www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume – 5 Issue -02 February, 2016 Page No. 15770-15779

A Novel Topology for Network Intrusion Detection with Anomaly Detection

[1]M.Prashant, [2]Ramesh Krishnan
[1]Internship Trainee,
Polaris India Pvt. Ltd.,
Chennai, India.
Email: prashantmuralidharan@gmail.com
Research Scholar
Department of ECE

Easwari Engineering College, Anna University
Email:eswaranphd@gmail.com

ABSTRACT

Intrusion detection has become an essential element of network administration thanks to the huge range of attacks persistently threaten our computers. Ancient intrusion detection systems area unit restricted and do not give a whole resolution for the matter. They look for potential malicious activities on network traffics; they generally succeed to search out true security attacks and anomalies. However, in several cases, they fail to observe malicious behaviors (false negative) or they fireplace alarms once nothing wrong within the network (false positive). Additionally, they need thorough manual process and human professional interference. Applying data processing (DM) techniques on network traffic information may be a promising resolution that helps develop higher intrusion detection systems. Moreover, Network Behavior Analysis (NBA) is additionally associate degree effective approach for intrusion detection. During this paper, we tend to discuss DM and NBA approaches for network intrusion observation and recommend that a mix of each approach has the potential to detect intrusions in networks additional effectively.

KEYWORDS

Network Intrusion Detection, Network Behavior Analysis, data processing Algorithms

I INTRODUCTION

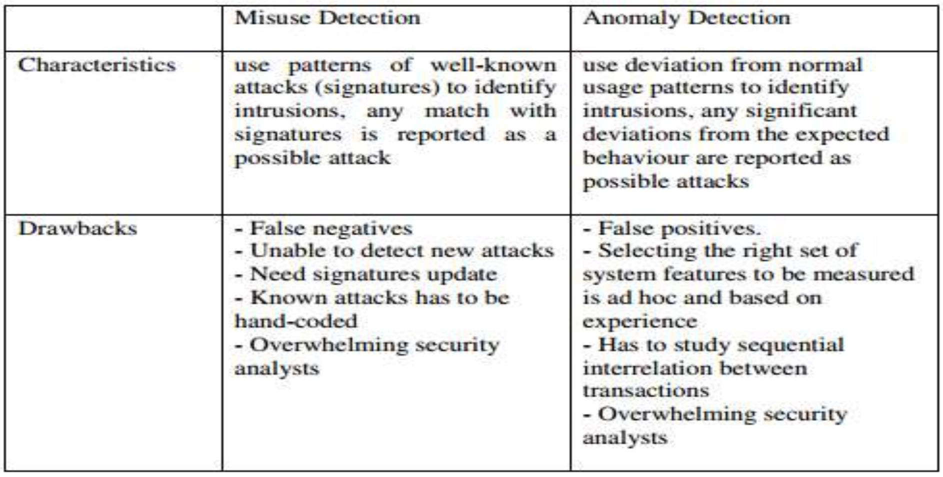
Nowadays, there exists an intensive growth in victimization web in social networking (e.g., instant messaging, video conferences, etc.), healthcare, e-commerce, bank transactions, and plenty of alternative services. These web applications would like a satisfactory level of security and privacy. On the other hand, our computers area unit below attacks and susceptible to several threats. there's associate degree increasing availableness of tools and tricks for assaultive and intrusive networks. Associate degree intrusion will be outlined as any set of actions that threaten the protection necessities (e.g., integrity, confidentiality, availability) of a computer/network resource (e.g., user accounts, file systems, and system kernels) [16,17]. Intruders have promoted themselves and fancied innovative tools that support numerous styles of network attacks. Hence, effective ways for intrusion detection (ID) became associate degree insistence ought to defend our computers from intruders. In general, there are 2 styles of Intrusion Detection Systems (IDS); misuse detection systems and anomaly detection systems [14, 16,17]. Most industrial IDS use the misuse strategy during which known intrusions area unit hold on within the systems as signatures. The system searches network traffics for patterns or user behaviors that match the signatures, if a pattern matched a signature; associate degree alarm is raised to somebody's security analyst United Nations agency decides what action ought to be taken supported the type of attack.

In such systems, better-known intrusions (signatures) area unit provided and hand-coded by human specialists supported there in depth expertise in distinguishing intrusions. Current misuse IDS area unit engineered based mostly on: professional systems (e.g., IDES, ComputerWatch, NIDX, P-BEST, ISOA) which use a collection of rules to explain attacks, signature analysis (e.g., Haystack, NetRanger, Real Secure, MuSig) wherever options of attacks area unit captured in audit path, state-transition analysis (e.g., STAT, USTAT and NetSTAT).

That uses state-transition diagrams, colored petri nets, (e.g., IDIOT), or case-based reasoning (e.g., AUTOGUARD) [16]. Anomaly detection [8,12], in contrast to misuse detection, will establish novel intrusions. It builds models for traditional network behavior (called profiles) and uses these profiles to observe new patterns that considerably deviate from them. These suspicious patterns could represent actual intrusions or might merely be new behaviors that require to be more to profiles. Current anomaly detection systems use statistical ways like variable and temporal analysis to spot anomalies; examples of these systems area unit day, NIDES, and EMERALD. Alternative anomaly detection systems area unit engineered based on professional systems like Computer Watch, Wisdom, and Sense [16]. Misuse IDS suffer from variety of major drawbacks, first, better-known intrusions need to be hand coded by experts. Second, signature library must be updated whenever a brand new signature is discovered, network configuration has been modified, or a brand new code version has been installed.

Third, misuse IDS area unit unable to observe new (previously unknown) intrusions that do not match signatures; they'll solely establish cases that match signatures. Thus, the system fails to identify a brand new event as associate degree intrusion once it's indeed associate degree intrusion, this can be known as false negative. On the opposite hand, current anomaly detection systems suffer from high proportion of false positives (i.e., an occurrence incorrectly known by the IDS as being associate degree intrusion once it's not) [16]. an extra disadvantage is that choosing the proper set of system options to be measured is spontaneous and supported expertise. a standard disadvantage in IDS is that for an outsized, complex network IDS will usually generate thousands or scores of alarms per day, representing an amazing task for the protection analysts [16, 17]. Table one shows a comparison between the 2 styles of intrusion detection

Table 1: a comparison between the two types of intrusion detection



	Misuse Detection	Anomaly Detection
Characteristics	use patterns of well-known attacks (signatures) to identify intrusions, any match with signatures is reported as a possible attack	use deviation from normal usage patterns to identify intrusions, any significant deviations from the expected behaviour are reported as possible attacks
Drawbacks	- False negatives - Unable to detect new attacks - Need signatures update - Known attacks has to be hand-coded - Overwhelming security analysts	- False positives. - Selecting the right set of system features to be measured is ad hoc and based on experience - Has to study sequential interrelation between transactions - Overwhelming security analysts

From the on top of discussion, we tend to conclude that ancient IDS face several limitations. This has crystal rectifier to associate exaggerated interest in up current IDS. Applying data processing (DM) techniques such as classification, clustering, association rules, etc, on network traffic information could be a promising answer that helps improve IDS [15-23]. Additionally, Network Behavior Analysis (NBA) is additionally associate effective approach for network intrusion detection [4,6,25,26].

During this paper, we tend to discuss DM and NBA approaches for network intrusion detection and recommend that a mixture of each approaches has the potential to notice intrusions in networks a lot of effectively. the remainder of this paper is organized as follows: in section a pair of we tend to provide background data and connected work. In section three we tend to discuss NBA systems. In section four we recommend associate ID model that integrates DM techniques and NBA. Finally, in section five, we tend to provide our conclusions and future work.

II BACKGROUND AND CONNECTED WORK

Intrusion detection is that the method of observation and analyzing the info and events occurring during a computer and/or network system so as to notice attacks, vulnerabilities and alternative security problems [16]. IDS will be classified in line with information sources into: host-based detection and network-based detection. In host-based detection, information files and OS processes of the host ar directly monitored to see specifically that host resources ar the targets of a specific attack. In distinction, network-based detection systems monitor network traffic information employing a set of sensors hooked up to the network to capture any malicious activities. Networks security issues can vary wide will and may and might} have an effect on totally different security necessities together with authentication, integrity, authorization, and convenience. Intruders will cause differing types of attacks like Denial of Services (DoS), scan, compromises, and worms and viruses [17,18].

During this paper, we emphasize on network-based intrusion detection that is mentioned within the next sub-section. The primary assumption in intrusion detection is that user and program activities will be monitored and modelled [16,17]. a group of processes represent the framework of intrusion ,detection, first, information files or network traffic ar monitored and analyzed by the system, next, abnormal activities ar detected, finally, the system raises associate alarm supported the severity of the mattack [16]. Figure one below shows a standard framework for ID. so as for IDS to be successful, a system is required to satisfy a group of necessities. IDS ought to be ready to notice a wide variety of intrusions together with far-famed and unknown attacks. this suggests that the system needs to adapt to new attacks and malicious behaviors. IDS also are needed to notice intrusions in timely fashion, i.e., the system may have to reply to intrusions in time period. This may represent a challenge since analyzing intrusions ould be a time intense method might which will that will} delay system response. IDS ar needed to be correct during a sense that minimizes each false negative and false positive error. Finally, IDS ought to gift analysis in easy, easy-to understand format so as to assist associatealysts get an insight of intrusion detection results [16].

Network-based Intrusion Detection

Network-based intrusion detection will be softened into 2 categories: packet-based anomaly detection and flow-based anomaly detection. Flow-based anomaly detection tends to rely on existing network parts, like routers and switches, to form a flow of data available for analysis. On the opposite hand, packet-based anomaly detection doesn’t admit alternative network components; it observes network traffic for the detection of anomalies. Flow-based anomaly detection is predicated on the idea of a network flow and flow records. A flow record is a summarized indicator that an exact network flow transpires which 2 hosts have communicated with one another antecedently at some purpose in time.

Typically, the flow record contains each the supply and destination scientific discipline addresses the supply and destination communications protocol or UDP network ports or ICMP sorts and codes, variety the amount the quantity} of packets and number of bytes transmitted in the session, and therefore the timestamps for each the beginning and finish of the network flow. Routers generate these flow records as they observe network traffic. By analyzing flow records and looking for uncommon amounts, directions, groupings and characteristics of the network flow, the network behavior analysis code will infer the presence of worms or perhaps DoS attacks during a network. the matter is that these flow records solely carry a outline of the data presented for analysis. Basically, this data is that the data concerning the network traffic. The actual network packets aren't accessible for additional analysis [9]. Packet-based anomaly detection code, not like its flow-based counterpart, doesn't use third party parts to generate the data of the network traffic. Instead, the whole packet-based analysis appearance at raw packets as they traverse the network links.

Observation of the network traffic will be done using either port mirroring or network faucets. Port mirroring, called SPAN (Switched Port Analyzer), is employed on a network switch to send a replica of all network packets seen on one switch port to a network observation affiliation on another switch port. Network faucets ar wont to create permanent access ports for passive observation. check Access Port (TAP) will produce a monitoring access port between any 2 network devices, together with switches, routers, and firewalls. an honest example to check the 2 detection methodologies is that of a large-scale SYN flood denial of service attack. Generally a large quantity of affiliation request packets ar generated by variety of compromised zombie machines. The supply addresses are indiscriminately generated [4].

A flow-based anomaly detection system solely sees that there's an oversized range of network flows, which are established from many purchasers to the particular server and port that's vulnerable. But, no helpful data on the far side that's forthcoming from a flow-based answer. Therefore, the network operator has the selection to either rate-shape or blocks all traffic to it server, with disastrous impact on even the valid traffic [4]. On the opposite hand, a packet-based anomaly detection system will extract the signature of the sinning packets. Often, large-scale attack tools initialize packet headers with bound, non-random information. for instance, the communications protocol window size or sequence range, that is publicized during a affiliation request packet, may well be mounted.

A packet-based anomaly detection system, that has access to the raw packet information, will notice this and provide a signature of the packets that solely block the sinning traffic, and leaves valid traffic untouched.

Since routers and switches tend to transport their network flow when there has been a amount of inactivity (on average concerning fifteen seconds), the “earliest a flow-based anomaly detection answer will begin to notice the anomaly is a minimum of fifteen seconds when its onset” [4]. After that, the detection algorithms will begin process, that additional adds to the delay in finding associate anomaly or not. During a flow-based anomaly detection system, the routers and switches ar the elements that produce the flow records. These flow records ar the sole insight into this network traffic.

The matter with this can be that a lot of anomalies and malicious activity may well be either designed to have an {effect on} the routers and switches or take them down as a facet effect of the particular cause of the attack. During this case, throughout the worst doable time, the flow-based system may fail to detect something within the middle of associate attack, since the router has unsuccessful. The packet-based anomaly detection system works in real time since it doesn’t rely on any third party components, like routers or switches. due to that there's no fifteen second time delay before the applied mathematics information on the network traffic is on the market to the code. As long as traffic is flowing on the network links, it's seen and analyzed. The detection algorithms are endlessly

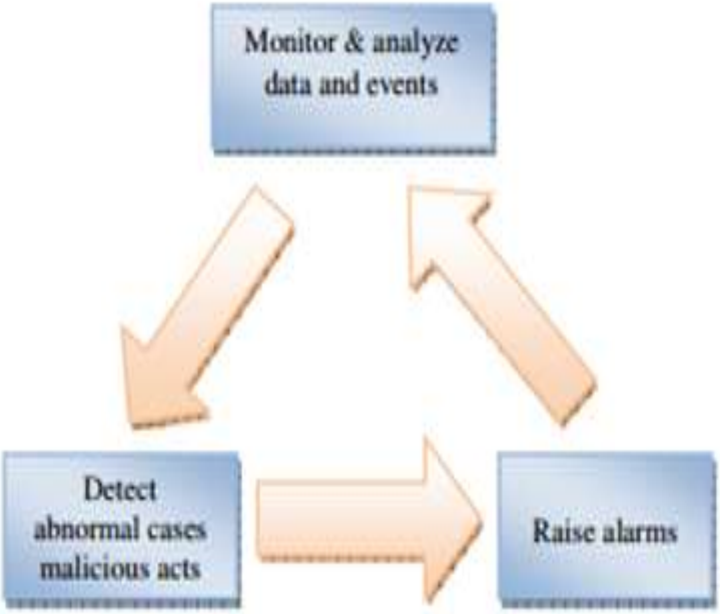

Monitor & analyze data and events
Detect abnormal cases malicious acts
Raise alarms

Fig.1: Traditional IDS Framework

III NETWORK BEHAVIOUR ANALYSIS

Within the last few years, Network Behavior Analysis (NBA) has been one of these emerging technologies that have been sold as a security management tool to improve the current network security status.

The main focus of NBA is to monitor inbound and outbound traffic associated with the network to ensure that nothing is getting into the servers, software, and application systems which helps enhance the overall security of the network at all levels. The author in [1] stated that approximately 25% of large enterprises systems will be using NBA by 2011.

The traditional security model of network as shown in figure 2 is not clear and has too many concerns. First of all, the model have little proactive capability attitude toward preventing any security incidents because the architecture is built with technologies that discover most security events in progress while it misses opportunities to detect and resolve other small threats before it become major problems for the network. Firewalls and intrusion detection systems are typically stationed at a network gateway, which doesn't stop laptops infected with malware or subversive employees from accessing the network.

A typical security tactic to overcoming this problem is to deploy firewalls and intrusion detection devices throughout the internal network [4]. This can get extremely expensive and can increase network maintenance and complexity even without addressing many of the security threats. Without NBA systems added to the security model, the architecture could require three to four times more intrusion prevention system devices that if it had it. Though intrusion detection and intrusion prevention systems can spot common and signature based attacks such as port scans, denial of services, and certain viruses, but they cannot trap the security attacks that fast spreading such as zero-day worms.

Other potential attacks such as reverse tunneling and island hopping look like normal traffic so there is no signature to detect the breach [4]. Since this traditional security model is event-based, log files become irrelevant as they do not provide a true picture of the internal control metrics for security administrators and auditors. This limitation forces companies into expensive manual process and lengthy audit cycles. Once these security events penetrate the internal network, the traditional model can provide little help.

The security devices tend to reside at either the perimeter or at gateways of the network, so there is a possibility that they might miss internal attacks in other network segments. The addition of a network behavior analysis system to anchor the traditional security architecture as in figure 3 can have several benefits. First benefit, NBA systems provide visibility into how both applications and services are being used within the network [5]. This allows for the identification of risky activities, creation of more secure network segments, fine tuning of corporate access policies, and the ability to deploy security appliances more effectively.

The NBA system's network monitoring capabilities allows for monitoring historical trends to help improve security over time. For example, a security administrator may see a security attack in the sales department of a company where managers travel with their laptops and have to access unsecured networks [6]. Using this information from the historical trends, the network security team can deploy security countermeasures such as an intrusion prevention device within that network segment.

NBA systems can also help detect attacks such as zero-day worms and suspicious insider activities across the network. In this respect, NBA can adapt the use of an intrusion detection system that tracks signature based security attacks faster. Finally, NBA systems can view the network in terms of the applications and users consuming services from specific servers.

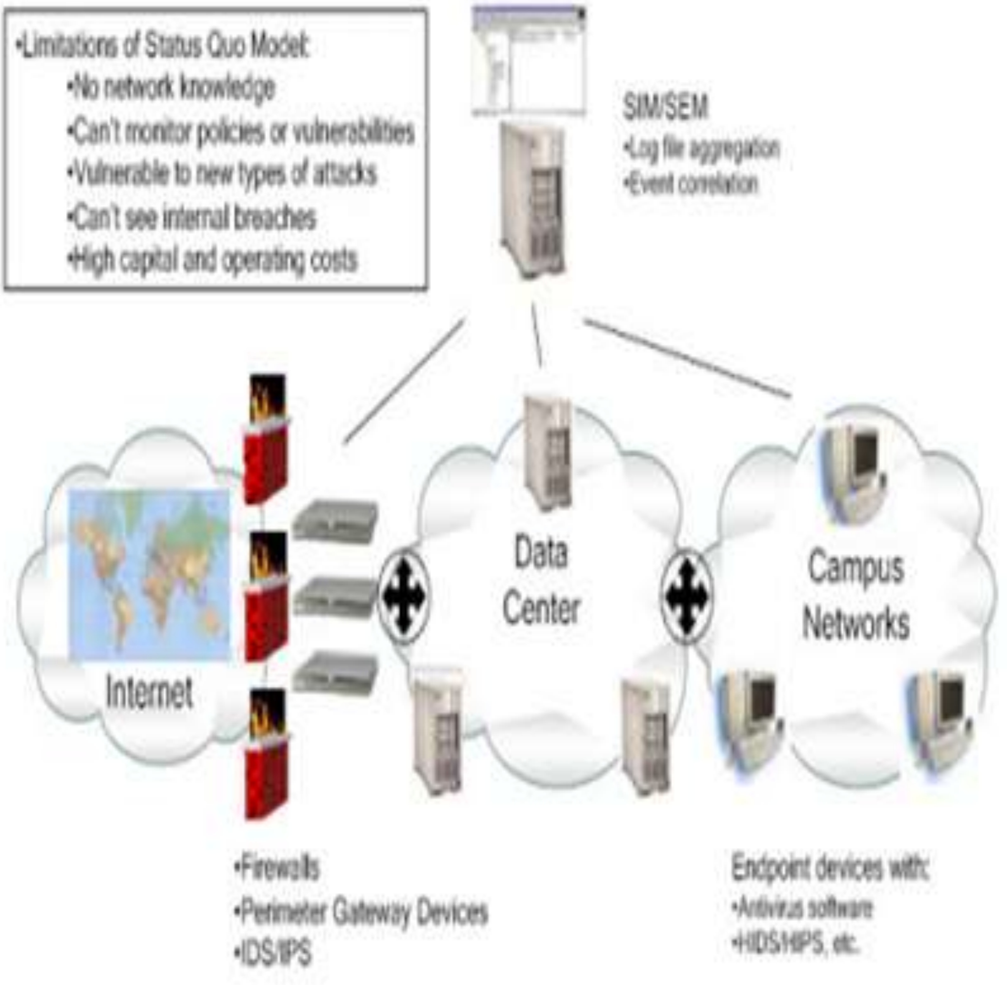
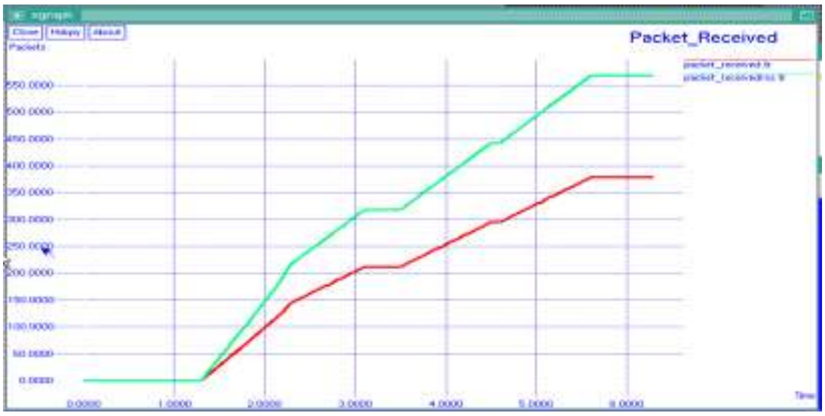

•Limitations of Status Quo Model:
•No network knowledge
•Can't monitor policies or vulnerabilities
•Vulnerable to new types of attacks
•Can't see internal breaches
•High capital and operating costs
SIM/SEM
•Log file aggregation
•Event correlation
Internet
Data Center
Campus Networks
•Firewalls
•Perimeter Gateway Devices
•IDS/IPS
Endpoint devices with:
•Antivirus software
•HIDS/HIPS, etc.

Fig.2: Traditional Network Defense Strategy Model (SANSI 2009), Source Enterprise Strategy Group

This helps organizations setup proper internal controls and enforces a network usage policy. This can prevent users from setting up their own servers or using inappropriate services. It also ensures that developers and development servers do not mingle with production systems [7].

IV PROPOSED IDS MODEL BASED ON DM AND NBA

Due to the many advantages of DM and NBA approaches in network intrusion detection, we suggest that a combination of both approaches can help develop a new generation of high performance IDS. In comparison to traditional IDS (Fig.1), IDS based on DM and NBA are generally more precise and require far less manual processing and input from human experts.



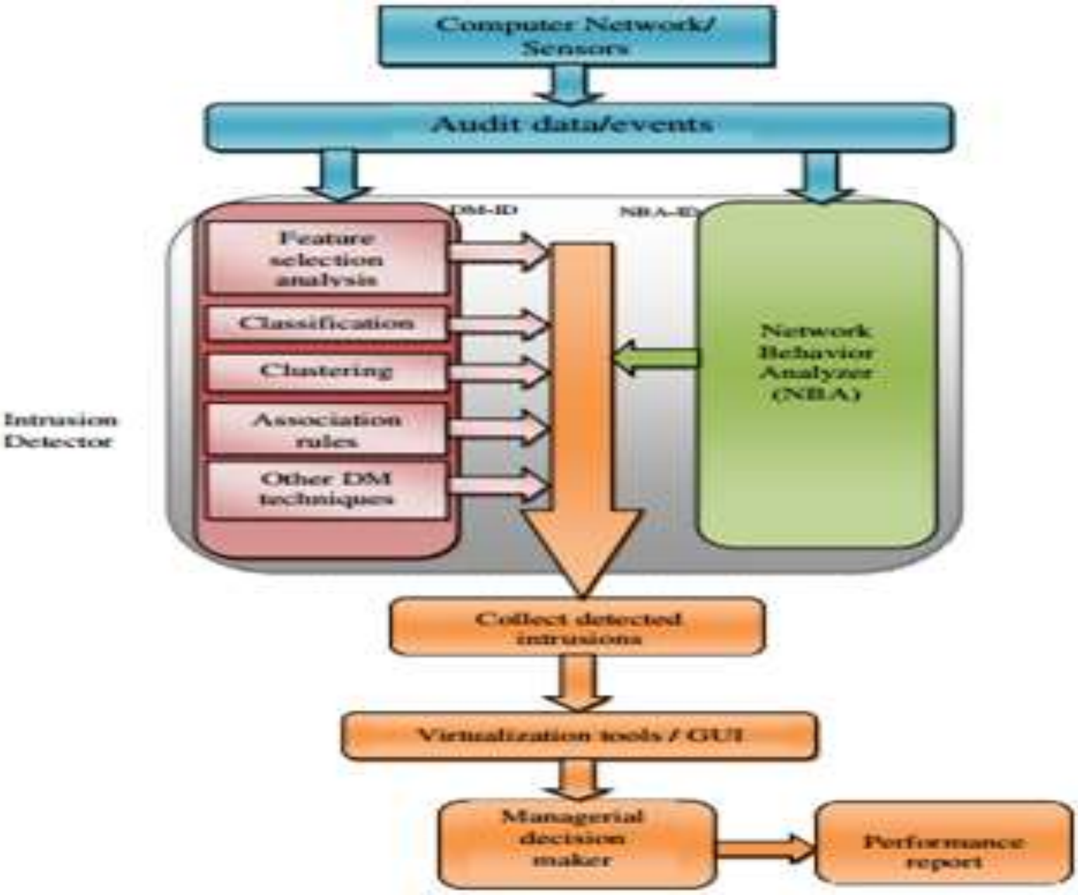

Computer Network/ Sensors
Audit data/events
DM-ID
NBA-ID
Feature selection analysis
Classification
Clustering
Association rules
Other DM techniques
Network Behavior Analyzer (NBA)
Intrusion Detector
Collect detected intrusions
Virtualization tools / GUI
Managerial decision maker
Performance report

Fig.4: The Proposed IDS model based on DM and NBA

Figure 4 shows the proposed IDS model based on DM and NBA. The system is composed of the following units:

• Computer network sensors: collect audit data and network traffic events and transmit these data to ID units.

• DM-ID unit: contains different modules that employ various DM algorithms and techniques (e.g., classification, clustering, etc.). Each module works independently to detect intrusions in the network traffic data.

• NBA-ID unit: deploys NBA to detect intrusions in the network audit data.

• Intrusions collection unit: collects detected intrusions from DM-ID and NBA-ID units.

• Visualization unit: help monitor and visualize the results of ID units.

• Managerial decision maker: analyzes intrusion results, evaluates system performance, takes decisions on detected intrusions, checks for false positives and false negatives, controls system operation, generates a performance report and decides if any changes/updates are needed.

V CONCLUSIONS AND FUTURE WORK

Traditional IDS suffer from different problems that limit their effectiveness and efficiency. In contrast DM and NBA are promising approaches for intrusion detection. In this paper, we discussed DM and NBA approaches for network intrusion detection. We suggested that a combination of both approaches may overcome the limitations in current IDS and leads to high performance ones. NBA can help cover the gap in traditional network systems, which considers a good move for most of industries to integrate NBA with advanced DM to achieve a better performance. NBA can significantly enhance the value of the data generated from IDS that use DM as intrusion detection technique by analyzing and correlating large amount of sequence data. We plan to put the suggested hybrid system model in practice and apply it on real world intrusion detection problems.

REFERENCES

[1] Schwartz, Matthew, "Beyond Firewalls and IPS: Monitoring Network Behavior." February 2006, available on http://esj.com/articles/2006/02/07/beyond-firewalls-and-ips-monitoring-networkbehavior.aspx

[2] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)", NIST Special Publication 800-94, 2007, Available online: http://csrc.nist.gov/publications/nistpubs/800- 94/SP800-94.pdf

[3] Conry-Murray, "Anomaly Detection On the Rise", June 2005, available on http://business.highbeam.com/787/article-1G1-132920452/anomaly-detection-rise-network-behavioranomaly-detection

[4] Enterprise Strategy Group, "Network Behavior Analysis Systems: The New Foundation of Defensein-Depth", Technical White Paper, November 2005. http://www.enterprisestrategygroup.com/

[5] Mazu Networks, "What You Can't See Can Hurt You: Ensuring Application Availability through Enterprise-Wide Visibility", November 2006. http://www.developertutorials.com/whitepapers/network-communications/

[6] Liebert, Chris, "Internal Threat Protection with Net-Based Detection, Prevention and Behavioral Systems", October 2006, http://www.mazunetworks.com/resources/analystreports/Internal_Threat_Protection_January_06.pdf. [7] Enterprise Management Associates: Behavioral Analysis Enables a New Level of Network Security Awareness, technical White Paper, June 2004. http://security.ittoolbox.com/research/behavioralanalysis-enables-a-new-level-of-network-security-awareness-3755

[7] Tanase, Matthew, " One of These Things is not Like the Others: The State of Anomaly Detection", 2010, http://www.symantec.com/connect/articles/one-these-things-not-others-state-anomalydetection [9] Esphion: Packet vs. flow-based anomaly detection. Technical White Paper, July 2005. http://trendmap.net/support/wp/ESP_WP_4_PACKET_V_FLOWS.pdf

[8] Network Intelligence, "Network Intelligence Integrates Network Behavior Analysis Solutions to Enable Broad Internal Threat Detection", June 2006, http://www.rsa.com/press_release.aspx?id=7564. International Journal of Computer Science & Information Technology (IJCSIT) Vol 3, No 6, Dec 2011 98

[9] Detroit Tigers Select Lancope's StealthWatch to Protect Comerica Park Network, October 2006. http://www.lancope.com/news-events/press-releases/detroit-tigers-select-lancopes-stealthwatch-toprotect-comerica-park-networ/

[10] C. Kruegel and G. Vigna. “Anomaly detection of web-based attacks”, in ACM CCS’03 [13] S. Mukkamala et al. “ Intrusion detection using neural networks and support vectHereby attaching passport size photograph of machines”, in IEEE IJCNN May 2002.

AUTHORS

Prashant.M received B.E degree in computer science and engineering from Anna University, Tamil Nadu, and India in 2015 respectively. Currently he is doing the full time internship Trainee in Polaris India Pvt. Ltd. He has published one international journal.

His research interests focus on the area of Network Security analytics, dynamic adaptation of MapReduce computations, data mining.

Ramesh Krishnan received Bachelor of Engineering and Master of Engineering degrees from Anna University, India in 2007 and 2010 respectively. Currently he is pursuing the full time Ph.D Degree at Anna University. He has published papers in four international journals and three international conferences. His research interests focus on the area of low-power, high-performance VLSI architectures and circuit design for digital communications and digital signal processing.