International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 3, 2016. ISSN: 2348-6600
Reference ID: IJCS-126 PAGE NO: 744-748

A Two Level Network Intrusion Detection System for MANET

R.kalaivani [#1], *M. Lalli* [*2]
[1]*Research Scholar , Bharathidasan University ,Trichy*
[2] **Assistant Professor, School of CSE & Applications, Bharathidasan University ,Trichy**

***Abstract*—** Intrusion detection has been the major necessities of the current information rich computing environment. Major challenges facing intrusion detection systems include the huge size of data to be analyzed and the ever -changing attack types. In order to enforce high protection levels against threats, a number of software tools are currently developed. In this paper, two grains levels intrusion detection system (IDS) is suggested (fine-grained and coarse-grained). In normal case, where intrusions are not detected, the most suitable IDS level is the coarse-grained to increase IDS performance. As soon as any intrusion is detected by coarse-grained IDS, the fine-grained is activated to detect the possible attack details. Very fast decision tree algorithm is used in both of these detection levels. Experimental results demonstrate that the proposed model is highly successful in detecting known and unknown attacks, and can be successfully adapted with packets' flow to increase IDS performance.

***Index Terms*— Network security; Intrusion detection system; Classification; Very fast decision tree algorithm, Manet, Mac**

I. INTRODUCTION

The rapid progress of information technology brings with itself more sources of information and more vulnerability to the available information. Protecting the networks from intrusion seems to be a major challenge in the current scenario. Computer networks are usually protected against attacks by a number of access restriction policies that act as a coarse grain filter. Intrusion detection systems (IDS) are the fine grain filter placed inside the protected network, looking for known or potential threats in network traffic and/or audit data recorded by hosts. The frequency of intrusions has increased to a large extent during the recent years, hence maintaining an effective intrusion detection system has become mandatory. Intrusion detection systems analyze packets to identify if they are legitimate. This process is complicated due to the generation of a huge number of packets in networks. Not all packets can be examined. Further, attacks differ in styles and operational levels. Hence a static intrusion detection system does not suffice. This mandates the need for a dynamic and learning intrusion detection system that can identify anomalous packets effectively in a huge network without hindering the process flow.

Although several IDS systems are available, the common objectives of these systems are to reduce the amount of false alarms, and to recognize new attacks in order to increase detection ratio. In this paper, the concentration is on detecting known and unknown attacks in fast networks in order to mitigate the influence of the attack by shrinking the time gap between the real attack and its detection.

This paper contribution is to build two grains levels IDS in order to detect abnormal behavior of network traffic and cope with fast networks. It is well known that the intrusion occurrence in networks with respect to normal traffic is rare. These motivate to build the proposed two grains levels IDS. These detection levels are fine-grained and coarse-grained. In normal case, where intrusions are not detected, the most suitable IDS level is the coarse-grained to increase monitoring performance. At the moment of intrusion is detected by coarse-grained IDS, the fine-grained IDS is activated to detect as most as possible of attack details. The coarse-grained IDS focuses on five packet features while fine-grained IDS works on 20 features. Very Fast Decision Tree (VFDT) algorithm is selected as a fast classifier. The advantages of the proposed system are processing and analyzing of high-speed network traffic, discovering and accurately identifying new attacks to reduce the false alarms to the maximum extent, and detecting the intrusion in real time.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 3, 2016. ISSN: 2348-6600
Reference ID: IJCS-126 PAGE NO: 744-748

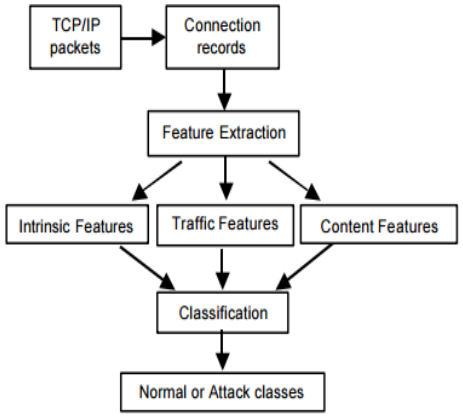


Fig.1 Steps in Intrusions Detection

II. Related Works

Nowadays, authors have designed numerous IDSs to detect computer and network intrusions. Several data mining techniques have been used to make networks' intrusions detectable. The first class of approaches uses decision trees (DT) to build attack model. Several variations of decision trees were used such as partial decision tree [3],C4.5[4],random forest [5], ID3 decision tree [6],andJ48[7].These decision trees models vary in the splitter measure (i.e. information gain, gain ratio, gini index), pruning technique, branching types, dataset types, etc. The common objective of these decision trees is to iteratively partition the given dataset into subsets where all elements in each final subset belong to the same class. These models have been built from network packets to detect network intrusions with high precision. The main issue with these methods is that they cannot be adaptive with distribution variation in network packets while the proposed system solved this problem by selecting algorithm which works with concept drift.

Another class of these approaches has used evolutionary computation [8]. Self-Organizing Map [7] and Multilayer Perceptron (MLP) [7] were trained to recognize normal from abnormal traffic. In addition, genetic programming [9] is achieved very high detection ratio combined with slow model. However, these techniques have performance issues and cannot work in online mode. One of the main goals of this paper is to enhance IDS performance. Different class of efficient data mining approaches is used to differentiate malicious traffic from normal ones. Bayes network classifier by Staniford et al. [10] is used to calculate the conditional probabilities of several connection features with respect to other connection features. The anomalous connection is determined using these probabilities. SVM is used by Eskin et al. [11], and Honig et al. [12] in addition to their clustering methods for unsupervised learning. The achieved performance was as good as or better than both of their clustering methods. In addition, Fuzzy logic rules by Luo [13] attempted to classify network data. The author verified that the combination of fuzzy logic with association rules and frequency episodes generates more abstract and flexible patterns for anomaly detection. The author approach utilizes fuzzy association rules and fuzzy frequency episodes to extract patterns for temporal statistical measurements at a higher level than the data level. An additional class of approaches proposed Multi-level IDSs to achieve highest attack detection rate. Multi-level IDS designed by Chen et al. [14] is composed of IDS, firewall, and a report system in order to present a unified report format to the end user. This multi-level IDS supports specific types of these integrated systems. This system focuses on reporting technique which is different from ours. The most related work to ours is the multi-level IDS (ML-IDS) by Al-Nashif [15] that uses autonomic computing to automate the control and management of ML-IDS. Three levels of granularities are used by ML IDS which are traffic flow, packet header, and payload. Then it employs a fusion decision algorithm to improve the overall detection rate and minimize the occurrence of false alarms. Genetic algorithm, neural network, least square and other approaches have been used in multiple-level decision fusion, which are different from the used technique in the proposed system. In addition, the proposed system focuses on designing lightweight IDS while ML-IDS goal is to be autonomic.

III. Existing System

The frequency of computer intrusions has increased rapidly during the last two decades. Intrusion Detection Systems (IDSs) are an essential component of a complete defense-in-depth architecture for network security. They collect and inspect packets, looking for evidence of intrusive behaviors. As soon as an intrusive event is detected, an alarm is raised giving the security analyst an opportunity to react promptly. Unfortunately, most of designed IDSs cannot cope

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 3, 2016. ISSN: 2348-6600
Reference ID: IJCS-126 PAGE NO: 744-748

with fast networks. Although several IDS systems are available, the common objectives of these systems are to reduce the amount of false alarms and to recognize new attacks in order to increase detection ratio.

IV. Proposed System

The proposed system is dedicated to detect intrusions on a network by using anomaly intrusion detection approach. This approach is used to detect the known and novel attacks in traffic network. The proposed system operates in two grains levels. The first one works with basic features while the second mode works with statistical features of captured packets.The proposed system is composed of two grains levels IDS that allows the system to analyze network traffic on different granularities. The two levels IDS is different from available IDSs in which it adapts with network situation when it is under attack or not. Its detection levels are Coarse-grained IDS and fine-grained IDS. In normal case, where intrusions are not detected, the most suitable level is the Coarse-grained IDS where five features are monitored to increase IDS performance. At the moment of intrusion is detected by Coarse-grained IDS, the fine-grained IDS is activated where 20 features are monitored to detect as most as possible of attack details. VFDT algorithm is selected as classifier to achieve this goal because it is capable of processing and analyzing of high-speed network traffic, and detecting the intrusion in real time.

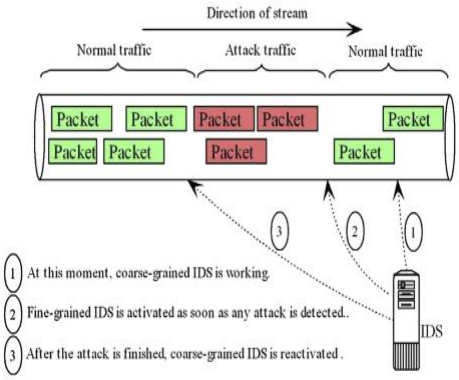


Fig 2.System Architecture

V. Algorithm Used

VFDT is a high-performance data mining system based on Hoeffding trees. Many of classification learning methods have been proposed, of which the decision tree learning method is commonly used. This is because it is fast and the description of classifiers that it derives is easily understood. One of the data stream algorithms that support the decision tree learning method is the VFDT. As data arrives, this data stream grows gradually while the data is classified. VFDT allows the use of either information gain or the Gini index as the attribute evaluation measure. It includes a number of refinements to the algorithm.

VI. Simulation & Result Analysis

Simulation shows the efficiency of VFDT algorithm. From analysis we can compare the results between simulations with VFDT and WatchDog Technique. Network Simulator 2 (NS-2) is used for simulation.

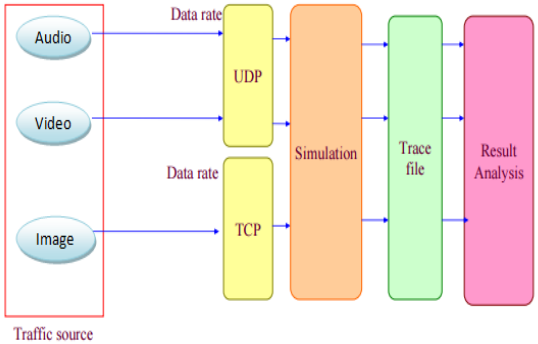
Introduction to NS-2

NS is a discrete event simulator targeted at networking research. Ns provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks.

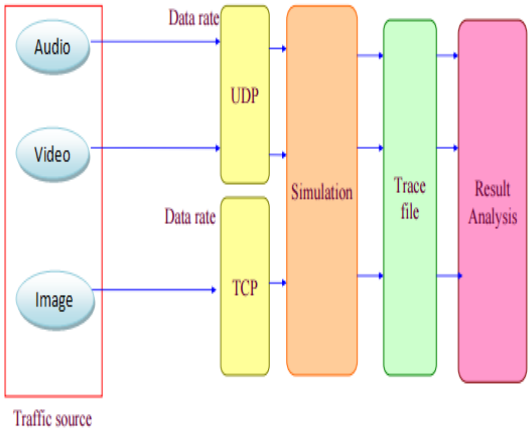
Simulation Scenario

Application

Audio and streaming video are encoded to packet data first and then send to network through User Datagram Protocol (UDP) transport. Packets arrival to receiver after travel a several time in network and are decoded by decoder.



International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 3, 2016. ISSN: 2348-6600
Reference ID: IJCS-126 PAGE NO: 744-748



RESULTS

The protocols are evaluated for packet delivery ratio, throughput, and average end-to-end delay.

Throughput comparisons

We know that throughput increases when connectivity is better. It can be observed that the performance of the WatchDog reduces drastically while VFDT is slightly better among the existing protocols.

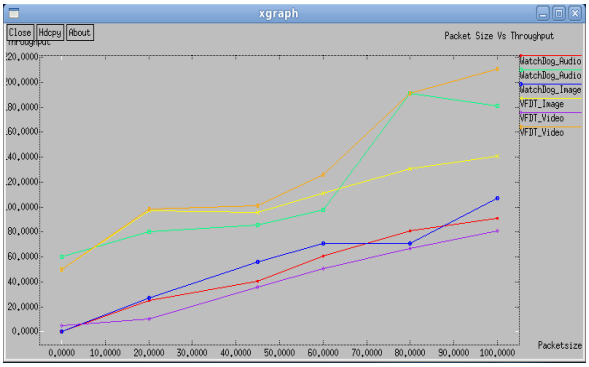
Throughput

It is defined as the total number of packets delivered over the total simulation time. The throughput comparison shows that the two algorithms performance margins are very close under traffic load of 50 and 100 nodes in MANET scenario and have large margins when number of nodes increases to 200.

Mathematically, it can be defined as:

Throughput= N/1000

Where N is the number of bits received successfully by all destinations.

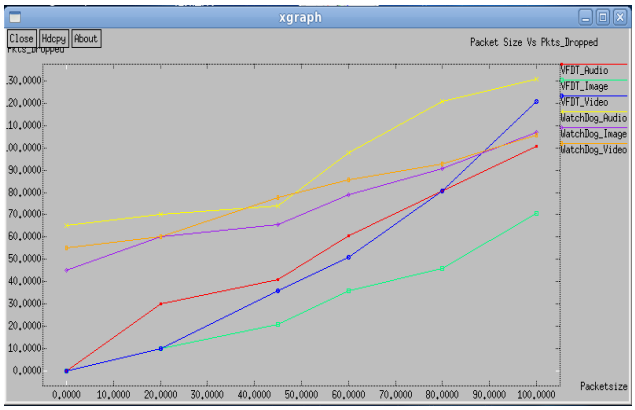


Packet Drop

Packet drop is defined as the total number of packets dropped during the simulation.

Mathematically, it can be defined as:

Packet lost = Number of packet send – Number of packet received

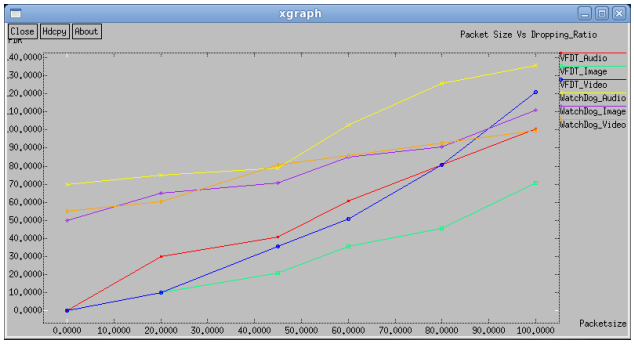


Packet Drop Ratio

Packet drop is defined as the ratio of total number of packets dropped during the simulation.

Mathematically, it can be defined as:

Packet Drop Ratio = Number of packet send / Number of packet received



International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 3, 2016. ISSN: 2348-6600
Reference ID: IJCS-126 PAGE NO: 744-748

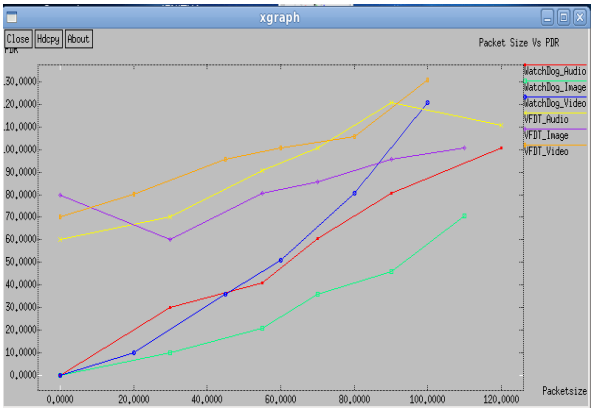
Packet delivery ratio

Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources.

Mathematically, it can be defined as:

PDR= S1÷ S2

Where, S1 is the sum of data packets received by the each destination and S2 is the sum of data packets generated by the each source.



Graphs show the fraction of data packets that are successfully delivered during simulations time versus the number of nodes. Performance of the WatchDog is reducing regularly while the VFDT is increasing. VFDT is better among the WatchDog protocol.

VII. Conclusions

Two levels IDS is proposed allowing the system to analyze network traffic on different granularities. It is different from the available IDSs in which it adapts with network situation when it is under attack or not. Its detection levels are coarse-grained IDS and fine grained IDS. These two detection levels are tested .VFDT has proved its efficiency in both generalization tree and new attacks detection.

References

[1] *R. Perdisci, G. Giacinto, F. Roli, Alarm clustering for intrusion detection systems in computer networks, J. Eng. Appl. Artif. Intell. 19 (2006) 429e438.*

[2] *D. Pedro, H. Geoff, Mining high speed data streams, in: ACM SIGKDD Conference on Knowledge Discovery and Data Mining, 2000, pp. 71e80.*

[3] *Mohammed M. Mazid, M. Shawkat Ali, Kevin S. Tickle, A comparison between rule based and association rule mining algorithms, in: 3rd IEEE International Conference on Network and System Security, 2009, pp. 452e455.*

[4] *G. Radhika, S. Anjali, C.J. Ramesh, Parallel misuse and anomaly detection model, Int. J. Netw. Secur. 14 (4) (2012) 211e225.*

[5] *P. Mrutyunjaya, R.P. Manas, Evaluating machine learning algorithms for detecting network intrusions, Int. J. Recent Trends Eng. 1 (1) (2009).*

[6] *Dewan M. Farid, H. Nouria, B. Emna, Z.R. Mohammad, M.R. Chowdhury, Attacks classification in adaptive intrusion detection using decision tree, World Acad. Sci. Eng. Technol.(2010) 27e44.*

[7] *A.N. Huy, D. Choi, Application of data mining to network intrusion detection: classifier selection model, in: Asia-Pacific Network Operation and Management Symposium, SpringerVerlag, Berlin, Heidelberg, 2008, pp. 399e406.*

[8] *M. Adnan, B. Abdulazeez, S.I. Adel, Intrusion detection and attack classifier based on three techniques, A Comp. Study. Eng. Technol. J. 29 (2) (2011) 233e254.*

[9] *M.F. Kamel, B. Aoued, Securing network traffic using genetically evolved transformations, Malays. J. Comput. Sci. 19 (2006) 3e23.*

[10] *S. Staniford, J.A. Hoagland, J.M. McAlerney, Practical automated detection of stealthy portscans, J. Comput. Secur. 10 (1e2) (2002) 105e136.*

[11] *. Eskin, A. Arnold, M. Preraua, L. Portnoy, S.J. Stolfo, A geometric framework for unsupervised anomaly detection: detecting intrusions in unlabeled data, in: D. Barbar, S. Jajodia(Eds.), Data Mining for Security Applications, Kluwer Academic Publishers, Boston, 2002.*

[12] *A. Honig, A. Howard, E. Eskin, S.J. Stolfo, Adaptive model generation: an architecture for the deployment of data mining based intrusion detection systems, in: D. Barbar, S. Jajodia (Eds.), Data Mining for Security Applications, Kluwer Academic Publishers, Boston, 2002.*

[13] *J. Luo, Integrating Fuzzy Logic with Data Mining Methods for Intrusion Detection, Mississippi State University, 1999 (Master thesis).*

[14] *T. Chen, P. Chen, T. Wang, Y. Chiu, S. Lai, Integrated multilevel intrusion detection and report system, in: Proceedings of the Fifth International Conference on Electronic Business,Hong Kong, 2005, pp. 463e469.*

[15] *Y. Al-Nashif, Multi-level Anomaly Based Autonomic Intrusion Detection System, University of Arizona, 2008 (PhD dissertation).*