



A Model of a Pragmatic Secure Intrusion Detection System for Local Area Networks

B. I. Ele^{1*}, U. R. Alo², B. C. E. Mbam³ and A. O. Ofem¹

¹Department of Computer Science, University of Calabar, Calabar Cross River State, Nigeria.

²Department of Computer Science, Ebonyi State University, Abakaliki Ebonyi State, Nigeria.

³Department of Computer Science, Michael Okpara Federal University of Agriculture, Umudike Abia State, Nigeria.

Article Information

DOI: 10.9734/BJMCS/2016/22190

Editor(s):

(1) Junjie Chen, Department of Electrical Engineering, University of Texas at Arlington, USA.

Reviewers:

(1) S. K. Srivatsa, Institute of Technology and Management, Tamil Nadu, India.

(2) Utku Kose, Usak University, Turkey.

Complete Peer review History: <http://sciencedomain.org/review-history/12517>

Original Research Article

Received: 22 September 2015

Accepted: 23 October 2015

Published: 02 December 2015

Abstract

Intrusion detection is very imperative in network systems due to outstanding vulnerabilities left unaddressed by current preventive network security measures such as firewalls and encryption software. The inefficiency, inaccuracy, high false alarm rates and lack of self-defensive mechanism of existing network security systems has continued to pose serious concern to network users, administrators and security professionals and thus needs urgent redress. Therefore, the target of this paper is to develop a model of a pragmatic secure intrusion detection system for local area networks using layered framework with conditional random fields that is capable of overcoming the apparent shortcomings of present intrusion detection systems. A critical analysis of existing IDSs was done using the structured system analysis and design methodology (SSADM) due to the sequential configuration of the proposed security system. Furthermore, a real-time response mechanism and a self-defensive mechanism for a network intrusion detection system (NIDS) was developed and implemented. The outcome of this study was a secured IDS that would proactively address potential security vulnerabilities by resisting and detecting attacks and security policy violations reliably and efficiently in local area networks, thus making it inevitable for use in our security conscious environment of the 21st century.

Keywords: Self-defensive mechanism; network intrusion detection system; fault tolerance; intrusion detection system; secure intrusion detection system; layered framework; conditional random fields.

*Corresponding author: E-mail: mydays2020@gmail.com, auzomarita@yahoo.com;

1 Introduction

Today's world is increasingly reliant on information systems and communications networks which connect them, from country-sized corporations to home and mobile users. The Internet in particular, and its related set of technologies have become nothing short of ubiquitous and increasing convergence between Information Technology and Telecommunications worlds, thus taking this reality even further. Hand in hand with this usage growth, came an increase in the number of attacks to those systems and networks, making protection from attacks increasingly significant [1]. Network intrusion detection systems can play an important role in the defense arsenal.

Network Intrusion Detection Systems (NIDSs) are assigned the critical role of monitoring the security state of the network; therefore, the NIDS itself is a primary target of attack. The NIDS must be able to operate in a hostile computing environment and exhibit a high degree of fault-tolerance which allows for a graceful degradation [2]. Fault tolerance is the ability of a system to respond gracefully to an unexpected hardware or software failure and thus an essential requirement for achieving dependable and secure systems [3].

A secured NIDS must be able to authenticate the administrator, audit administrator actions, mutually authenticate NIDS devices, protect the NIDS data, and resistant, hence not creating additional vulnerabilities. When guarding computer systems or networks against attacks, the conventional approach is to deploy a number of protective mechanisms in order to secure them. However, this approach has some limitations [4]: it is difficult to build systems which are absolutely secure; it may be impractical to replace a vast existing and possibly insecure infrastructure in favour of a new one; the prevention-based approach constrains user's activities, making them less productive; crypto-based systems cannot defend against lost or stolen keys or passwords; and secure systems can still be vulnerable to insiders. These limitations justify the use of other approaches. Intrusion detection systems can provide a second line of defense by enabling early detection of intrusion activities, dissuading intruder's intentions or enabling the collection of information about intrusion techniques that can be used to strengthen the prevention facilities [5].

The ability of the intrusion detection system to resist attacks against itself is an essential property of any IDS. For example, compromised IDS will probably not report an intrusion no matter how clever the detection mechanisms are. In addition, compromised IDS can be a source of severe information leakage and this leakage is not limited to information that originates from the target systems, that is the systems under surveillance, but can also contain information related to the IDS and its operation [6]. Therefore, the target of this study is to develop a model of a pragmatic secure intrusion detection system for local area networks that is resistant to attacks and cannot be compromised or exploited during an attack and as such can detect attacks efficiently and reliably.

2 Problem Definitions

There exist various problems that induce the complexity and inefficiency of intrusion detection systems such as insecurity of the security system, low detection accuracy, unbalanced detection rates for different attack types and high rates of false alarms. Existing intrusion detection systems for local area networks are practically and completely insecure because they lack self-defensive mechanism and as such cannot detect network based attacks efficiently and reliably since they can easily be compromised and exploited during an attack.

Furthermore, in some new malwares, their attack mechanisms are much more sophisticated and difficult to detect. They no longer stay at the stage of using IDS evasion techniques. Some of them try to attack IDS and make the system break down. For instance, in 2007, Coretez Giovanni developed a malware known as **Stick**. This malware executes a large number of simulated attacks in a short time. This causes the IDS on a target machine to get overloaded and then the system can stop responding [7]. Therefore, it is necessary to develop a model of a pragmatic secure intrusion detection system for local area networks that has the ability to defend itself and detect network based attacks efficiently and reliably.

3 Review of Related Works

Majority of the research on security and intrusion detection has addressed the security of the target systems. However, only a few attempts have been made to address the security of the intrusion detection system (IDS) itself. In the work of Debar, Dacier and Wespi [8], **fault tolerance** was introduced as a property that addresses the IDS' ability to resist attacks. In [9], the authors also identified the lack of research in this field and introduced **security** as "the ability of the system to withstand hostile attack against the system itself".

The security that does exist in modern commercial IDSs is centered primarily on concealment, such as unaddressable network cards. This, in our opinion, is security by obscurity. There are a few notable exceptions in this area according to the authors in [10,11].

An extensive set of requirements for tamper proofing network intrusion detection systems was first introduced for Next-generation Intrusion Detection Expert System (NIDES) and clearly identified in a research report by Neumann [12]. He suggests that tamper proofing NIDES can be achieved by fulfilling a series of goals related to the authenticity, integrity and confidentiality of the analysis system (NIDES) and its components. The report proposes the protection of audit data and the analysis system rule-base via subsystem encapsulation. In addition, proper authentication and separation of roles play an important role in securing NIDES. To prevent reverse engineering of the rule-base, that is detection policy, Neumann proposes the use of encryption. Although encryption prevents external users from reading or modifying the rule base, it does not prevent the rule base of a subverted node from being disclosed or modified. A malicious user that has gained control of a node can find a stored encryption key by exploiting the random nature of such keys [13]. Furthermore, password sniffer attacks can be utilized to obtain encryption keys as they are entered by the user.

4 Layered Framework for Intrusion Detection

The Layered Network Intrusion Detection System (LNIDS) draws its motivation from the Airport Security model, where a number of security checks are performed one after the other in a sequence. Similar to this model, the LNIDS represents a sequential Layered Approach and is based on ensuring availability, confidentiality, and integrity of data and services over a network.

The goal of using a layered model is to reduce computational complexity and the overall time required to detect anomalous events. The time required to detect an intrusive event is significant and can be reduced by eliminating the communication overhead among different layers. This can be achieved by making the layers autonomous and self-sufficient to alert and block an attack without the need of a central decision-maker [14].

Fig. 1 gives a generic representation of the framework.

4.1 Layered Framework Model of the Proposed Network Intrusion Detection System

Fig. 2 represents a '3' layer structure where every layer in itself is a small intrusion detection module which is specifically trained to detect only a single class of attack, for instance the denial of service (DoS) attacks. In this paper, three layers are defined that corresponds to the three attack groups. They are R2L layer, DoS layer and U2R layer. A number of such sub-systems are then deployed sequentially, one after the other. This serves dual purpose; first, every layer can be trained with only a small number of features which are significant in detecting a particular class of attack. Second, the size of the sub-system remains small and hence, it performs efficiently.

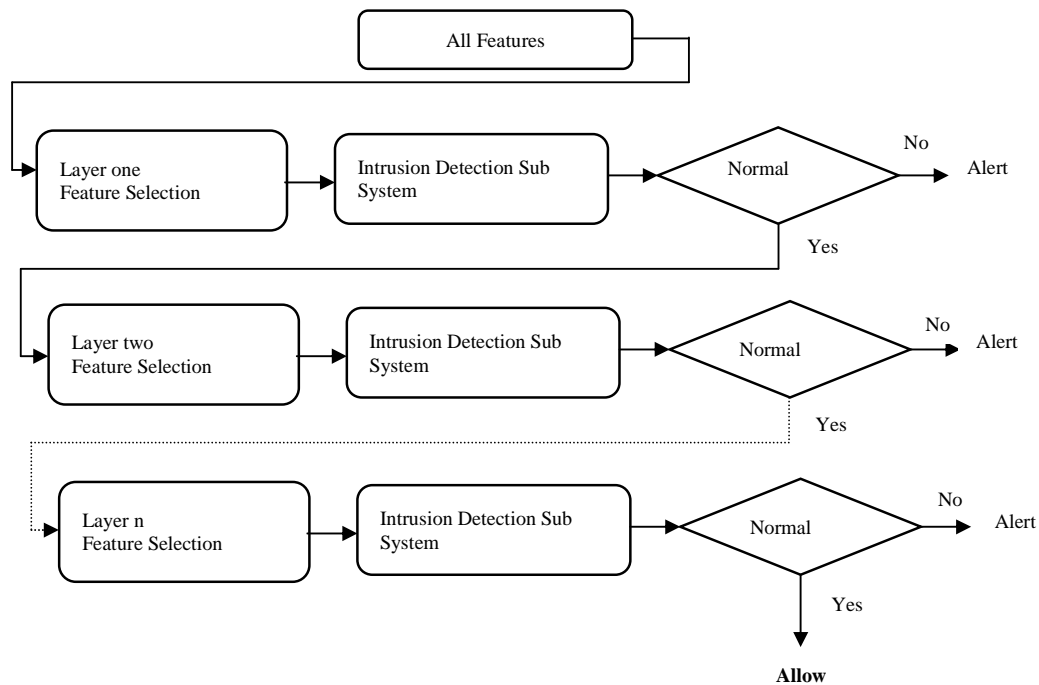


Fig. 1. Generic representation of layered network intrusion detection system

5 Conditional Random Fields for Intrusion Detection

Conditional models are probabilistic systems that are used to model the conditional distribution over a set of random variables. Such models have been extensively used in the natural language processing tasks. Conditional models offer a better framework as they do not make any unwarranted assumptions on the observations and can be used to model rich overlapping features among the visible observations [15].

Maxent classifiers [16,17], Maximum Entropy Markov Models [18,19,20], and CRFs [21,22] are such conditional models. The advantage of CRFs is that they are undirected and are thus, free from the Label Bias and the Observation Bias [15]. The simplest conditional classifier is the Maxent classifier based upon maximum entropy classification, which estimates the conditional distribution of every class given the observations [17]. The training data is used to constrain this conditional distribution while ensuring maximum entropy and hence maximum uniformity.

CRFs are undirected graphical models used for sequence tagging. The prime difference between CRF and other graphical models such as the HMM is that the HMM, being generative, models the joint distribution, whereas the CRF are discriminative models and directly model the conditional distribution, which is the distribution of interest for the task of classification and sequence labeling [21].

Similar to HMM, the naive Bayes is also generative and models the joint distribution. Modeling the joint distribution has two disadvantages. First, it is not the distribution of interest, since the observations are completely visible and the interest is in finding the conditional probability for the observations, which is the conditional distribution. Second, inferring the conditional probability from the modeled joint distribution, using the Bayes rule, requires the marginal distribution. To estimate this marginal distribution is difficult since the amount of training data is often limited and the observation x contains highly dependent features that are difficult to model and therefore strong independence assumptions are made among the features of an observation. This results in reduced accuracy [23]. CRFs, however, predict the label sequence y given the

observation sequence x . This allows them to model arbitrary relationship among different features in an observation x [22]. CRFs also avoid the observation bias and the label bias problems, which are present in other discriminative models, such as the maximum entropy Markov models. This is because the maximum entropy Markov models have a per-state exponential model for the conditional probabilities of the next state given the current state and the observation, whereas the CRFs have a single exponential model for the joint probability of the entire sequence of labels given the observation sequence [24].

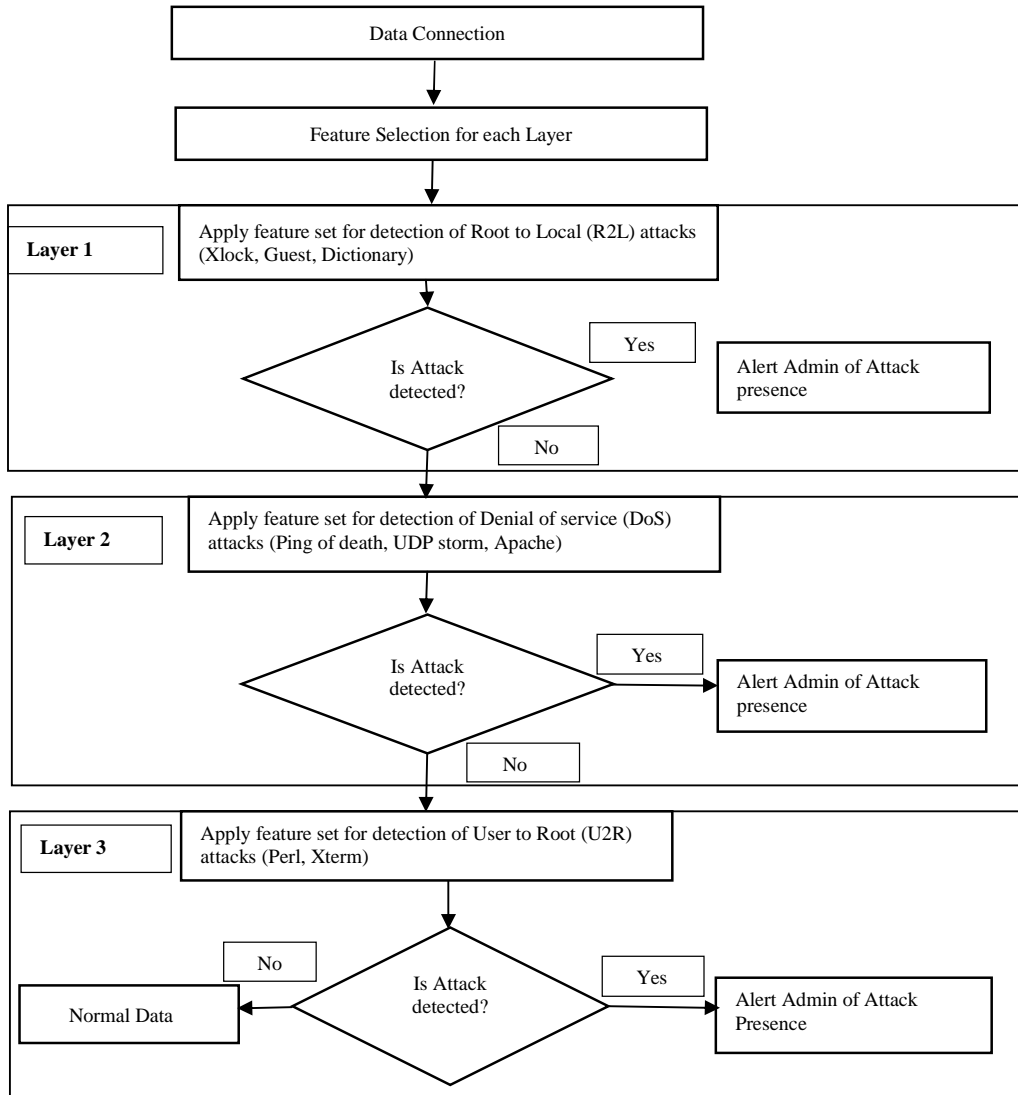


Fig. 2. Layered framework model of the proposed network intrusion detection system

The task of intrusion detection can be compared to many problems in machine learning, natural language processing, and bioinformatics. The CRFs have proven to be very successful in such tasks, as they do not make any unwarranted assumptions about the data. Hence, the CRFs are strong candidates for intrusion detection. See Fig. 3 for graphical representation of a Conditional Random Field.

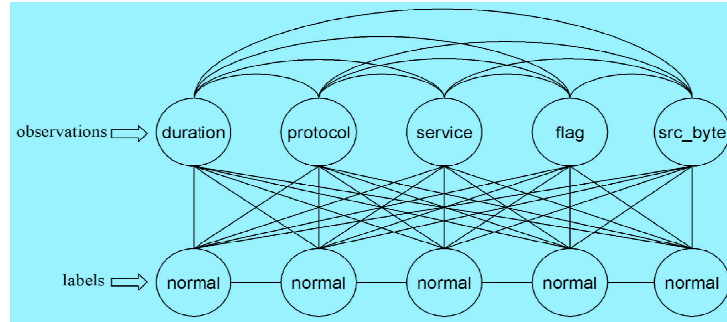


Fig. 3. Graphical representation of a conditional random field

Source: [21]

6 Information Dominance as a Stronger Notion of Security for IDS

In both theoretical and practical perspectives, one can model intrusion detection system (IDS) as a trusted entity surrounded by untrustworthy adversaries. The goal of the IDS is to detect any attempt to violate the boundaries of its domain and the target systems contained. This goal can only be accomplished as long as the IDS succeed in maintaining its integrity to the extent that it still has an operational advantage. That is, even if some information about the IDS is disclosed to a malicious adversary, it can still be possible to meet operational requirements [25]. To meet these requirements, we introduce in this study a new property described as **information dominance**. The meaning of information dominance for IDS is that information contained within an intrusion detection entity must be kept private to malicious adversary that is confidentiality requirement. In addition, the information must be protected from unauthorized alteration, fabrication and deletion that is integrity requirement as it may lower the operational advantage of the IDS [26]. The IDS must always maintain information dominance as compared with any external adversary. This allows the IDS to use its information system and capabilities to achieve an operational advantage while denying these capabilities to an intruder. In the field of information warfare, information dominance is an essential property [27]. We proposed that the property of information dominance for IDS should include confidentiality of audit data, confidentiality of detection policy; integrity of audit data and integrity of detection policy.

6.1 Confidentiality of Audit Data

Audit data generated by entities within a domain contains sensitive information not to be disclosed outside the members of the domain. Such information includes information about users or their activities as well as application related data conceivably containing classified information. In some cases, the mere existence of an event may be confidential as it reveals some form of activity. A principle of minimum knowledge transfer should be followed to avoid disclosure of confidential data. Consequently, raw audit data should never be distributed outside the boundaries of the domain.

6.2 Confidentiality of the Detection Policy

In security services, such as firewalls, the detection policy is distributed to a small number of entities. A distributed security service, like fully distributed IDS, requires the policy or parts of the policy to be known to all domains. Assuming an architecture where the number of domains is large, there is a non-negligible probability that the policy is disclosed to a malicious adversary who succeeds in penetrating one or more of the domains. Clearly, the clandestineness of the detection policy cannot rely upon the integrity of neighboring domains or even upon the integrity of its own domain. The detection policy should be protected against disclosure to malicious adversaries. It should not be possible to deduce the detection policy given the information gained by penetrating a domain or a node contained within a domain.

6.3 Integrity of Audit Data

The audit data are the basis for all analysis in search of intrusions. Hence, an intruder violating the integrity of the audit data can seriously affect the detecting capability. Even the most advanced IDS will fail to meet its operational requirements if the integrity of audit data has been violated. Therefore, the audit data should be protected against unauthorized alteration, deletion and insertion.

6.4 Integrity of the Detection Policy

The detection policy states which activities are considered as intrusions and which are not. Hence, manipulation of the detection policy can cause the IDS to fail to detect an intrusion. The detection policy should thus be protected against unauthorized alteration, deletion and insertion.

7 Methodology

In this study, the structured system analysis and design methodology (SSADM) was adopted. This methodology was employed to bring out detailed description of the system as well as providing avenue for easy modification of the system as the need may arise in future and produce effective and efficient system. SSADM is suitable for analyzing and designing large systems like the one proposed in this study as it gives out a clearer view and representation of the modules, procedures, and functions with their respective relationships, as such giving the designers a complete analysis for the development of efficient system that meet specifications as contained in the specification documents.

7.1 High Level Model of the Proposed Network Intrusion Detection System

Below is a block diagram representation of the high level model of the proposed network intrusion detection system:

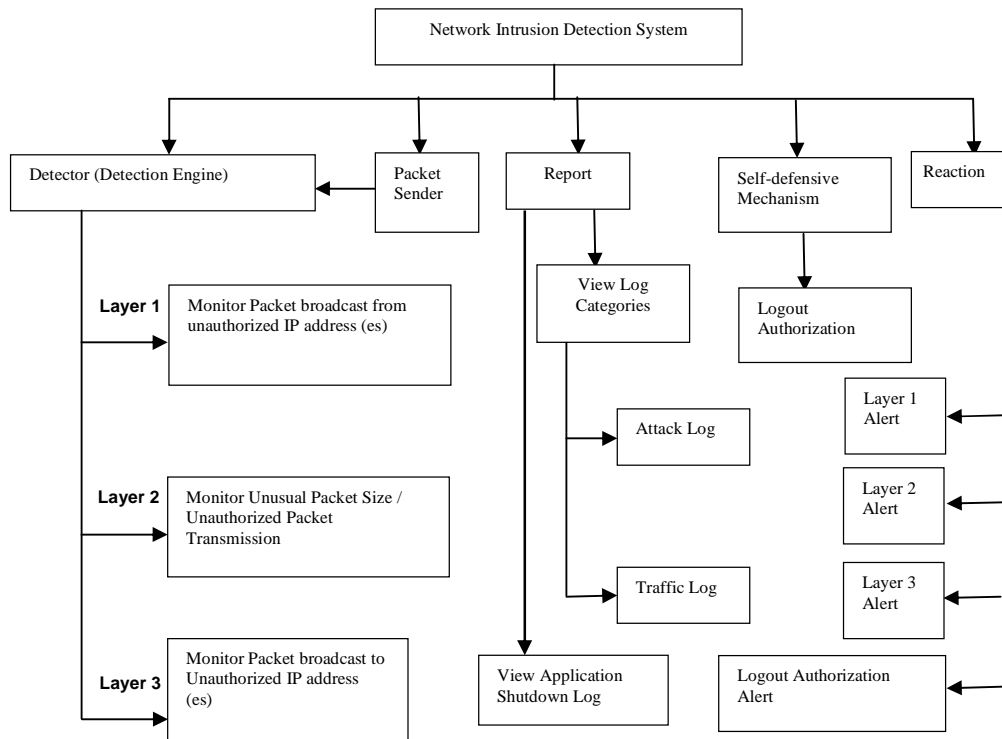


Fig. 4. High level model of the proposed network intrusion detection system

The detector is the analysis engine that used the IDS policies to analyze the network packets received from the packet sender. The detector represents a ‘3’ layer subsystem where each layer is a sub-module of the security mechanism that are specially skilled to identify only a particular class of intrusion, for instance, the denial of service attacks.

Packet sender is a component of the proposed system that is responsible for sending network packets to the detector for analysis. The report is a component of the system that represent the output of the detection process in the form of attack log and traffic log, which are stored as log files in the view categories component of the system. The self-defensive mechanism is the protection subsystem of the proposed network intrusion detection system (NIDS). The logout authorization component is used to implement the self-defensive mechanism of the proposed NIDS. The reaction component consists of the layer1 alert, layer2 alert, layer3 alert and the logout authorization alert.

7.2 Overall Data Flow Diagram of the Proposed Security System

The overall data flow diagram explains the flow of data in the system in detail. Here, all the key procedures of the system, their inputs and outputs are depicted. See Fig. 5 for the overall data flow diagram of the proposed security system.

7.3 Mathematical Specifications of the Proposed System

The basis of intrusion detection systems is the classification of events into normal and abnormal classes using mathematical representations. The classification criteria are probabilistic in nature and therefore the conditional random field model that is a conditional probability distribution model was adopted in this study.

Mathematical representation of the conditional random field model is as given below:

$$P(x_1, x_2, \dots, x_t) = \frac{1}{Z} (\vec{x}) * (\prod_{c \in c} \Psi_c(x_c)) \quad (1)$$

The conditional probability can be written as

$$P(\vec{y} / \vec{x}) = \frac{P(\vec{y}, \vec{x})}{P(\vec{x})}$$

Thus,

$$P(\vec{y} / \vec{x}) = \frac{1}{Z} (\vec{x}) * (\prod_{c \in c} \Psi_c(x_c)) * (y_c, x_c) \quad (2)$$

where:

$$Z(\vec{x}) = \sum \prod_{c \in c} \Psi_c(y_c, x_c)$$

x is the observation sequence (x_1, x_2, \dots, x_t)

y is the label sequence (y_1, y_2, \dots, y_t)

Ψ is the potential function.

$[\]$ is the feature weight

Summing over all possible label sequences ensures that it is a probability distribution.

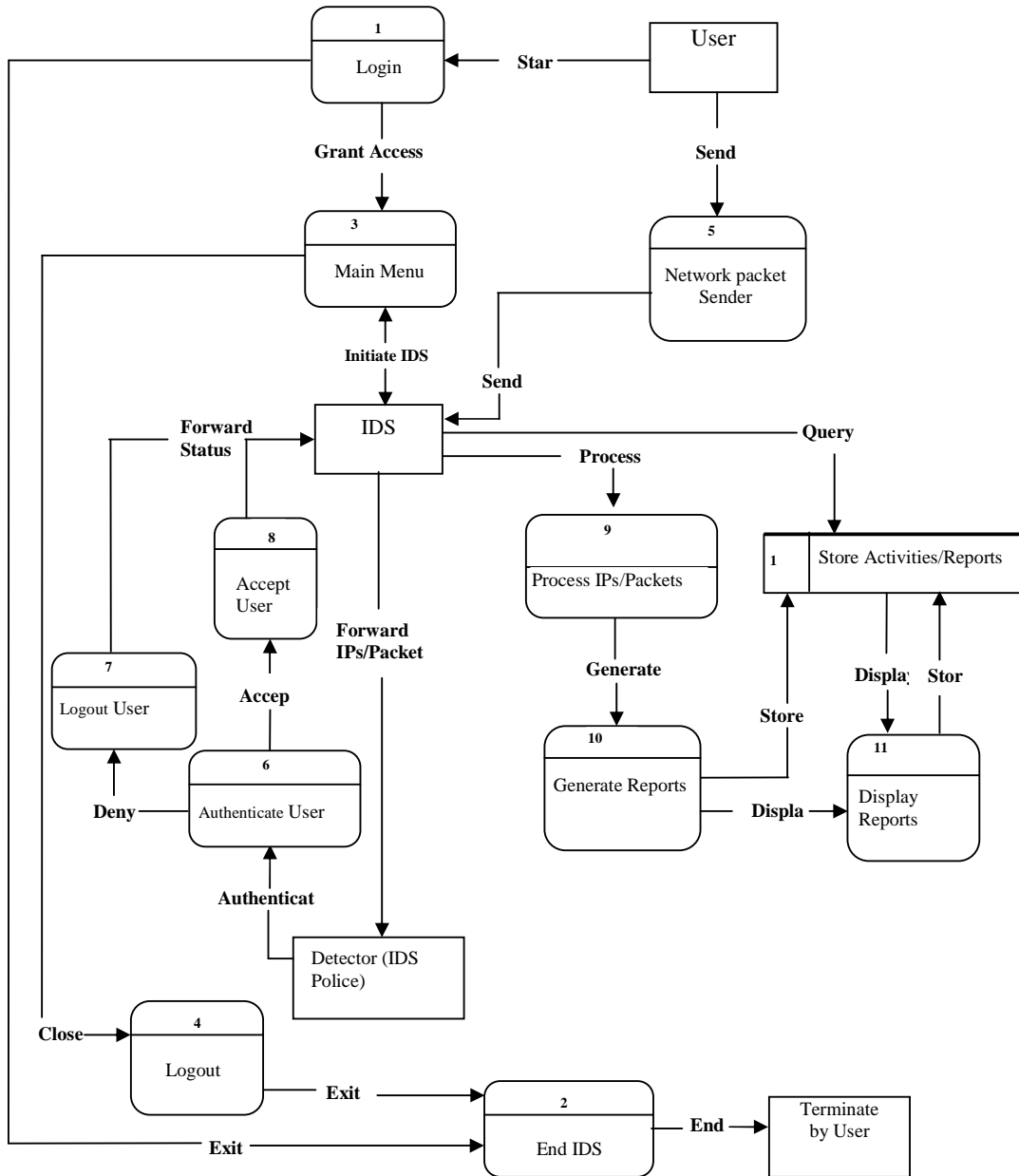


Fig. 5. Overall data flow diagram of the proposed security system

7.4 Algorithm for Self-defensive Mechanism of the Proposed Security System

- i. Start
- ii. Try to close or terminate the program using the quit application window
- iii. On form close event, display the logout authorization window
- iv. Enter username and password

- v. If username and password corresponds to the administrator’s username and password on the logout table then terminate the program and stop monitoring, else the program continues running and monitoring
- vi. Stop

7.5 Main Menu Design

The user interface design for the proposed system is as shown in Fig 6:

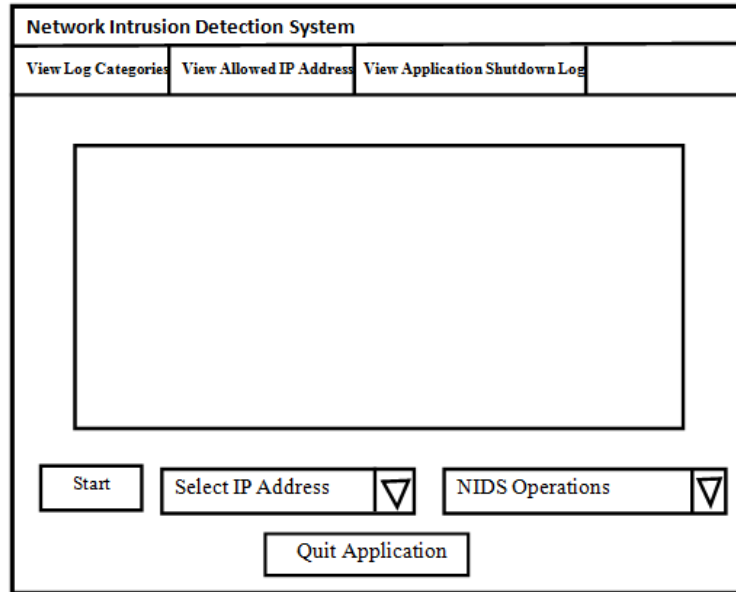
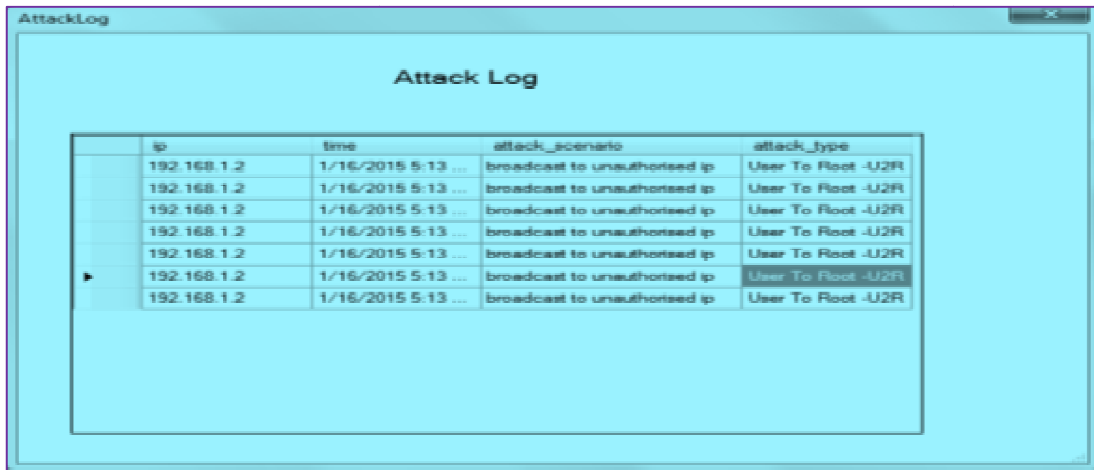


Fig. 6. User interface design of the proposed system

The user interface or main menu consists of the title of the application (Network Intrusion Detection System), View Log Categories, View Allowed IP Addresses, View Application Shutdown Log, Start/Stop, Select IP Addresses, NIDS Operations and the work space. The title of the application is Network Intrusion Detection System. The View Log Categories consist of the normal traffic log and attack log. All normal network traffics are stored on the traffic log and all attacks detected are stored on the attack log. The View Allowed IP is used to display the allowed internet protocol (IP) addresses in the network. The View Application Shutdown Log is used to display logout username, date and time of the logout attempt and successful or unsuccessful logout attempts. The start option is used to initiate the system. The Select IP Addresses option is used to select the required IP address or addresses. The NIDS operation option is used to choose NIDS operation to be performed at any point in time and to categorize the nature and type of network attacks, that is, there is an option to select the NIDS operation by simply clicking on the look down triangle in the NIDS operation windows. The operations include monitoring packet broadcast from unauthorized internet protocol (IP) addresses, monitoring unusual packet size, monitoring unauthorized packet transmission and monitoring packet broadcast to unauthorized IP addresses. The Quit Application module contains the Self-defensive mechanism and it is used to terminate or shutdown the system if the user is authorized to do so. The self-defensive mechanism, though not visible in the interface, but embedded in the Quit Application module protect the entire network intrusion detection system developed in this study from subverting to network attacks, that is making the security system resistant to network attacks. The self-defensive mechanism actually act as an attack resistant mechanism, that is, the proposed network intrusion detection system and its detection techniques are designed to resist attacks that target their own resources, providing assurance that the monitoring capability is not easily disabled.

8 Results and Discussion

- (i) The developed system is simple, scalable and flexible in operation, and does not only detect attacks but also identifies the type of attack, which enhances efficient analysis of future attacks and devoid of false alarm generation. Fig. 7 shows a screen display of the attack log for monitoring packet broadcast from unauthorized internet protocol address.



The screenshot shows a window titled "AttackLog" with a table of attack records. The table has four columns: ip, time, attack_scenario, and attack_type. The data is as follows:

ip	time	attack_scenario	attack_type
192.168.1.2	1/16/2015 5:13 ...	broadcast to unauthorized ip	User To Root -U2R
192.168.1.2	1/16/2015 5:13 ...	broadcast to unauthorized ip	User To Root -U2R
192.168.1.2	1/16/2015 5:13 ...	broadcast to unauthorized ip	User To Root -U2R
192.168.1.2	1/16/2015 5:13 ...	broadcast to unauthorized ip	User To Root -U2R
192.168.1.2	1/16/2015 5:13 ...	broadcast to unauthorized ip	User To Root -U2R
192.168.1.2	1/16/2015 5:13 ...	broadcast to unauthorized ip	User To Root -U2R

Fig. 7. Attack log for monitoring packet broadcast from unauthorized IP address

- (ii) The developed system is able to operate in real-time (function instantaneously) by promptly launching reaction mechanism once an intrusion is identified and this helps to minimize the effect of attack on the network. Fig. 8 depicts a screen shot of alert for monitoring unusual or excess packet size.

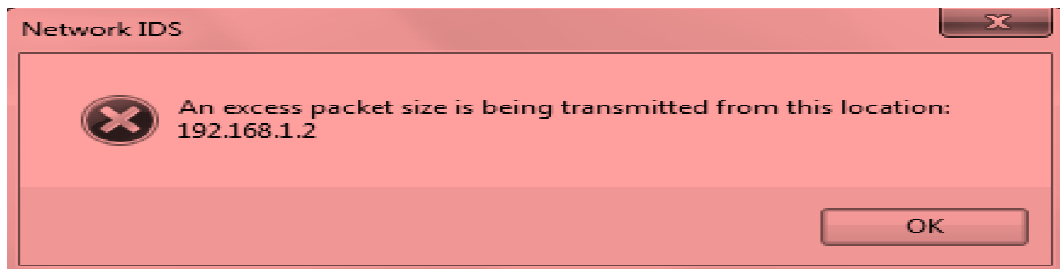


Fig. 8. Alert for monitoring unusual packet size

- (iii) The inclusion of self-defensive mechanism using logout authorization in the developed system is the major significant feature of this study since existing intrusion detection systems lack such mechanism, that is, the developed system has a self-defensive mechanism which is resistant to any attack, as other security systems that can be exploited during an attack are unable to detect attacks efficiently and reliably. See Fig. 9 for a screen shot of the logout authorization module, Fig. 10 for a screen shot of alert for unauthorized shutdown and Fig. 11 for a screen shot of shutdown log demonstrating functionality of the self-defensive mechanism of the developed system.

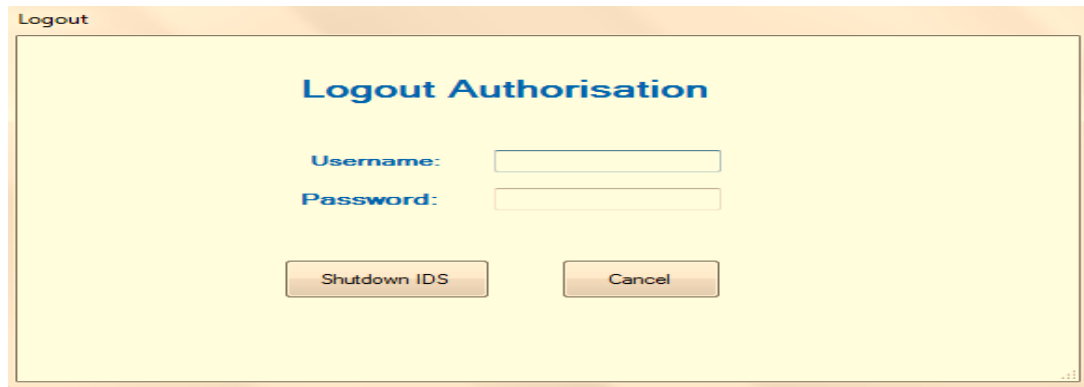


Fig. 9. Screen shot of the logout authorization

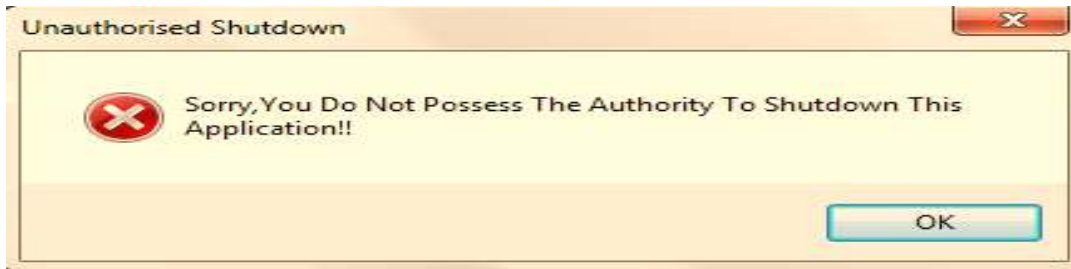


Fig. 10. Screen shot of alert for unauthorized shutdown

Username	Logout Time	Authorised Shutdown Attempt?
David	1/16/2015 5:17 ...	No
Umoh	1/16/2015 5:17 ...	No
Emeka	1/16/2015 5:17 ...	No
ele	1/16/2015 5:18 ...	Yes
Umoh	1/16/2015 2:28 ...	No
David	1/16/2015 2:28 ...	No
Eneje	1/16/2015 2:28 ...	No
Agona	1/16/2015 2:28 ...	No
Emeka	1/16/2015 2:29 ...	No
ele	1/16/2015 2:29 ...	Yes

Fig. 11. Shutdown log demonstrating the functionality of the self-defensive mechanism of the developed system

9 Conclusion

This study focused on the development of a model of a pragmatic secure intrusion detection system (IDS) for local area networks. In this study, the suitability of conditional random fields and layered framework for building secure, robust and efficient model of intrusion detection system for local area networks was examined. In particular, a pragmatic secure intrusion detection model for local area networks was developed and implemented which addresses the critical problems identified in section 2 that severely affect the large scale deployment of present intrusion detection systems in local area networks.

The study observed that layered framework can be used to build efficient and secure intrusion detection systems. In addition, the framework offers ease of scalability for detecting different variety of attacks as well as ease of customization by incorporating domain specific knowledge. The framework also identifies the type of attack, hence, specific intrusion response mechanism can be initiated which helps to minimize the impact of the attack.

The study also observed that conditional random fields are strong candidates for building secure and efficient network intrusion detection systems. Integrating the layered framework with the conditional random fields can be used to build secure, effective and efficient network intrusion detection systems. Using conditional random fields as intrusion detectors result in a moderate false alarms and thus, the attacks can be detected with very high level of accuracy.

Finally, the developed system has the advantage that the number of layers can be increased or decreased depending upon the environment in which the system is deployed and can also defend itself against attacks, giving flexibility and confidence to the network administrators and security professionals. This work is open for further research and/or implementation for other network system(s).

Competing Interests

Authors have declared that no competing interests exist.

References

- [1] George S, James XD, Alan G, Barbara JM, Schwartz A. Information technology security handbook. Global Information and Communication Technologies Department. Washington DC – USA; 2003.
- [2] Ang C, Stolfo SJ. A Quantitative analysis of the insecurity of embedded network devices: Results of a wide area scan. M.Sc. Thesis, Department of Computer Science, Columbia University; 2013.
- [3] Avizienis A, Laprie JC, Randell B, Landwehr C. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable Secure Computing*. 2004;1(1):11-33.
- [4] Kim DS, Park JS. Network-based intrusion detection with support vector machines. Proceedings of information networking, networking technologies for enhanced internet services. International Conference on Information Networking (ICOIN '03). 2003;747-756.
- [5] Stallings W. Network security essentials: Applications and standards (Second edition ed.). (Pearson Education, Ed.) Upper Saddle River, New Jersey: Prentice Hall; 2003.
- [6] Onarlioglu K, Buyukkayhan AS, Robertson W, Kirde E. Sentinel: Securing legacy Firefox extensions. *Computers and Security*. 2015;49:(0).
- [7] Coretez G. Stick: A potential denial of service against IDS systems; 2007. Retrieved 12/04/2011 Available:<http://xforce.iss.net/xforce/alerts/id/advise74>
- [8] Debar H, Dacier M, Wespi A. Towards a taxonomy of intrusion-detection systems. IBM Research Division, Zurich Research Laboratory; 1998.
- [9] Polakis I, Maggi F, Zanero S, Keromytis AD. Security and privacy measurements on social networks: experiences and lessons learned. In Proceedings of the 3rd International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, BADGERS' 14, Wroclaw, Poland, September; 2014.

- [10] Frank Y, Fengmin G, Chandru S, Wu SF, Rance CW. Architecture design of a scalable intrusion detection system for the emerging network infrastructure. Technical Report CDRL A005, Department of Computer Science, North Carolina State University, Raleigh, USA; 1997.
- [11] Massey AK, Breux TD. Introduction to IT privacy: A handbook for technologists. In International Association of Privacy Professionals; 2014.
- [12] Neumann PG. Architectures and formal representations for secure systems. Final Report; SRI Project 6401; Deliverable A002; 1995.
- [13] Shamir A, Nico VS. Playing hide and seek with stored keys. Weizmann Institute of Science, Israel; and Cipher Corporation Limited, England; 1998.
- [14] Boggs N, Stolfo SJ. ALDR: A new metric for measuring effective layering of defenses. Layered Assurance Workshop; 2011.
- [15] Guleri D, Chavan MK. A study and comparative analysis of conditional random fields for intrusion detection. *International Journal of Research in Computer Science*. White Globe Publications, Baramati. 2012;2(4):31-38.
- [16] Ratnaparkhi A. A maximum entropy model for part-of-speech tagging, proceedings conference on empirical methods in natural language processing (EMNLP '96). Association for Computational Linguistics. 1996;133-142.
- [17] Harremoës P, Topsøe F. Maximum entropy fundamentals. *Entropy*. 2001;3(3):191-226.
- [18] McCallum A, Freitag D, Pereira F. Maximum Entropy markov models for information extraction and segmentation. Proceedings of 17th International Conference on Machine Learning (ICML '00). 2000; 591-598.
- [19] Tang A, Beggs JM. A Maximum entropy model applied to spatial and temporal correlations from cortical networks *in vitro*. *Journal of Neuroscience*. 2008;28(2):505–518.
- [20] Biondi F, Legay A, Nielsen B, Wasowki A. Maximizing entropy over Markov processes. In Proceedings of the 7th International Conference on Language and Automata Theory and Applications, April 2013, Bilbao, Spain. 2013;128–140.
- [21] Lafferty J, McCallum A, Pereira F. Conditional random fields: Probabilistic models for segmenting and labeling sequence data. Proceedings of 18th International Conference on Machine Learning (ICML '01). 2001;282-289.
- [22] Fersini E, Messina E. Named entities in judicial transcriptions: Extended conditional random fields. Proceedings of the 14th international conference on Computational Linguistics and Intelligent Text Processing, Springer-Verlag, Berlin, Heidelberg. 2013;317–328.
- [23] Jain R, Abouzakhar NS. Hidden markov model based anomaly intrusion detection. The 7th International Conference for Internet Technology and Secured Transactions. 2012;528-533.
- [24] Sutton C, McCallum A. An introduction to conditional random fields for relational learning. *Introduction to Statistical Relational Learning*; 2006.
- [25] Srivastava A, Kundu A, Sural S, Majumdar AK. Credit card fraud detection using hidden markov model. *IEEE Transactions on Dependable and Secure Computing*. 2008;5(1):37-47.

- [26] Antonini A, Maggi F, Zanero S. A Practical attack against a KNX-based building automation system. In Proceedings of the 2nd International Symposium for ICS & SCADA Cyber Security Research, St. Polten, Austria, September; 2014.
- [27] Bruce DC. Proactive Self-defense in cyberspace. The Institute of Land Warfare: The Association of the United States Army; 2009.

© 2016 Ele et al.; This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Peer-review history:

The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)

<http://sciencedomain.org/review-history/12517>