International Journal of Advanced Multidisciplinary Research (IJAMR)
ISSN: 2393-8870
www.ijarm.com
Coden:IJAMHQ(USA)

Research Article

An efficient method to detect Sybil attack using genetic optimization algorithm in Manet

Er. Ruhika Badhan[1] and Er. Bhubneshwar Sharma[2*]

[1]M.Tech Student, Department of Electronics and Communication Engineering, S.S.C.E.T,
Under Punjab Technical University, India
[2]Assistant Professor, Department of Electronics and Communication Engineering, S.S.C.E.T,
Under Punjab Technical University, India
*Corresponding Author : *bhubnesh86@gmail.com*

Keywords

ALOHA,
DARPA.

Abstract

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology. A Mobile Ad hoc Network (MANET) consists of a set of communicating wireless mobile nodes or devices that do not have any form of fixed infrastructure or centralized authority. The security in MANET has become a significant and active topic within the research community. This is because of the high demand in sharing streaming video and audio in various applications .Once MANET is setup it quickly facilitate communications in a hostile environment such as battlefield or emergency situation likes disaster rescue operation. In spite of the several attacks aimed at specific nodes in MANET that have been uncovered, some attacks involving multiple nodes still receive little attention. A reason behind this is because people make use of security mechanisms applicable to wired networks in MANET and overlook the security measures that apply to MANET. Furthermore, it may also have to do with the fact that no survey or taxonomy has been done to clarify the characteristics of different multiple node attacks. This paper addresses the mentioned gap by providing a proper definition and categorization of Sybil attacks in MANET. The whole simulation will take place in MATLAB environment. In the end performance is measured by using the parameters like network load and throughput.

I. Introduction

- Vehicular Ad hoc Networks (VANETs) are used for communication between vehicles and roadside equipment. Intelligent vehicular ad hoc networks (InVANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents.

- Smart Phone Ad hoc Networks (SPANs) leverage the existing hardware (primarily Bluetooth and Wi-Fi) in commercially available smart phones to create peer-to-peer networks without relying on cellular carrier networks, wireless access points, or traditional network infrastructure. SPANs differ from traditional hub and spokenetworks, such as Wi-Fi Direct, in that they support multi-hop relays and there is no notion of a group leader so peers can join and leave at will without destroying the network.

- Internet based mobile ad hoc networks (iMANETs) are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. For example, multiple sub-MANETs may be connected in a classic Hub-Spoke VPN to create a geographically distributed MANET. In such type of networks normal ad hoc routing algorithms don't apply directly. One implementation of this is Persistent System's CloudRelay.

- Military / Tactical MANETs are used by military units with emphasis on security, range, and integration with existing systems. Common waveforms include the US Army's SRW, Harris's ANW2 and HNW, Persistent Systems' Wave Relay, Trellisware's TSM and Silvus Technologies' StreamCaster.

- A mobile ad-hoc network (MANET) is an ad-hoc network but an ad-hoc network is not necessarily a MANET.

In the previous couple of decades the world has turn into a worldwide town by prudence IT sector. Information Technology (IT) is developing step by step. Organizations have a tendency to utilize more difficult system situations. Regardless of the endeavors of system heads and IT merchants to secure the computing situations, the dangers posed to individual protection, organization security and different resources by attacks upon systems and PCs. The Mobile Ad hoc Networks (MANETs) are unquestionably a piece of this revolution [1]. A MANET is an accumulation of wireless devices or hubs that impart by dispatching packets to each other or for another device/hub, without having any framework controlling information for routing. MANET hubs have boundless network and versatility to different hubs. Having a secured transmission and correspondence in MANET is a key issue because of the way that there are different sorts of attacks that the mobile system is interested in [2]. To secure correspondence in such systems, understanding the at risk security attacks to MANET is an extraordinary task and concern. MANET’s experience the ill effects of a mixed bag of security attacks and dangers, for example, Denial of Service (DoS), flooding attack, mimic attack, wormhole attack, black hole attack, etc [3].Past studies demonstrate that there are distinctive classifications of attacks on MANET, for example, Passive and Active attacks, Internal and External attacks and the Routing and Packet Forwarding attacks. Some of these attacks are termed as single attacks while some are alluded to as attacks on numerous hubs and are noxious. In this paper, we make investigation on the Sybil attacks against MANET and provide a new categorization of multiple node attacks. In addition, based on the characteristics of these attacks, a proper definition of such attacks in MANET will be presented. After that,the simulations that will be done using genetic algorithm in DSR protocol.

II. Characterstics

The growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid-1990s. Many academic papers evaluateprotocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput, ability to scale, etc.

1. **Distributed operation***:* There is no foundation system for the focal control of the system operations; the control of the system is dispersed among the hubs. The hubs included in a MANET ought to collaborate with one another and impart among themselves and every hub goes about as a hand-off as required, to actualize particular capacities, for example, directing and security [10].
2. **Multi hop routing***:* When a hub tries to send data to different hubs which is out of its correspondence run, the packet ought to be sent through one or more middle hubs.
3. **Autonomous terminal***:* In MANET, every portable hub is an autonomous hub, which could work as both a host and a router.
4. **Dynamic topology***:* Nodes are allowed to move subjectively with distinctive paces; accordingly, the system topology may change haphazardly and at any time. The hubs in the MANET alertly build up routing among themselves as they go around, setting up their own system.
5. **Light-weight terminals***:* In greatest cases, the hubs at MANET are portable with less CPU capacity, low power memory and little memory size.

III Applications

Areas	Possible scenarios
Military Scenarios	Military communications and automated battle fields mainly based on MANET network.
Rescue	MANET helps in Disaster recovery, means additional of fixed infrastructure
Data networks	The exchange of data between mobile devices is also based on MANET.
Device operations	Wireless connections between various mobile devices are dependent on device networks.
Free internet connection	It also allows us to share the internet with other mobile devices.

Conclusion

Peer to peer systems play an ever-increasingly important part in our daily lives. However, most of the peer-to-peer systems are vulnerable to Sybil attacks. In order to design more efficient and practical Sybil defences, we proposed an implementation based on Genetic algorithm which is essentially a search heuristic or evolutionary algorithm that mimics the process of evaluation. Genetic algorithms (GAs) are computer based search techniques patterned after the genetic mechanisms of biological organisms that have modified and flourished inaltering extremely bloodthirsty surroundings. Previous decade has witnessed many thrilling advances in the use of genetic algorithms (GAs) to solve optimization tribulations in process control systems. Genetic algorithms (GAs) are the resolution for optimization of hard problems quickly, reliably and accurately. As the complication of the real-timecontroller increases, the genetic algorithms (GAs) applications have grown in more than equal measure.

References

[1] S. Buchegger, C. Tissieres, and J.-Y. L. Boudec, “A test-bed for misbehavior detection in mobile ad-hoc networks: How much can watchdogs really do,” in Proc. 6th IEEE Workshop Mobile Comput. Syst. Appl., Dec. 2004, pp. 102–111.

[2] A. Parameswaran, M. I. Husain, and S. Upadhyaya, “Is RSSI a reliable parameter in sensor localization algorithms: An experimental study,” in Proc. F2DA, 2009.

[3] C. Bettstetter, G. Resta, and P. Santi, “The node distribution of the random waypoint mobility model for wireless ad hoc networks,” IEEETrans. Mobile Comput., vol. 2, no. 3, pp. 257–269, Jul.–Sep. 2003.

[4] H. Bidgoli, The Internet Encyclopedia, vol. 3. New York: Wiley, 2004, p. 127.

[5] I. Chlamtac, M. Conti, and J. J.-N. Liu, “Mobile ad hoc networking: Imperatives and challenges,” Ad Hoc Netw., vol. 1, no. 1, pp. 13–64, 2003.

[6] J. R. Douceur, “The Sybil attack,” presented at the Revised Papers from the First Int. Workshop on Peer-to-Peer Systems, 2002, pp. 251–260.

[7] J. Newsome, E. Shi, D. Song, and A. Perrig, “The Sybil attack in sensor networks: Analysis and defences,” presented at the 3rd Int. Symp.
Information Processing in Sensor Networks (IPSN), 2004, pp. 259–268.

[8] B. Parno and A. Perrig, “Challenges in securing vehicular networks,” in Proc. 4th Workshop HotNets, 2005, pp. 1–6.

[9] K. Hoeper and G. Gong, “Bootstrapping security in mobile ad hoc networks using identity-based schemes,” in Security in Distributedand Networking Systems (Computer and Network Security). Singapore: World Scientific, 2007.

[10] S. Hashmi and J. Brooke, “Toward Sybil resistant authentication in mobile ad hoc networks,” in Proc. 4th Int. Conf. Emerging SecurityInform., Syst. Technol., 2010, pp. 17–24.