there is wormhole ini the network. Otherwise data packet will transfer to the next node.

z

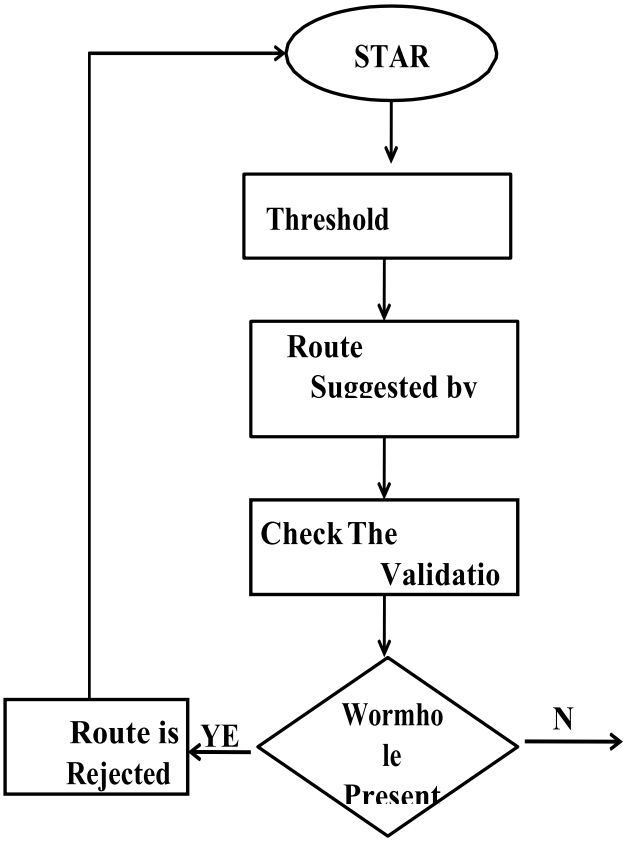

Figure 5.8 Framework of Algorithm.

Expected Outcome

The dissertation presents a straightforward method for identifying wormholes in ad hoc networks. To ascertain whether an AI wormhole exists, this technique uses routing variations between neighbors. In addition to being confined and requiring minimal effort, the approach guarantees that no specific hardware, location data, or precise node synchronization are needed. Simulations for various node distributions for wormholes and connectivity models have been used to test this technique. The approach has great detection probability with few false alarms that rely on the threshold value below all evaluated scenarios.

Conflict of Interest: The corresponding author, on behalf of all authors, confirms that there are no conflicts of interest to disclose.

REFERENCES

[1] Muhannad Tahboush and Mary Agoyi "A Hybrid Wormhole Attack Detection in Mobile Ad-Hoc Network (MANET)" in IEEE, Received December 28, 2020, accepted January 11, 2021, date of publication January 13, 2021, date of current version January 22, 2021. *Digital Object Identifier 10.1109/ACCESS.2021.3051491,* VOLUME 9, 2021.

[2] Rajendra Prasad P, Shivashankar "Enhanced Energy Efficient Secure Routing Protocol for Mobile Ad-Hoc Network" Global Transitions Proceedings 3 (2022) 412–423, ScienceDirect. https://doi.org/10.1016/j.gltp.2021.10.001, journal homepage: http://www.keaipublishing.com/en/journals/global-transitions-proceedings/

[3] Saad Al-Ahmadi "A Novel Energy-efficient Wormhole Attack Prevention Protocol for WSN based on Trust and Reputation Factors" ISBN: 978-989-758-551-7; ISSN: 2184-4380 DOI: 10.5220/0010951400003118, In Proceedings of the 11th International Conference on Sensor Networks (SENSORNETS 2022), pages 191-201.

[4] Soo-Young Shin; Halim, E.H., "Wormhole attacks detection in MANETs using routes redundancy and time-based hop calculation," in *ICTC, 2012 International Conference on* , vol., no., pp.781-786, 15-17 Oct. 2012

[5] Xiangyang Li, Wireless Ad Hoc and Sensor Networks: Theory and Applications, Cambridge University Press.

[6] HimaniBathla, KanikaLakhani, “A Novel Method for Intrusion Detection System to Enhance Security in Ad hoc Network,” journal of computing, volume 2, issue 5, may 2010.

[7] TiranuchAnantvalee, Jie Wu, a Survey on Intrusion Detection in Mobile Ad Hoc Networks.

[8] Guang Gong, KatrinHoeper, Pre-Authentication and Authentication Models in Ad Hoc Networks.

[9] Y. C. Hu, A. Perrig, and D. B. Johnson, “Packet leashes: a defense beside wormhole attacks in W networks,” in Proc. of IEEE INFOCOM, 2003.

[10] P. Papadimitratos and Z. J. Haas, “Secure routing for mobile ad hoc W networks,” in Proc. of CNDS, 2002.

[11] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding- Royer, “A secure routing protocol for ad hoc networks,” in ProcOf IEEE ICNP, 2002.

[12] L. Hl and lEvans, “Using directional antennas to avert wormhole attacks,” in Proc. of NDSS, 2004.