



A Bayesian Network Model for a Zimbabwean Cybersecurity System

GABRIEL KABANDA

Atlantic International University 900 Fort Street Mall 40 Honolulu, Hawaii 96813, USA.

Abstract

The purpose of this research was to develop a structure for a network intrusion detection and prevention system based on the Bayesian Network for use in Cybersecurity. The phenomenal growth in the use of internet-based technologies has resulted in complexities in cybersecurity subjecting organizations to cyberattacks. What is required is a network intrusion detection and prevention system based on the Bayesian Network structure for use in Cybersecurity. Bayesian Networks (BNs) are defined as graphical probabilistic models for multivariate analysis and are directed acyclic graphs that have an associated probability distribution function. The research determined the cybersecurity framework appropriate for a developing nation; evaluated network detection and prevention systems that use Artificial Intelligence paradigms such as finite automata, neural networks, genetic algorithms, fuzzy logic, support-vector machines or diverse data-mining-based approaches; analysed Bayesian Networks that can be represented as graphical models and are directional to represent cause-effect relationships; and developed a Bayesian Network model that can handle complexity in cybersecurity. The theoretical framework on Bayesian Networks was largely informed by the NIST Cybersecurity Framework, General deterrence theory, Game theory, Complexity theory and data mining techniques. The Pragmatism paradigm used in this research, as a philosophy is intricately related to the Mixed Method Research (MMR). A mixed method approach was used in this research, which is largely quantitative with the research design being a survey and an experiment, but supported by qualitative approaches where Focus Group discussions were held. The performance of Support Vector Machines, Artificial Neural Network, K-Nearest Neighbour, Naive-Bayes and Decision Tree Algorithms was discussed. Alternative improved solutions discussed include the use of machine learning algorithms specifically Artificial Neural Networks (ANN), Decision Tree C4.5, Random Forests and Support Vector Machines (SVM).



Article History

Received: 26 November 2019

Accepted: 3 January 2020


Keywords

Autonomous Robotic Vehicle;
Artificial Neural Networks;
Bayesian Network;
Cybersecurity;
Decision Tree C4.5;
Fuzzy Logic;
Machine Learning Methods;
Random Forests And
Support Vector Machines (Svm).

CONTACT Gabriel Kabanda ✉ gabrielkabanda@gmail.com 📍 Atlantic International University 900 Fort Street Mall 40 Honolulu, Hawaii 96813, USA.



© 2019 The Author(s). Published by Oriental Scientific Publishing Company

This is an  Open Access article licensed under a Creative Commons license: Attribution 4.0 International (CC-BY).

Doi: <http://dx.doi.org/10.13005/ojcs12.04.02>

Introduction

Background

The monotonic increase in the use of the internet has precipitated the advent of Network Intrusion Detection Systems (NIDS). The NIDS draw a distinction between the legitimate network users from malicious ones, and monitor system usage to identify behaviour breaking the security policy (Bringas, P.B., and Santos, I., 2010, p.229). Bayesian Networks (BNs) are directed acyclic graphs that have an associated probability distribution function and these graphical probabilistic models are used for multivariate analysis (Bringas, P.B., and Santos, I., 2010, p.231).

$$P(x) = \prod_{i=1}^n p(x_i | \Psi_i) \quad \dots(1)$$

There are many intrusion identification methods and these include a semi-supervised fuzzy clustering algorithm based on isomeric distance and sample density for network intrusion detection (Kylili *et al.*, 2018), but this method is constrained by the data sample dimension, and it is difficult to effectively deal with the problem of large scale network intrusion signal recognition. Based on deep research of hidden Markov model intrusion detection method, combined with the characteristics of global optimization of genetic algorithm, Wu (2018) used the genetic algorithm to optimize the model for the sensitive problem of hidden Markov model to initial parameters, and proposed an identification method based on hidden Markov model for ship communication network intrusion signal.

Statement of the Problem

The phenomenal growth in the use of internet-based technologies has resulted in various organizations being subjected to cyberattacks. The classical security measures, such as a firewall, have proved to be inadequate, as hackers deliberately avoid firewall protection. It is, therefore, of primordial importance to find effective solutions that can dynamically and adaptively defend the network systems. What is required is a network intrusion detection and prevention system based on the Bayesian Network structure for use in Cybersecurity.

Purpose of Study

The purpose of this research is to develop a structure for a network intrusion detection and prevention

system based on the Bayesian Network for use in Cybersecurity. There is need to find effective solutions that can dynamically and adaptively defend the network systems, and so Bayesian networks allow for prediction, generalization, and planning.

Research Objectives

The objectives of this research were to

- Determine the cybersecurity framework appropriate for a developing nation like Zimbabwe.
- Evaluate network detection and prevention systems that use Artificial Intelligence paradigms.
- Analyse Bayesian Networks that can be represented as graphical models and are directional to represent cause-effect relationships
- Develop a Bayesian Network model that can handle complexity in cybersecurity.

Research Questions

The main research question is

What Bayesian Network model is most appropriate for a network detection and prevention cybersecurity system?

The sub research questions were

- What is the most appropriate cybersecurity framework for a developing nation?
- How are Artificial Intelligence paradigms used in network detection and prevention systems?
- How can Bayesian Networks be represented as graphical models that also represent cause-effect relationships?
- How do you develop a Bayesian Network model that can handle complexity in cybersecurity?

Review of the Literature

Conceptual Framework

According to Wu (2018, p.2), there are two main advantages to the preprocessing of the network signal by the principal component analysis (PCA) method:

- PCA can reduce the dimension of the network signal collected on the receiving device, that is, extract the fluctuation signal related to the network activity, reduce the amount

of calculation and improve the recognition accuracy.

- As the background noise of the network environment is random and irregular, PCA can use the relative change rate to eliminate the noise in the background environment.

Wu (2018) proposed a hidden Markov model-based intrusion signal recognition method for ship communication network for the problem of low recognition accuracy and initial parameter sensitivity in the current network intrusion recognition method, where the principal component analysis method was used to denoise and classify the network continuous signals by selecting appropriate k value. In the

process of building and training hidden Markov model, an improved genetic algorithm was used to optimize the initial parameters of the hidden Markov model. Karimpour *et al.*, (2016, p.2) categorized the intrusion detection approaches into four parts as follows

- Feature-based approaches
- Decomposition-based approaches
- Community-based approaches
- Window-based approaches

The training phase of the tracking approach is shown on Figure 1 below.

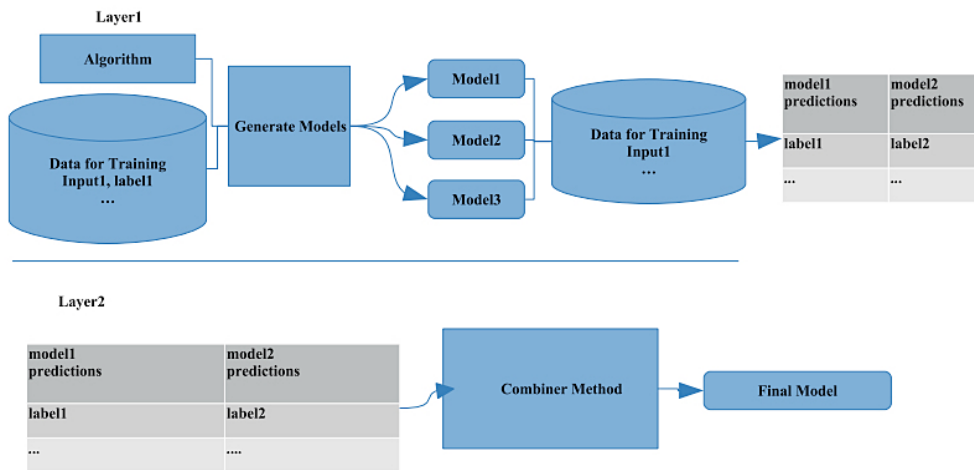


Fig.1: Training phase of tracking approach (Source: Demir, N., and Dalkilic, G., 2017, p.4)

The conceptual framework of the research is premised on the National Institute of Standards and Technology (NIST) framework. The NIST Cybersecurity Framework seeks to provide organizations with a common way to:

- describe their current (as-is) cybersecurity state or posture.
- describe their desired cybersecurity state.
- identify and prioritize opportunities for improvement within the context of a continuous and repeatable process.
- make progress assessment towards a desired cybersecurity state.
- make internal or external communication to stakeholders about cybersecurity risk.

The cybersecurity challenges that are being faced in developing countries include the following.

- Infrastructure (International Telecommunications Union, 2009).
- Legal frameworks (Norwegian Institute of International Affairs, 2018).
- Harmonization of legislation (Bande, 2018).
- Balancing harmonization and country specific needs (ITU, 2012).
- Systems (Schia, 2018).
- Education and awareness (Tagert, 2010), (Schia, 2018).
- Cybersecurity knowledge (The United Nations

- Economic Commission for Africa Policy Brief, 2014).
- Affordability and funding (Muller, P. L, 2015)
- Perceived low susceptibility to attacks (Tagert, 2010).
- Lack of adequate frameworks that speak to their cybersecurity needs (Tagert, 2010).

- Reporting cybercrime (The Republic of Mauritius Cybercrime strategy 2017-2019, 2017).
- Data sharing.

The research work is further founded on the General deterrence theory (GDT), illustrated by the elements shown on the diagram shown on Figure 2 below.

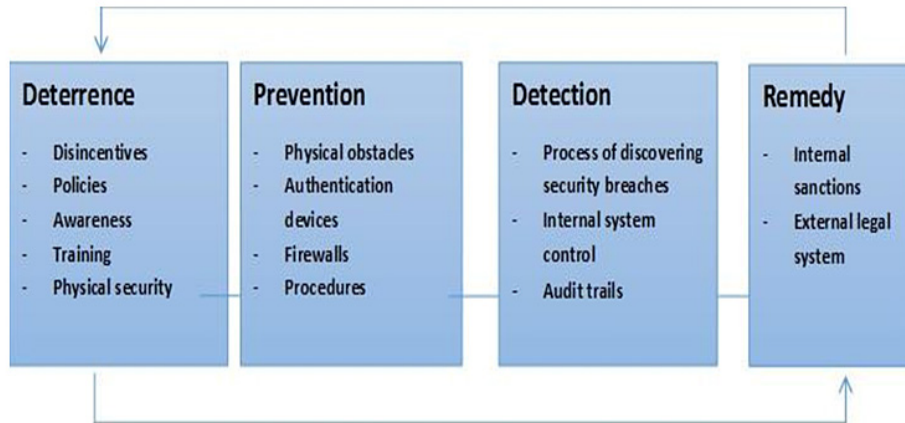


Fig. 2: Elements of the General Deterrence Theory (GDT). Source: Alanezi *et al.*, (2014)

The Game Theory approach describes the interaction process among the attacker and the protecting agent in order to balance and strategize the prediction of the behaviour of the attacker in the search to find an equilibrium point for optimal results. Game theory amply illustrates multi-person decision scenarios as games where each player gets the best possible rewards for self by making appropriate choices of actions, while expecting the logical actions from the other opponents. According to Chukwudi *et al.*, (2017), a game is a narrative or an account of the strategic reciprocal actions between opponents including payoffs of and constraints for actions that players can undertake but doesn't specify the exact actions taken. A player is the primary entity of a game responsible for making decisions and then taking action and can represent a machine, a person, or a group of persons within a game (Chukwudi *et al.*, 2017). In the field of cybersecurity, game theory will take into account the wrangle between the cyber attackers and the cyber victims where their decision strategies are closely related. An important element in this theory is the capacity to analyze the possible large number of cyber threat scenarios in a cyber system (Hamilton, 2002).

Chaos theory is a specialised application of dynamical systems theory with a focus on the qualitative study of unstable, aperiodic behaviour in deterministic, non-linear, dynamical systems (Kabanda, G., 2013). In seeking to understand the behaviour of a complex system, Chaos theory reconstructs its attractor to obtain qualitative understanding. Chaos theory asserts relationships of qualitative (or topological) similarity between the abstract models and the actual systems under study. Its great value is in varying and analyzing models of natural systems for the purposes of adaptability and comparison (Kabanda, G., 2013). Chaos is a sub-discipline of complexity. There are three aspects of Chaos that relate to fractal patterns, bounded infinity, and unpredictability (Smitherman, S., 2014, p.6).

Data mining or knowledge discovery in databases (KDD), is the automated process of extraction of patterns of knowledge implicitly stored in large databases, data warehouses, and other massive information repositories. According to Madigan, D. (2008, p.3), data mining is purposed to find interesting patterns, predictive models, and hidden relationship in data. In this way, the extraction of

interesting (non-trivial, implicit, previously unknown and potentially useful) patterns or knowledge from huge amount of data (interesting patterns) is realised. Some of the common tasks in data mining include predictive modeling, segmentation, summarization and visualisation. Neural network methods have had a great impact on pattern recognition by proving a taxonomy of models with large but not unlimited flexibility of a large number of parameters. Multi-layer perceptrons and radial basis functions (RBFs) are the two most widely used neural network architectures.

Cryptography protects information by encrypting it into an unreadable format, called cipher text. The message can only be deciphered into plain text by the recipient who possess a secret key. Cryptographic algorithms can be classified in various ways, depending on the number of keys that are employed for encryption and decryption (Kessler, 2019, <https://www.garykessler.net/library/crypto.html>). The importance of cryptography in computer technology is centered on three areas, which are Authentication, Integrity and Confidentiality. Applications of Cryptography include the following.

- Cryptography Is Applied In Many Areas Of Computer Technology, Especially Wherever Information Needs To Be Kept Confidential.
- Modern Cryptography Is Used By Governments, Military, Financial Institutions, Medical Institutions, Space Agencies, Portable Smart Devices, Social Media Platforms And Several Other Sectors Of Business And Society. The Latest Common Use Of Cryptography Is The Creation Of Virtual Money, Called Crypto-Currency. Crypto-Currency Is Not Governed By The Normal Banking Systems Of The World. It Is Traded By Anyone, Unfortunately That Also Includes Money Launderers, Terrorist Financiers Because Normal Systems Cannot Trace The Funds' Movements. The Levels Of Encryption Are Very High To Keep This Money Secure On The Various Platforms. The Types Of Crypto-Currency That Exist So Far Are Bitcoin, Eos, Cardano (Ada), Neo, Monero (Xmr), Dash, Zcash (Zec), Ripple (Xrp), Ether And Litecoin (Ltc).
- Other Applications For Cryptography Are Protecting Stored Files, Full Disk Encryption

Which Is Additional Protection To The Operating System And Not Just The Stored Files, Device Locking Encryption That Is Built To Activate Each Time The Device Is Locked, Virtual Private Networks (Vpn) As A Way Of Creating An Encrypted Connection Between A Remote User And A Site, Secure Web Browsing Used When Users Visit Sites That Facilitate Financial Transactions Or Communication That Must Be Confidential, Secure Messaging, And Protecting Confidentiality In Cloud Or Third-Party Computing.

In Machine Learning (ML), the primary focus is the development of computer programs that can access data and use it learn to for themselves (<https://www.expertsystem.com/machine-learning-definition/>). Large amounts of data are required in ML for the analysis by computers to learn. It takes time resources to achieve effective machine learning. Organisations or individual users aim to improve how they work and experience life. Having computer systems that can take over some tasks that cannot be programmed in faster and more accurate ways than a human being, helps to achieve these desired improvements. The benefits of using AI and machine learning in cybersecurity include automated protection, faster response and protection, personalization, learning to adapt to the situation unobtrusively, usability. Applications of Machine Learning include the following.

- Virtual Personal Assistants, e.g. Siri, Alexa, Google, etc.
- Predictions while Commuting, as in Traffic Predictions and Online Transportation Networks which assist commuters to travel faster in the most cost effective way possible.
- Videos Surveillance where AI learns to understand and predict human behaviour through body movement.
- Social Media Services which help users to connect online with People they may know by learning profiles on platforms such as Facebook.
- Email Spam and Malware Filtering which filter possible spam through learning a user's email patterns and common recipients.
- Customer Support Services that respond to basic customer queries.
- Search Engine Result Refining.

- Product Recommendations for the users browsing patterns on shopping websites to predict and recommend the desired products.
- Online Fraud Detection to determine genuine and potentially fraudulent online transactions.

a structure with a high posterior probability on a given dataset.

The instance-specific Greedy Equivalence Search (IGES) method by Jabbari, F., *et al.*, (2018, p.179) had limitations but can be improved and extended through the following ways

Modern Literature (2018-2019)

Bayesian Networks can be considered as causal models and learned from observational data, which has wide applicability in different areas of life (Jabbari, F., *et al.*, 2018, p.169). Jabbari, F., *et al.*, (2018, p.169) viewed a given person as a joint set of causal mechanisms, where each mechanism is typically shared with many other people, but the joint set is essentially unique to that person. For that given person, the causal learning task is to construct the correct set of mechanisms for that person from the features we know about the person and from a training set of data on many other people. This instance-specific causal learning approach is applicable to other causal systems, even beyond human biology. A Bayesian Network (BN) as a graphical model represents probabilistic relationships among a set of variables (Jabbari, F., *et al.*, 2018, p.171). It follows that the Greedy Equivalence Search (GES) is a state-of-the-art method for learning a BN structure from observational data. According to Jabbari, F., *et al.*, (2018, p.171), GES algorithm consists of a forward equivalence search (FES) and backward equivalence search (BES). Each forward and backward step in GES involves scoring a single node given its parents; therefore, it requires a node-wise decomposable score. The development of a Bayesian approach for learning a BN structure amounts to search for

- understand better the reason for the relatively lower recall of the instance-specific BN models and try to increase it while retaining precision;
- b) extend the IGES algorithm to iteratively learn an instance-specific model for each instance in the training set and use an aggregate of those models to define the population-wide model;
- attempt to prove that IGES is guaranteed to find the data-generating instance-specific causal model for a test instance in the large sample limit;
- develop an instance specific score to learn BN structures that contain other types of variables (e.g., continuous or a mixture of continuous and discrete variables);
- develop more informative structure and parameter prior probabilities;
- extend the experimental evaluations.

However, the work by Jabbari, F., *et al.*, (2018) provides support that the proposed IGES method is a promising approach to discover a BN structure that better models the relationships among variables of a given instance T, rather than a population wide model. Figure 3 below shows the Probabilistic graphical models.

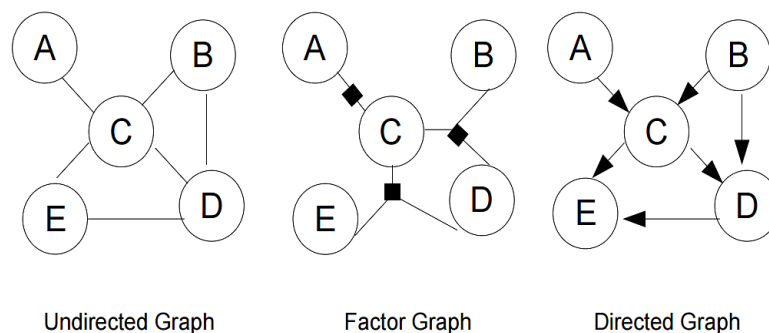


Fig. 3: Probabilistic Graphical Models

The open society of the internet presents unprecedented risks of cyber-attacks on computer systems and data. The process of intrusion detection often includes data collection, data pre-processing, intrusion recognition, and reporting and response (Xiao, L., 2016, p.1). Effective and efficient intrusion detection systems are needed to promptly detect and prevent intrusion to fight against extraordinarily intelligent cyber-attacks. Xiao (2016, p.1) categorised the intrusion detection systems into signature-based intrusion detection, anomaly based intrusion detection, and hybrid intrusion detection.

According to Liao *et al.*, cited in Xiao, L. (2016, p.10), there are three main challenges in current intrusion detection researches.

- Lower the false negative rate is one focus for signature-based intrusion detections, especially for some zero-day attacks. Furthermore, lower the false positive rate is a focus for anomaly-based intrusion detection.
- Collect training data set to build intrusion detection system. An intrusion may cause changes in some network traffic features. A problem of great interest in the training of intrusion detection systems is how to select key and effective features from a huge set of possible related features.
- Enable intrusion detection systems to respond promptly and be real time.

Methodology

Presentation of the Methodology

Research Philosophy

According to Lather (1986) as cited by Kivunja and Kuyini (2017) a research paradigm gives a reflection of the researcher's opinions. According to Lincoln and Guba (1985) as cited by Kivunja and Kuyini (2017) a paradigm has four parts which are explained below.

Epistemology of a paradigm

The word epistemology is a Greek word which means knowledge (Kivunja and Kuyini, 2017) and is concerned with the theory of knowledge (Walliman, N., 2011).

Ontology of a Paradigm

According to Scotland (2012) as cited by Kivunja and Kuyini (2017), ontology is a division of philosophy that deals with the assumptions made in believing that something is real or makes sense.

Methodology of a Paradigm

According to Keeves (1997) as cited by Kivunja and Kuyini (2017), methodology is an umbrella term used to cover research methods, research design and procedures used in a planned investigation to find out something.

Axiology of a Paradigm

Axiology handles the ethical issues taken into consideration when conducting research (Kivunja and Kuyini, 2017). Ethical considerations focus on four key concepts that have to be respected when dealing with data and participants. According to Slote (1985) cited in Kivunja and Kuyini (2017), these are Privacy, Accuracy, Property and Accessibility and the acronym that denotes them is PAPA.

Positivist Paradigm

Kivunja and Kuyini (2017) state that the positivists believe that truth is out there and can be revealed through research and the role of the researcher is to find it and explain it. They also believe that theory is universal and can be applied in all settings or contexts. The positivist paradigm defines a worldview called the scientific method (Shah, S.R., and Al-Bargi, A., 2013) of investigation which is anchored on an experimental methodology.

Interpretivist/Constructivist Paradigm

Lincoln and Guba (1985) and Morgan (2007) cited in Kivunja and Kuyini (2017), presented this paradigm as one where in the world numerous realities are in existence and reality is too complex to control every variable. In this regard context is extremely important for knowledge and understanding.

Critical /Transformative Paradigm

This paradigm follows a worldview that centres its research in issues of social injustice (Shah S.R., and Al-Bargi, A., 2013) and aims at addressing political, economic and social issues which lead to

oppression, conflict and struggle. It strives to change politics in order to address inequality and injustice hence the name transformative (Kivunja and Kuyini, 2017). According to Guba and Lincoln (1988) and Martens (2015) cited in (Kivunja and Kuyini, 2017).

Pragmatic Paradigm

Philosophers inclined to the pragmatic paradigm subscribe to the worldview that says it is impossible to access the truth of the real world by employing a single scientific method as supported by the Positivist paradigm or construct social reality under Interpretivist paradigm. According to Cresswell (2003) and Martens (2015) cited in Kivunja and Kuyini (2017) this world view puts it clearly that research must be feasible and the researcher should use what works given the research problem without worrying about whether the questions are exclusively quantitative or qualitative. The best approaches to the acquisition of knowledge and every methodology that helps knowledge discovery should be used as guided by the purpose of the study. In this research, an Interpretivist or Constructivist paradigm was used.

Interpretivist Paradigm/Constructivist Paradigm

According to Guba and Lincoln (1989) as cited by Kivunja, C., and Kuyini, A.B. (2017, p.26), this paradigm is purposed to understand the viewpoint of the subject under study so as to interpret what the subject is thinking or the meaning that s/he is making of the situation or setting. It is based on the idea that reality is socially constructed and there is no single reality or truth hence the name constructivist paradigm. There is also need to understand the individuals than just to follow laws that are generic and for that reason theory does not come before research but follows it based on data generated from the research.

The Pragmatism Paradigm

The Pragmatism paradigm used in this research, as a philosophy is intricately related to the Mixed Method Research (MMR). The paradigm comprises four elements, namely, epistemology, ontology, methodology and axiology. The Pragmatic paradigm advocates a relational epistemology, a non-singular reality ontology, a mixed methods methodology, and a value-laden axiology which benefits people (Kivunja, C., and Kuyini, A.B., 2017, p.26). Pragmatism acknowledges the full dialectics

between knowledge and action, where proper action is knowledgeable action and proper knowledge is actable knowledge. Pragmatism is a philosophy of knowledge construction that emphasizes practical solutions to applied research questions and the consequences of inquiry (Peter, G.R., *et al.*, 2005, p.9). Peter, G.R. (2005, p.9) put it simply that pragmatists opt for methods and theories that are more useful to use within specific contexts (e.g., answers to practical problems), not those that reveal underlying truths about the nature of reality.

Research Methodology

A research methodology can be viewed as a procedural or step by step outline or framework within which research is done, according to Remenyi *et al.*, (1998) as cited by Mohajan (2018). Research methodology can be quantitative, qualitative or mixed. In this research, a mixed method approach was taken. The research method of mixed methods is largely quantitative with the research design being a survey and an experiment, but supported by qualitative approaches where Focus Group discussions are held. According to Cresswell, J.W. (2014), in a mixed methods methodology the researcher mixes both qualitative and quantitative data and employs the practices of both qualitative and quantitative research. It is also underpinned by the pragmatic paradigm. Research methodology can be quantitative, qualitative or mixed.

Research Design or Methods

The choice of the qualitative research methodology in this research is guided by the underlying Interpretivist paradigm that seeks to understand the thought process of respondents in a certain context and generate new concepts or theories. Statistical intrusion detection involves creation and analysis of user profiles based on each user's observed behavior, hence the form of supervised classification.

Data Collection/Generation Through Focus Groups

A focus group is a qualitative data collection method in which a researcher or researchers and respondents assemble to discuss a certain research topic (Freitas *et al.*, 1998). According to Hancock *et al.*, (2007), focus groups look a lot like interviews but focus group records can be analysed so as to discover the ways in which the participants interact with each

other and influence each other's voiced ideas which does not happen in a one on one interview. Topic guides are normally used so as to avoid loss of focus on the topic under study. According to Kitzinger (1995) as cited by Dilshad and Latif (2013), focus groups are mostly favourable when a researcher wants to find out the people's understanding and experiences about the problem and reasons behind their particular pattern of thinking. Focus groups give a chance to the marginalized groups of the society to divulge their feelings about their needs and problems. In this research, focus groups were used and the researcher led the discussion and respondents responded to open ended questions. A sample size is the number of respondents from which the researcher gets the required information (Kumar, 2011). The sample size is 8. A total of 8 participants attended a Cybersecurity Workshop facilitated by the researcher at the Harare International Conference Centre (HICC), on Thursday 7th and Friday 8th March, 2019. This is the Focus Group that was used at this stage of the research project.

Quantitative Data Collection of KDD'99 Dataset

The research uses the KDDCup 1999 intrusion detection benchmark dataset in order to build an efficient network intrusion detection system. The primary data, with about 10 million records and 42 attributes, was obtained from <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>. However, a sample of 494,020 instances were selected for data analysis.

Population and Sampling Technique

The research established the population, the sample frame, determined the sample design and the sample size and sampling technique as detailed in the sections below. A sample size is the number of respondents from which the researcher gets the required information (Kumar, R., 2011). Saunders *et al.*, (2009) defines a population as the full set of cases from which a sample is taken. Population also refers to the whole group of things of importance that the researcher wishes to study (Saunders *et al.*, 2009). The sample is 2 million network intrusion detection and prevention records. For this

study the unit of analysis was the KDD'99 Dataset where 494,020 instances for network intrusion detection records were analysed. The sampling frame is defined by Saunders *et al.*, (2009) as a comprehensive list of members of the population from which a sample is drawn. Since the population size is finite and known the Researcher will use the Yamane's formula to arrive at a sample size (Saunders *et al.*, 2009). A 95% confidence level (0.05) was used to calculate the sample size for the study. The study utilized the purposive sampling method.

Data Analysis Methods

The primary data collected from KDD'99 Dataset. From a population of 10 million network traffic data, a sample of 494,020 records of primary data with 42 variables was analysed using mainly the SNORT open source software and other Bayesian Network supportive platforms such as NCSS 2019, Pass 2019, GeNIe 2.3, WinBUGS14, BayES and Analytica 5.1. From the data collected, we need to find patterns, connections, relationships, and meaningful insights from the data. Both quantitative and qualitative data was analysed.

The primary data collected consist of 42 attributes. The required key variables are the following types of attacks

- DoS - Denial of Services
- Scan.
- Local access
- User to root
- 5.Data

Detailed Analysis

Bayesian networks allow for prediction, generalization, and planning. The analysis of attack can be structured according to the schema shown on Figure 4 below.

The SNORT open source software and other Bayesian Network supportive platforms such as NCSS 2019, Pass 2019, GeNIe 2.3, WinBUGS14, BayES and Analytica 5.1, were used to analyse the quantitative data.

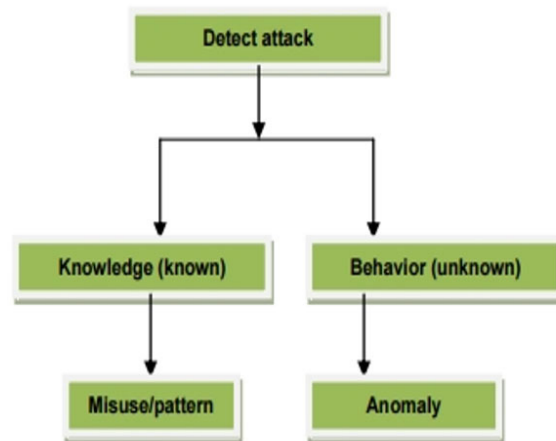


Figure 4: Analysis of Attack (Source: Murugan, S., and Rajan, M.S., 2014, p.2)

Figure 4: Analysis of Attack (Source: Murugan, S., and Rajan, M.S., 2014, p.2)

Problems with Cybersecurity in Zimbabwe

The Focus Group gave the following as the problems with Cybersecurity in Zimbabwe.

- There is a problem on the clarity on responsibilities or ownership of who deals with what with regards to Cybersecurity. Some regard it as an ICT problem or technical problem and yet it is more social than technical.
- The Ubiquitous nature of technology and advances in the Internet of Things (IoT) presents serious challenges, where many smaller devices are now accessing the internet and yet present a high risk on cybersecurity. Telecommuting has become more common worldwide and so one cannot tell whether the device scanning your organisation is from home, down the street or from any part of the world.
- Security is being regarded as an after thought, i.e. Cybersecurity strategy is not part of the Business Strategy of the organizations.
- Over dependence on one service provider is not safe, e.g. Ecocash. In the unlikely event of a breakdown, the whole nation cannot do financial transactions. A national payment system is required and should be provided by the Government or national system to guarantee assurance of services for services of national significance.
- The African culture in Zimbabwe is still weak and has had very little exposure on the cyber space, and has not matured on the use of plastic money. Cyber criminals often take advantage of such a situation.
- We must demand redundancy from the service providers and so Service Level Agreements (SLAs) must be enforced and followed through.
- Affordability and availability of electricity to only 3% of the population and internet access to only 47% of the population in Zimbabwe gives room to manipulation by all kinds of criminals.
- There is need for technical measures and clear Cybersecurity Visions that are implementable in our environment.
- The awareness training programmes need to be conducted more frequently even up to the grassroots level to raise awareness in Zimbabwe.
- There is need for a national skills audit on Cybersecurity so that we swiftly address the skills gaps and delinquency in the competence levels. Furthermore, the few Zimbabweans well exposed to Cybersecurity are suffering from Brain Drain as they are targeted for employment in other countries.
- The national ICT Policies and Cybersecurity policies are not simplified enough for ordinary citizens and people at grassroots levels to understand and implement.
- Our own education system is too weak on Cybersecurity skills. There is need to introduce mandatory Cybersecurity courses at certificate,

- diploma and degree levels. For non-graduates, the courses can be introduced somehow.
- The awareness on cybersecurity laws and legal frameworks is almost zero, and so the nation needs to be equipped to handle cybercrime.

Table 1: The Cybersecurity Framework elements

Cybersecurity Framework	Identify Protect Detect Respond Recover is a series of documented processes that are used to define policies and procedures around the implementation and ongoing management of information security controls in an enterprise environment.
Governance, Risk & Compliance	The over-arching organization's approach covers Governance, risk management, and compliance.
Incident Response & Governance	An organized approach to addressing and managing the aftermath of a security breach or cyberattack.
Operations & Administration	The task of identifying an organization's information assets and the documentation needed for policy implementation, standards, procedures, and guidelines to ensure confidentiality, integrity, and availability.
Communication Strategy & Planning	A detailed process that involves initial assessment, planning, implementation and constant monitoring.
Strategy	The definition of the need for an action, the impact of that particular action and driving forces behind the action

The project identified the cybersecurity framework elements shown on Table 1.

An evaluation of the different Artificial Intelligence (AI) techniques that can be used in support of Intrusion (Anomaly and Misuse) Detection Systems was conducted in order to provide better Intrusion Detection and Prevention. The research shed some light on techniques such as Machine Learning (ML), Neural Network and Fuzzy Logic, and how

these can be coupled with NIDS to detect attacks on private networks. Since most of the Intrusion Detection System are signature based, to develop such a sophisticated Intrusion Detection System that can detect and prevent already known and predict unknown attacks is technically unfeasible. An Intrusion Detection System (IDS) can either be bifurcated as a Network IDS (NIDS) or as a Host IDS (HIDS).

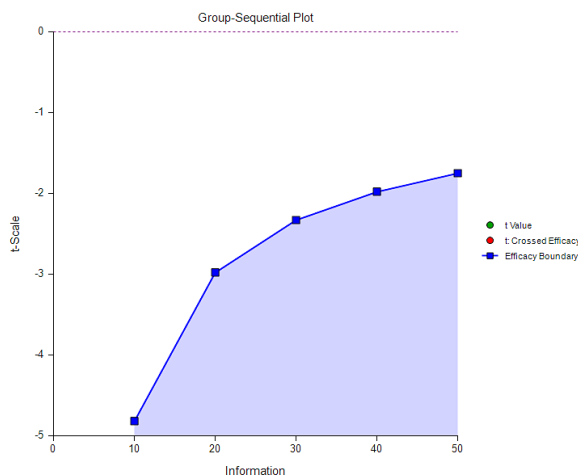


Fig. 5: Group-Sequential Boundary Plot at Stage 0

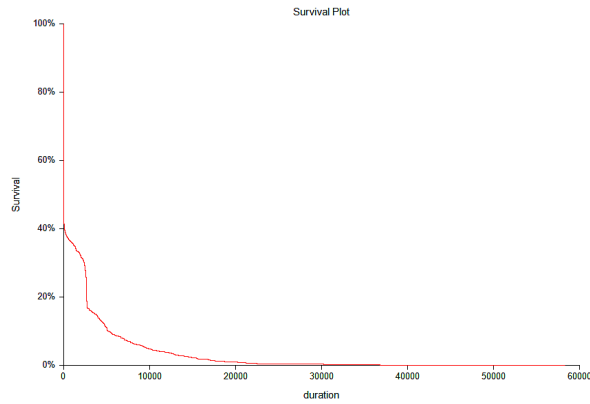


Fig. 6: Kaplan-Meier Survival Curve(s)

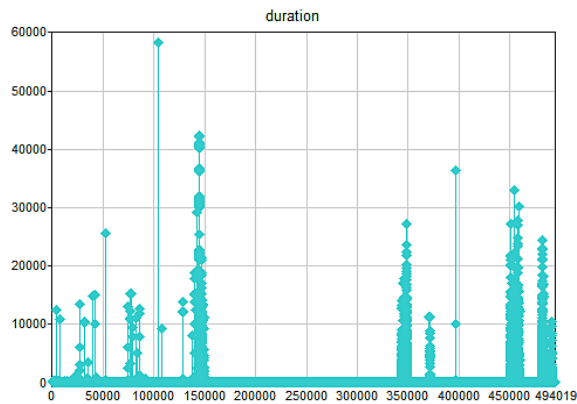


Fig. 7: Time Series of the variable Duration

The results of the T-Tests for the two means for the Network Intrusion Detection and Prevention System is summarised below and shown on Figure 5 and

Figure 6. Time series of the Duration variable is shown on Figure 7.

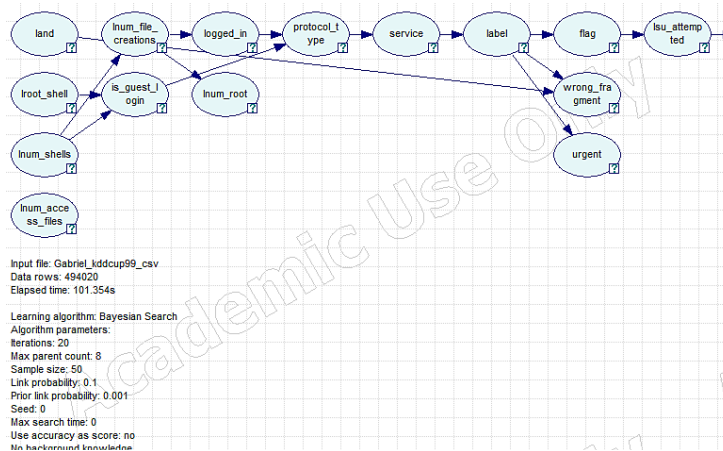


Fig. 8: Bayesian Network Structure

From the primary data of 494,020 records, there are 42 variables that were analysed where the protocol_type has value tcp and service of value http.

The consequent strength of influence is shown on Figure 9.

The Bayesian Network structure derived is shown on Figure 8 below.

The bar chart of the node properties are shown on Figure 10.

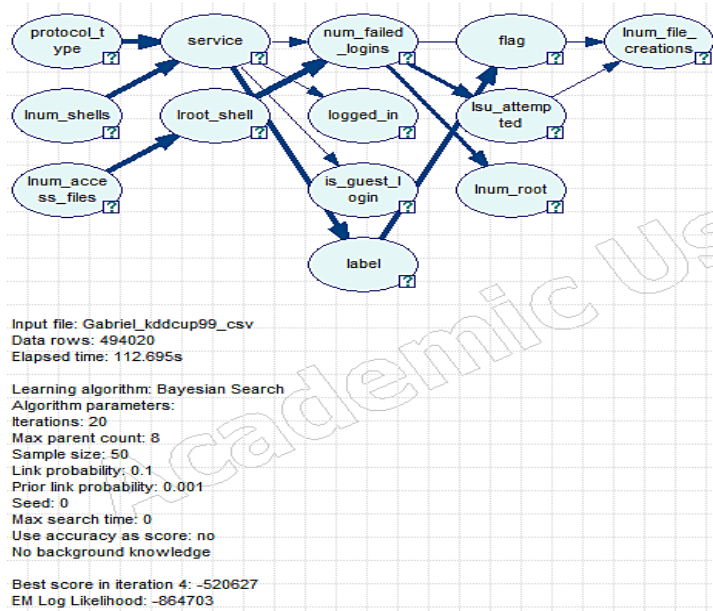


Fig. 9: Strength of Influence

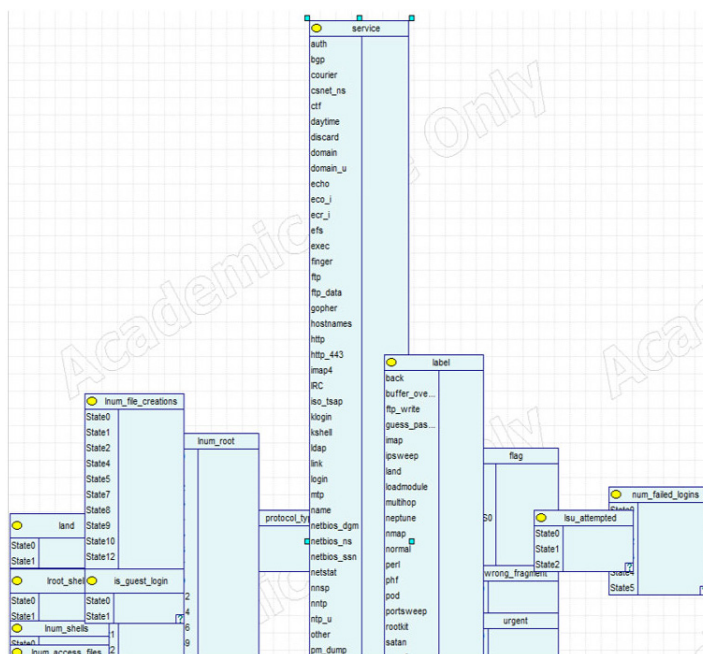


Fig. 10: Bar Chart of Node Properties

Overall Outcomes

The cybersecurity challenges that are being faced in developing countries, like Zimbabwe, include the following.

- Infrastructure (International Telecommunications Union, 2009)
- Legal frameworks (Norwegian Institute of International Affairs, 2018)
- Harmonization of legislation (Bande, 2018).
- Balancing harmonization and country specific needs (ITU, 2012)
- Systems (Schia, 2018)
- Education and awareness (Tagert, 2010), (Schia, 2018)
- Cybersecurity knowledge (The United Nations Economic Commission for Africa Policy Brief, 2014)
- Affordability and funding (Muller, P. L, 2015)
- Perceived low susceptibility to attacks (Tagert, 2010)
- Lack of adequate frameworks that speak to their cybersecurity needs (Tagert, 2010)
- Reporting cybercrime (The Republic of Mauritius Cybercrime strategy 2017-2019, 2017)
- Data sharing

Organizational policies should spell out the procedures for handling information security, with some legal assistance. The policies should cover the following areas (Nielsen, R., 2015, p.14).

- Personal Electronic Devices (PED)
- Acceptable Use
- Records Retention
- Identity Protection
- Server, Service and Project Computing Security
- Data Encryption

The Cybersecurity Vision consists of the following five elements

- Talent centricity
- Strategy and innovation
- Risk focus
- Intelligence and agility
- Resilience and scalability

The research shed some light on techniques on Machine Learning (ML), Neural Networks and Fuzzy Logic and how these may be coupled with an intrusion detection and prevention system to detect attacks on private networks. The benefits of using AI and machine learning in cybersecurity are as follows:

- Automated protection
- Faster response and protection
- Personalization
- Learn to adapt to the situation unobtrusively
- Usability

The perfected Bayesian Network structure is shown on Figure 11.

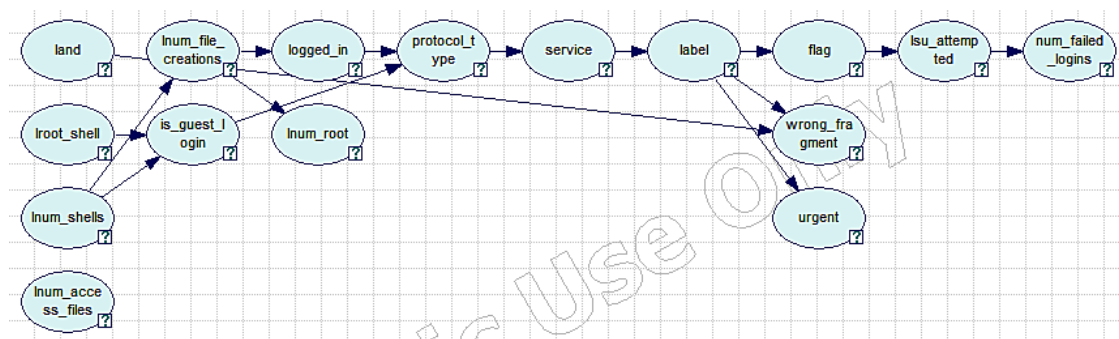


Fig. 11: Bayesian Network structure

A Bayesian Network is represented as a directed acyclic graph. Each node of a Bayesian network (BN) is a label that is an attribute of the problem, and these attributes are binary which can take the value TRUE or FALSE, which means that a random

variable is associated with each attribute. Several problems are faced in the use of BNs.

- The correspondence between the graphical structure and associated probabilistic structure

for purposes of simplifying all the problems of inference problems in graph theory;

- The operation for transposition of the causal graph to a probabilistic representation.

The Naive Bayes is a two-layer Bayesian network that assumes complete independency between the nodes, and is an application of BNs in anomaly detection.

Analysis

The cybersecurity challenges that are being faced in developing countries, like Zimbabwe, include the following:

- Infrastructure
- Legal frameworks
- Harmonization of legislation
- Balancing harmonization and country specific needs
- Systems
- Education and awareness
- Cybersecurity knowledge
- Affordability and funding
- Perceived low susceptibility to attacks
- Lack of adequate frameworks that speak to their cybersecurity needs
- Reporting cybercrime
- Data sharing.

The key components of a Cybersecurity Framework with the supportive strategies, in accordance with the National Institute of Standards and Technology (2018) (<http://www.nist.gov/cyberframework>), requires a clear focus on the need to identify, protect, detect, respond and recover from potential threats and attacks. The intrusion detection and prevention system (IDPS) components must first and foremost be secure since it is the primary target of attackers who try to prevent the IDPSs functioning of detecting attacks or to access the sensitive data on IDPSs like host configuration and known vulnerabilities. The recommended security control measures are:

- Remove Unnecessary Services, Applications and Protocols
- Configure Users, Groups, and Authentication
- Configure Resource Controls
- Install Additional Security Controls
- Test the System Security
- Security Maintenance
- Logging
- Data Backup and Archive
- Access Control Scheme

The Bayesian Network Model developed is shown on Figure 12.

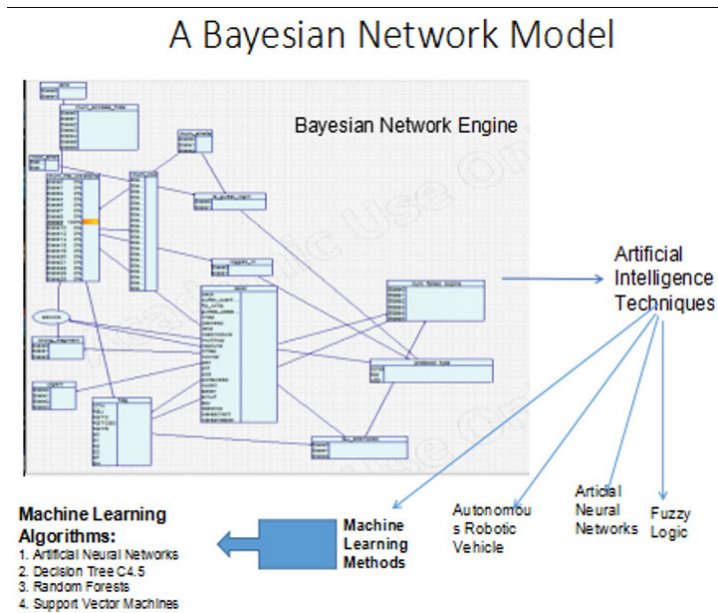


Fig. 12: The Bayesian Network Model developed

A majority of the currently available network security techniques cannot cope with the dynamic and increasingly complex nature of the attacks on distributed computer systems. Therefore, an automated and adaptive defensive tool is a necessary and sufficient condition of computer

networks. Artificial Intelligence (AI) technologies such as Artificial Neural Networks (ANN) have been adopted to improve detection performance.

The pros and cons of data mining techniques are shown on Table 2 below.

Table 2: Advantages and disadvantages of data mining techniques (Source Almutairi, A. (2016) p.43)

Technique	Advantages	Disadvantages
Genetics Algorithm	<ul style="list-style-type: none"> - Finding a Solution for any optimization problem. - Handling multiple solution Search space. 	<ul style="list-style-type: none"> - Complexity to propose a problem space. - Complexity to select the optimal parameters. - The need to have local searching searching technique for effective functioning.
Artificial Neural Network	<ul style="list-style-type: none"> - Adapts its structure during training without need to program it. 	<ul style="list-style-type: none"> - Not accurate results with test data as with training data.
Naive Bayes Classifier	<ul style="list-style-type: none"> - Very simple structure. - Easy to update. 	<ul style="list-style-type: none"> - Not effective when there are high dependency between features.
Decision tree	<ul style="list-style-type: none"> - Easy to understand - Easy to implement 	<ul style="list-style-type: none"> - Work effectively only with attributes having discrete values. - Very sensitive to training sets, irrelevant features and noise.
K Mean	<ul style="list-style-type: none"> - Very easy to understand. - Very simple to implement in solving clustering problems. 	<ul style="list-style-type: none"> - Number of clusters is not automatically calculated. - High dependency on initial centroids.

The summary of the comparative analysis is illustrated on Table 3 below.

determine if a malicious event (i.e., an intrusion) has occurred, and each time a malicious event is detected, the IDS raises an alert (Bolzoni, D., 2009, p.13). The overall user of an IDS is influenced by False positives, rather than false negatives.

An intrusion detection system is known to monitor computer systems and networks in order to

Table 3: Performance of Support Vector Machines, Artificial Neural Network, K-Nearest Neighbour, Naive-Bayes and Decision Tree Algorithms

Parameter	SVM	ANN	KNN	NB	DT
Correctly classified instances	24519	24123	25051	22570	25081
Incorrectly classified instances	673	1069	141	2622	111
Kappa Statistic	0.9462	0.9136	0.9888	0.7906	0.9911
Mean Absolute Error	0.0267	0.0545	0.0056	0.1034	0.0064
Root Mean Squared Error	0.1634	0.197	0.0748	0.3152	0.0651
Relative Absolute Error	5.3676%	11.107%	1.1333%	20.7817%	1.2854%

It is possible to build an intrusion detection system for containers running in the cloud environment, as the presented enriched data representation and framework allows the development of accurate, efficient, and intelligent intrusion detection Systems for cloud computing using machine learning algorithms (Aljebreen, M.J., 2018, p.6). The summary characteristics of an intrusion detection system (IDS are that (Aljebreen, M.J., 2018, p.11) it.

- Runs continuously without human supervision.
- Is fault tolerant to able to recover from crashes.
- Is simply tailored to a specific network.
- Adapts to behaviour changes of user/system over time.
- Works in real-time.
- Detects maximum number of intrusions with minimum number of false?positive alarms.
- Is self-monitored.
- Is self-configurable to the security policies changes.
- Operates while maintaining minimum overhead

There are various numbers of artificial neural networks algorithms. Multilayer perceptrons is one of the most popular types of neural network that is used in many applications such as intrusion detection. It was chosen to be used by Aljebreen, M.J. (2018, p.32) as an effective alternative to more traditional statistical techniques, as it can be trained to approximate virtually any smooth, measurable function; it is not concerned with data distribution and makes no prior assumptions about that; it models highly non-linear functions; and it can be trained to accurately generalize when presented with unseen data in the testing data.

The data structure of Decision Tree C4.5 follows the divide-and-conquer strategy, and its a well-known algorithm that can be used for classification and regression (Aljebreen, M.J., 2018, p.32). There are many decision tree algorithms, and the most well-known algorithm to build trees is the C4.5 algorithm which is most appropriate in developing a classification based intrusion detection system.

The random forests algorithm adds an additional layer of randomness to bagging. In bagging (Bootstrap aggregation), multiple trees are fit in to subsampled data where the prediction is calculated

by averaging the majority votes of each tree's response. However, in random forests, each node is split differently by using the best split among a subset of predictors that is picked randomly at that node; which helps to overcome the overfitting problem. Random forests also have an ability to handle high dimensional data (Aljebreen, M.J., 2018, p.33).

The principle of the support vector algorithm (SVM) is to derive a hyperplane, which maximizes the separating margin between the positive and negative classes (Aljebreen, M.J., 2018, p.34). The SVM algorithm becomes popular for its generalization ability, especially for its high number of features, m , with low numbers of data points, n . However, training the SVM with a dimensional quadratic programming (QP) problem involves large matrix operations that result in large numbers of computations which lead to slow performance. Of late, many enhancements have been applied to the SMO algorithm which increases its performance even more than before. Hence, the SVM algorithm in general has been used for decades for both anomaly and misuse detection.

Conclusion

The main research question was-
What Bayesian Network model is most appropriate for a network detection and prevention cybersecurity system?

The purpose of this research was to develop a structure for a network intrusion detection and prevention system based on the Bayesian Network for use in Cybersecurity. The objectives of this research were to

- Determine the cybersecurity framework appropriate for a developing nation.
- Evaluate network detection and prevention systems that use Artificial Intelligence paradigms.
- Analyse Bayesian Networks that can be represented as graphical models and are directional to represent cause-effect relationships
- Develop a Bayesian Network model that can handle complexity in cybersecurity.

The objectives of the research were achieved. It is of primordial importance to secure the intrusion

detection and prevention system (IDPS). Supportive security control measures and policies are required. There are numerous cybersecurity challenges that are being faced in developing countries, like Zimbabwe.

An evaluation of Artificial Intelligence paradigms for network detection and prevention systems covered machine learning methods, autonomous robotic vehicle, artificial neural networks, and fuzzy logic. To develop such a sophisticated Intrusion Detection System that can detect and prevent already known and predict unknown attacks is technically unfeasible since most of the Intrusion Detection Systems are signature based. The current trend is to use Expert Systems, Neural Network, Genetic Algorithm, Fuzzy Logic and other AI techniques in improving the capabilities of IDS. Expert Intrusion Detection Systems are being developed for recognising and learning through patterns. Neural networks are trained for a specific problem domain provide reasonable solutions with representative sets of training data, but is not able to handle streaming data, and therefore, it is necessary for the individual protecting our system, to take off-line the data whenever he needs to train the model and to run it to the updated set of representative data. The Generic Vehicle Architecture specification equipped with a variety of popular communication and sensing technologies can be handy and makes a promisory note. Due to their dependence on sensing, communication and artificial intelligence, cyber-physical systems, such as cars, drones and unmanned vehicles are attractive targets for attacks that cross the cyber-physical divide, from forcing a car to veer off road, to hijacking a drone or overwhelming a driverless car's lidar sensors. Fuzzy Logic is most effective when solving complex problems, where it consists of a fuzzy set of elements where the membership of any element in the fuzzy set can vary from 0 to 1. Fuzzy Rough C-Means will partition the data into 2 classes: lower approximation and boundary.

The research used the KDDCup 1999 intrusion detection benchmark dataset in order to build an efficient network intrusion detection system. From a population of 10 million network traffic data, a sample of 494,020 instances of primary data with

42 variables was analysed using mainly the SNORT open source software and other Bayesian Network supportive platforms such as NCSS 2019, Pass 2019, GeNle 2.3, WinBUGS14, BayES and Analytica 5.1. A structural equation modelling was done for the Bayesian Network model and the Bayesian Network structure developed. The performance of Support Vector Machines, Artificial Neural Network, K-Nearest Neighbour, Naive-Bayes and Decision Tree Algorithms was discussed. Alternative improved solutions discussed include the use of machine learning algorithms specifically Artificial Neural Networks (ANN), Decision Tree C4.5, Random Forests and Support Vector Machines (SVM).

Effective and efficient intrusion detection systems are needed to promptly detect and prevent intrusion to fight against extraordinarily intelligent cyber-attacks. Anomaly-based intrusion detection methods establish models from normal behaviors and identify audited data by measuring the deviation between observed data and the built models. Sequential data is everywhere, e.g., sequence data that represents changes in the system such as the change in state; in biosequence analysis or text processing and temporal data that models a system that is dynamically changing or evolving over time in speech recognition, visual tracking or financial forecasting for example. A problem of great interest in the training of intrusion detection systems is how to select key and effective features from a huge set of possible related features. Dynamic Bayesian networks (DBNs) are used for modeling sequential data.

A Bayesian Network model was developed with the supportive Artificial Intelligence techniques (machine learning methods, autonomous robotic vehicle, artificial neural networks, and fuzzy logic) and with options of the most efficient machine learning algorithms (Artificial Neural Networks (ANN), Decision Tree C4.5, Random Forests and Support Vector Machines (SVM)). More realistic and diverse up-to-date network data would be most appropriate for use in machine learning for purposes of a network intrusion detection and prevention system.

Further research work is required on new efficient machine learning algorithms for Bayesian Networks, starting with Artificial Neural Networks (ANN),

Decision Tree C4.5, Random Forests and Support Vector Machines (SVM). The recommended future direction would be to develop an Expert Intrusion Detection System.

Acknowledgement

I deeply appreciate the Atlantic International University for supporting this research work as part of my Doctor of Science degree in Computer Science.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Conflict of interest

There is no conflict of interest associated with this publication.

References

- ALJEBREEN, M.J., (2018). Towards Intelligent Intrusion Detection Systems for Cloud Computing, Ph.D. Dissertation, Florida Institute of Technology, 2018.
- ALANEZI, A.A., (2014). Development of an Orally Disintegrating Mini-Tablet (ODMTs) Containing Metoclopramide HCl to Enhance Patient Compliance, Master of Science Thesis, University of Toledo, 2014, http://rave.ohiolink.edu/etdc/view?acc_num=mco1417861431.
- ALMUTAIRI, A., (2016). Improving intrusion detection systems using data mining techniques, Ph.D Thesis, Loughborough University, 2016.
- BANDE S., (2018). Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities. *International Journal of Cyber Criminology* Volume 12 Issue 1 January-June 2018.
- BOLZONI, D., (2009). Revisiting Anomaly-based Network Intrusion Detection Systems, Ph.D Thesis, University of Twente, The Netherlands, ISBN: 978-90-365-2853-5, ISSN: 1381-3617, DOI: 10.3990/1.9789036528535.
- BRINGAS, P.B., and Santos, I., (2010). Bayesian Networks for Network Intrusion Detection, Bayesian Network, Ahmed Rebai (Ed.), ISBN: 978-953-307-124-4, InTech, Available from: <http://www.intechopen.com/books/bayesian-network/bayesian-networks-for-network-intrusion-detection>.
- CHUKWUDI, L., Lopez R., Wager, T.D., Silvers, J.A., and Buhle, J.T., (2014), Cognitive Reappraisal of Emotion: A Meta-Analysis of Human Neuroimaging Studies, *Cerebral Cortex*, Volume 24, Issue 11, 1 November 2014, Pages 2981–2990, <https://doi.org/10.1093/cercor/bht154> <https://academic.oup.com/cercor/article/24/11/2981/301871>.
- DEMIR, N., and Dalkilic, G., (2017). Modified stacking ensemble approach to detect network intrusion, *Turkish Journal of Electrical Engineering & Computer Sciences*, Accepted/Published Online: 15.11.2017, <http://journals.tubitak.gov.tr/elektrik/>
- International Telecommunication Union, (2009). Global Security Report.
- International Telecommunication Union, (2012). http://www.itu.int/net/pressoffice/press_releases/2012/70.aspx#.XI-UZoyxWfA
- JABBARI, F., Visweswaran, S., and Cooper, G.F., (2018), Instance-Specific Bayesian Network Structure Learning, *Proceedings of Machine Learning Research* vol 72, 169-180, 2018, PGM 2018.
- KABANDA, G., (2013). "African context for technological futures for digital learning and the endogenous growth of a knowledge economy", *Basic Journal of Engineering Innovation (BRJENG)*, Volume 1(2), April 2013, pages 32-52, <http://basicresearchjournals.org/engineering/PDF/Kabanda.pdf>
- KARIMPOUR, J., Lotfi, S., and Siahmarzkooh, A.T., (2016). Intrusion detection in network flows based on an optimized clustering criterion, *Turkish Journal of Electrical Engineering & Computer Sciences*, Accepted/Published Online: 17.07.2016, <http://journals.tubitak.gov.tr/elektrik>
- KESSLER, G.C., (2019). An Overview of Cryptography. [Online]. Available from: <https://www.garykessler.net/library/crypto.html> [Accessed: 30 April 2019].
- KIVUNJA, C., and Kuyini, A.B., (2017).

- Understanding and Applying Research Paradigms in Educational Contexts, *International Journal of Higher Education*, Vol. 6, No. 5, September 2017, Published by Sciedu Press 26, ISSN 1927-6044, E-ISSN 1927-6052, <http://ijhe.sciedupress.com>; doi:10.5430/ijhe.v6n5p26 URL: <https://doi.org/10.5430/ijhe.v6n5p26>.
16. KUMAR, R., (2011). *Research Methodology: A step by step guide for beginners 3rd ed.* London: Sage Publishers.
 17. KYLILI, A., Fokaides, P.A., Ioannides, A., and Kalogirou, S., (2018). Environmental assessment of solar thermal systems for the industrial sector, *Journal of Cleaner Production*, 176, 99-109.
 18. MADIGAN, D., (2008). *Data Mining: An Overview*, <http://www.stat.columbia.edu/~madigan>, retrieved on 6th April, 2019.
 19. MOHAJAN, H.K., (2018). Qualitative Research Methodology in Social Sciences and Related Subjects. *Journal of Economic Development, Environment and People*. Volume 7 Issue 1, 2018 pp 23-48.
 20. MORGAN, D.L., (2013). Pragmatism as a Paradigm for Social Research, *Qualitative Inquiry*, 201X, Vol XX(X) 1–9, © The Author(s) 2013, <http://www.sagepub.com/journalsPermissions.nav>, DOI: 10.1177/1077800413513733,
 21. MULLER, P.L., (2015). *Cybersecurity Capacity Building in Developing Countries. Opportunities and Challenges*. Norwegian Institute of International Affairs.
 22. MURUGAN, S., and Rajan, M.S., (2014). Detecting Anomaly IDS in Network using Bayesian Network, *IOSR Journal of Computer Engineering (IOSR-JCE)*, e-ISSN: 2278-0661, p- ISSN: 2278-8727, Volume 16, Issue 1, Ver. III (Jan. 2014), PP 01-07, www.iosrjournals.org
 23. National Institute of Standards and Technology, (2018). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*.
 24. NIELSEN, R. (2015). *CS651 Computer Systems Security Foundations 3d Imagination Cyber Security Management Plan*, Technical Report January 2015, Los Alamos National Laboratory, USA.
 25. PETER, G.R., Artur, P., and Peter, H.F., (2005). "A Pragmatic Research Philosophy for Applied Sport Psychology", Ph.D Dissertation, Kinesiology, Sport Studies and Physical Education Faculty Publications, 80, 2005, https://digitalcommons.brockport.edu/pes_facpub/80.
 26. SAUNDERS, M.N.K., Thornhill, A., and Lewis, P., (2009). *Research Methods for Business Students (5th Edition)*, Publisher: Pearson; ISBN-13: 978-0273716860, ISBN-10: 0273716867, <https://www.amazon.com/Research-Methods-Business-Students-5th/dp/0273716867>.
 27. SCHIA, N.N., (2018), The cyber frontier and digital pitfalls in the Global South, *Third World Quarterly*, 39:5, 821-837, DOI: 10.1080/01436597.2017.1408403, pages 821-837, <https://www.tandfonline.com/doi/abs/10.1080/01436597.2017.1408403>
 28. SINGH, R., Ahlawat, M., and Sharma, D., (2017). A Review on Radio over Fiber communication System, *International Journal of Enhanced Research in Management & Computer Applications*, ISSN: 2319-7471, Vol. 6, Issue 4, April-2017.
 29. SMITHERMAN, S., (2014). *Chaos and Complexity Theories: Creating Holes and Wholes in Curriculum*, The Chaos and Complexity Theories SIG at the AERA Annual Meeting, San Diego, CA, on Thursday, April 15, 2004.
 30. STALLINGS, W., (2015). *Operating System Stability*. Accessed on 27th March, 2019. <https://www.unf.edu/public/cop4610/ree/Notes/PPT/PPT8E/CH15-OS8e.pdf>.
 31. THE Mauritius Cybercrime Strategy 2017-2019, (2017). <http://certmu.govmu.org/English/Documents/Cybercrime%20Strategy/National%20Cybercrime%20Strategy-%20August%202017.pdf>.
 32. UNITED Nations Economic Commission for Africa. (2014). *Tackling the challenges of cybersecurity in Africa*.
 33. XIAO, L., (2016). *Intrusion detection using probabilistic graphical models*, PhD Dissertation, Iowa State University,
 34. WU, L.Y., Li, S.L., and Gan, X.S., (2017). Network anomaly intrusion detection CVM model based on PLS feature extraction, *Control and Decision*, 32(4), 755-758.
 35. WU, H., Wang, Z., and Wang, C., (2016). Study on the recognition method of airport perimeter intrusion incidents based on laser detection technology, *Turkish Journal of Electrical*

- Engineering & Computer Sciences*, Accepted/
Published Online: 20.10.2016, <http://journals.tubitak.gov.tr/elektrik>.
36. WU, W., (2018). Ship communication network intrusion signal identification based on Hidden Markov model, In: Liu, Z.L. and Mi, C. (eds.), *Advances in Sustainable Port and Ocean Engineering*, *Journal of Coastal Research*, Special Issue No. 83, pp. 868–871. Coconut Creek (Florida), ISSN 0749-0208.
37. WU, S., Zhu, W., Li, H., Yu, I.T., Lin, S., Wang, X., and Yang, S., (2010). Quality of life and its influencing factors among medical professionals in China, *International Archives of Occupational and Environmental Health*, 83(7), 753-761.