International Journal of Advanced Technology in Engineering and Science
Vol. No.9, Issue No. 05, May 2021
www.ijates.com
ijates
ISSN 2348 - 7550

An Assessment of Wormhole Attack Detection Methods in Ad-Hoc Networks

[1]Pranav Sharma, [2]Prashant Singh , [3]Amit Kumar Pandey,[4]Dhyanender Jain

[1,2,3,4] *Department of Information Technology*

[1,2,3,4] *Dr. Akhilesh Das Gupta Institute of Technology & Management, New Delhi, India.*

pranav001.shr@gmail.com[1],prashant.ert@gmail.com[2],amitpandey33@gmail.com[3], dhyanendra.jain@gmail.com[4]

Abstract

As the network grows in complexity and size, it becomes more difficult to handle attacks on ad-hoc networks. Machine learning is one of the best ways to deal with attacks on ad-hoc networks. Machine learning is a technique that automatically learns the pattern of complex networks and then develops techniques for attack detection. This paper outlines the various techniques that can be used to detect wormhole attacks and explains machine learning, deep learning, and classification methods for intrusion detection.This paper also discusses the methods for collecting data and the security features that are required to protect it.

Keywords: MANET, VANET, ML,AI

INTRODUCTION

A Mobile Ad-hoc Network is a group of mobile nodes randomly and dynamically located so that interconnections among nodes can change on a continuous basis. An ad-hoc network is a temporary distributed network system. It is made up of dynamic links between nodes and doesn't rely on existing network infrastructures (e.g. router, gateway or regular power supply). Ad-hoc networks are a type of peer to peer network. Each node performs data collection, storage, processing, and forwarding [5]. Because of its low cost and ease of deployment, mobile ad-hoc networks have great potential to be an infrastructure-less network for critical applications. Ad-hoc network is also known as "on-the fly" network, or "spontaneous networks". The following are the applications of Mobile Ad-hoc Network: Vehicular networks are wireless networks that connect vehicles to each other via wireless. It's useful for safety, danger alarms, comfort like navigation, and conjunction on the road to drivers in vehicular environments [1]. Smartphone ad-hoc networks (SPANs), which transform smartphones and tablets into routers, provide an alternative means of information dispersal in cases where other infrastructure is not available or overwhelmed. For military operations, Army tactical MANETs (Army tactical MANETs) are needed. These networks are also dynamic due to the mobility of nodes and intermittent line-of sight (LOS) connectivity. In a tactical military network, MANETs are advantageous because they can self-form and heal themselves. Air Force UAV Ad-hoc networks were used by the US Air Force to collect data and sense foreign environments without putting pilots at risk. Multiple UAVs can communicate and work together as a team. When a UAV is attacked, it can quickly be sent wirelessly to its data. UAV ad-hoc communication network can also be called UAV instantsky network. NavyAd-hoc networks allow ship-area networks to be created at sea. They enable high-speed wireless communications between ships, enhance their sharing of multimedia data and imaging, and facilitate better coordination in battle operations. Sensor nodes can be used to sense different parameters such as temperature, humidity and vehicle movement. Home automation can also be done using an ad-hoc smart lighting network. It controls the lighting in the home using a smartphone or computer. Ad-hoc Street lights networks are useful for controlling street lights in smart cities. An ad-hoc network can be used to communicate between robots in order to share information locally and distribute tasks in the most efficient and effective way. Hospital ad-hoc networks allow sensors, videos and instruments to be interconnected wirelessly. This allows for patient monitoring in clinics and hospitals, as well as doctor and nurse alert notifications. It also makes it possible to quickly make sense of such data at fusion points, saving lives. When disasters occur such as floods, storms or earthquakes, an ad-hoc network is used. When radio towers have been destroyed or collapsed, a wireless communication network can be used to quickly and instantly communicate with other people. Weather monitoring, rescue operations and mobile conferencing are just a few of the many uses for an ad-hoc network. Bluetooth, IEEE 802.11 wireless fidelity, data acquisition operations on hostile terrain. IEEE802.15.3 wireless PA, Ultra-wideband UWB supports Ad-hoc network.

PROBLEM STATEMENT

Ad-hoc networks are necessary to protect against DoS attacks and against malicious or selfish nodes. For detecting security problems in the network, intrusion detection and prevention are used. It is necessary to gather data about network security and network behaviour for attack detection methods. The illusion created by colluding nodes is that two distant (geographically separated) nodes are connected. It appears as though the nodes are neighbors. They are actually distinct from one another. The wormhole attack aims to make the man in the middle attack, and then drop the packets. The malicious node intercepts data packets from one node and tunnels them into another. You can create the tunnel using either a wired connection or a long-range high bandwidth wireless link operating in a different frequency range. As illustrated in the Fig. This tunnel is known as a wormhole, according to the Fig. This makes the node more attractive, so more packets can be routed through them. This attack blocks the discovery of actual routes. The Fig. The malicious node e.g. 5 is shown in the Fig. The shortcut route (A,B) connects two points in the space. This will short-circuit the network, disrupting the routing. This link is the cheapest to get to the destination. These nodes are necessary for transmission to the destination. [shi2013]
It will be difficult to detect attacks if security data isn't trustworthy. Data collection is a crucial component of attack detection using machine-learning methods. When collecting data, we need to be aware of certain features such as the trustworthiness of Security-related Data, confidentiality, privacy and integrity, as well as authentication, non-repudiation, real time stability, and synchronization.

Literature Review

Intrusion detection systems (IDS), an IDS can recognize multiple attacks simultaneously. IDS can be divided into different types based on their detection methods: Anomaly based intrusion detector systems (ABIDs), knowledge based intrausion detection system (KBIDS), specification based intrusion detection systems [SBIDS], Hybrid intrusion detect systems (HIDS), and other intrusion detection system (OIDS).We have covered the data collection process for detecting network attack in this paper. The ABIDS protocol DSR protocol node collects two inputs in ABIDS: the change ratio of route entries, and the change ratio number of hops. The ABDIS is used to detect attacks caused by forged routing protocol RERP messages. The ABIDS generates a model according the acceptable behaviours and activities, and alarms if any of these activities or behaviours are significantly different from the profile. Knowledge-based intrusion detection systems, or KBIDS, use state transition analysis to detect attacks. A state change from a secure state to one that is compromising can indicate an intrusion. A tool called AODVSTAT was developed [7] to detect packet drops and spoofing attacks in AODV protocol. AODVSTAT is a system where an observer node monitors traffic flow and collects UPDATE messages from another observer. A node can observe the traffic flow and determine if a neighbour node forwards the message at a specific time. The data collected is real so there is no need to verify data trustworthiness. KBIDS keeps track of the specific attack pattern and will trigger an alarm if the observed events match those patterns. Finite state automata can be used to determine the correct behaviour of nodes in specification-based intrusion detection systems. The behaviour of neighbour nodes is monitored by a node that collects Hello message, topology control message (TC) and local data. For DoS attacks to be identified, the node compares monitored data with Finite state automata specification. SBIDS extracts correct operations from monitored data with certain constraints. If the specifications are not met, the SBIDS identifies the attacks. Hybrid intrusion detection system (HIDS), is a combination of the ABIDS and KBIDS described above. [Joseph2008] and others proposed a cross-layer routing attack detection system for the protection against packet dropping, spoofing, and rushing attacks. CRADS employs non-linear detection techniques based upon the support vector machine. CRADS collected data from different layers such as network layer MAC layer, and physical layer to increase routing information. Network characteristics matrix (NCM) and derived matrix (DM) parameters. These parameters are collected by a cluster in a during route Discovery of AODV protocol. NCM includes RREP, RREQ and TTL. DM contains control packet overhead, (CPO), no. Dropped packets CPD, DR. Another intrusion detection systems (OIDS), such as the cloud intrusion detection software, select node to be a monitor node and detects intrusions locally or globally.

Mahendraprasad, explained how classification methods can be used to detect intrusions in an ad-hoc network. Cost matrix was used to evaluate five supervised classification algorithms. The goal of classifiers is to reduce the number of unexpected attacks that are possible during intrusion detection testing. Cross validation is used to tune classifiers so that data can also be collected for the same type of attack. It is important that intrusion detection systems not only detect errors but also have the lowest possible cost. All models can be compared based on different traffic conditions such as mobility of network, number and malicious nodes, sampling time, type of attack, and sampling interval. There are five well-known classification algorithms:

multilayer perception (MLP), linear, Naive bayes, Gaussian mixture models (GMM), and support vector machines (SVM).

Authors[5],provided a device to detect Dos attacks and privacy attacks. The device was equipped with a capture tool and a deep learning detection model. They use Deep neural network (DNN) detection model to detect DoS attacks, convolution neural network (CNN), and long short term memory (LSTM) detection models for XSS attack and SQL attack. These models are highly accurate in precision, recall and f1 score. There are many hidden layers in deep neural networks. Deep learning methods are more capable of learning than machine learning methods due to the number of layers. Data processing extracts features from the data and captures network traffic data.

In research paper [6], suggested multi rate delay per hop indicator (M-DelPHI), which is an extension of DelPHI protocol to detect wormholes in AODV protocol. It takes into account multi-rate channel, processing delay, as well as neighbour monitor. M-DelPHI has a 90% wormhole detection rate and a 20% false alarm rate, while DelPHI has an 80% detection rate. RTT is used to detect wormhole attacks in Delphi. RTT can change with multirate transmission so Delphi is not a reliable method for wormhole detection in an ad-hoc network. Sometimes the RTT is higher because of a lower transmission rate between two nodes that do not have wormhole tunnel, but DelPHI declares them route suspect and removes them from the route table. This results in false positives.

The author separated DelPHI into two phases: the data collection phase and the delay calculation phase. The RTT and number of hops are calculated in data collection phase. The hops between source and destination are calculated and the delay per hop value is calculated in the data calculation phase.

Conclusion

We have discussed the many applications of an ad-hoc network in various fields, as well as wormhole attack that degrades network performance. Our goal is to analyze the methods of wormhole attack detection. This paper lists the methods for detecting wormhole attacks and compares machine learning methods. Security related data is required for detection mechanism. When collecting security-related data, security threats can also be present. We have discussed in this paper the requirements for data collection, data collection methods, and the features of collected data.

References

1. Frederic,DrouhinSebastien, Bindel," Routing and Data Diffusion in Vehicular Ad Hoc Networks Building Wireless Sensor Networks " ,Application to Routing and Data Diffusion,2017, Pages 67-96 https://doi.org/10.1016/B978-1-78548-274-8.50003-9
2. Ying Mao, Jiayin Wang , "Building Smartphone Ad-Hoc Networks with Long-range Radios", 978-1-4673-8590-9/15/$31.00 (c)2015 IEEE
3. D. Reina. S. Toral. P. Johnson. F. Barrero. A survey on probabilistic broadcast strategies for wireless ad hoc network, Ad Hoc Netw. 25 (2015) 263-292.

4. C.-M. Chao and J.-P. Sheu. I. Chou et al., An adaptive quorum based energy conserving protocol to IEEE 802.11 ad hoc network, Mobile Comput. IEEE Trans. 5 (5) (2006) 560-570.
5. S. Al-Sultan, M.M. Al-Doori. A.H. Al-Bayatti. H. Zedan. Comprehensive survey of vehicular ad hoc networks, J. Netw. Comput. Appl. 37 (2014) 380-392.

6. E. A. Panaousis and L. Nazaryan, "Securing AODV Against Wormhole attacks in Emergency MANET Multimedia Communications", Sep. 7-9 2009, London, UK.
7. S. Brands and D. Chaum "Distance-bounding protocol," in Theory and Application of Cryptographic Techniques. pp. 344-59, 1993
8. S. Capkun and L. Buttyan (with J. Hubaux), "Sector: Secure Tracking of Node Encounters within Multi-hop WirelessNetworks", Proc. ACM Workshop on Security of Ad Hoc and Sensor Networks 2003
9. Yih-Chun Hu and Adrian Perrig-- "Packet leashes: A defense against Wormhole Attacks on Wireless Networks", In Proceedings IEEE Conference on Computer Communications (Infocom), 2003 pp. 1976-1986
10. Mahendraprasad, SachinTripathi, Keshav Dhal, "Wormhole attack detection within ad hoc networks using machine learning technique" 10th ICCCNT – 2019 July 6-8 2019,IIT – Kanpur IEEE – 45670
11. Gao Liu and Zheng Yan. Survey of data collection for security measurement and attack detection in mobile ad-hoc networks. Journal of Network and Computer Applications (2018).
12. Shi, F., Liu, W., Jin, D., & Song, J. ,"A countermeasure against wormhole attacks in MANETs using analytical hierarchy process methodology, Electron Commer Res (2013) 13:329-345 DOI 10.1007/s10660-013-9122-3 ,springer