A SURVEY OF INTRUSION DETECTION SYSTEMS

AGUSHAKA, J. O.*, EKE C. I. AND DAUDA, A.

Department of Computer Science, Federal University Lafia, Nasarawa State.
***Corresponding author: jagushaka@yahoo.com**

Article received: 14th January, 2015; Article accepted: 13th February., 2015.

ABSTRACT

There is currently a need for an up-to-date, thorough survey of the field of intrusion detection. This paper presents such a survey of the important research on intrusion detection systems to date. It should be noted that the main focus of this survey is intrusion detection systems, in other words major research efforts that have resulted in prototypes that can be studied both quantitatively and qualitatively. We touched a number of open questions related to intrusion detection. However, there are a number of unresolved issues regarding the scope of analysis that an IDS performs and the interoperability of intrusion detection systems

Keywords: Intrusion Detection Systems, mobile agents, network security, data mining

INTRODUCTION

The rapid proliferation of computer networks has changed the prospect of network security. This is caused by increase in Internet based technology; new application areas for computer network have emerged. At the same time, wide spread progress in the Local Area Network (LAN) and Wide Area Network (WAN) application areas in business, financial, industry, security and healthcare sectors made us more dependent on the computer networks. An easy accessibility condition causes computer networks to be vulnerable against several threats from hackers. Threats to networks are numerous and potentially devastating. Up to the moment, researchers have developed Intrusion Detection Systems (IDS) capable of detecting attacks in several available environments. A boundlessness of methods for misuse detection as well as anomaly detection has been applied. Many of the technologies proposed are complementary to each other, since for different kind of environments some approaches perform better than others.

Intrusion Detection is the process of observing and analyzing the events arising in a computer or network system to identify all security problems. Intrusion detection systems are the ‘burglar alarms’ (or rather ‘intrusion alarms’) of the computer security field. Intrusion detection as defined by(Verwoerd and Hunt,2002) is "the problem of identifying individuals who are using a computer system without authorization (`crackers') and those who have legitimate access to the system but are abusing their privileges (the `insider threat')". (Defenget al., 2000) said IDS provides three important security functions; monitor, detect and respond to unauthorized activities.

According to, (Jaiganeshet al., 2013), Intrusion detection techniques are traditionally categorized into two methodologies: anomaly detection and misuse detection. Anomaly detection is based on the normal behavior of a subject (e.g., a user or a system); any action that significantly deviates from the normal behavior is considered intrusive. Misuse detection catches intrusions in terms of the characteristics of known attacks or system vulnerabilities; any action that conforms to the pattern of a known attack or vulnerability is considered intrusive. In addition to the hacking, new entities like Worms, Trojans and Viruses introduced more panic into the networked society. As the current situation is a relatively new phenomenon, network defenses are weak. However, due to the popularity of the computer networks, their connectivity and our ever growing dependency on them, realization of the threat can have devastating consequences. Securing such an important infrastructure has become one area of priority for many researchers.

Intrusion Detection

A system cannot naturally prevent the intruder from getting into the system, noticing the intrusion will provide the security officer with valuable information. The Intrusion Detection (ID)is considered to be the first line of defense for any security system. (Smaha,1988) in his paper established that Early IDS implementations employed a monolithicarchitecture under which data collected at a single host was analyzed at a central point, at or adjacent to thepoint of collection. Also, (Heberleinet al., 1990) said that because monitoring account activity on a single host does not revealattacks involving multiple hosts, IDS designers subsequently developed network-based IDSs that use a model of the network traffic to infer anomalies or misuses from low-level network packets traveling among hosts. A network-based Intrusion Detection System usually consists of a network application (or sensor) with a Network Interface Card (NIC) working in promiscuousmode and a separate management of interface. IDS is placedon a network segment or boundary and monitor all traffic onthat segment. (Fung and Mangasarian,2005) identified that the current trend in intrusion detection is tocombine both host based and network based information todevelop hybrid systems that are more efficient.

Use of Artificial Intelligence in Intrusion Detection

Artificial Intelligence could make the use of IntrusionDetection Systems a lot easier than it is today. They couldlearn the preferences of the security officers and showthe kind of alerts first that the officer has previously beenmost interested. As always, the hardest thing with learning Artificial Intelligence (AI) is to make them learn the right things. (Manninen, 2003) focused on finding out how to make an IDS environment learn the preferences and work practices of a security officer, and how to make it more usable by showing the most often viewed anomalies first. Also, noise always causes problems, regardless of the used intrusion detection methods. Configuring an AI-based IDS is easier than configuring a traditional IDS. This decreases deployment costwhich is an important factor for companies. Because of this,they could more easily test different easy-to-deploy IDSs tosee which of them is the mostsecure and requires the leastmonitoring in their network. Another interesting aspect is theuse of an Artificial Immune System (AIS) for network intrusion detection.

(Kim and Bentley,2001)focused on one significant component of a complete AIs, static clonal selection with a negative selection operator, describing this system in detail. Three different data sets from the UCI repository for machine learning are used in the experiments. They identified two important factors, the detector sample size and the antigen sample size, are investigated in order to generate an appropriate mixture of general and specific detectors for learning non-self-antigen patterns. The results of series of experiments suggest how to choose appropriate detector and antigen sample sizes. These ideal sizes allow the AIS to achieve a good non-self-antigen detection rate with a very low rate of self-antigen detection. They conclude that the embedded negative selection operator plays an important role in the AIS by helping it to maintain a low false positive detection rate. An approach toward user behavior modeling that takes advantage of the properties of neural algorithms is another area of focus. (Debar et al.,1992)Described and obtained results on preliminary testing of this approach. The basis of the approach is the IDES (Intruder Detection Expert System) which has two components, an expert system looking for evidence of attacks on known vulnerabilities of the system and a statistical model of the behavior of a user on the computer system under surveillance. This model learns the habits a user has when he works with the computer, and raises warnings when the current behavior is not consistent with the previously learned patterns. The authors suggest the time series approach to add broader scope to the model. They therefore feel the need for alternative techniques and introduce the use of a neural network component for modeling user's behavior as a component for the intrusion detection system. Wireless sensor networks (WSNs) are distributed in nature where sensor nodes operate independently without any centralized authority.

(Alrajeh and Lloret,2013)presented a critical study on genetic algorithm, artificial immune, and artificial neural network (ANN) based IDSs techniques used in wireless sensor network (WSN). In genetic algorithm, the selection module derives most suitable answer or solution for some specific problem. When the genetic algorithm is applied to an IDS, several issues were taken into account. The first one is the type of intrusion detection system purpose, and the second one is the element where it will be applied. (Khangamwa, 2012) investigated the use of a novel Artificial Intelligence (AI) approach to intrusion detection based on network traffic anomaly detection. The AI technique used is based on the Hierarchical Temporal Memory (HTM) paradigm developed by Numenta, which is a relatively new AI concept that mimics the operation of the neocortex area of the human brain. They evaluated the scheme using the corpus of data from Massachusetts Institute of Technology, Lincoln Laboratories in USA and their results show that HTM based intrusion detection can achieve relatively high success rates in identifying anomalous traffic in computer networks, it also shows that HTM based schemes can achieve very fast detection rates making them a very good alternative for real time intrusion detection engine.

Embedded Programming and Intrusion Detection

Networked sensor systems are seen by observers as an important technology that will experience major deploymentin nextfew years for a variety of applications.Adding different security methods is animportant and essential procedure toenhance the operation and safety of suchsystem. In their paper, (Qutaibaet al., 2012)focused on the designand implementation challenges to localizean embedded version of SNORT IntrusionDetection System into wireless gatewaynodes. Their design takes into account the"embedded" nature of the gateways andtheir limited resources and suggestsdifferent methods and protocols to achieveits goals. The obtainedresults provethepossibility to insert IDS functionality in thesystem with minimum effect of its normaloperation.

(Macia-Perez *et al.,* 2011) proposed aNetworkIntrusionDetectionSystem(NIDS)embedded in aSmart Sensorinspired device,under a Service Oriented Architecture (SOA) approach, able tooperate independently as ananomaly-based NIDSor integrated,transparently, in aDistributed Intrusion Detection System(DIDS). A full functional prototype has also been developed. Thisprototype has been used to validate the proposal. The resultsshow that the device exhibits a very stable behavior and iscapable to provide a service, as critical as the intrusiondetection service is, under really adverse conditions ofnetwork traffic load. Also, (Yoon et al., 2013) presented theSecureCoreframework that, coupled with novelmonitoring techniques, is able to improve the security of real-time embedded systems. Through the architectural and the theoretical support, their intrusion detection mechanism implemented could detect violations earlier than just a pure safety-driven method, Simplex. This helps in achieving reliable control for physical systems. The isolation achieved by Secure Core and the monitoring mechanisms presented by GaIT also prevents attackers from causing harm to the physical systems, even if they gain total control of the main controller. Evaluation results showed that with careful analysis and design of certain parameters, one can achieve a low misclassification rate and higher intrusion detection rates.

Agent Based Intrusion Detection

Implementing an effective intrusion detection capability is an elusive goal, not solved easily or with a single mechanism. However, mobile agent technology goes a long way toward realizing the ideal behavior desired in an Intrusion Detection System (IDS). A number of advantages of using mobile code and mobile agent computing paradigms over their static counterparts have been identified in the work of (Lange and Oshima, 1998). In his paper, (Jansen,2002)found out that while not a perfect solution, mobile agent technology goes a long way toward being able to realize the ideal behavior wanted from an IDS. Not only do aspects of the detection side of the equation benefit, but also, and perhaps more significantly, there sponse side of the equation is improved significantly. Because present day IDSs do not inherently involve mobile agent technology, we do not expect a wholesale transition to this paradigm.

However, the technology lends itself to gradual adoption and use. Because of the noted advantages, particularly with respect to responding to an intrusion, mobile agent technology has the potential for gaining an initial foothold and expanding its reach over time. There are two approaches in implementing an agent based technology. In the first approach, autonomous distributed agents are used to both monitor the system and communicate with other agents in the network. In the second approach, mobile agents are used to travel through the network and collect information or to perform some tasks.

(Jaisankaret al., 2009) presents a network intrusion system framework using mobile agent, which is able to detect user anomalies in two levels: user activity and program operation. On the user level, the system can detect unauthorized use of programs correctly and on the program level, the excessive use of system resources can be detected. This framework consists of the use of a large number of small mobile agents, which operates independently from the others; however, they all cooperate in monitoring the system, forming complex IDS. In specific period, number of intrusions were created and with help of simulation. At all the time periods, the simulation showed above 95%ability to detect the intrusion. A Dynamic Countermeasure Method for Large-Scale Network Attacks was proposed by (LiuandUppala, 2006). This project uses Snort as the IDS and two types of agents; Snortsam and Gnipper vaccine. Snortsam is an intelligent agent that integrates with Snort to perform a block operation on a remote firewall. This allows Snort to block intruding connections by generation of dynamic ip Tables firewall rules. Snortsam will request a block on firewall host where it resides. Gnipper vaccine is a dynamic agent that resides on a host and capable of dropping any malicious packets. It will propagate one hop at a time towards the source of the attackers thus disabling the ability of the attacker to ping the intended victim.

In their paper, (Alouf et al., 2002) evaluated and compared the performance of two approaches for locating an agent (e.g. a code) in a mobile agent environment. The first approach dynamically creates a chain of forwarders to locate a moving agent whereas the second one relies on a centralized server to perform this task. Based on a Markov chain analysis, they compute the performance of each scheme (time to reach an agent, number of forwarders) and compare them first with simulations and second with experimental results obtained by using ProActive, a Java library. Depending on the system parameters we identify the best scheme and observe that within a LAN the server yields the best performance whereas the forwarders yield the best performance within a MAN

Role of Network Model in IDS

This means to define normal and abnormal behavior of the network system. The most frequent behavior of (events within) the system during a certain time period is called the normal behavior of the system. The least frequent behavior of (event within) the system during a certain time period is called anomaly or abnormal behavior. It is clear from the literature, that researchers have followed deferent approaches to improve accuracy and performance of their proposed IDS. In their work, (Joo et al., 2003)proposed method utilizes the neural network model to consider the cost ratio of false negative errors to false positive errors. A neural network contains no domain knowledge in the beginning, but it can be trained to make decisions by mapping exemplar pairs of input data into exemplar output vectors, and adjusting its weights so that it maps each input exemplar vector into the corresponding output exemplar vector approximately. In order to measure the performance of IDS, two types oferrors are identified, false positive errors and false negative errors according to the threshold value of the neural network. Compared with false positive errors, false negative errors incur a greater loss to organizations which are connected to the systems by networks. The results of the empirical experiment indicate that the neural network model provides very high performance for the accuracy of intrusion detection. The results show that the efforts to adjust the cost ratio between false positive errors and false negative errors are important for reducing the total cost of errors, i.e. IDS performance.

Also, (Okafor et al., 2013) discussed, analyzed and developed novel security architecture for secure transactions in Virtual Private Network (VPN) environments. Open standard VPN has been in use for a long time without addressing the security holes in VPN wired and wireless networks. They presented SMART Network Security System (SNSS) which is shown to be very reliable and supports multiple functionalities for both LAN and WLAN VPN setups. In deployment context, the SNSS have a Multilayer Access Point Intrusion Detection System (MAPIDS) sensor for monitoring traffic and network behavior. Also, in their model, the security features were configured and tested in the simulator for authentication, confidentiality, integrity and auto-replay, which characterizes the model. In the work, the link throughput is the area analyzed from the global and object palette of the OPNET simulator, which indicates the receiving and sending of data packets considering the security configurations.

In his survey paper, (Kumar, 2007) described the design and architecture of a number of different NIDS and the various configurations, in which they are employed in the network. Specifically, they focus on two important classes of NIDS: signature based and anomaly based. We thoroughly investigated their benefits and drawbacks, and discussed a number of attack and vulnerabilities than they can combat. A NIDS can detect attacks, and anomalous conditions, additionally they can also provide a number of key information which can be used to identify the nature of attack, its origin and propagation characteristics. First and foremost, most NIDS often reports the location of the attacker or hacker (from where the attack has been triggered). However, the location is commonly expressed as an IP address, which is not reliable information, as the smart attackers often change the IP address in the attack packets, which is called IP address spoofing. Finally they discuss the future trends in this space, where we argue that a more distributed version of NIDS is on the horizon and that the NIDS mechanisms need to be standardized. The key challenge then remains in devising the algorithms that can detect anomalies with a fairly high degree of confidence. Although this is an active research topic, it still is questionable when such algorithms will be devised that can be used in a commercial setting

CurrentTrends in IDS

In the past two decades with the rapid progress in theInternet based technology, new application areas forcomputer network have emerged. At the same time, widespread progress in the Local Area Network (LAN) andWide Area Network (WAN) application areas in business,financial, industry, security and healthcare sectors made usmore dependent on the computer networks. All of theseapplication areas made the network an attractive target forthe abuse and a big vulnerability for the community. The first step in securing a networked system is to detect the attack. Even if the system cannot prevent the intruder from getting into the system, noticing the intrusion will provide the security officer with valuable information. The Intrusion Detection (ID) can be considered to be the first line of defense for any security system. Some of the researchers are more interested in applying rule based methods to detect the intrusion.

Data mining using the association rule is also one of the approaches used by some researchers to solve the intrusion detection problem. Researchers such as (Barbara et al., 2001and Yoshida, 2003)have used these methods. Others haveproposed application of the fuzzy logic concept into theintrusion detection problem area. Works reported by(Dickerson and

Dickerson,2000 and Bridges and Rayford,2000)are examples of those researchers that follow this approach.Some researchers even used amultidisciplinary approach,for example, (Gomez and Dasgupta,2002) have combined fuzzy logic,genetic algorithm and association rule techniques in theirwork. Due to its nature, the data miningapproach is widely appreciatedin this field of research.

Some researchers have tried to use the Bayesianmethodology to solve the intrusion detection problem. Themain idea behind this approach is the unique feature of theBayesian methodology. For a given consequence, using theprobability calculations Bayesian methodology can moveback in time and find the causeof the events. This featureis suitable for finding the reason for a particular anomaly inthe network behavior. Using Bayesian algorithm, systemcan somehow move back in time and find the cause for theevents. This algorithm is sometimes used for the clusteringpurposes as well. Although using theBayesian for the intrusion detection or intruder behaviorprediction can be very appealing, however, there are someissues that one should be concerned about them. Since theaccuracy of this methodis dependent on certainpresumptions, distancing from those presumptions willdecrease its accuracy. Usuallythese presumptions are basedon the behavioral model of the target system. Selecting aninaccurate model may lead to an inaccurate detectionsystem. Therefore, selecting an accurate model is the firststep towards solving the problem. Unfortunately due to thecomplexity of the behavioral model within this systemfinding such a model is a very difficult task.

Related Works

In their work, (Kabiri and Ghorbani,2005) reported that in orderto be able to secure a network against the novel attacks;the anomaly based intrusion detection is the bestway out. However, due to its immaturity there are stillproblems with respect to its reliability. These problemswill lead to high false positives in any anomaly-basedIDS. As a solution, usually a hybrid approachis used. In network-based IDS, agent based systems play an essential role. In such systems a distributed processing architecture is a must and system has to collect information from different components within the network. Implementing such architecture, one should avoid increasing the network traffic. Another aspect of the IDS design is the issue of themissed attacks. If some attacks are not detected by theIDS, there are no means to notice them. However, they did not consider IDScapable of anomaly and signature based intrusion detectionespecially when dealing with high volume of data.

Nowadays researchers have interested on intrusion detection system using Data mining techniques as an artful skill. IDS is a software or hardware device that deals with attacks by collecting information from a variety of system and network sources, then analyzing symptoms of security problems. An overview of intrusion detection systems is given in (Jaiganeshet al., 2013)and they introduced the reader to some fundamental concepts of IDS methodology. Also, they discuss the primaryintrusion detection techniques. In this paper, they emphasizes data mining algorithms to implement IDS such as Support Vector Machine,Kernelized support vector machine, Extreme Learning Machine and Kernelized Extreme Learning Machine. Classification techniques evaluate and classify the data into known classes. Each data sample is marked with a known class label. Also these techniques are used to learn a model using the training set data sample. This model is used to classify the data samples as anomalous behaviour data or the normal behaviour data. Support Vector Machines (SVM’s) can only perform as a linear classifiers and regressors. By using the kernel trick, SVM’s are able to perform both non-linear classification and regression. Non-linear classifiers are created by applying the “kernel trick” to maximum-margin hyper planes. In the resulting algorithm, every “dot-product” positioned is replaced by a non-linear kernel function. Extreme Learning Machine (ELM) is a new emergent technology which provides good generalization performance for both classification and regression problems at highly fast learning speed. Even though Support Vector Machine can produce better generalization performance, it has two drawbacks as well. The intensive computation involved in its training which is at least quadratic with respect to the number of training examples. For large complex applications, it generates large network size It draws the conclusions on the basis of implementations accomplished using various data mining algorithms. Combining more than one data mining algorithms may be used to eliminate disadvantages of one another.

Security of Wireless sensor network (WSN) becomes a very important issue with the rapid development of WSN that is vulnerable to a wide range of attacks due to deployment in the hostile environment and having limited resources. Wireless sensor network (WSN) refers to a system that consists of number of low-cost, resource limited sensor nodes to sense important data related to environment and to transmit it to sink node that providesgateway functionality to another network, or an access point for human interface. Intrusion detection system is one of the major and efficient defensive methods against attacks in WSN. A particularly devastating attack is the sleep deprivation attack, where a malicious node forces legitimate nodes to waste their energy by resisting the sensor nodes from going into low power sleep mode. The goal of this attack is to maximize the power consumption of the target node, thereby decreasing its battery life. Existing works on sleep deprivation attack have mainly focused on mitigation using MAC based protocols, such as S-MAC, T-MAC, B-MAC, etc. In (Bhattasali and Chaki,2011), a brief review of some of the recent intrusion detection systems in wireless sensor network environment is presented. They propose a framework of cluster based layered countermeasure that can efficiently mitigate sleep deprivation attack in WSN. A lightweight model, Insomnia Mitigating Intrusion Detection System (IMIDS) is proposed for Heterogeneous Wireless Sensor Network (HWSNET) to detect insomnia of stationary sensor nodes. It uses cluster based mechanism in an energy efficient manner to build a five layer hierarchical network to enhance network scalability, flexibility and lifetime. The low energy constraints of WSN necessitate the use of a hierarchical model for IDS. The divide sensor network into clusters which are again partitioned into sectors Simulation results on MATLAB exhibit the effectiveness of the proposed model in detecting sleep-deprivation attacks.

CONCLUSION

The aim of this paper is to review the current trends in Intrusion Detection Systems (IDS). In comparison to some mature and well settled research areas, IDS is a young field of research. However, due to its mission critical nature, it has attracted significant attention towards itself. Density of research on this subject is constant lyrising and everyday more researchers are engaged in this field of work. The threat of a new wave of cyber or network attacks is not just a probability that should be considered, but it is an accepted fact that can occurate any time. The current trend for the IDS is far from are liable protective system, but instead the main idea is to make it possible to detect novel network attacks. A major problem in the IDS is the guarantee for the intrusion detection. This is the reason why in many cases IDSs are used together with a human expert. Desired features for the IDS depend on both the methodologyand the modeling approach used in building theIDS. Just extracting features is not useful for the ID. Extraction should be followed with a second stage where patterns are produced using the extracted features. In evaluating intrusion detection systems, the three most important qualities that need tobe measured are completeness, correctness, and performance. The coordinated deployment of multiple intrusion detection systems promises to allow greater confidence in the results of and to improve the coverage of intrusion detection, making this a critical component of any comprehensive security architecture.

This paper has touched upon a number of open questions related to intrusion detection. However, there are a number of unresolved issues regarding the scope of analysis that an IDS performs and the interoperability of intrusion detection systems. There have recently been a number of efforts including the Common Intrusion Detection Format (CIDF) and the IETF standardization effort motivated towards providing interoperability among intrusion detection systems. Although it will likely be some time before a standard framework finds its way into widespread use so more research is needed in this direction.

REFERENCES

Alouf, S., Huet, F. and Nain, P. (2002)"Forwarders vs. Centralized Server: An Evaluation of Two Approaches for Locating Mobile Agents". Rap.derech. No4440, INRIA.

Alrajeh N. A. and Lloret J., (2013) “Intrusion Detection Systems Based on Artificial Intelligence Techniques in Wireless Sensor Networks,” International Journal of Distributed Sensor Networks, vol. 2013, Article ID 351047, 6 pages, 2013. doi:10.1155/2013/351047.

Barbara D., Couto J., Jajodia S.,and Wu N., (2001) “Special section on datamining for intrusion detection and threat analysis: Adam: a test bed for exploring the use of data mining in intrusion detection,” ACSIGMOD Record, vol. 30, pp. 15–24.

Bhattasali T., and Chaki R., (2011) “A Survey of Recent Intrusion Detection Systems for Wireless Sensor Network”, in 4th International Conference on Network Security and Applications (CNSA-2011), Springer, pp. 268-280.

Bridges S. M. and Rayford M. V., (2000) “Fuzzy data mining andgenetic algorithms applied to intrusion detection,” in Proceedings of the Twenty third National Information Systems SecurityConference. National Institute of Standards and Technology.

Debar H., Becke M., SibonD. I, (1992) "A neural network component for an intrusion detection system", In Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy.

Defeng Wang, Yeung, D.S., and Tsang, E.C., (2007) “WeightedMahalanobisDistance Kernels for

Support Vector Machines”, IEEETransactions on Neural Networks, Vol. 18, No. 5, Pp. 1453-1462.

Dickerson J. E. and Dickerson J. A., (2000) “Fuzzy network profilingfor intrusion detection,” inProceedings of NAFIPS 19thInternational Conference of the North American Fuzzy InformationProcessing Society, pp. 301–306, Atlanta, USA.

Fung G. M. and Mangasarian O. L., (2005) “MulticategoryProximal Support Vector Machine Classifiers”, Springer Science andBusiness Media, Machine Learning, 59, 77–97.

Gomez J. and Dasgupta D., (2002)“Evolving fuzzy classifiers for intrusiondetection,” in Proceedings ofthe 2002 IEEE Workshop on theInformation Assurance, West Point, NY, USA.

HeberleinL. T, Dias G.V., Levitt K. N., Mukherjee B., Wood J., and Wolber D., (1990) “A NetworkSecurity Monitor,” Symposium on Research in Security and Privacy, pp.296-304.

Jaiganesh V. ,Mangayarkarasi S. , Sumathi P.. (2013) “Intrusion Detection Systems: A Survey andAnalysis of Classification Techniques” International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 4.

Jaisankar N., Saravanan R. and SwamyK. D., (2009) “Intelligent Detection System Framework Using Mobile Agents”, IJNSA Journal, Vol 1, No 2.

Jansen W. A., (2002) "Intrusion detection with mobile agents", Computer communication (15): page: 1392-1401.

Joo, D., Hong, T., Han, T. (2003) “The Neural Network Models for IDS Based on the Asymmetric Costs of False Negative Errors and False Positive Errors”. Expert Systems with Applications 25: pp. 69-75.

KabiriP. and GhorbaniA. A., (2005) “Research on Intrusion Detection and Response: A Survey:” International Journal of Network Security, Vol.1, No.2, PP.84–102.

KhangamwaG. (2012)“Detecting Network Intrusions Using Hierarchical Temporal Memory” AFRICOMM Springer DOI: 10.1007/978-3-642-23828-4_5.

Kim J. and Bentley P. J., (2001) "Towards an artificial immune system for network intrusion detection: an investigation of clonal selection with a negative selection operator", Evolutionary Computation, 2001. Proceedings of the 2001 Congress on, Vol 2, pp 1244 - 1252.

Kumar S.(2007) ”Survey on current network Intrusion DetectionTechniques”12/19/2007sailesh@arl.wustl.edu

Lange D. and Oshima M. (1998) “Programming and Deploying Java Mobile Agents with Aglets”,ISBN:0-201-32582-9, Addison-Wesley.

Liu, Z., andUppala, R. (2006).“A Dynamic Countermeasure Method for Large-Scale Network Attacks”.University of Carolina.

Macia-Perez F., Mora-Gimeno F., Marcos-Jorquera D., Gil-Martinez-Abarca J. A., Ramos-Morillo H. and Lorenzo-Fonseca I. (2011) "Network intrusion detectionsystem embedded on a smart sensor", IEEE Trans.Ind. Electron., vol. 58, no. 3, pp.722 -732.

ManninenM. (2003), "Using Artificial Intelligence in Intrusion Detection Systems", Helsinki University of Technology.

Okafor K.C., Okezie C.C., Udeze C.C., Okwuelu N. (2013). “SMART IDS: An Enhanced Network Security Model in IP-MPLS Based Virtual Private Network”. Afr. J. of Comp & ICTs.Vol 6, No. 3.Pp135- 146.

Qutaiba I. A.* Sahar L., Enaam F., (2012) “SecuringWireless Sensor Network (WSN) Using Embedded IntrusionDetectionSystems” IraqJ. Electrical and Electronic Engineering Vol. 8 No .1.

SmahaS. E., (1988) “Haystack: An Intrusion Detection System,” Fourth Aerospace Computer SecurityApplications Conference, pp.37-44.

Verwoerd and Ray Hunt, (2002) “Intrusion Detection techniques and approaches”,Computer Communications, Volume 25, Issue 15, Pages1356-1365.

Yoshida K., (2003) “Entropy based intrusion detection,” in Proceedings ofIEEE Pacific Rim Conference on Communications, Computers andsignal Processing (PACRIM2003), vol. 2, pp. 840–843. IEEE Explore.

Yoon, M. K., Mohan, S., Choi, J., Kim, J. E., &Sha, L. (2013). “SecureCore: A multicore-based intrusion detection architecturefor real-time embedded systems”. In Real-Time and Embedded Technology and Applications Symposium (RTAS), 2013 IEEE19th (pp. 21-32).