***I.J. Wireless and Microwave Technologies*, 2020, 2, 30-41**
Published Online April 2020 in MECS(http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2020.02.04

***Available online at* http://www.mecs-press.net/ijwmt**

A Bayesian Belief Network Model For Detecting Multi-stage Attacks With Malicious IP Addresses

[a]Alile S.O , [b]Egwali A.O

[a,b] *Department of Computer Science University of Benin, Benin City, Edo State, Nigeria*

Received: 01 November 2019; Accepted: 28 December 2019; Published: 08 April 2020

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 intelligently designed that they are able to elude detection from most network instruction detection systems and they are capable of penetrating sophisticated defenses. In this paper, we proposed and simulated a Bayesian Belief Network Model to predict Multi-stage Attacks with Malicious IP. The model was designed using Bayes Server and tested with data collected from cyber security repository. The model had 99% prediction accuracy.

Index Terms: Multi Stage Attack; Malicious IP Address; Bayesian Belief Network

1. Introduction

Over the years, there has been an increased threat to network security and network security experts have struggled to combat these rising threats by developing sophisticated intrusion detection system. Of these threats, the multi stage attack is most difficult attack to detect because they are so intelligently designed, that they are capable of eluding detection and penetrating sophisticated defenses [1]. The multi stage attacks are attacks perpetrated by hackers in stages to exploit vulnerabilities of the system or network. They are carried out in different stages or steps by the attacker, where each stage of the attack solely relies on the completion of the preceding stage [2]. The steps usually involved in this type of attack are; scanning of the network, breaking into a host (computing device) on a network, installation of tool that aids execution of an attack on the compromised host and an inside scan initiated from the target host [3].

*Corresponding author. Tel.: +2347036444086,_+2347033247730
E-mail address: solomon.alile@physci.uniben.edu, annie.egwali@uniben.edu

One major atrocious feature of multi stage attack is that when it attacks a device on the network, there exist a huge possible of compromising the entire network. In such scenarios in other to protect the network, the compromised device is placed on a blacklist.

A blacklist is a group of entities such as IP addresses, MAC addresses or software programs that are blocked from interacting with other computing devices on the network [4].

The means of identifying the malicious computing devices is to use the IP address of the device which uniquely identifies the malicious device on the Network. An IP address is malicious if the device for which the IP address is associated on the network is used to perpetuate a network attack. Such attack could be access attack, data manipulation attack or denial of service attack to mention but a few.

In [5], they reported a multi stage attack on an organization. The attack occurred in four stages and took a period of four months to successfully complete the attack. The attack crippled the organization and they incurred a huge loss. In recent past, several techniques have been applied in detecting multi-stage [2,5,6,7,8,9,10,11,12,13] but they generated a lot of false negative during testing and were unable to detect malicious IP addresses used to perpetuate multistage attacks.

In this paper, Bayesian Belief Network (BBN) was utilized in detecting multi-stage attacks with malicious IP addresses. 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. In this paper, BBN was our technique of choice because of its capability to make predictive inference.

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 Multistep 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 multistage 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] fuzzy logic was employed in predicting multistage attack. In their work they proposed and designed a multi-stage attack prediction framework placing emphasis on IP address information. Although the system had a high multistage 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 multistage 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 multistage 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 multistage attacks. However, the system failed to detect malicious IP addresses utilized to perpetuate multistage 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 Bayesian network to correlate and evaluate attack scenarios. They tested the model using DARPA's Grand Challenge Problem (GCP) data set. The outcome of their experiment showed that the model is capable of predicting relationship in similar attack events and capable of predicting multistage attack plan. The outcome of the experiment indicated that the model failed to detect malicious IP addresses.

3. Bayesian Belief Network

Bayesian Belief Network (BBN) is directed acyclic graphical model that uses probability to show conditional dependencies that exist amongst nodes on a graph [14].It is a complex probabilistic network that combine 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.

Bayesian network is based on the Bayes theorem which relies on probability.

The Bayes theorem is represented in the mathematical equation below:

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

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".

P(b/a) is the conditional probability of event "b" happening given that event "a" has already occurred. It is called the "Likelihood".

P(b) is the probability of event "b" happening without any information about event "a". It is called the "Marginal Likelihood".

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

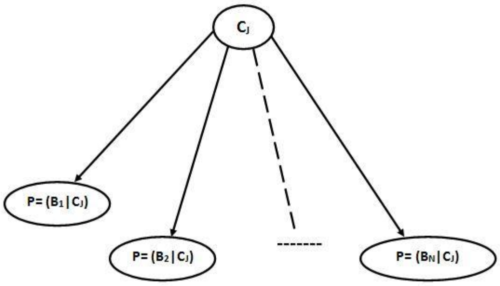


Fig. 1. A pictorial representation of a Bayesian Network

Some advantages of this model are: it is quite fast in making inferences, the resulting probabilities are easy to interpret and the learning algorithm is quite simple and the model adequately combines with utility functions to make optimal inferences. In this paper, we intend to detect multistage attack with malicious IP addresses using Bayesian Belief Network (BBN). A model consisting of 61 nodes where each node represents a form of network attack will be designed using Bayes Server. A cybersecurity dataset will be used to train and test the system. Using the Pareto Principle, 80% of the dataset will be used to train the model while the remainder will be used in testing the model. The aim of the model is to achieve a high level of detection accuracy with the use of IP address.

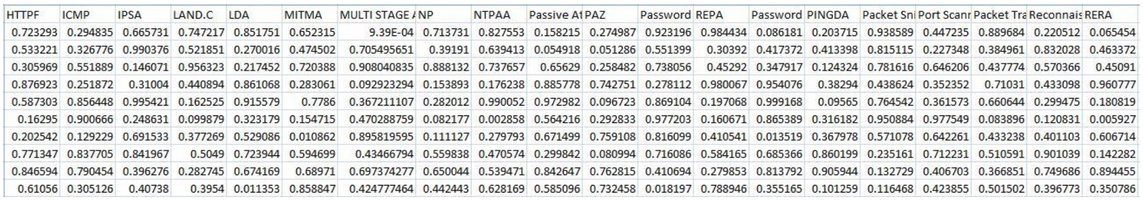
4. Methodology

Simulation, Result and Discussion

The dataset used in training, testing and predicting Multi-stage attack was retrieved from [15]. The dataset consist of 61 attacks and each attack has a value which represents the probability of such attack in causing multi stage attack. These attacks are Access Attack (AA), Active Attack (ACA), Advance Attack (ADA), Application Attack (APPA), Address Resolution Protocol Spoofing (ARPS), Scanning Attack (SA), Barbedwire Attack (BARBWA), Brute Force Attack (BFA), Blackhole Attack (BLA), Byzantine Attack(BYZA), CPU Hogging Attack (CHA), Cryptography(Crypto), Distributed Denial Of Service (DDoS), Domain Network Server Spoofing Attack (DNSA), Denial of Service (DoS), Eavesdropping Attack (EA), Tribe Flood Network 2000 Attack (TFN2A), Email Bomb Attack(EMBA), Fabrication Attack (FA), Hacking Software Programs (HSP), Hyper Text Transfer Protocol Flooding Attack (HTTPA), Internet Control Message Protocol Packet Internet Groper (ICMP Ping), IP Spoofing Attack (IPSA), Land.C Attack (Land.C), Location Disclosure Attack (LDA), Masquerading Attack (MA), Multi- Stage Attack (MSA), Network Ping (NP), Network Time Protocol Amplification Attack(NTPAA), Passive Attack (PA), Protocol Analyzer (PAZ), Password Cracking Programs (PCP), Repudiation Attack (REPA), Ping of Death Attack (PINGDA), Packet Sniffing (PS), Port Scanning Utility (PSU), Packet Traffic Monitoring (PTM), Reconnaissance Attack (RA), Rerouting Attack (RERA), Rushing Attack (RUSHA), Social Engineering (SE), Session Attack (SESA), Session Hijacking Attack (SHA), Slowloris Attack (SLOWA), Smurf Attack (SMA), Session Replay Attack (SRA), Sybil Attack (SYBA), Transmission Control Protocol Syn Flood Attack (TCPSFA), Trinoo Attack (TRIA), Trinity Attack(TRINA), Trojan Horse (TRJH), User Datagram Protocol Flood Attack (UDPFA), Unauthorized Attack (UA), Tribe Flood Network Attack (TFNA), Wormhole Attack (WA), Botnet (Bot),

Password Guessing (PG), Man-in-The-Middle Attack (MITMA), Data Manipulation Attack (DMA) and a column which indicated the class (Malicious) of the IP Address associated to such multi stage attack.

Figure 2 below shows a sample the dataset



HTTPF	ICMP	IPSA	LAND.C	LDA	MITMA	MULTI STAGE A	NP	NTPAA	Passive At	PAZ	Password	REPA	Password	PINGDA	Packet Sni	Port Scanr	Packet Tra	Reconnais	RERA
0.723293	0.294835	0.665731	0.747217	0.851751	0.652315	9.39E-04	0.713731	0.827553	0.158215	0.274987	0.923196	0.984434	0.086181	0.203715	0.938589	0.447235	0.889684	0.220512	0.065454
0.533221	0.326776	0.990376	0.521851	0.270016	0.474502	0.705495651	0.39191	0.639413	0.054918	0.051286	0.551399	0.30392	0.417372	0.413398	0.815115	0.227348	0.384961	0.832028	0.463372
0.305969	0.551889	0.146071	0.956323	0.217452	0.720388	0.908040835	0.888132	0.737657	0.65629	0.258482	0.738056	0.45292	0.347917	0.124324	0.781616	0.646206	0.437774	0.570366	0.45091
0.876923	0.251872	0.31004	0.440894	0.861068	0.283061	0.092923294	0.153893	0.176238	0.885778	0.742751	0.278112	0.980067	0.954076	0.38294	0.438624	0.352352	0.71031	0.433098	0.960777
0.587303	0.856448	0.995421	0.162525	0.915579	0.7786	0.367211107	0.282012	0.990052	0.972982	0.096723	0.869104	0.197068	0.999168	0.09565	0.764542	0.361573	0.660644	0.299475	0.180819
0.16295	0.900666	0.248631	0.099879	0.323179	0.154715	0.470288759	0.082177	0.002858	0.564216	0.292833	0.977203	0.160671	0.865389	0.316182	0.950884	0.977549	0.083896	0.120831	0.005927
0.202542	0.129229	0.691533	0.377269	0.529086	0.010862	0.895819595	0.111127	0.279793	0.671499	0.759108	0.816099	0.410541	0.013519	0.367978	0.571078	0.642261	0.433238	0.401103	0.606714
0.771347	0.837705	0.841967	0.5049	0.723944	0.594699	0.43466794	0.559838	0.470574	0.299842	0.080994	0.716086	0.584165	0.685366	0.860199	0.235161	0.712231	0.510591	0.901039	0.142282
0.846594	0.790454	0.396276	0.282745	0.674169	0.68971	0.697374277	0.650044	0.539471	0.842647	0.762815	0.410694	0.279853	0.813792	0.905944	0.132729	0.406703	0.366851	0.749686	0.894455
0.61056	0.305126	0.40738	0.3954	0.011353	0.858847	0.424777464	0.442443	0.628169	0.585096	0.732458	0.018197	0.788946	0.355165	0.101259	0.116468	0.423855	0.501502	0.396773	0.350786

Fig. 2. Snapshot of Dataset

The Bayesian model was designed using Bayes-Server platform. The Bayesian belief network for predicting multi stage attack was designed such that the nodes on the network are linked based on the probability of an attack resulting to another. To blacklist an IP address on the network we analyze the attack perpetuated by the device.

In our model for an IP address to be denoted as a malicious IP such IP must have perform any of the following attacks; 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. The malicious IP address is categorized into various classes each class indicating the risk level of such IP address.

Figure 3 shows the BBN model for detecting multistage attack with malicious IP Addresses.

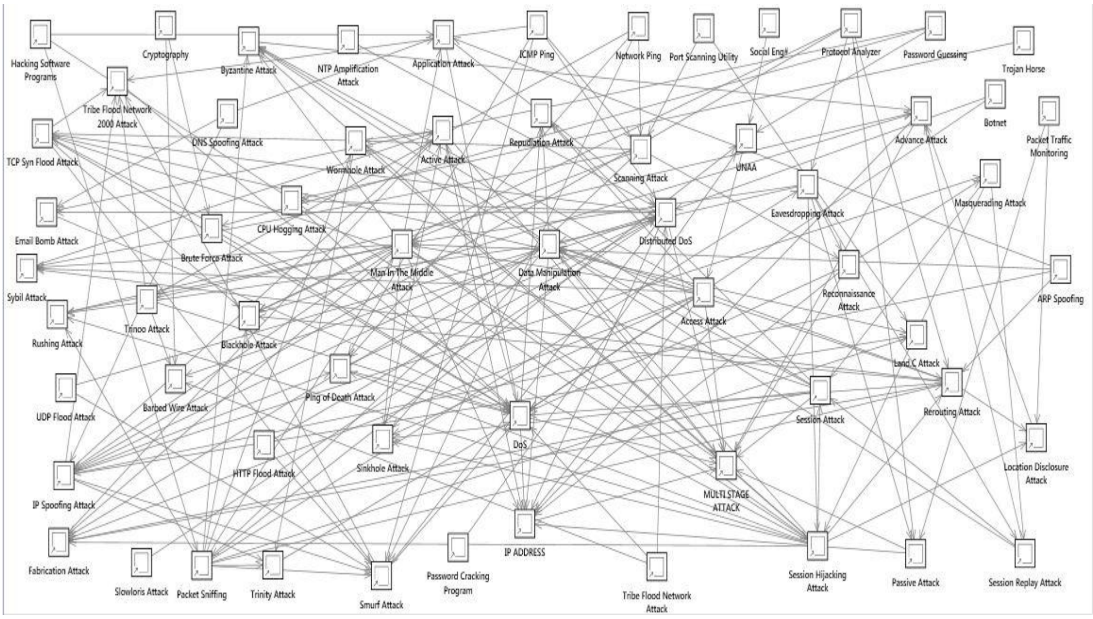


Fig. 3. Bayesian Belief Network Model for Detecting Multi-stage attacks with Malicious IP.

So, to mathematically represent our model we have:

$$\text{Multi Stage Attack} = \prod_{i=1}^{61} \quad \text{P}(\text{Attack}_\text{i}|\text{Parents}(\text{Attack}_\text{i}) \tag{2}$$

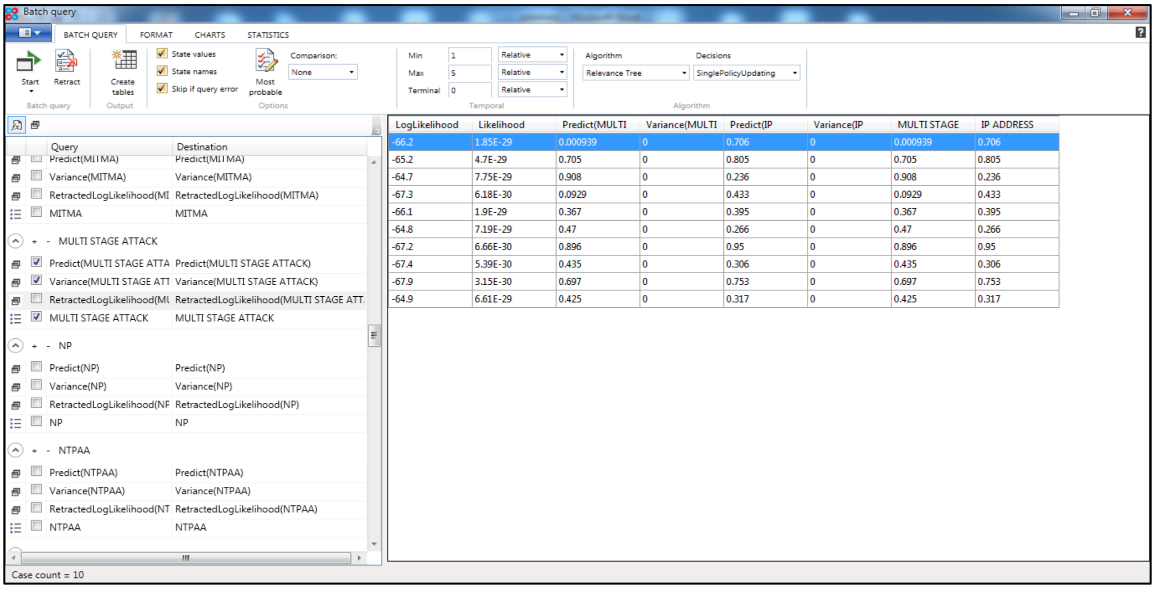
Where,

Attack: Node with an attack

Parents (Attack$_i$) = Nodes that converge on Attack$_{i..}$

The dataset was used to train and test the model. Upon completion of training and testing the BBN model, the test data converged at time series 3. The log likelihood value for each case was recorded.

Figures 4, 5, 6,7,8,9 and 10 shows log likelihood batch query chart for predicting multi-stage attack with IP Information, association/strengths of nodes of the model, feature importance chart for nodes in the model, the in-sample anomaly detection chart, the log likelihood Attack Graph for Detecting Multi-stage Attack with IP Information, the mesh query plot for the loglikelihood chart and Multi-stage Attack Detection Results chart respectively. The result generated from the simulation indicated that the network was able to predict 99% multistage attack on the dataset accurately and it had a log likelihood of 62.99 on the test dataset.



☑ State values
☑ State names
☑ Skip if query error

Comparison: None

Min	1	Relative
Max	5	Relative
Terminal	0	Relative

Algorithm: Relevance Tree

Decisions: SinglePolicyUpdating

	Query	Destination
□	Predict(MITMA)	Predict(MITMA)
□	Variance(MITMA)	Variance(MITMA)
□	RetractedLogLikelihood(MI	RetractedLogLikelihood(MITMA)
□	MITMA	MITMA
	+ - MULTI STAGE ATTACK	
☑	Predict(MULTI STAGE ATTA	Predict(MULTI STAGE ATTACK)
☑	Variance(MULTI STAGE ATT	Variance(MULTI STAGE ATTACK)
□	RetractedLogLikelihood(MU	RetractedLogLikelihood(MULTI STAGE ATT.
☑	MULTI STAGE ATTACK	MULTI STAGE ATTACK
	+ - NP	
□	Predict(NP)	Predict(NP)
□	Variance(NP)	Variance(NP)
□	RetractedLogLikelihood(NP	RetractedLogLikelihood(NP)
□	NP	NP
	+ - NTPAA	
□	Predict(NTPAA)	Predict(NTPAA)
□	Variance(NTPAA)	Variance(NTPAA)
□	RetractedLogLikelihood(NT	RetractedLogLikelihood(NTPAA)
□	NTPAA	NTPAA

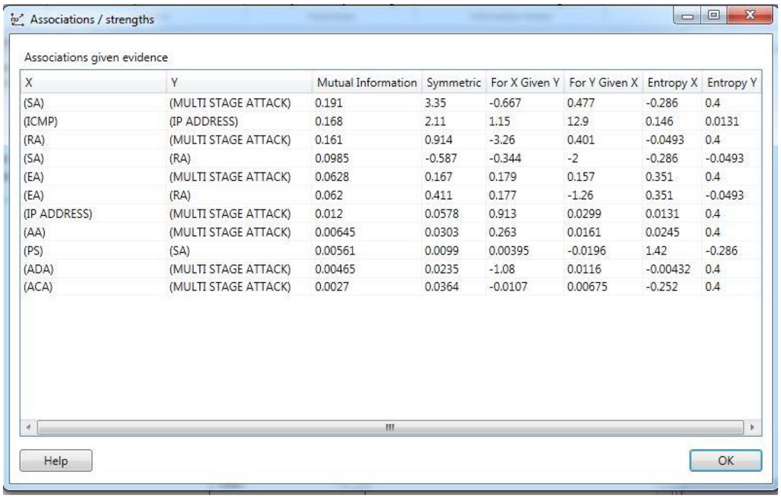
LogLikelihood	Likelihood	Predict(MULTI	Variance(MULTI	Predict(IP	Variance(IP	MULTI STAGE	IP ADDRESS
-66.2	1.85E-29	0.000939	0	0.706	0	0.000939	0.706
-65.2	4.7E-29	0.705	0	0.805	0	0.705	0.805
-64.7	7.75E-29	0.908	0	0.236	0	0.908	0.236
-67.3	6.18E-30	0.0929	0	0.433	0	0.0929	0.433
-66.1	1.9E-29	0.367	0	0.395	0	0.367	0.395
-64.8	7.19E-29	0.47	0	0.266	0	0.47	0.266
-67.2	6.66E-30	0.896	0	0.95	0	0.896	0.95
-67.4	5.39E-30	0.435	0	0.306	0	0.435	0.306
-67.9	3.15E-30	0.697	0	0.753	0	0.697	0.753
-64.9	6.61E-29	0.425	0	0.317	0	0.425	0.317

Case count = 10

Fig. 4. The Loglikelihood Chart Batch Query for Detecting Multi-stage Attack with IP Information

This loglikelihood chart batch shows the result of the test data.

In Experiment 1: the value of Predict(Multistage) was 0.000939 compared to 9.39E-05 and the value of Predict(IP) was 0.706 compared to 0.706222843330884. Experiment 2: the value of Predict(Multistage) was 0.705 compared to 0.705495650811725 and Predict(IP) was 0.805 compared to 0.804881363796469. Experiment 3: the value of Predict(Multistage) was 0.908 compared to 0.908040834959557 and (IP) was 0.236 compared to 0.236028234904242 up to Experiment 10. Hence, the system results showed a 0.01% value difference between the prediction results and original test data of 100% resulting to 99% prediction accuracy.



Associations given evidence

X	Y	Mutual Information	Symmetric	For X Given Y	For Y Given X	Entropy X	Entropy Y
(SA)	(MULTI STAGE ATTACK)	0.191	3.35	-0.667	0.477	-0.286	0.4
(ICMP)	(IP ADDRESS)	0.168	2.11	1.15	12.9	0.146	0.0131
(RA)	(MULTI STAGE ATTACK)	0.161	0.914	-3.26	0.401	-0.0493	0.4
(SA)	(RA)	0.0985	-0.587	-0.344	-2	-0.286	-0.0493
(EA)	(MULTI STAGE ATTACK)	0.0628	0.167	0.179	0.157	0.351	0.4
(EA)	(RA)	0.062	0.411	0.177	-1.26	0.351	-0.0493
(IP ADDRESS)	(MULTI STAGE ATTACK)	0.012	0.0578	0.913	0.0299	0.0131	0.4
(AA)	(MULTI STAGE ATTACK)	0.00645	0.0303	0.263	0.0161	0.0245	0.4
(PS)	(SA)	0.00561	0.0099	0.00395	-0.0196	1.42	-0.286
(ADA)	(MULTI STAGE ATTACK)	0.00465	0.0235	-1.08	0.0116	-0.00432	0.4
(ACA)	(MULTI STAGE ATTACK)	0.0027	0.0364	-0.0107	0.00675	-0.252	0.4

Fig. 5. The Association/Strengths Chart of Nodes of the model.

The association/strength chart shows the association that exist amongst nodes given evidence of a node event occuring. This chart consists of Mutual Information, symmetric Information, For (X Given Y). For (Y Given X), Entropy X and Entopy Y respectively.

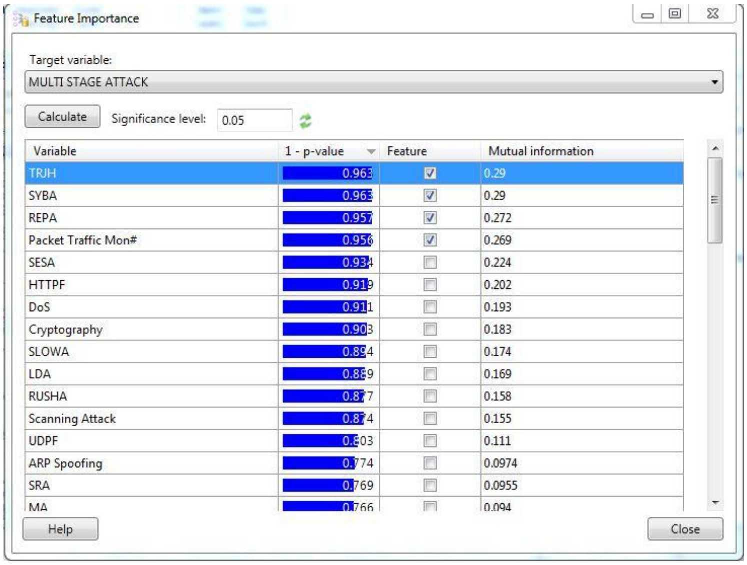
Mutual Information: specifies the relationship with nodes directly connected to one another and assigned a value (e.g. the mutual relationship between Multistage Attack and SA(Scanning Attack) nodes and has the value of 0.191 to show the closeness).

Sysmmetric information: shows nodes that are around the axis of the location of SA and Multistage Attack nodes in the model and having a value of 3.35 showing it is quite futher away from the two nodes.

For (X Given Y): shows the probability of Event X(SA) happeniing given there is evidence that an Event Y(multistage attack) has already occurred and having a value of -0.677.

For (Y Given X):): shows the probability of Event Y(Multistage Attack) happening given there is evidence that an Event (SA) has already occurred and having a value of 0.477. Entropy X: is the degree of disorderness or randomness of X in the model.

Entropy Y: is the degree of disorderness or randomness of Y in the model.



Target variable: MULTI STAGE ATTACK

Significance level: 0.05

Variable	1 - p-value	Feature	Mutual information
TRJH	0.963	☑	0.29
SYBA	0.963	☑	0.29
REPA	0.957	☑	0.272
Packet Traffic Mon#	0.956	☑	0.269
SESA	0.934	□	0.224
HTTPF	0.919	□	0.202
DoS	0.911	□	0.193
Cryptography	0.903	□	0.183
SLOWA	0.894	□	0.174
LDA	0.889	□	0.169
RUSHA	0.877	□	0.158
Scanning Attack	0.874	□	0.155
UDPF	0.803	□	0.111
ARP Spoofing	0.774	□	0.0974
SRA	0.769	□	0.0955
MA	0.766	□	0.094

Fig. 6. The Feature Importance Chart for Nodes in the Model

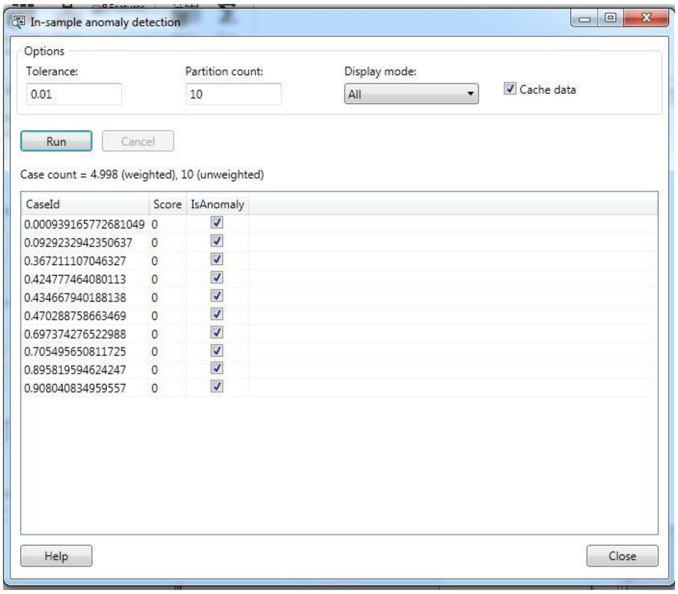
The Feature Importance Chart shows p-value of the variable (nodes), feature and mutual information in reference to the Multistage Attack Node.

The p-value signifies the likelihood (probability)of the nodes being involved in the execution of a multistage attack.

The Feature box is checked if that particular node is fully involved in the said attack.

The mutual information shows the relationship with nodes directly connected to one another (i.e. in this case the direct relationship of the nodes with the multistage attack node)and assigned a value.

The Significance Level signifies the margin of error in the detection of multistage attack.



Tolerance: 0.01
Partition count: 10
Display mode: All
☑ Cache data

Case count = 4.998 (weighted), 10 (unweighted)

CaseId	Score	IsAnomaly
0.000939165772681049	0	☑
0.0929232942350637	0	☑
0.367211107046327	0	☑
0.424777464080113	0	☑
0.434667940188138	0	☑
0.470288758663469	0	☑
0.697374276522988	0	☑
0.705495650811725	0	☑
0.895819594624247	0	☑
0.908040834959557	0	☑

Fig.7. The In-sample Anomaly Detection Chart

The In-sample Anomaly Detection Chart shows 10 experimental results of detecting Multistage attack. Each Case is assigned an ID(Identification value) which is the value of the Predict(Multistage) in Fig.4. The IsAnomaly checkbox is checked to identify that each case is an executed multistage attack. The 10 cases of multistage attack has a case count value of 4.998 (weighted) which signifies the importance of the cases leading to a execution of a multistage attack. The tolerance is the margin of error that could be encoutered as regards to the detection of the multistage attacks.

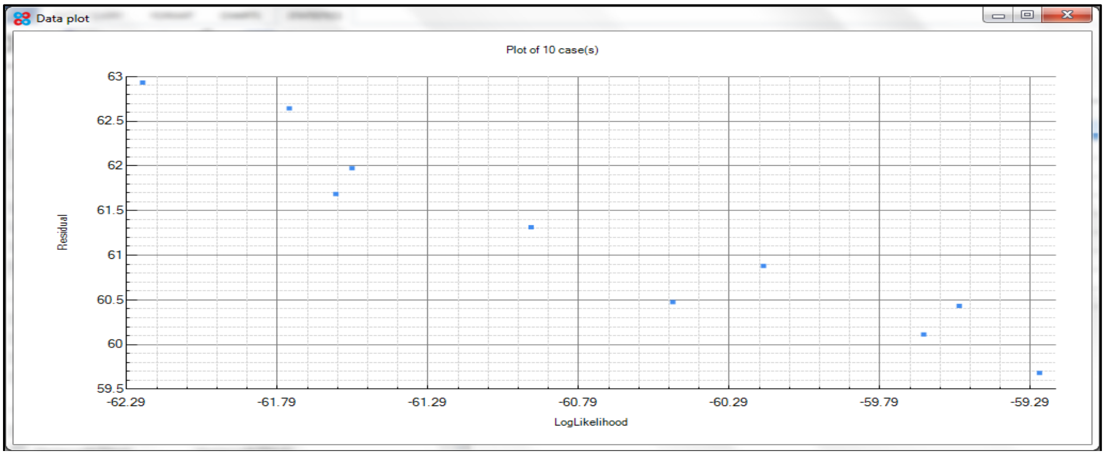


Fig. 8. The Loglikelihood Attack Graph for Detecting Multi-stage Attack with IP Information

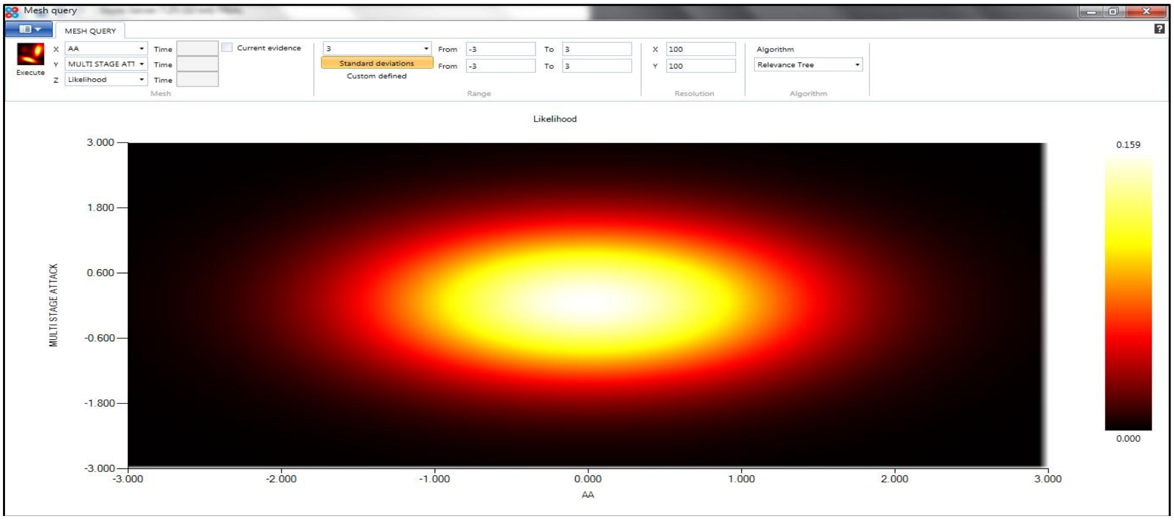
This loglikelihood graph for detecting multistage attack shows the residual values on the vertical axis plotted against the loglikelihood values on the horizontal axis which are independent variables. A residual value is a measure of how much a regression line vertically misses a data point. Regression 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.

In this graph, it shows that 10 experimental cases resulted in value of 59.6, 60.1, 60.4, 60.49, 60.99, 61.3, 61.3, 61.7, 61.99, 62.6 and 62.99 respectively.

Ideally, residual values should be equally and randomly spaced around the horizontal lines. Taking a view of the system' experimental results values obtained from the horizontal lines on the graph, it can be seen that the point where the residual value and the loglikelihood independent variable meets at 62.99 on the horizontal line with 63 being the highest value that can be reached.

The residual value attained is 62.99 and loglikelihood independent value is -62.29, the difference between both values is 0.71 which is the predicted value.

Hence, in this system the highest residual value, a loglikelihood independent value can attain is 63. With 63, being the 100 % residual value mark, to get our prediction accuracy percentage, we have highest residual value subtracted from predicted value i.e. 100% -0.71= 99.29% residual loglikelihood percentage value.


Mesh query

MESH QUERY

X AA
Y MULTI STAGE ATT
Z Likelihood

□ Current evidence

3
Standard deviations
From -3 To 3
From -3 To 3

X 100
Y 100

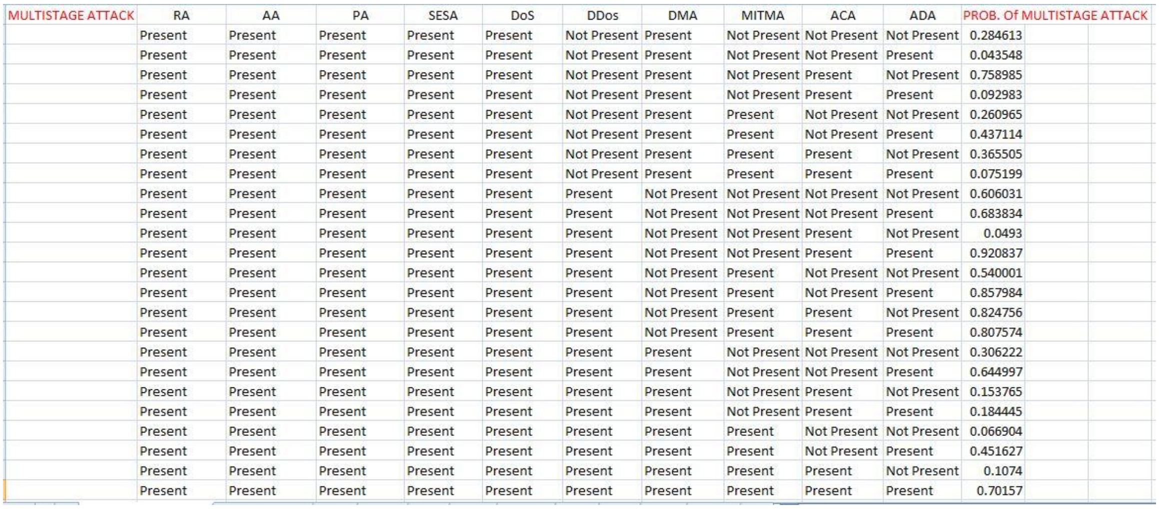
Algorithm Relevance Tree

Fig. 9. The Mesh Query Plot for the Loglikelihood of a Single Attack (Access Attack, [AA]) Being involved in a Multi-stage Attack.

The mesh query plot shows the loglikelihood/likelihood of a node in this case Access Attack (AA) being involved in the execution of a multistage attack. The Node (multistage attack) is plotted on the Y-axis and the other node Access attack (AA) plotted along the X-axis.

In this context, the Red contour signifies the likelihood of an AA being involved in a multistage attack with the contour ranging from interval -1.600 to 1.000 on the Y-axis and interval -1.500 to1.500 on the X-axis.

The Yellow contour shows the loglikelihood of an AA being involved in a multistage attack with the contour ranging from interval -0.600 to 0.600 on the Y-axis and interval -1.000 to 1.000 on the X-axis.



MULTISTAGE ATTACK	RA	AA	PA	SESA	DoS	DDos	DMA	MITMA	ACA	ADA	PROB. Of MULTISTAGE ATTACK
	Present	Present	Present	Present	Present	Not Present	Present	Not Present	Not Present	Not Present	0.284613
	Present	Present	Present	Present	Present	Not Present	Present	Not Present	Not Present	Present	0.043548
	Present	Present	Present	Present	Present	Not Present	Present	Not Present	Present	Not Present	0.758985
	Present	Present	Present	Present	Present	Not Present	Present	Not Present	Present	Present	0.092983
	Present	Present	Present	Present	Present	Not Present	Present	Present	Not Present	Not Present	0.260965
	Present	Present	Present	Present	Present	Not Present	Present	Present	Not Present	Present	0.437114
	Present	Present	Present	Present	Present	Not Present	Present	Present	Present	Not Present	0.365505
	Present	Present	Present	Present	Present	Not Present	Present	Present	Present	Present	0.075199
	Present	Present	Present	Present	Present	Present	Not Present	Not Present	Not Present	Not Present	0.606031
	Present	Present	Present	Present	Present	Present	Not Present	Not Present	Not Present	Present	0.683834
	Present	Present	Present	Present	Present	Present	Not Present	Not Present	Present	Not Present	0.0493
	Present	Present	Present	Present	Present	Present	Not Present	Not Present	Present	Present	0.920837
	Present	Present	Present	Present	Present	Present	Not Present	Present	Not Present	Not Present	0.540001
	Present	Present	Present	Present	Present	Present	Not Present	Present	Not Present	Present	0.857984
	Present	Present	Present	Present	Present	Present	Not Present	Present	Present	Not Present	0.824756
	Present	Present	Present	Present	Present	Present	Not Present	Present	Present	Present	0.807574
	Present	Present	Present	Present	Present	Present	Present	Not Present	Not Present	Not Present	0.306222
	Present	Present	Present	Present	Present	Present	Present	Not Present	Not Present	Present	0.644997
	Present	Present	Present	Present	Present	Present	Present	Not Present	Present	Not Present	0.153765
	Present	Present	Present	Present	Present	Present	Present	Not Present	Present	Present	0.184445
	Present	Present	Present	Present	Present	Present	Present	Present	Not Present	Not Present	0.066904
	Present	Present	Present	Present	Present	Present	Present	Present	Not Present	Present	0.451627
	Present	Present	Present	Present	Present	Present	Present	Present	Present	Not Present	0.1074
	Present	Present	Present	Present	Present	Present	Present	Present	Present	Present	0.70157

Fig. 10. Multi-stage Attack Detection Results Chart

This chart shows the probabilities of 10 main attacks namely Reconnaissance Attack (RA), Access Attack (AA), Passive Attack (PA), Session Attack (SESA), Denial of Service Attack (DoS), Distributed Denial of Service (DDoS), Man in the Middle Attack (MITMA), Active Attacks (ACA) and Advance Attack (ADA) respectively.

This detection results showed the probability of having all the aforementioned attacks involved in a multistage attack denoted as:

P(Multistage Attack| RA,AA,PA,SESA, DoS, DDoS, MITMA,ACA,ADA)= 0.70157

From the experiment it can be seen that our model has a higher residual log likelihood value which is 62.99. Comparing the log likelihood from the experiments conducted by Qin and Lee (2004) and Cole (2013) which are 6.55 and 9.84 respectively, it is obvious our model has a better prediction accuracy. The higher prediction accuracy achieved by our model could be due to the size of the dataset used in training and testing the model.

5. 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 utilized a Bayesian Belief Network model to predict multi stage attack. The network had 61 nodes with each node representing a unique attack. The model was trained and tested and it had an accuracy of 99% in predicting multi stage attack with malicious IP addresses. The 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 multistage 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 Multistage 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 Multistage 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”. Pp 1-5. Georgia Institute of Technology,Atlanta, GA 30332, U.S.A.{xinzhou, wenke}@cc.gatech.edu

[14] 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/

[15] Cybersecurity IDS Dataset (2018): “Cybersecurity Intrusion Detection System Dataset”. Retrieved 10th June 2018, from URL: http://www.cybersecurity.unsw.adfa.edu.au/ADFA%20IDS%20Datasets/.

Authors’ Profiles

Alile Solomon Osarumwense obtained his Diploma in Data Processing degree from University of Benin in 2004, B.Sc. degree in Computer Science in 2012 from Lagos State University (LASU), Ojo, Lagos and M.Sc in Computer Science from University of Benin in 2019. He is a Cisco Certified Network Associate (Routing and Switching) and System Engineer. His area of interest includes Information Technology, Soft Computing, Machine Learning and Cybersecurity. He is currently conducting research works in the area of cybersecurity. He is a member of International Computer Science and Engineering Society (ICSES), Institute For Engineering Research and Publication (IFERP), International Association of Engineers (IAENG), International Association of Engineers Society of Computer Science (ISCS), International Association of Engineers Society of Wireless Networks (ISWN), International Association of Engineers Society of Scientific Computing (ISSC), International Association of Engineers Society of Internet Computing and Web Services (ISICWS), International Association of Engineers Society of Information System Engineering (ISISE), International Association of Engineers Society of Data Mining (ISDM), International Association of Engineers Society of Artificial Intelligence (ISAI), and International Association of Engineers Society of Software Engineering (ISSE).

Egwali Annie Oghenerukevbe is a Professor of Cybersecurity at the Department of Computer Science, Faculty of Physical Sciences, University of Benin, Benin City, Nigeria. Her area of interests includes Information Technology, Software Engineering, Gender studies, E-commerce, Electronic Marketing and Cyber Security. To date, she has supervised several undergraduate and postgraduate students. She is currently carrying out research works relating to cyber security. She is a member of International Network for Women Engineers and Scientists (INWES), IEEE (The Institute of Electrical and Electronics Engineers), Nigerian Computer Society (NCS), Third World Organizations of Women Scientists (TWOWS) and Computer Professionals [Registration Council] of Nigeria (CPN).

How to cite this paper: Alile S.O , Egwali A.O, " A Bayesian Belief Network Model For Detecting Multi-stage Attacks With Malicious IP Addresses ", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.10, No.2, pp. 30-41, 2020.DOI: 10.5815/ijwmt.2020.02.04