International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 4
ISSN: 2454-4248
509 – 511

A Review on Data Mining Techniques towards Various Intrusion Detection Systems in MANET

P. Bharathisindhu,
Research scholar,
Bharathiar university,
Coimbatore.
bharathisindhu.p@gmail.com

S. Selva Brunda
Professor and Head,
Department of Computer Science Engineering,
Cheran College of Engineering, Karur.
brindhaselva@yahoo.com

ABSTRACT*:* The computer network and its application over the various platforms has the tremendous growth. This exploits vulnerabilities over the network and it is very tough to solve the security issues. The vast number of intrusion over the network leads to failure of network. There are many IDS available for detecting the intrusion. This paper argues the various Data mining techniques available and how it helps to achieve the goal with higher accuracy on IDS. Also this paper discusses and compare with traditional approaches of DM practices on IDS. Also the paper tells the user about IDS and IPS for the network with data mining approaches and suggesting the user for selecting the preferable approach for finding the intrusion over the network effectively.

Keywords*: Network Intrusion Detection system, Intrusions, Data mining techniques*

*****

I. INTRODUCTION

Nowadays internet playing a vital role and all the commercial services are done through internet. So the security is an important issue in transferring data from place to place. The data must be secure and efficiently move on the networks. Many intruders trying to track down or misuse of networks and its information. Intrusion detection system helps to identify the intrusion over the network. The classification of IDS are Network based IDS an d Host based IDS. The Network based IDS helps to analyze the flow of information among networks. The Host based IDS examine the application used on the network and examine the files and logs of the host. There are various models of intrusion detection available that helps the IDS to do better. The mail aim of the IDS is to minimize false positives and false negatives.

MANET is Mobile Adhoc Network consists of wireless nodes without any infrastructure or central administration. Nodes in the networks are communicating each other with in the range. The protocol helps to forward the packets which are out of transmission range. The routing protocol maintains the route for effective communication.

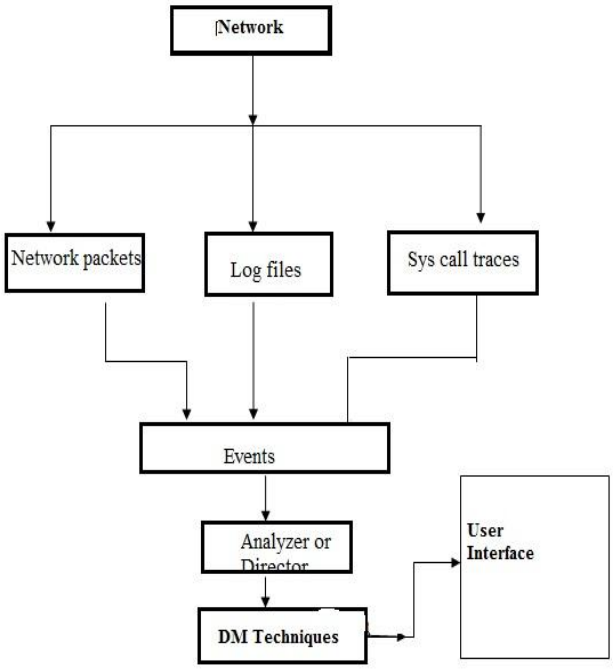

Fig 1.Working of IDS

MANET is vulnerable to attacks or intrusion because of its open infrastructure. The IDS on MANET helps to detect the intrusion and keep the network safe by isolating the intruded node away from the network. Here DM approaches helps to make the process easier. By applying DM techniques we can extract the patterns from the large databases.

 ISSN: 2454-4248
509 – 511

II. RELATED WORK

Mobile Ad-hoc Network id generally defined as a network that has mobile devices forming a temporary network without the aid of any centralized administration. MANET does not have any centralized control or fixed infrastructure. The router helps to connect all the nodes in MANET and the addressing of nodes must be needed. For sending the packets from source to destination, the optimal path or optimal route is to be determined. The routing table in each and every node update the touting information of the communication. The routing protocol such as Distance Vector routing, Link state routing. The security issues in Manets are black hole attack, grey hole attack, worm hole attack, passive eaves dropping, Denial of service, flow disruption, Resource Depletion, Data integrity attacks. Security plays a very big role in MANETs due to its vulnerability and flat infrastructure. MANETs are very much prone to intrusions or attacks [1]. MANET services on military battlefield, sensor networks, medical services, personal area networks.

MANETs and its types such as Active and Passive. Based on the features it is broadly classified into Data traffic attack and Control traffic attacks [2]. In paper [3], the author proposed various measures against security attacks in MANETS.

III. NTRUSION DEECTION SYSTEMS

The Intrusion derive from the Latin word 'Intrudere'. It means an interjection or an unwelcome visit. The intruders do some unauthorized activity on the network. The Intrusion Detection System is a device or software application that monitors the network or system activities for malicious activities over the network.

Zibusiso et al [4] describes the history of IDS and versions of IDS. The taxonomy of IDS showed anti-intrusion approaches, prevention, pre-emption, deflection, detection and autonomously counted.

Ramasamy et al[5] investigated the behaviour of selfish nodes which drop the packets and the node is called misbehaviour node and the network isolate the node from the network.

Aishwarya et al [6] proposed the concept called active route and through that route the data packets send the source to destination. Here the misbehaving node is isolated and never used in the network again.

Marti et al [7] proposed and widely used technique called watch dog mechanism. This watch dog mechanism in IDS helps to identify the misbehaving nodes by eves dropping on the passive modes. This method helps to decide whether the packets to send to next hop or not. The drawbacks of this method were not addressed of issues like receiver collision, false misbehaving report, ambiguous collisions, limited transmitted power and partial dropping.

In paper [8], Liu et al introduced the TWOACK scheme and it overcomes the collision and limited transmission power that were not addressed by Watch dog mechanism. The every packet of data moves over the consecutive nodes that has acknowledged and sent to the destination from source.

In paper [9], both ACk and TWOACK has combined and proposed the AACK scheme. This AACK scheme is used when the ACK is not received by the nodes within the interval of time. The EAACK (Enhanced Adaptive Acknowledgement) scheme is proposed and is the combination of all the three techniques of ACK,S-ACK,MRA are proposed in paper[10].

IV. DATAMINING TECHNIQUES

Data mining refers to extracting the knowledge from the large amount of data. The data mining techniques are used with IDS is expensive when constructed manually. There are two types of data set network based and host based dataset. The data mining algorithm helps to give alarm to the system when the attack is detected. The frameworks of IDS are pre-processing, association rule mining, find sequence patterns, construct features. In paper [11], Aruna et al discussed briefly about the concept of data mining, challenges and applications. The different areas were using DM techniques and tools. In paper [12] Rajesh and Vikrant investigated NSL-KDD dataset that was increased version of KDD99 dataset. The class attributes has 21 classes that fall under probe attacks,U2R attacks, Remote to Local attacks and DOS(Denial of Service). The various models of data mining helps to determine the process in easiest way are artificial Neural Networks, Support Vector Machine, and Multivariate adaptive regression (MARs) [13].

In [14],Jaina et al, proposed various algorithms of classification and clustering algorithms for Intrusion detection system. The K-Means algorithm helps to partitions the data in K clusters with their similarities. In paper [16], Desale et al proposed a Genetic algorithm based feature selection approach for IDS helps to search the selecting features. Here the investigation is carried out with popular approaches such as correlation feature selection, Information gain, correlation attribute evolution which improves the classifier and accuracy of the Naive Bayes algorithm. Using Euclidean distance, it helps to find the distance between two objects. Here KDD Cup99 Dataset is selected for Intrusion Detection process. If the IDS detect the attack then it raises an alarm.

In paper [16] Desale et al proposed the comparison of two types of algorithms namely c4.5 and SVM. The Dataset is pre-

 ISSN: 2454-4248
509 – 511

processed and it is applied in C4.5 and SVM algorithms finally justified that C4.5 algorithm is better than SVM.

V. FUTURE WORKS

The Researchers can propose the work with Data mining techniques such as Classification, Clustering, Association Rule mining, Genetic algorithms, and neural networks. Data mining techniques in Intrusion detection system helps to identify the attacks or misbehaving node as fast as traditional techniques and report it to the administration. In MANETS, Intrusion Detection system with Data mining techniques helps to isolate the misbehaving node from the whole network.

VI. CONCLUSION

The paper discussed about various Data mining techniques used for finding the Intrusion detection in IDS in Mobile Ad-hoc Networks. Also this paper focus on the IDS models, Datasets which helps for the researcher for choosing the best one for their development. The IDS with Data mining algorithm helps to detect the intrusions and will produce the fast response rate to the user. The Data mining algorithms helps to reduce the false alarm rate and increase the speed of finding misbehaviour nodes in mobile ad-hoc networks.

REFERENCES

[1]. PriyaGoyal, Sahil Batra, Ajt Singh “A Literature Review of Security attacks in Mobile adhoc Networks”, International Journal of Computer Applications, volume 9, pg.no 10975-8882, Nov 2010

[2]. Aniruddha Bhattachariyya, Arnab Banerjee, Dipayan Bose, “Different types of attacks in Mobile Adhoc Networks: prevention and Mitigation Techniques”

[3]. Vaishnavi.J.Deshmukh, Sapna.S.Kaushik, “Routing Attack Survey for Mobile Adhoc Networks”, International Journal of Advanced Research in Computer and Communication Engineering ,Vol 2,No.1,2016

[4]. Zibusiso Dewa and Leandros.A.Marglaras, “Data mining and Intrusion Detecton Systems”, International Journal of Advanced Computer Science and Appicaitons, Vol 7, No.1, 2016

[5]. Ramasamy Murugan, Arumugam Shanmugam, “A Timer Based Acknowledgement Scheme for Node misbehaviour detection and Isolation in MANET”, International Journal of Network security, Vol 15, No.1, pp 182-188, Jan 2013

[6]. Aishwarya Sagar Anand Ukey,Meenu Chawla, “ Detection of Packet dropping attack using Improved Acknowledgement Based Scheme in MANET”, International Journal of computer science Issues, Vol.7,Issue 4,No.1,July 2010

[7]. Marti.S.Giuli, T.J.Lai, k. And Baker.M, “ Mitagating Routing Misbehaviour in Mobile Adhoc Networks”, International conference on Mobile computing and Networking, Mobicom’00 , NY, 255-265

[8]. K.Liu, J.Deng, P.K.Varshney and K.Balakrishnan, “ An Acknowlwdgement based Approach for the detection of routing misbehaviour in MANETs”, Mobile computing,Vol.6,No.5,PP.536-550,May 2007

[9]. T.Sheltami, A.AL.Roubaiey,E.Shakshuki and A.Mahmoud, “ Video Transmission Enhancement in presence of Misbehavinig nodes in MANETS”, Multimedia Systems, Vol.15,No.5,pp.273-282,Oct.2009

[10]. Nan Kang,Elhadi M.Shakshuki, Tarek R.Shetami, “ Detecting Misbehaving Nodes in MANETs”, iWAS2010,8-10 November 2010, Paris, France

[11]. Aruna J.Chamatkar, Dr.P.K.Butey, “ Importance of Data mining with different types of Data Applications and Challenging Areas”, International journal of Engineering Research and Applicaitons,Vol.4,Issue 5(version 3),May 2014,pp.38-41

[12]. Rajesh Wankhede, Vikrant Chole, “ Intrusion Detection System using Classification Techniques”, International Journal of computer Applications, Volume 139,No.11,April 2016

[13]. Krishna Kant Tiwari,Susheel Tiwari, Sriram Yadav, “ Intrusion detection using Data mining Techniques”, International Journal of Advanced Computer Technology, ISSN 2319-7900

[14]. Jaina Patel, Krunal Panchal, “ Effective Intrusion detection system using data mining Technique”, Iournal of Emerging Technologies and Innovative Research, Volume 2, Issue 6, June 2015

[15]. Sushil Kumar Chaturvedi, Prof. Vineet Richariya, Prof. Nirupama Tiwari, “ Anomaly Detection in Network using Data mining technologies”, International Journal of Emerging Technology and Advanced Engineering, Vol.2, No.5, May 2012, ISSN. 2250-2459

[16]. K.S.Desale and R.Ade “Genetic algorithm based feature selection approach for Effective Intrusion Detection System” in computer communication and Informatics, 3 rd International Conference, 2015, pp1-6.