International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

A Review on Various Approaches for Attack Detection in MANET

Ravi Verma[1], Manasvi Mannan[2]

Research Scholar, Punjab College of Engineering & Technology, Lalru, Pb.

HOD, Punjab College of Engineering & Technology, Lalru, Pb.

Abstract: ***MANETs are a sort of Wireless specially appointed system that typically has a routable systems administration environment on top of a Link Layer impromptu system. Mobile ad hoc networks (MANETs) turn out to be very useful in the current application areas for networks that require ad hoc connectivity as well as mobility. While the MANET routing protocols were designed it was assumed that there is no chance to have a malicious node in the network that does not co operate with each other to transmit data. Because of this fact, the network layer of MANETs is vulnerable to attacks of several kinds. Here in this paper, different kinds of attacks on MANETs are discussed first and then some protection mechanisms against those attacks are discussed. Comparisons of these mechanisms are also included.***

Keywords: Mobile ad hoc networks, Attacks, Network Security, Intrusion Detection, and Network layer security.

1. Introduction

1.1 MANET

A Mobile Ad-hoc Network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. Each of the nodes has a wireless interface to communicate with each other.

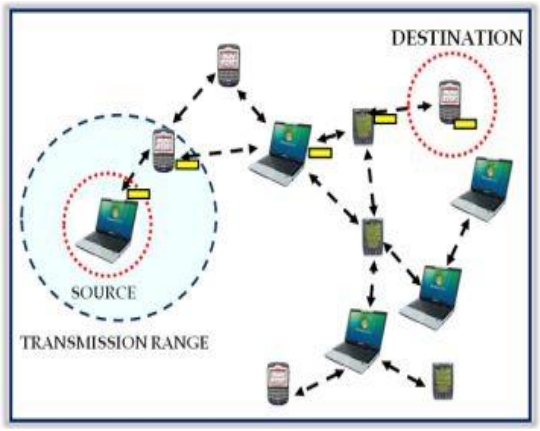

Fig 1.1: MANET

These networks are fully distributed, and can work at any place without the help of any fixed infrastructure as access points or base stations. MANETs are a sort of Wireless specially appointed system that typically has a routable systems administration environment on top of a Link Layer impromptu system [1].

1.2 Types of MANET

1.2.1 Vehicular Ad hoc Networks (VANETs): are utilized for correspondence in the middle of vehicles and roadside supplies. Clever vehicular impromptu systems (InVANETs) are a sort of manmade brainpower that helps vehicles to act in insightful behavior amid vehicle-to-vehicle impacts.

1.2.2 Smart Phone Ad hoc Networks(SPANs): influence the current equipment (basically Bluetooth and Wi-Fi) in financially accessible advanced cells to make distributed systems without depending on cell transporter systems, remote access focuses or customary system base. Compasses contrast from customary center and talked systems [2], for example, Wi-Fi Direct, in that they help multi-jump transfers and there is no thought of a gathering pioneer so companions can join and leave freely without destroying the system [3].

1.2.3 Internet based versatile impromptu systems(I MANETs): are specially appointed systems that connection portable hubs and altered Internet-portal hubs. Case in point, numerous sub-MANETs may be associated in an exemplary Hub-Spoke VPN to make a geologically circulated MANET. In such sort of systems ordinary impromptu directing calculations don't have any significant bearing straightforwardly.

1.2.4 Military/ Tactical MANETs: are utilized by military units with accentuation on security, extent, and coordination with existing frameworks. Basic waveforms incorporate the US Army's SRW, Harris' ANW2 and HNW, Persistent Systems' Wave Relay, Trellisware's TSM and Silvus Technologies' Stream Caster [4].

1.3 Security Attacks in MANET

1.3.1 Passive attack: in this type of attack, the intruder only performs some kind of monitoring on certain connections to get information about the traffic without injecting any fake information.

1.3.2 Denial of service attack: Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network.

1.3.3 Traffic Analysis: In MANETs the data packets as well as traffic pattern both are important for adversaries. For example, confidential information about network topology can be derived by analyzing traffic patterns.

1.3.4 Snooping: It is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing [5].

1.3.5 Active attack: In this type of attack, the intruder performs an effective violation on either the network resources or the data transmitted; this is done by International Journal on New Computer Architectures and Their Applications causing routing disruption, network resource depletion, and node breaking.

1.3.6 Flooding attack: In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance [6].

1.3.7 Black hole Attack: Route discovery process in AODV is vulnerable to the black hole attack. The mechanism, that is, any intermediate node may respond to the RREQ message if it has a fresh enough routes, devised to reduce routing delay, is used by the malicious node to compromise the system. In this attack, when a malicious node listens to a route request packet in the network, it responds with the claim of having the shortest and the freshest route to the destination node even if no such route exists. As a result, the malicious node easily misroute network traffic to it and then drop the packets transitory to it.

1.3.8 Jamming: Jamming is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication. In this type of attack, the jammer transmits signals along with security threats. Jamming attacks also prevents the reception of legitimate packets [7].

1.3.9 Malicious code attacks: malicious code attacks include, Viruses, Worms, Spywares, and Trojan horses, can attack both operating system and user application. Malicious hackers (crackers) frequently use snooping techniques to monitor key strokes, capture passwords and login information and to intercept e-mail and other private communications and data transmissions [8].

2. Review of Literature

Thorat, S.A. et al [1] "Outline issues in trust based directing for MANET" In MANET hubs help one another in information steering. MANET functions admirably if the partaking hubs coordinate with one another. It is unrealistic to expect that, all hubs taking an interest in an open MANET are helpful and legitimate. For individual hubs it might be beneficial to be non-helpful and selfish. However non-participation, selfishness and malignant conduct of the taking part hubs may come about into breakdown of a MANET. Trust based directing calculations expect to distinguish making trouble and non-collaborating hubs in the MANET. These calculations improve the system execution by using reliable hubs in viable way and punishing non-agreeable hubs.

Durai, K.N. et al [2] "Vitality proficient irregular cast DSR convention with intervention gadget in MANET" Mobile Ad hoc systems (MANET) essentially have dynamic topology, as the directing framework's rundown of neighboring hubs and switches changes its area every once in a while. MANET's regularly expends parcel of transmission capacity, as the medium is imparted to different hubs. MANET hubs devour more power, regardless of the possibility that they don't participate in dynamic correspondence. The downside is fundamentally due to limits of the innovation and directing conventions accessible. MANET's are helpless against assault as they impart a remote medium to framework less spine. The framework proposes a Routing convention in MANET which empowers effective utilization of force and transmission capacity in Mobile Ad-hoc systems (MANET).

Sheik, R. et al [3] "Security issues in MANET: A survey" Sometimes the physically dispersed registering gadgets in a system may be keen on figuring some capacity of their private inputs without revealing these inputs to each other. This sort of reckoning falls under the class of Secure Multiparty Computation (SMC). The answer for SMC issues in Mobile Ad hoc Networks (MANET) can be found with the adjustment of the information inputs or with some anonymization procedure. MANETs are the remote systems of the versatile registering gadgets with no backing of any altered base. The versatile hubs utilize any of the radio innovation like Bluetooth, IEEE 802.11 or Hiperlan for specifically corresponding with one another. The hubs carry on as hosts and in addition switches. The security challenges in the MANET emerge because of its dynamic topology, defenseless remote connection and migrant environment. A distinguishing proof system is required between the hubs utilizing ID and the certifications. This security building design all the while prompts protection issues. Some system is required which keeps a hub to take in the personality or the accreditations of different hubs.

Meenakshi Patel et al [4] —Detection of Malicious Attack in MANET A Behavioral Approach" Topology of MANET is dynamic in nature due tothis characteristic in this network build routing mechanism moreconvoluted and anxious and consequently nodes are morevulnerable to compromise and are predominantly susceptible todenial of service attack (DoS) assail launched by malicious nodesor intruders. Reactive routing for instance AODV is trendier than table driven routing exploit flooding to find outroute. Attackers used this conception to initiate DoS attack akinto flooding; black hole and gray hole are the branded attack inMANET. In this paper we have projected a novel automaticsecurity mechanism using SVM to defense against maliciousattack occurring in AODV. Proposed method uses machinelearning to categorize nodes as malicious.

LinqiangGe et al [5] –On effective sampling techniques for host-based intrusion detection in MANET" Tactical Mobile Ad Hoc Network (MANET) demands a robust, diverse, and

resilient protected communication and computing environment enabling network-centric operation with minimal downtime. Nevertheless, the nature of MANET causes security risks because mobile nodes are deployed in the open field and wireless communication makes the information accessible by anyone. Conducting cyber attack monitoring and detection in a tactical MANET becomes challenging because of limited resources and it's infra structureless network environment. To address this issue, we first study the host-based detection architecture to monitor and detect cyber attacks and then develop sampling techniques to balance the tradeoff between detection accuracy and bandwidth overhead. We also investigate the impact of host-based attack detection on MANET.

3. Approaches Used

Support Vector Machines: Support vector machine based method is basically used for detection of malicious nodes and to restrict the data transmission through these nodes. For each specified input SVM receives a set of input data. In this proposed technique, SVM collects all the behavior of each node in the network and then validate and classify those nodes according behavior of node. All of the nodes are classified either trusted or un-trusted with the help of the SVM classifier integrating with MANET. Classify in two class normal or abnormal nodes. In this, the PDR of packet dropping attack is decreased with compare to the proposed scheme. To overcome of problem, Authorhave taken 30% of malicious nodes in packet dropping attack to analyze the parameter. SVM is a trust based approach in which train data are used. SVM used kernel function for classification as per behavior of node [7].

AODV: AODV avoids the ``counting to infinity'' problem from the classical distance vector algorithm by using sequence numbers for every route. The counting to infinity problem is the situation where nodes update each other in a loop. Ais not updated on the fact that its route to D via C is broken. This means that A has a registered route, with a metric of 2, to D. C has registered that the link toD is down, so once node B is updated on the link breakage between C and D, it will calculate the shortest path to D to be via A using a metric of 3. C receives information that B can reach D in 3 hops and updates its metric to 4 hops. A then registers an update in hop-count for its route to D via C and updates the metric to 5. And so they continue to increment the metric in a loop. AODV defines three types of control messages for route maintenance:

Intrusion Detection Techniques: An(IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of —flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. NIDS is a network security system focusing on the attacks that come from the inside of the network (authorized users). When we classify the designing of the NIDS according to the system interactivity property, there are two types: on-line and off-line NIDS. On-line NIDS deals with the network in real time and it analyses the Ethernet packet and applies it on the some rules to decide if it is an attack or not. Off-line NIDS deals with a stored data and pass it on some process to decide if it is an attack or not.

Component-based software development (CBSD): Component-based software development (CBSD) is an emerging discipline that promises to take software engineering into a new era. Building on the achievements of object-oriented software construction, CBSD aims to deliver software engineering from a cottage industry into an industrial age for Information Technology, wherein software can be assembled from components, in the manner that hardware systems are currently constructed from kits of parts. This volume provides a survey of the current state of CBSD, as reflected by activities that have been taking place recently under the banner of CBSD, with a view to giving pointers to future trends. The contributions report case studies — self-contained, fixed-term investigations with a finite set of clearly defined objectives and measurable outcomes — on a sample of the myriad aspects of CBSD [10].

4. Conclusion

MANET is part of networking that deal with mobile ad-hoc network. In the process of MANET different types of protocol have been utilized for realizable communication b/w the nodes mobile ad-hoc network has been connect b/w different nodes. These nodes communicate with each other without interference of any external architecture. Various types of attack have been performed in the MANET. That disrupts the performance of the overall network. These several attack have been done by malicious nodes available in the network. To overcome the issues of detection of malicious nodes in the network machines learning approach can be utilized that detect the malicious nodes on the basis of PDR, PMOR and PMISR. On the basis of these parameters we conclude that our system gives us better results.

References

[1] Thorat, S.A., Kulkarni, P.J. —Design issues in trust based routing for MANET"*International Conference onComputing, Communication and Networking Technologies (ICCCNT), 2014*, pp. 1 – 7.
[2] Durai, K.N., Baskaran, K. —Energy efficient random cast DSR protocol with mediation device in MANET"*International Conference onAdvanced Computing and Communication Systems (ICACCS), 2013*, pp. 1 – 5.
[3] Sheikh, R., Singh Chande, M., Mishra, D.K. —Security issues in MANET: A review"*Seventh International Conference on Wireless and Optical Communications Networks (WOCN), 2010*, pp. 1 – 4.
[4] Meenakshi Patel—Detection of Malicious Attack in MANET A Behavioral Approach", IEEE Conf. on Malicious attack, 2012, pp. 388-393.
[5] LinqiangGe —Oneffective sampling techniques for host-based intrusion detection in MANET", IEEE Conf. on military communications, 2012, pp 1 – 6.
[6] Shak Keera —Optimal path selection technique for flooding in link state routing protocol uses forwarding

mechanisms in MANET", IEEE Conf. onCommunication and Computational Intelligence (INCOCCI), 2010, pp 318 – 323.

[7] Khuu, P.C "Efficient Dissemination Techniques for MANET Routing Control Messages", IEEE Conf. onWireless Communications and Networking, 2009, pp 1 – 6.

[8] Hwan-SeokYang "Authentication Techniques for Improving the Reliability of the Nodes in the MANET", IEEE Conf. on IT Convergence and Security (ICITCS), 2014, pp 1 – 3.

[9] Mitrokotsa, Aikaterini "Intrusion Detection with Neural Networks and Watermarking Techniques for MANET", IEEE Conf. on Pervasive Services, 2007, pp118 – 127.

[10] Rahman, F.M., Gregory, M.A. "4N intelligent MANET routing algorithm" *Australasian Telecommunication Networks and Applications Conference (ATNAC), 2011*, pp. 1 – 6.

[11] Shah, N., DepeiQian "Cross-Layer Design to Merge Structured P2P Networks over MANET"*16th International Conference onParallel and Distributed Systems (ICPADS), 2010*,pp. 851 – 856.

[12] Moradi, Z.,Teshnehlab, M., Rahmani, A.M. "Implementation of neural networks for intrusion detection in manet"*International Conference onEmerging Trends in Electrical and Computer Technology (ICETECT), 2011*, pp. 1102 – 1106.