International Journal of Academic Multidisciplinary Research (IJAMR)
ISSN: 2643-9670
Vol. 4, Issue 5, May – 2020, Pages: 1-8

A Casual Network Based System for Predicting Multi-stage Attack with Malicious IP

[1]Alile Solomon Osarumwense , [2]Egwali Annie Oghenerukevbe

Department of Computer Science, University of Benin, Benin City, Edo State, Nigeria
Email: [1]solomon.alile@physci.uniben.edu [2]annie.egwali@uniben.edu

Abstract: *Multi-stage attacks are attacks executed in phases where each phase of the attack solely relies on the completion of the preceding phase. These attacks are so cleverly designed that they are able to elude detection from most network instruction detection systems and they are capable of infiltrating sophisticated defenses. In this paper, we proposed and designed a probabilistic inference system for predicting Multi-stage attack with malicious IP based on a supervised machine learning technique called Casual Network; otherwise known as Bayesian Belief Network (BBN) Model. The BBN model was designed on Unbbayes Simulator. The fusion of the proposed inference system and BBN model will assist in the prediction of perpetrated multi-stage attacks from computing devices and its means of identification on a computer network (IP address) before the completion of the said attack and hence help reduce the effects of this kind of attacks on networks by providing information which can be used as a measure to safeguard against this kind of stylish attack.*

Keywords: Multi-stage Attack; Malicious IP Addresses; Prediction; Detection; Casual Networks; Bayesian Belief Network

Introduction

In time past, security breach to networks has amplified due to threats with cybersecurity experts making efforts to resist these threats by designing classy intrusion detection systems. Of these threats, multi-stage attack is the most intricate attack to identify due to the fact that they are cleverly designed, that they are able to evade detection and infiltrate complex defenses [1]. The multi-stage attacks are attacks are attacks committed by advanced persistent threat (APT) in stages to take advantage of loopholes in systems or networks. This attack is executed in different stages or phases by the attacker, where each phase of the attack is exclusively dependent on the conclusion of the previous stage [2]. The procedure involved in this kind of attack are; scanning of the network, breaking into a host (computing device) on a network, installation of tool that aids implementation of an attack on the compromised host and an inside scan initiated from the target host [3]. One major horrifying attribute of multi-stage attack is when it is perpetuated on a computing device on a network; there is a colossal certainty of exposing the whole network. In scenarios such as this, to guard the network, the device whose vulnerabilities have been exploited is placed on a list called the blacklist.
A blacklist is an assembly of entities like IP addresses, MAC addresses or software applications which are impeded from interrelating with other computing devices on the network [4].

The means of recognizing the harmful computing device is to employ the IP address of the device which distinctively identifies the device with harmful intent on the network. An IP address is categorized as being malicious if the device for which the IP address is associated on the network is utilized to execute a network attack.
These attacks could be access attack, data manipulation attack or denial of service attack to mention but a few.
In [5], a perpetuated multi-stage on an organization was reported. The attack was executed in four stages and successfully completed the said attack after period of four months. The attack cause severe damage to the organization and they incurred a huge loss.

Recently in the past, several techniques have been utilized in detecting multi-stage in the works of [2, 5,6,7,8,9,10,11,12,13 and 14] but they generated a lot of false negative during testing and were unable to detect malicious IP addresses used to execute multi-stage attacks.
Hence, it is of essence to develop an efficient system for generating inferences for predicting multi-stage attacks with malicious IP which will be utilized in safeguarding networks against this kind of cleverly designed attacks within a shorter time.
In this paper, a system and Casual Network (Bayesian Belief Network) model for predicting multi-stage attacks with malicious IP addresses was proposed. Bayesian Belief Networks (BBN) has showed the capability of learning and generating predictive inferences based on inputs. BBN is a complex probabilistic network that combines expert knowledge and observed datasets. It maps out cause and effect relationships between variables and encodes them with probability that signify the amount in which one variable is probable to influence another.

2. Related Works

Several studies have been conducted on detecting multi-stage attacks using IP address. In [2], an online system that detects multi-step attack was developed. It utilized online multi-step attack detection tool (OMADT). The system was trained and tested with cyber security dataset. The system demonstrated high ability in terms of accuracy, speed, alert correlation, online multi-step attacks detection and generating online attack scenarios but it failed to detect malicious IP addresses.
In [5], a Network Intrusion Detection Systems (NIDS) for detecting multi-step attack was designed. The system offer both real-time and historical traffic analysis to identify multi-step attack. Although, the system failed to classify malicious IP addresses.
In [6], a hybrid system comprising of Principal Component Analysis (PCA) and Deep learning was utilized in detecting multi-stage attack. The system was able to predict accurately two (2) out of the four (4) broad classes of attacks analyzed. Despite the high level of prediction accuracy, the system failed in classifying malicious IP addresses.
In [7], Fuzzy Logic was employed to detect multi-step attacks. The proposed detection system was able to achieve a high detection rate. However, the system was unable to make bi-directional inferences from the dataset.
In [8], a soft computing technique based on rules called Fuzzy Logic was employed in predicting multi-stage attack. In their work they proposed and designed a multi-stage attack prediction framework placing emphasis on IP address information. Although the system had high multi-stage attack prediction accuracy, it was unable to identify multi-stage attacks in situations where the IP addresses were involved in the flow of packets and messages on a network.
In a similar study conducted in [9], they combined Data Mining and Fuzzy Logic to predict multi-stage attack. The model was incapable in classifying malicious IP addresses on the network.
Multi-stage attacks were detected using Bayesian Belief Network in [10]. In this work, the author showed the problem associated with multi-stage attack in the presence of uncertainty and his model solely focused on the linear attack topology. The outcome of the experiment indicated that the model failed to detect malicious IP addresses.

In [11], Data Mining was utilized in capturing behavioural patterns of advanced persistent threat. The system results showed a high level of accuracy in terms of predicting multi-stage attacks. However, the system failed to detect malicious IP addresses utilized to perpetuate multi-stage attacks.
In [12], Hidden Markov Models (HMM) was employed in detecting multi-stage attack. The system results showcased the use of HMMs as a defense against complex cyber attacks. The result of system showed the model was unable to detect malicious IP addresses.

In [13], Casual Networks were employed in recognizing and predicting network attack plan. In their work, they used BBN to correlate and evaluate attack scenarios. They tested the model using DARPA's Grand Challenge Problem (GCP) dataset. The outcome of their experiment showed that the model is capable of predicting relationship in similar attack events and capable of predicting multi-stage attack plan. The outcome of the experiment indicated that the model failed to detect malicious IP addresses.

In [14], a system was developed using Fuzzy Cognitive Maps (FCM) to detect multi-stage attacks. The system results efficiently detected the presence of a multi-stage attack in real-time. However, the system is not capable of making bi-directional inference.

3. Casual Network (Bayesian Belief Network)

A Casual Network also known as Bayesian Belief Network (BBN) is directed acyclic graphical model that uses probability to show conditional dependencies that exist amongst nodes on a graph [15]. It is a complex probabilistic network that combines expert knowledge and experimental datasets. It maps out cause and effect relationships between variables and encodes them with probability that signify the amount in which one variable is probable to influence another. Bayesian network is based on the Bayes theorem which relies on probability.
The Bayes theorem is represented in the mathematical equation below:

$$P(a|b) = \frac{P(b|a)P(a)}{P(b)} \quad (1)$$

Where,

P(a) is the probability of event "a" happening without any information about event "b". It is called the "Prior".
P(a/b) is the conditional probability of event "a" happening given that event "b" has already occurred. It is otherwise called the "Posterior".
So the equation for equation for our Bayesian model is now:

$$P(Attack = \prod_{i=1}^{n} P(Attack_i|Parents(Attack_i))$$

Where,

Attack: Node with an attack

n = number of nodes on the BN model

Parents ($Attack_i$) = Nodes that converge on $Attack_i$..

P(Attack) is a joint distribution probability function of the BN model and it is based on the parent dependency of each attack. The joint density probability of the BN model is represented below:

P(Attack1, Attack 2, Attack 3 … Attack61)= P(Attack 61|Attack 60, Attack 59 … Attack1) * P(Attack 61|Attack 60, Attack 59 … Attack1)* P(Attack 2|Attack 1)*P(Attack1).

The Naive Bayes classifiers are often represented as a type of directed acyclic graph (DAG). The Directed Acyclic Graph (DAG) comprises of vertices representing random variables and arrows connecting pairs of nodes. Figure 1 shows a pictorial representation of a Bayesian Network

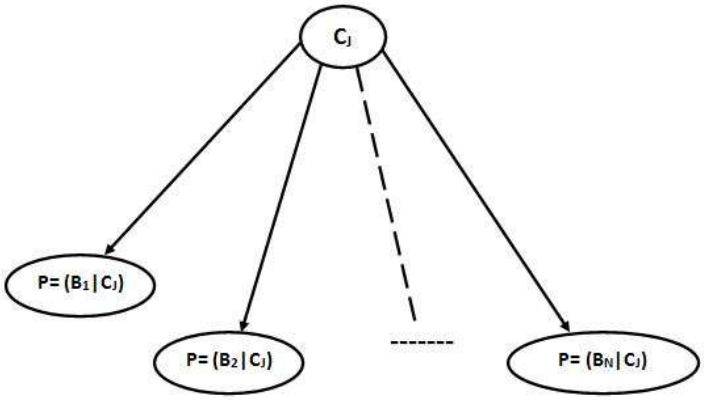

Figure 1: *A Pictorial Representation of a Bayesian Belief Network*

4. Methodology

4.1 Proposed Casual Network Model

The proposed predictive model relies on Bayesian theorem to make predictive inferences. It comprises of nodes which signify an event (cause) and arrows called edges (effect) used to illustrate the intercasual relationship amongst the nodes. The nodes and edges structure forms a graph, thus earning the name directed acyclic graph (DAG)).

Figure 2 below shows the pictorial representation of proposed casual network model for predicting multi-stage attacks with malicious IP.

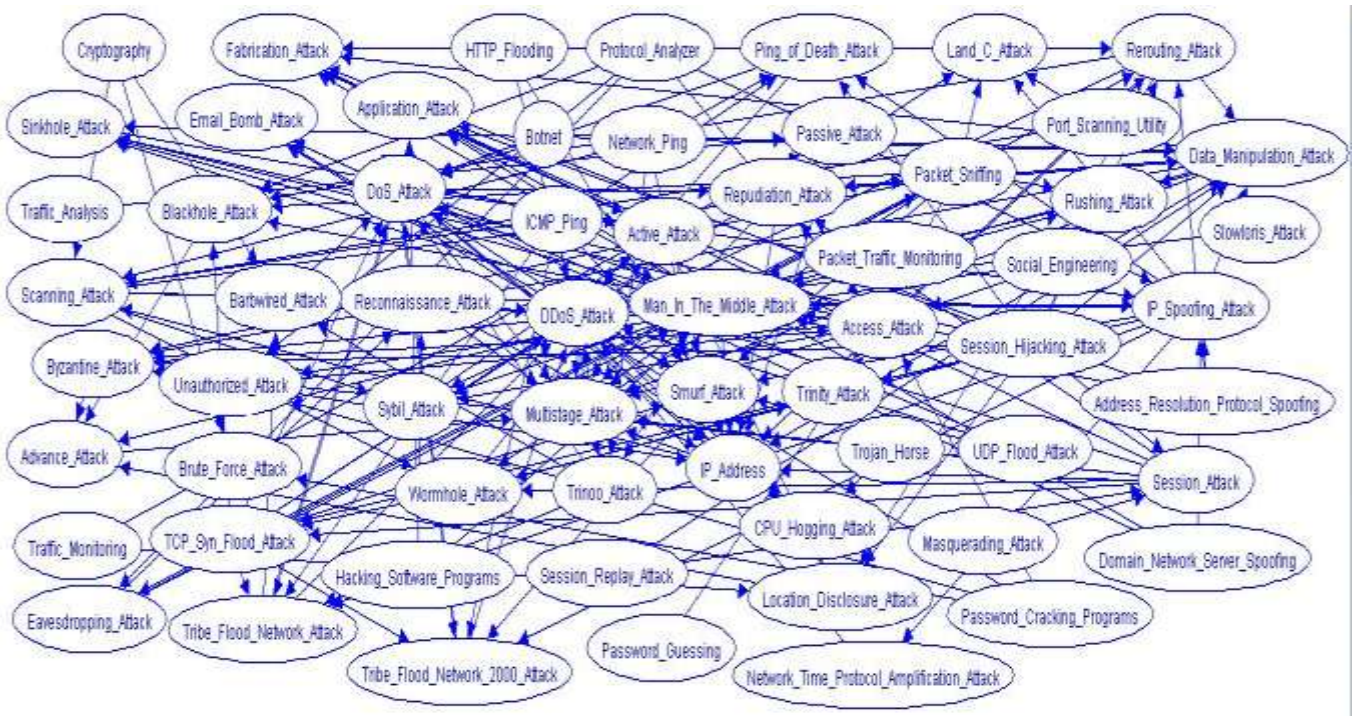

Figure 2: *Proposed Casual Network Model for Predicting Multi-stage Attacks with Malicious IP.*

However, this proposed predictive model has 2 essentials features which are Qualitative and Quantitative in nature.

4.1.2 Qualitative

This section of the model consists of the directed acyclic graph (DAG), nodes or vertices which indicates random variables and edges or arrows showing direct influence. Nodes represent one or more variables. The directed links (arrows) are used when nodes directly influence each other. It should be noted that nodes may influence each other indirectly via other nodes. Each node requires a probability distribution conditioned on its parents (if any). For example, the Bayesian Belief Network model can represent graphically the cause and effect relationship between different constituent parts of different scenarios.
Furthermore, it also has the ability of demonstrating independence based on condition i.e., which circumstances are appropriate and have influence on events and which circumstances are inappropriate as the case maybe.
Inappropriate meaning that knowledge with respect to the circumstances become irrelevant once the cause of the circumstances are recognized.

4.1.3 Quantitative

This section consists of a collection of probability distributions based on condition. E.g. P (RA|SA, EA) = P (SA| ICMP, NP, PSU) and P(EA| PS,PAZ), where P= Probability, RA= Reconnaissance Attack, SA= Scanning Attack, EA= Eavesdropping Attack, ICMP= Internet Control Message Protocol Packet Internet Groper, NP= Network Ping, PSU=Port Scanning Utility and PAZ=Protocol Analyzer, P (RA|SA, EA) meaning the probability of Reconnaissance Attack occurring(the effect or event) given there is evidence of a Scanning Attack and Eavesdropping Attack (Cause of Effect or Event) all combined is called the posterior. (SA| ICMP, NP, PSU) and P (EA| PS, PAZ) meaning the probability of Scanning and Eavesdropping Attack, all combined called the likelihood. It gives information about the latest probability distributions.
In the case of a perpetrated multi-stage attack, the Bayesian Belief Network (BBN) has the capability to give latest information on the probability distribution when fresh attack and attack mode data are derived. The BBN model is built to represent the unlikelihood in the procedure that aids attack situations evaluation. The model shows the intercasual relationship between attacks and its attack mode and made up of 61 nodes with each node representing a type of attack connected to other attacks using arrows showing conditional independence and intercasual relationship.

The main node (Vertex) which is labeled Multi-Stage Attack is situated at the middle of the model with 10 main attacks nodes and 1 node labeled IP address connected to it via arrows which are called Edges, while the other 49 nodes in the model are sub-attacks connected to the 10 main attacks nodes via arrows.

There are nodes that are regarded as ancestors, parents and children nodes. Ancestor nodes are nodes that are independent of its child (parent node) offspring (e.g. Network Ping (NP) etc), Parent nodes are conditionally independent on its offspring (e.g. SA (Scanning Attack), EA (Eavesdropping Attack) etc) and the child nodes are directly dependent on its parent's node. (E.g. RA (Reconnaissance Attack), AA (Access Attack)).

The prediction of Multi-Stage Attack from this proposed model is done using a Joint Probability Density Function which aids the development of a Bayesian attack graph, where each attack and attack mode is assigned probabilistic values which is used to compute the existence of a single attack and Multi-stage attacks. We could multiply all node distributions together and get the probability distribution based on its combination (i.e. Joint probability distribution) over all variables. The joint probability distribution of the model is identified clearly through marginal and conditional considering the independence relationships based on condition between the variables. The predictive inference (reasoning) that will be obtained from this model is based on cause of an attack and effect of the attack (i.e. the probability of an event (attack) occurring given evidence or symptoms (prior information) of the attack's mode) which is bi-directional that is an attack can occur, if there is evidence of the cause of that attack and vice versa.

Bayesian Network models can perform bi-directional modeling within a single structure because variables are not specified as being solely for input or for output, but by applying the Bayesian theorem, the direction of the relationship can be reversed.

Given, $P(Y|X) = \underline{P(X,Y)} / P(X)$:The probability of Event Y occurring given evidence of X).

For example, using the Bayesian Model above, the Probability of a Reconnaissance Attack occurring depends on the evidence of a Scanning and Eavesdropping Attack and it represented as; P(RA|SA,EA)= (P(ICMP Ping), P(NP), P(PSU), P(PS), P(PAZ), where SA= Scanning Attack(ICMP PING, Network Ping AND Port Scanning Utility) and EA= Eavesdropping Attack(Protocol Analyzer and Packet Sniffing) respectively.

$P(X,Y) = P(Y|X)*P(X) = P(X|Y)*P(Y)$;$P(Scenario1|Evidence) = P(Evidence|Scenario1)*P(Scenario1) / P(Evidence)$

IP addresses of computing devices in a network that perform any of the analyzed attacks in the model based on probability are considered a malicious IP addresses. Hence, the IP addresses are blacklisted.

The probability of an IP address being malicious is denoted as follows:

P (IPIM|RA, AA, SESA, DMA, MITMA, DoS, DDoS, ACA, ADA, PA), where IPIM is probability of an IP address being malicious given it has participated in network traffic involving Reconnaissance Attack, Access Attack, Session Attack, Data Manipulation Attack, Man-In-The-Middle-Attack, Denial of Service Attack, Distributed Denial of Service Attack, Active Attack, Advance Attack and Passive Attacks respectively.

Lastly, IP address assigned to computing devices which are of a class and used to perpetrate multi-stage attacks can be predicted using the model.

The probability of malicious IP address being a class A IP address is denoted as follows:

P (IPCA|1.0.0.1,1.0.0.2,1.0.0.3,…….,126.255.255.254) meaning the probability of malicious IP address being a class A IP address is that the IP address must be in the range between 1.0.0.1 to 126.255.255.254.

The probability of malicious IP address being a class B address is denoted as follows:

P (IPCB| 128.1.0.1, 128.1.0.2, 128.1.0.3,……, 191.255.255.254) means the probability of malicious IP address being a class B IP address is that the IP address must be in the range between 128.1.0.1 to 191.255.255.254.

The probability of malicious IP address being a class C address is denoted as follows:

P (IPCC| 192.0.1.1, 192.0.1.2, 192.0.1.3,……..,223.255.254.254) means the probability of malicious IP address being a class C IP address is that the IP address must be in the range between 192.0.1.1 to 223.255.254.254.

The probability of malicious IP address being a class D address is denoted as follows:

P (IPCD| 224.0.0.0,224.0.0.1, 224.0.0.2,……..,239.255.255.254) means that the probability of malicious IP address being a class D IP address is that the IP address must be in the range between 224.0.0.0 to 239.255.255.254.

Lastly, the probability of malicious IP address being a class E address is denoted as follows:

P (IPCE| 240.0.0.1, 240.0.0.2, 240.0.0.3,……,254.255.255.254) which means the probability of malicious IP address being a class E IP address is that the IP address must be in the range between 240.0.0.1 to 254.255.255.254.

4.1.4 The Proposed System Architecture for Predicting Multi-stage Attacks with Malicious IP

The proposed system architecture for predicting multi-stage with Malicious IP addresses on a computer network comprises of a Protocol Analyzer, Network Sniffing Module, IP Checker Module, Probabilistic Reasoning Module (Bayesian Belief Network Model).

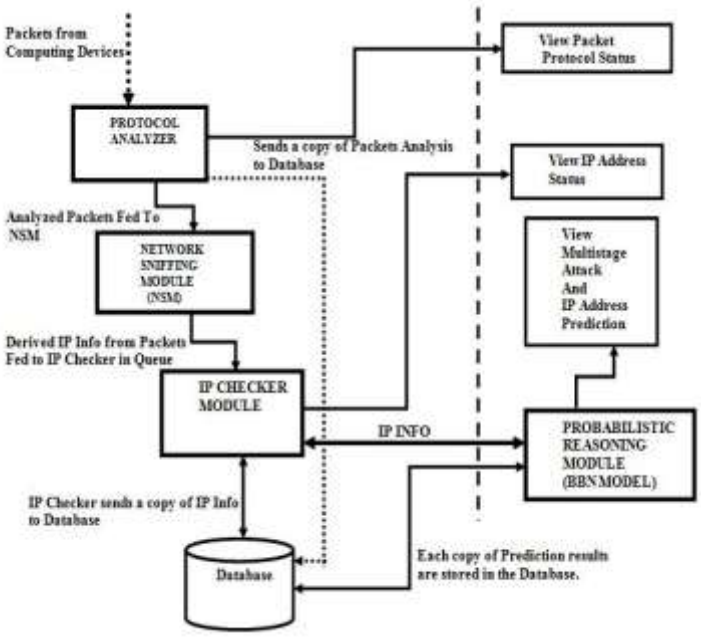

Figure 3. Proposed System Architecture for Predicting Multi-stage Attacks with Malicious IP

Packets which are blocks of data transmitted across a network are generated from computing devices within the network and outside the networks. These computing devices that transmit the packets have a means of identification on their respective networks and are called IP addresses.

Before the transmission of packets can take place, the communicating devices will establish a connection via the use of handshake mechanism. This mechanism notifies the communicating devices the type of transmission protocols that will aid the transmission of packets between the devices, port numbers that will be used to transmit packets and other conditions that must be satisfied before transmission goes through.

As packets travels from source (internal and external computing devices) they go through the protocol analyzer module.

The Protocol Analyzer analyses the packet to check which protocol aided the transmission of the packets and displaying the packet protocol status when it has been duly confirmed by this module. E.g. HTTP (Hyper Text Transfer Protocol), UDP (User Datagram Protocol) and File Transfer Protocol. The results of the analysis carried on the packets is sent to the database and to the next module called the Network Sniffing Module.

The Network Sniffing module tracks the network traffic using TCP (Transmission Control Protocol) dump tool. This tool has effect over many computer operating systems. Furthermore, this tool is regarded as a command line that simplifies the combination process with other modules.

It can also be employed with other software programs like Wireshark to derive a graphical model. The TCP dump tool views and understand network packets then analyzes it to derive IP addresses and it transmits the messages in a queue that will be consumed by the next module which the IP Checker module.

The IP Checker module collects the messages from the Network Sniffing Module, and then it checks its database to see if the IP address is within its pool of IP addresses resident in the database. If the IP address is situated within the database, it displays a message stating that the IP address status which includes the network class of IP address and other information relating the IP address which can viewed and also sends a copy of the IP information to the next module called the Probabilistic Reasoning Module which is the Bayesian Belief Network Model.

The Probabilistic Reasoning Module relies on Bayesian theorem which predicts occurrence of an event, given there is evidence of the event occurring based on prior information of the event's occurrence.

The IP info received from the IP checker is analyzed using the Bayes theorem embedded in the Bayesian Belief Network simulator computing the joint probability distribution function and showing the intercasual relationship exist between the nodes which are variables.

After computation of the variables, the Probabilistic Reasoning module predicts whether a IP address is a malicious IP address, if it participated in the perpetration of a single attack or a multi-stage attack (attacks perpetrated in stages where one stage of the attack is executed based on completion of the previous stage).

The attacks can be any of the ten main attacks analyzed by the model which are Reconnaissance Attack, Access Attack, Data Manipulation Attack, Denial of Service, Distributed Denial of Service, Passive Attacks, Advance Attacks, Active Attacks, Man-In-The-Middle Attack, Session Attacks and/or any of the other 49 attacks represented by nodes in the Bayesian Belief Network model.

Finally, the system displays the results of the prediction which whether a perpetrated attack is a single or multi-stage attack with a IP address or IP addresses with malicious tendencies.

It is important to note that the higher the residual loglikelihood value obtained in the system, the better the system prediction accuracy of perpetrated multi-stage attacks with IP information. A residual value is a measure of how much a regression line vertically misses a data point. Regression lines are the best fit of a set of data. The lines are categorized as averages; a few data points will fit the line and others will miss. Ideally, residual values should be equally and randomly spaced around the horizontal lines.

Conclusion

Detecting multi-stage attack is very difficult because of its intelligent design. To safeguard a network, network security experts need to improve on existing technologies for detecting multi stage attacks. In this paper we proposed a system and BBN model to predict multi stage attack with malicious IP. The network had 61 nodes with each node representing a unique attack. The model was designed using Unbbayes Simulator. The proposed system can be deployed on computer network infrastructures to provide information which will be used to safeguard computer networks. It will also bring about improvement in the following areas: Multi-stage Attack Prediction, Multi-stage attacks Detection, Blacklisting of malicious IP addresses and Computer Network Security in general. Future research should be geared towards improving multi-stage attacks prediction using MAC address and devices that utilizes VPN.

REFERENCES

[1] Dawkins J. and Hale J (2004) A Systematic Approach to Multi-stage Network Attack Analysis, IEEE. pp1-3.
[2] Amiri and Nowroozi (2015): “OMADM: Online Multi-step Attack Detection Method”. International Journal of Computer & Information Technologies (IJOCIT). ISSN = 2345-3877. pp 2.
[3] Valeur,F., Vigna, G., Kruegel, C. and. Kemmerer, R. A. (2004): “Comprehensive Approach To Intrusion Detection Alert Correlation,” IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 3, Jul. 2004. pp 1- 8
[4] Rouse, M. (2016): “Blacklist Definition”. Retrieved from URL: www.techtarget.com/definition/blacklist/.
[5] Papadopoulos, P., Petsas, T., Christou G. and Vasiliadis, G (2015):“MAD-A Middleware Framework for Multi-step Attack Detection”. Institute of Computer Science, Foundation for Research and Technology-hellas. pp 2.
[6] Ibor, A.E., Oladeji, F.A., Okunoye, O.B., Uwadia, C.O. (2019): “Deep Learning Model for Predicting Multi-stage Cyberattacks”. The Journal of Computer Science and Its Applications, Vol. 26, No 1, June, 2019.
[7] Almseidin, M., Piller, I., Al-Kasassbeh, M., and Kovacs, S., (2019): “Fuzzy Automaton as a Detection Mechanism for the Multi-Step Attack”. International Journal on Advanced Science Engineering Information Technology, Vol.9 (2019) No. 2, ISSN: 2088-5334. pp 1-12.
[8] Almutairi, A.Z., Flint, J.A. and Parish, D.J., (2015): “Predicting multi-stage attacks based on IP information”. IN: Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015), 14th-16th December 2015, London, pp. 384-390.
[9] Almutairi, A.Z., Flint, J.A. and Parish, D.J., (2016): “Predicting Multi-stage Attacks Based on Hybrid Approach”. International Journal for Information Security Research, 5 (3), pp. 582 – 590.
[10] Cole, R. (2013): “Multi-Step Attack Detection via Bayesian Modeling under Model Parameter Uncertainty”. pp 3-92.
[11] Katipally, R., Gasior W., Cui, X., and Yang, L.(2010):"Multi stage Attack Detection System for Network Administrators using Data Mining" pp1-4.

[12] Ourston, D., Matzner. S., Stump, W., and Hopkins, B. (2003): "Applications of Hidden Markov Models To Detecting Multi-stage Network Attacks". System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference. Print ISBN: 0-7695-1874-5, INSPEC Accession Number: 8150553, DOI: 10.1109/HICSS.2003.1174909. pp. 1-10.

[13] Qin, X. and Lee, W. (2004): "Attack Plan Recognition and Prediction using Casual Networks". Georgia Institute of Technology,Atlanta, GA 30332, U.S.A.{xinzhou, wenke}@cc.gatech.edu. pp 1-5

[14] Aparicio-Navarro, F.J., Chambers, J.A., Kyriakopoulos, K.G., Ghafir, I. and Lambotharan, S. (2019): " Multi-stage Attack Detection Using Contextual Information". Publisher:IEEE. figshare. https://hdl.handle.net/2134/34219. https://doi.org/10.1109/MILCOM.2018.8599708.

[15] Ben-Gal, I. (2007). "Bayesian Networks". Encyclopedia of Statistics in Quality and Reliability. John Wiley and Sons, Ltd. Retrieved May 15th 2018 from www.eng.tau.ac.il/bengal/BN.pdf/