International Journal of Academic Information Systems Research (IJAISR)
ISSN: 2643-9026
Vol. 4, Issue 4, April – 2020, Pages: 44-53

Man-In-The-Middle Attack Detection Based on Bayesian Belief Network

Egwali A.O[1], Alile S.O[2]

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

Abstract: *Man-in-The-Middle (MiTM) attack is one of the most intimidating forms of attack on a computing device where an attack occurs without the victim having the slightest knowledge that a breach in security has occurred. These attacks are so smartly planned that they are able to elude detection from most network instruction detection systems and they are capable of penetrating sophisticated defenses. In the past, several systems have been developed to defend against MiTM attack, but they generated a lot of false negative during testing and were unable to detect Man-in-The–Middle attack and its various forms. Hence, In this paper, we proposed and simulated a Bayesian Belief Network model to predict Man-in-The-Middle attack. The model was designed using Bayes Server and tested with data collected from cyber security repository. The model had a 99% prediction accuracy.*

Keywords: Man-in-The-Middle Attack; Bayesian Belief Network

1. Introduction

The evolution of the computer networks has brought communication amongst devices at a level never attained before. This communication allows computing devices to process raw data and transfer information within a platform called network.
A network is a collection of devices such as computers, mobile handheld devices and other computer peripherals connected via a communication medium or pathway that allow these devices to share files and resources amongst themselves.
This communication medium brings about interconnectivity between people and computing devices at very high stage that have never been visualized before. With the advent of mobile handheld device like tablets and phones communication among devices has become seamless thus leading to easy sharing of information among individuals.
Information (including sensitive ones) stored on server databases situated on several network can be easily accessed via computing devices on the popular network of networks called the Internet.
In [1] it was stated that due to the interconnectivity of these networks, the chances of a security breach to these networks such as unauthorized access, which can affect these connected devices is on the rise.
This act can be perpetrated by advanced persistent threat (APT) from either within or outside the network raising concerns over network security which can be in form of network attacks.
[2] defined Network attack as a term used to describe an intrusive activity on a network and its devices by carefully analyzing the network environment in order to retrieve information about network in order to exploit vulnerabilities of networks or open channels, ports which may involve unauthorized access to resources.
However, there are several attacks that cause a breach to network and information passed along the communication channel. Of these attacks, Man-in-the-middle attack is one of the most frightening forms of attack on a computing device where an attack occurs without the victim having little or no knowledge that a breach in security has occurred as stated by [3].
A Man-in-The-Middle attack (MiTM) is classified as a type of cybersecurity attack that makes provision for an advanced persistent threat (APT) to surreptitiously snoop in on a conversation (i.e. eavesdrop) on the communication channel between two computing devices. The execution of the attack takes place in between two legitimately communicating hosts, allowing the attacker to meddle on a conversation that they are not meant to listen to, hence the name "man-in-the-middle" for its position between two legitimate communicating devices as stated by [4].
MiTM attacks are categorized as one of the foremost forms of cyber attack with network security experts searching for ways to prevent attackers from causing damage or eavesdropping on communication amongst computing devices.
In [5], a scenario of MiTM attack that occurred in an organization was made known where an advanced persistent threat incorporated themselves in-between two hosts (client and a server). The attacker took control of communication amongst the two computing device hereby intercepting data, files or information transferred amongst the devices. This attack paralyzed the organization leading to a huge unaccountable loss.
Furthermore, there are several types of man in the middle attacks namely Rogue Access Point Attack, ARP Spoofing Attack, MDNS Spoofing Attack, DNS Spoofing Attack, Eavesdropping Attack, IP Spoofing Attack, Email Hijacking Attack, HTTP Spoofing Attack, SSL Spoofing Attack and Man-in the-Browser Attack respectively. Of the aforesaid types, Spoofing attacks are the most perpetuated type of MiTM attack as stated by [6].

In the past, several techniques have been utilized to mitigate MiTM attack in the works of [7], [8], [9], [10], [11], [12], [13], [14], [15], [16] and [17] respectively they generated a lot of false negative during testing and were unable to detect Man-in-The–Middle attack and its various kinds.

In this paper, we intend to employ Bayesian Belief Networks (BBN) for detecting Man-in-The-Middle attack. Bayesian Belief Networks are 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

In the past, several studies have been conducted on detecting Man-in-the-Middle attacks and its various kinds.

In [7], MiTM attacks were detected using a static analysis algorithm called Precise Timing. The system results showed the ability to classify perpetuated MiTM attacks. However, the development and verification of the timing model for the system was very expensive, time consuming, and error prone.

In [8], a system was proposed for detecting man-in-the-middle attacks using Secure Socket Layer (SSL) certificate. The system allowed users to directly determine man-in-the-middle attack effectively. However, SSL authentication is time-consuming, it also allows insecure encryption on a network which can aid execution of a MITM attack.

In [9], a system was developed to detect MiTM attack using a protocol called SignatureCheck. The system showed the ability to detect man-in-the-middle attacks on SSL and TLS by detecting timing differences between a standard SSL session and executed MITM attack. However, digital signatures have short lifespan, highly dependent on technology, SSL authentication is time-consuming, also allows insecure encryption on a network which can aid execution of a MiTM attack.

In [10], a system was developed and framework proposed to detect session hijacking which is a kind of MiTM attack on computer network. The system showed the ability to detect session hijacking attack effectively. However, the system failed to detect the other types of MiTM attacks hereby detecting just one type of MiTM Attack which shows its biasness.

In [11] a system was proposed called MIDAS (Man-in-the-middle Distributed Assessment System). This system utilized pinning-in-the-host techniques to pinning-in-the-net techniques, by enabling mechanisms to validate certificates as they travel through a given network. The purpose of the system was to analyze between trusted and not trusted certificates as they pass through the network. The Trust in certificates was achieved using Public Key Infrastructures (PKIs), which employ trusted certificate authorities (CAs) to establish certificate validity chains. However, the system reasoning module based on Bayesian Network was never built nor implemented.

In [12], a system was proposed for detecting man-in-the middle attacks using the timestamps of TCP packet headers. The system accurately detects Man-in-the-Middle attacks with a low probability of false positives. However, the system was limited to non-mobile systems showing its biasness.

In [13], a system was proposed that detected MiTM attack based on attack behaviour pattern using a machine learning technique called K-Nearest Neighbor (KNN) Algorithm with Bregman divergence. The system results showed high ability to clearly conclude that an MiTM attack had taken place. However, the KNN Algorithm employed is a lazy learner i.e. it does not learn from the training data which is based on expert knowledge.

In [14], a system was developed that defended against MiTM Attack using Nash equilibrium and proposed a learning algorithm. The system results showed the ability to efficiently detect MITM attacks. However, the Nash equilibrium technique utilized by the system leads to untenable and sub-optimal outcomes.

In [15], a system was developed that utilized Ping Echo Analysis to detect MiTM attacks in LANs called Vesper. The system results showed that Vesper is capable of detecting end-point, in-line, and in-point MiTM attacks. However, the ping echo utilized by the system are often given low treatments by routing devices and hosts, network traffic description based on ping echo is likely to be inaccurate due to measurement errors that emanates from ping echo usage.

In [16], a system was developed to detect MiTM attacks using a machine learning technique called decision tree. The system solved the problem of selective jamming attacks in networks that leads to the execution of other attacks such as MiTM attack. However, decision trees are also prone to errors in classification due to differences in perceptions.

In [17], recent works of intrusion detection by attack techniques were reviewed especially types of MITM attacks with demonstration against SSL environment in the network layer. Awareness of MiTM attack was established and presented precautionary measures against this kind of attack. However, no system was implemented to mitigate MiTM attacks.

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 [18].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.

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

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".
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 Belief Network

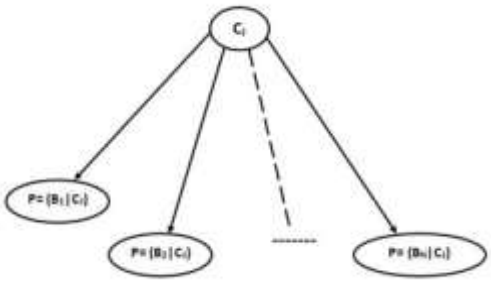

Figure 1: A pictorial representation of a Bayesian Belief Network

Some advantages of this model are: it is quite speedy in making inferences; the resultant probabilities are easy to interpret with the learning algorithm quite simple to comprehend and the model has the capability to adequately combine with utility functions to make optimal inferences. In this paper, we intend to detect Man-in-the-Middle (MiTM) attack with its various kinds using Bayesian Belief Network (BBN). A model consisting of 26 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 utilized to train the model while the remainder will be employed in testing the model. The aim of the model is to achieve a high level of detection accuracy of perpetuated MiTM attack.

4. Methodology

Simulation, Discussion and Results

The dataset used in training, testing and predicting Man-in-the-middle attack was retrieved from [19]. The dataset consist of 26 attacks and each attack has a value which represents the probability of such attack in causing Man-in-The-Middle attack. These attacks are Eavesdropping Attack (EA), Application Attack (APPA), Address Resolution Protocol Spoofing Attack (ARP), Scanning Attack (SA), Session Attack (SESA), Session Hijacking Attack (SHA), Man-in-The-Middle Attack (MITMA), Hypertext Transfer Protocol Spoofing Attack (HTTPS), Malware (MAL), Network Ping (NP), Internet Protocol Spoofing Attack (IPSA), Hacking Software Programs (HSP), Rogue Access Point Attack (RAP), Multicast Domain Network Server Spoofing Attack (MDNSS), Domain Network Server Spoofing Attack (DNSS), Packet Sniffing (PS), Port Scanning Utility (PSU), Man-in-the-Middle-Browser Attack (MITB), Protocol Analyzer (PAZ), Secure Socket Layer Spoofing Attack (SSLS), Internet Control Message Protocol Packet Internet Groper (ICMP Ping), Email Hijacking Attack (EH), Session Replay Attack (SRA), Packet Traffic Monitoring (PTM), IP Address and MAC Addresses associated with the MiTM attack. The figure 2 below shows a sample of the cybersecurity dataset utilized to develop the BBN model in figure 3.

DNSS	AI	APPA	ARPS	DNSS	EA	EH	HSP	HTTPS	ICMP	IP ADDRESS	IPSA	MAC	MAL	MDNSS	MITB	MITMA	NP	PAZ	PS	PSU	RTM	RAP	SA	SESA	SHA	SRA	SSLS
9.39E-04	0	-0.893	-1.67	0.264	1.09	-1.52	0.991	1.5	-0.298	0.888	-1.02	0.891	-1.63	0.189	-1.46	-0.681	0.478	1.16	0.306	-1.25	-1.22	0.619	0.186	-0.244	0.539	1.35	0.402
0.705496	0	0.8	-0.0364	0.89	-0.677	-0.07...	0.305	-0.0701	0.109	-1.83	0.834	0.105	0.994	0.614	-0.736	1.84	-0.506	2.76	0.0...	-0.542	0.983	0.121	-0.814	0.16	1.07	-0.857	-0.893
0.908041	0	0.206	-1.67	-0.607	0.271	-0.843	-0.764	0.0303	0.652	0.158	-0.909	1.35	0.888	0.431	1.38	-0.678	-0.983	0.317	-0.89	-3	0.129	-0.89	1.73	-0.965	1.75	1.24	0.121
0.092923	0	0.361	1.02	0.681	0.561	0.362	1.37	1.27	-0.0191	-0.367	1.72	-0.0714	-0.174	-1.12	-0.248	0.646	-0.669	-2	-0.8	-0.557	0.734	2.55	0.0494	0.38	0.443	1.2	1.3
0.367211	0	1.98	-0.746	-1.35	0.751	1.01	0.831	-1.67	-0.687	0.749	-0.0718	-0.00882	-0.267	2.29	1.23	0.783	-0.55	-0.83...	0.822	-0.14	-0.679	-0.233	-0.289	-1.33	1.01	-1.14	0.209
0.470289	0	-0.888	1.74	0.757	-0.662	0.847	-0.057	0.23	0.423	-0.0268	-0.857	1.25	0.0497	0.899	-0.0...	-0.818	0.749	1.11	-0.3...	0.611	0.77	-0.866	-0.733	0.0471	-0.798	0.428	0.851
0.89582	0	1.071	0.99	-0.498	1.51	-1.32	-0.314	-0.267	1.22	0.436	-0.146	-1.87	-2.05	-1.46	1.3	-0.443	2.42	-0.814	1.79	1.49	-0.0728	2.79	0.855	-1.14	-0.185	-0.886	-0.292
0.434698	0	1.41	0.543	1.21	1.45	1.52	-1.43	1.97	-0.225	0.221	0.564	0.438	-0.94	0.151	1.6	-1.38	1.09	-0.558	-0.7...	-0.51	0.0739	1.52	-0.858	-0.123	0.589	1.27	-0.37
0.697174	0	1.0592	0.505	0.619	-1.29	0.866	-0.874	-1.2	-0.307	-0.616	0.831	-0.355	-0.684	0.47	0.665	2.15	-0.785	1.73	-2.55	-0.144	0.214	-0.502	-0.687	0.377	-1.13	1.15	0.248
0.424777	0	0.856	0.434	-0.784	0.664	-0.382	1.91	0.471	0.238	-1.98	2.32	0.134	0.584	-0.0992	1.85	-1.83	-1.32	-0.13	0.530	-0.796	-0.0835	0.964	0.5	-0.156	-0.659	0.0317	-0.818
	0	-1.75	0.167	0.895	0.116	1.18	1.25	-0.87	-0.989	-0.319	-0.558	-0.966	-0.684	0.257	-0.0...	0.568	0.617	-0.936	0.144	1.92	1.73	0.654	-0.257	-1.42	-0.534	0.486	-0.16
	0	0.682	0.859	-0.604	-0.0283	1.11	-0.466	0.209	-0.852	-0.131	-1.15	0.901	0.0581	-0.416	0.271	-0.503	-0.0797	-1.6	-0.5...	-0.149	-1.05	-0.15	0.808	-0.667	2.07	-0.434	-0.149
	0	0.168	-1.67	0.518	0.879	0.842	0.00...	-0.384	0.98	-0.265	0.901	-0.557	0.0835	-1.68	0.424	0.795	-1.59	-0.248	0.862	0.0223	-0.927	0.664	-2.84	-0.795	0.543	0.397	1.28
	0	0.558	-0.479	0.655	-1.06	-0.675	-1.26	0.866	0.892	-0.00394	-0.0724	0.328	-0.236	-0.269	0.421	-0.00678	-1.01	-0.129	-0.4...	-1.47	0.576	-1.52	1.05	-0.444	0.352	-2.1	-0.53
	0	-0.175	-1.53	-1.39	-0.0623	-1.17	0.737	0.93	0.133	0.719	-2.95E...	1.94	0.459	0.426	0.382	-0.837	1.52	-0.06...	-0.4...	-0.0577	-1.86	-1.39	0.17	2.48	-0.341	0.134	-0.783
	0	-1.39	-0.164	0.338	2.1	1.35	-0.846	-1.16	0.14	0.0287	-1.23	-0.709	-0.234	1.24	0.555	-1.21	0.711	-0.417	0.954	-0.137	-0.572	-2.45	1.31	0.193	-1.11	-1.61	0.0548
	0	-0.303	-1.48	-0.245	-1.26	2.39	1.81	0.601	2.52	1.31	0.226	0.132	0.813	0.206	-0.203	-0.0138	1.13	0.721	0.0...	0.996	1.81	1.96	-1.07	0.89	0.52	-1.66	1.54
	0	-0.781	0.625	0.467	0.425	0.903	0.348	-0.108	-0.688	1.87	-1.49	0.689	0.283	0.473	0.273	-0.24	-0.0559	-0.394	-0.81	1.43	0.522	0.869	-0.0692	-1.63	0.236	1.7	0.539
	0	0.586	-0.725	-0.58	0.466	0.182	-0.002	-1.96	0.937	0.324	-0.239	-1.21	0.861	-1.45	1.67	0.859	-1.47	0.504	0.625	0.544	1.84	0.77	0.153	-0.128	-0.89...	-0.909	-1.66
	0	0.0572	-0.508	1.07	-0.943	1.32	1.27	0.293	1.44	0.585	1.41	0.992	0.22	-0.264	-0.132	0.709	0.238	0.978	-1.19	-0.55	1.1	-1.62	-1.07	0.429	-1.2	0.629	-1.17
	0	0.845	-1.2	1.02	1.53	-0.171	-0.189	-0.00...	-0.792	0.142	-0.365	-0.338	1.14	-0.791	0.04	-0.366	-0.472	-0.301	0.166	0.0859	-0.845	0.382	0.016	-0.839	-0.823	-0.751	1.3
	0	0.472	0.794	0.371	-1.93	1.99	0.803	0.994	1.56	-0.4	0.662	-0.487	-1.15	0.625	-1.65	-0.881	-0.765	0.333	1.36	0.152	-0.538	0.868	1.16	-0.409	-0.198	-2.72	1.27
	0	0.319	0.114	1.81	-1.98	0.684	0.0126	-0.409	-0.807	0.894	-0.979	-1.02	-0.188	-1.28	-1.07	-0.852	-1.03	0.283	-0.5...	-0.652	0.7	1.05	-1.28	-0.345	-1.93	-0.0684	-0.837
	0	0.513	-0.671	-0.617	0.695	-0.204	-0.578	1.27	0.1	0.252	-0.605	-0.251	-0.647	1.24	-0.282	1.34	-1.65	1.09	-0.0...	-0.655	0.217	1.42	0.383	0.728	-0.515	-0.438	-0.303

Figure 2: Snapshot of Cybersecurity Dataset

The Bayesian model was designed using Bayes-Server platform. The Bayesian Belief Network for predicting Man-in-The-Middle attack was designed such that the nodes on the network are linked based on the probability of an attack resulting to another. In our model for an attack to be denoted as a Man-in-The-Middle attack such attack must have perform any of the following attacks; are Eavesdropping Attack (EA), Application Attack (APPA), Address Resolution Protocol Spoofing Attack (ARP), Scanning Attack (SA), Session Attack (SESA), Session Hijacking Attack (SHA), Hypertext Transfer Protocol Spoofing Attack (HTTPS), Internet Protocol Spoofing Attack (IPSA), Rogue Access Point Attack (RAP), Multicast Domain Network Server Spoofing Attack (MDNSS), Domain Network Server Spoofing Attack (DNSS), Session Replay Attack (SRA), Man-in-the-Middle-Browser Attack (MITB), Secure Socket Layer Spoofing Attack (SSLS) and Email Hijacking Attack (EH) respectively.

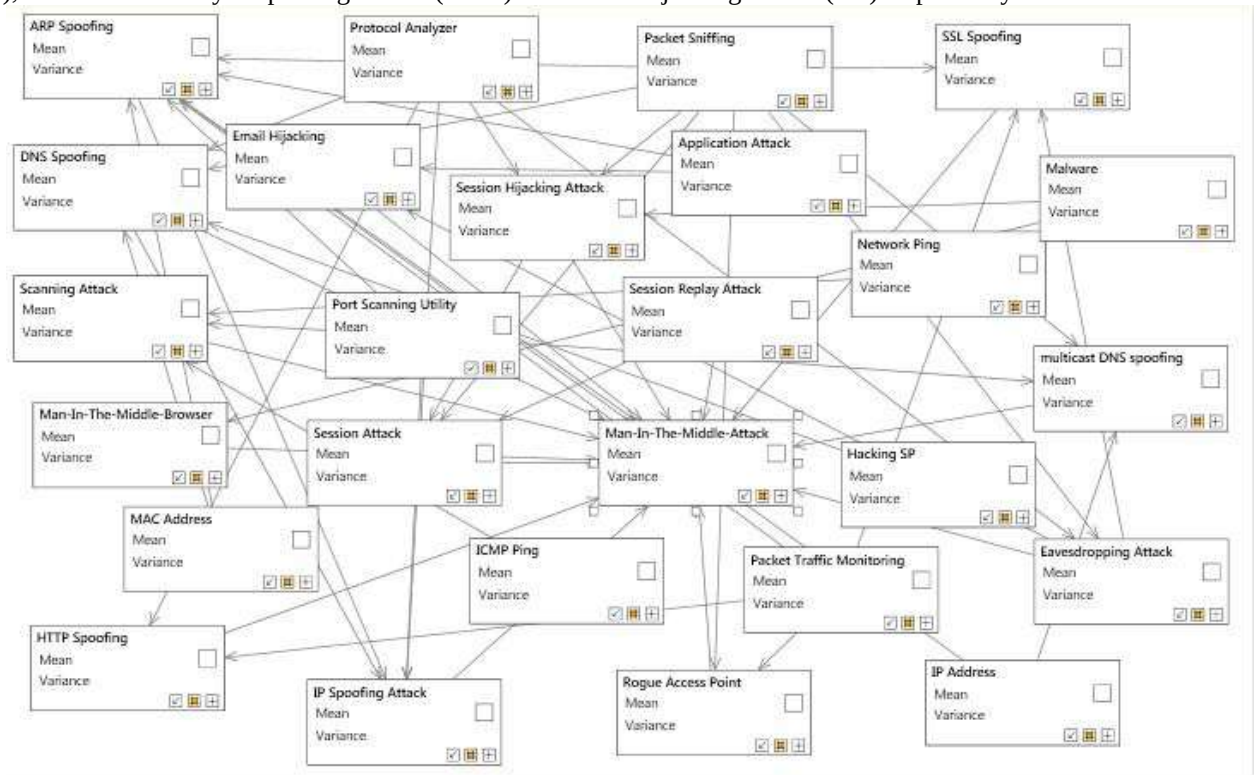

Figure 3: Bayesian Belief Network Model for Detecting Man-in-The-Middle Attack.

The above dataset in figure 2 was employed by the Bayes Server Simulator to design the BBN model for detecting Man-in-The-Middle attack and its various kinds which is shown in figure 3 below.

After designing the BBN model from the cybersecurity dataset as shown in figure 3 above, to mathematically represent our BBN model we have:

$$\text{Man} - \text{in} - \text{The} - \text{Middle Attack} = \prod_{i=1}^{26} P(\text{Attack}_i | \text{Parents}(\text{Attack}_i) \quad (2)$$

Where,
Attack: Node with an attack
Parents (Attack_i) = Nodes that converge on $\text{Attack}_{i..}$

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 2. The log likelihood value for each case was recorded.
Figure 4, 5, 6,7,8 and 9 shows log likelihood batch query chart for predicting Man-in-The-Middle attack , feature importance chart for nodes in the model, the in-sample anomaly detection chart, the log likelihood attack graph for detecting Man-in-The-Middle attack, the mesh query plot for the loglikelihood chart and Man-in-The-Middle Attack detection results chart respectively. The result generated from the simulation indicated that the network was able to predict 99% MiTM attack on the dataset accurately and it had a log likelihood of 26.21 on the test dataset.

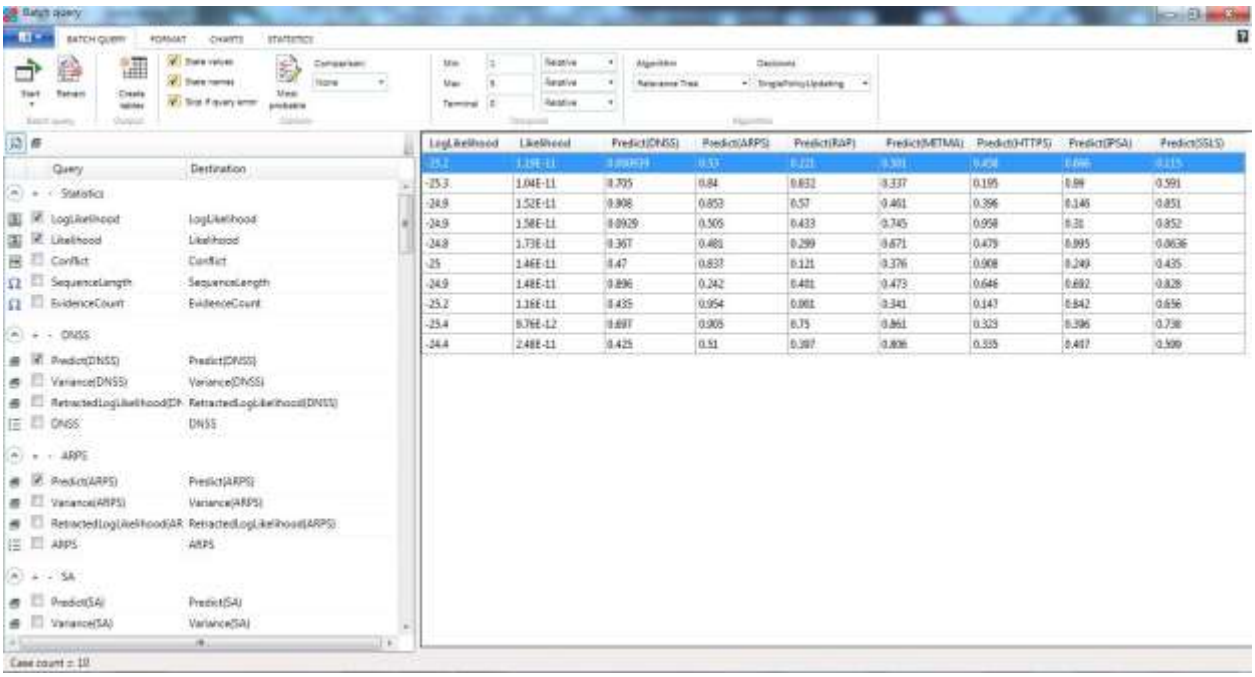

Figure 4: The Loglikelihood Chart Batch Query for Detecting Man-in-The-Middle Attack

This loglikelihood chart batch shows the result of the test data.
In Experiment 1: the value of Predict(MITMA) was 0.501 compared to 0.500827709584672 and the value of Predict(DNSS) was 0.000939 compared to 0.000939165772681049, Predict(ARPS) was 0.53 compared to 0.530423268937056, Predict(RAP) was 0.221 compared to 0.22051187591599, Predict(HTTPS) was 0.458 compared to 0.458435315306961, Predict (IPSA) was 0.666 compared to 0.665730880418207 and Predict(SSLS) was 0.115 compared to 0.114506542769504.
Experiment 2: the value of Predict(MITMA) was 0.337 compared to 0.337365793213798, Predict(DNSS) was 0.705 compared to 0.705495650811725, Predict(ARPS) was 0.84 compared to 0.840028317504334, Predict(RAP) was 0.832 compared to 0.832028302705737, Predict(HTTPS) was 0.195 compared to 0.195252655965284, Predict(IPSA) was 0.99 compared to 0.990376351715899 and Predict (SSLS) was 0.591 compared to 0.590890435110309.

Experiment 3: the value of Predict(MITMA) was 0.461 compared to 0.460851794004761, Predict(DNSS) was 0.908 compared to 0.908040834959557, Predict(ARPS) was 0.853 compared to 0.852759241898598, Predict(RAP) was 0.57 compared to 0.570365625961246, Predict(HTTPS) was 0.396 compared to 0.396265075715765, Predict(IPSA) was 0.146 compared to 0.146071005660792 and Predict (SSLS) was 0.851 compared to 0.850814013147289 through 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.

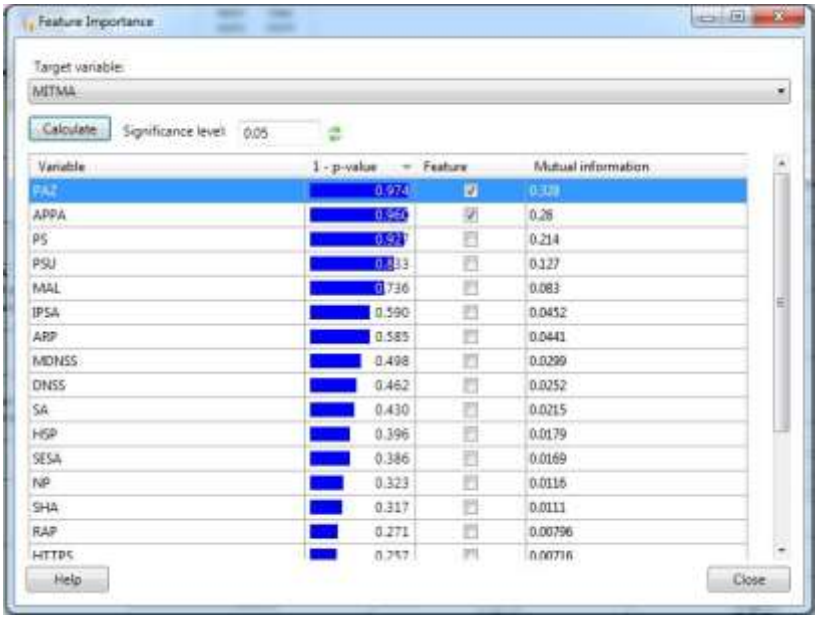

Figure 5: The Feature Importance Chart for Nodes in the Model

The Feature Importance Chart shows p-value of the variable (nodes), feature and mutual information in reference to the Man-in-The-Middle attack node.
The p-value signifies the likelihood (probability)of the nodes being involved in the execution of a Man-in-The-Middle attack.
Feature signifies that the said attack in involved in the pertuated Man-in-The-Middle attack. The check 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 Man-in-The-Middle attack node) and assigned a value.
The Significance level signifies the margin of error in the detection of Man-in-The-Middle attack.

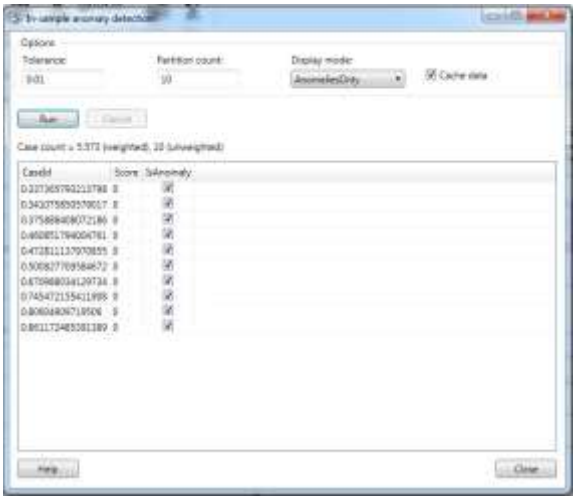

Figure 6: The In-sample Anomaly Detection Chart

The In-sample Anomaly Detection Chart shows 10 experimental results of detecting Man-in-The-Middle attack. Each Case is assigned an ID(Identification value) which is the value of the Predict(MITMA) in Figure.4.The IsAnomaly checkbox is checked to identify that each case is an executed Man-in-The-Middle attack. The 10 cases of Man-in-The-Middle attack has a case count value of 5.573 (weighted) which signifies the importance of the cases leading to a execution of a MiTM attack. The tolerance is the margin of error that could be encoutered as regards to the detection of the Man-in-The-Middle attacks.
After the BBN model in figure 3 was designed and simulated, a loglikelihood attack graph was generated and shown in figure 7 below.

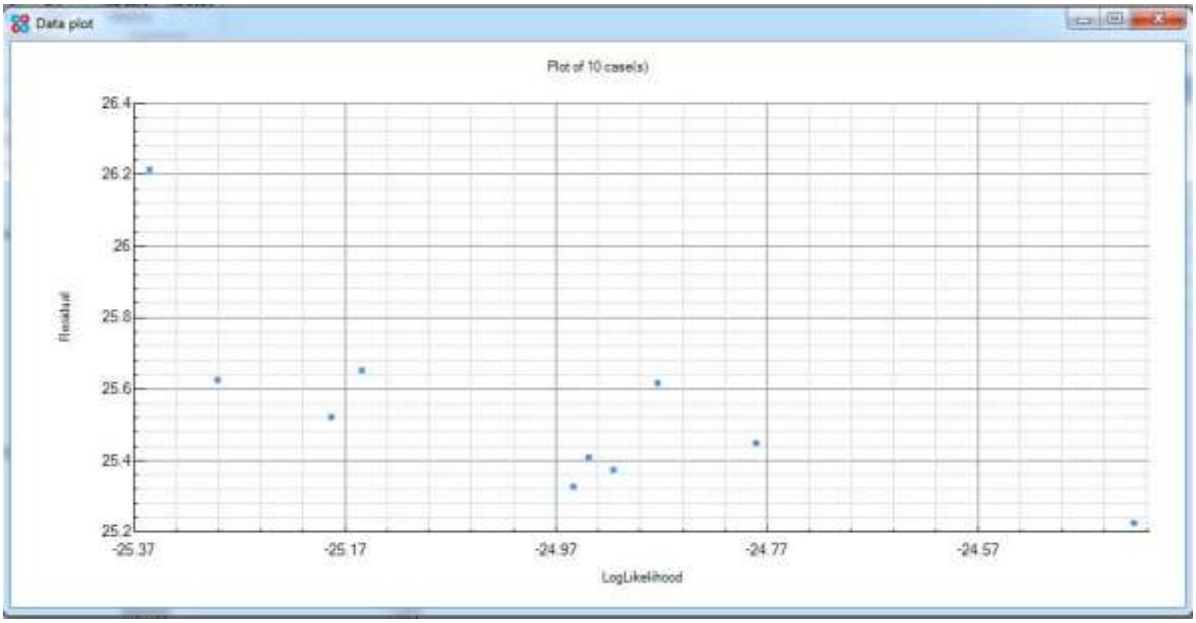

Figure 7: The Loglikelihood Attack Graph for Detecting Man-in-The-Middle Attack

This loglikelihood graph for detecting Man-in-The-Middle 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. Ideally, residual values should be equally and randomly spaced around the horizontal lines.
The values obtained from the horizontal lines on the graph are the residual values while the values obtained on the vertical lines are the loglikelihood values.
In this loglikelihood attack graph, 10 experimental cases were conducted and generated the following results: 25.21, 25.30, 25.35, 25.40, 25.43, 25.50, 25.61, 25.62, 25.63, and 26.21 residual values; loglikelihood values of -24.37, -24.79, -24.85, -24.89, -24.91,-24.93,-24.95, -25.14, 25.21,-25.28 and -25.37 respectively.
The generated results showed the progression in detecting an MiTM attack in each experimental case, as the simulation was conducted, the loglikelihood values was getting larger and closer to the optimal result. It is of note that the higher the loglikelihood, the better the accuracy. The highest values attained in the attack graph for the residual and loglikelihood are 26.21 and -25.37 respectively. Hence, the difference between the aforesaid residual and loglikelihood values is 0.84 which serves as the predicted value.
To obtain the detection accuracy percentage, we find the difference between the apex residual value (26.40) and the predicted value (0.84). Note the apex residual value stands as the 100% mark. Hence, 26.40 - 0.84 = 25.56 which is equivalent to 99.16% detection accuracy.

Figure 8: The Mesh Query Plot for the Loglikelihood of a Single Attack (Address Resolution Protocol Spoofing, [ARP]) Being involved in a Man-in- The-Middle Attack.

The mesh query plot shows the loglikelihood/likelihood of a node in this case Address Resolution Protocol Spoofing attack (ARP) being involved in the execution of a Man-in-The-Middle attack (MITMA). The Node (Man-in-The-Middle Attack.) is plotted on the Y-axis and the other Address Resolution Protocol Spoofing attack (ARP) plotted along the X-axis.
In this context, the Red contour signifies the likelihood of an ARP being involved in a Man-in- The-Middle attack with the contour ranging from interval -1.500 to 1.600 on the Y-axis and interval -1.500 to1.500 on the X-axis.

MITMA	SESA	SHA	APPA	EA	SA	HTTPS	IPSA	ARPS	MITB	EH	MDNSS	DNSS	RAP	SSLS	PROB. OF MITMA
	Present	Present	Present	Not Present	Present	Not Present	Not Present	Not Present	Present	Not Present	Not Present	Present	Present	Not Present	0.192498
	Present	Present	Present	Not Present	Present	Not Present	Not Present	Present	Present	Not Present	Not Present	Present	Not Present	Present	0.08933
	Present	Present	Present	Not Present	Present	Not Present	Present	Not Present	Not Present	Not Present	Not Present	Present	Not Present	Not Present	0.205253
	Present	Present	Present	Not Present	Present	Not Present	Present	Present	Present	Present	Not Present	Not Present	Present	Not Present	0.329308
	Present	Present	Present	Not Present	Present	Present	Not Present	Not Present	Not Present	Present	Present	Not Present	Present	Not Present	0.465701
	Present	Present	Present	Not Present	Present	Present	Not Present	Present	Not Present	Present	Not Present	Not Present	Not Present	Present	0.310025
	Present	Present	Present	Not Present	Present	Present	Present	Not Present	Not Present	Present	Present	Present	Not Present	Present	0.151956
	Present	Present	Present	Not Present	Present	Present	Present	Present	Present	Not Present	Present	Present	Not Present	Present	0.226647
	Present	Present	Present	Present	Not Present	Not Present	Not Present	Not Present	Not Present	Present	Not Present	Present	Not Present	Not Present	0.066382
	Present	Present	Present	Present	Not Present	Not Present	Not Present	Present	Present	Not Present	Not Present	Not Present	Present	Not Present	0.446881
	Present	Present	Present	Present	Not Present	Not Present	Present	Not Present	Not Present	Present	Present	Not Present	Present	Present	0.285841
	Present	Present	Present	Present	Not Present	Not Present	Present	Present	Not Present	Present	Present	Not Present	Not Present	Present	0.368753
	Present	Present	Present	Present	Not Present	Present	Not Present	Not Present	Present	Present	Not Present	Not Present	Present	Present	0.122837
	Present	Present	Present	Present	Not Present	Present	Not Present	Present	Present	Not Present	Present	Not Present	Present	Not Present	0.026813
	Present	Present	Present	Present	Not Present	Present	Present	Not Present	Not Present	Not Present	Present	Present	Not Present	Not Present	0.106678
	Present	Present	Present	Present	Not Present	Present	Present	Present	Present	Present	Not Present	Not Present	Present	Present	0.074986
	Present	Present	Present	Present	Present	Not Present	Not Present	Not Present	Not Present	Present	Present	Not Present	Not Present	Not Present	0.01488
	Present	Present	Present	Present	Present	Not Present	Not Present	Present	Not Present	Not Present	Not Present	Not Present	Present	Present	0.446255
	Present	Present	Present	Present	Present	Not Present	Present	Not Present	Present	Present	Not Present	Not Present	Present	Not Present	0.281738
	Present	Present	Present	Present	Present	Not Present	Present	Present	Not Present	Not Present	Not Present	Present	Not Present	Present	0.103375
	Present	Present	Present	Present	Present	Present	Not Present	Not Present	Present	Present	Present	Not Present	Not Present	Not Present	0.220743
	Present	Present	Present	Present	Present	Present	Not Present	Present	Not Present	Present	Not Present	Not Present	Present	Present	0.304975
	Present	Present	Present	Present	Present	Present	Present	Not Present	Present	Not Present	Present	Not Present	Present	Not Present	0.16262
	Present	Present	Present	Present	Present	Present	Present	Present	Present	Present	Present	Present	Present	Present	0.839759

Figure 9: Man-in-The-Middle Attack Detection Results Chart

The Yellow contour shows the loglikelihood of an ARP being involved in a Man-in- The-Middle attack with the contour ranging from interval -0.700 to 0.550 on the Y-axis and interval -0.960 to 1.000 on the X-axis. Figure 9 below displays the Man-in-The-Middle attack detection results derived from the simulation carried out.

This chart shows the probabilities of 14 main attacks namely are Application Attack (APPA), Address Resolution Protocol Spoofing Attack (ARP), Domain Network Server Spoofing Attack (DNSS), Eavesdropping Attack (EA), Email Hijacking Attack (EH), Hypertext Transfer Protocol Spoofing Attack (HTTPS), Internet Protocol Spoofing Attack (IPSA), , Man-in-the-Middle-

Browser Attack (MITB), Multicast Domain Network Server Spoofing Attack (MDNSS), Rogue Access Point Attack (RAP), Scanning Attack (SA), Session Attack (SESA), Session Hijacking Attack (SHA) and Secure Socket Layer Spoofing Attack (SSLS) respectively.

This detection results showed the probability of having all the aforementioned attacks involved in a Man-in-The-Middle attack denoted as:

P(Man-in-The-Middle Attack| SESA,SHA,APPA,EA, SA, HTTPS, IPSA,ARPS,MITB, EH, MDNSS, DNSS, RAP, SSLS) = 0.839759.

From the experiment it can be seen that our model has a higher residual log likelihood value which is 26.21 and a 99.16% residual loglikelihood percentage accuracy value. Comparing the 99.16% detection accuracy value from the experiments conducted by Li et al (2017) and Feng and Louise (2013) which are 94% and 89% 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

Man-in-the-Middle attack detection is very difficult because of its intelligent execution pattern. To defend a network, cybersecurity experts need to improve on existing technologies for detecting Man-in-The-Middle attacks. In this paper we utilized a Bayesian Belief Network model to predict Man-in-The-Middle attack. The network had 26 nodes with each node representing a unique attack. The BBN model in figure 3 was trained and tested and it had an accuracy of 99% in predicting Man-in-The-Middle attack. The system can be utilized 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: Man-in-the-Middle Attack Prediction, Man-in-the-Middle Attack Detection and Computer Network Security in general. Future research should be geared towards improving Man-in-The-Middle attacks prediction using Masked IP addresses and devices that utilizes network traffic signal jammers softwares.

REFERENCES

[1] Feit, J. (2017): "The IoT Can Open You Up To Cyber attacks; Stop them with Proper Security Practices". Retrieved 9th January, 2019, from https://www.buildings.com/articles-details/articlesid/21193/title/do-you-Iot-devices-risk-security-breach/

[2] SebastianZ (2013). : "Security 1.1-Part3-Various Types of Network Attacks". Retrieved 8th January, 2019, from URL: www.symantec.com/connect/articles/security-11-part-3-various-types-of-network-attacks/.

[3] Thurimella, R. and Mitchel, W. (2009): "Cloak and Dagger: Man in the middle and Insidious Attacks" IJISP 2009. DOI:10.4018/jisp.2009100704. pp 1-28.

[4] Rapid7(2019): "Man-in-the-Middle (MITM) Attacks: MITM Techniques, Detection, and Best Practices for Prevention". Retrieved from URL: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/

[5] Dobran, B. (2019):" What are Man in the Middle Attacks & How to Prevent MITM Attack With Examples". Retrieved from URL: Retrieved from URL: https:www.phoenixmap.com/blog/man-in-the-middle-attacks-prevention/

[6] Mallik, A., Ahsanb, A., Shahadata, M.M.Z. and Tsou, J.C. (2019): "Man-in-The-Middle Attack: Understanding in simple words". International Journal of Data and Network Science 3 (2019). pp 77–92.

[7] Aziz, B. and Hamilton, G. (2009):"Detecting Man-in-the-Middle Attacks by Precise Timing". Conference Paper · January 2009. DOI: 10.1109/SECURWARE.2009.20 · Source: DBLP. Retrieved From URL: https://www.researchgate.net/publication/221215527. pp 1-7

[8] Lee, J., Tu, C., and Jung, S. (2012): "Man-in-the-middle Attacks Detection Scheme on Smartphone using 3G Network". Internet 2012 ; The Fourth International Conference on Evolving Internet. Copyright (c) IARIA, 2012. ISBN: 978-1-61208-204-2. pp 65-70

[9] Benton, K. and Bross, T. (2013): "Timing Analysis of SSL/TLS Man in the Middle Attacks". INFO I-521: Spring 2012. arXiv:1308.3559v1 [cs.CR] 16 Aug 2013. pp 1-9.

[10] Feng, X. and Louise, J. (2013):"MITM Attack Detection on Computing Networks".The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue: The Proceeding of International Conference on

Soft Computing and Software Engineering 2013 [SCSE'13], San Francisco State University, CA, U.S.A., March 2013. Doi: 10.7321/jscse.v3.n3.78, e-ISSN: 2251-7545. pp 514-516

[11] De la Hoz, E., Cochrane, G., Moreira-Lemus, J.M., Paez-Reyes, R., Marsa-Maestre, I., Alarcos, B.: (2014):"Detecting and Defeating Advanced Man-In-The-Middle Attacks against TLS".2014 6th International Conference on Cyber Conflict P.Brangetto, M.Maybaum, J.Stinissen (Eds.) 2014 © NATO CCD COE Publications, Tallinn pp 209-221

[12] Vallivaara, V., Sailio M. and Halunen, K.(2014):"Detecting Man-in-the-Middle Attacks on Non-Mobile Systems". CODASPY'14, March 3–5, 2014, San Antonio, Texas, USA. ACM 978-1-4503-2278-2/14/03.http://dx.doi.org/10.1145/2557547.2557579. Retrieved From URL: https://www.researchgate.net/publication/260563099. pp 131-133

[13] Eigner, O., Kreimel, P. and Tavolato, P.(2016):"Detection of Man-in-the-Middle Attacks on Industrial Control Networks". Conference Paper · August 2016. DOI: 10.1109/ICSSA.2016.19. Retrieved From URL: https://www.researchgate.net/publication/313953467. pp 1-6.

[14] Li, S., Li, X., Hao, J., An, Bo., Feng, Z., Chen, K. and Zhang, C.(2017):"Defending Against Man-In-The-Middle Attack in Repeated Games".Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence (IJCAI-17). pp 327-331

[15] Mirsky, Y., Kalbo, N., Elovici, Y., and Shabtai, A.(2018):"Vesper: Using Echo-Analysis to Detect Man-in-the-Middle Attacks in LANs".. Article *in* IEEE Transactions on Information Forensics and Security · March 2018 DOI: 10.1109/TIFS.2018.2883177. Retrieved From URL:https://www.researchgate.net/publication/323627250. pp 1-18.

[16] Raghupathi,T, Sivabalan, M., Jeganath, S. S., Sudar, K. M. (2019):"Preventing Man in the Middle Attack Using Machine Learning".International Journal of Research in Engineering, Science and Management. Volume-2, Issue-11, November-2019, www.ijresm.com | ISSN (Online): 2581-5792. pp 327-331

[17] Efe, A., Kalkanci, G., Donk, M., Cihangir, S., and Uysal, Z.(2019): "A Hidden Hazard: Man-in-The-Middle Attack in Networks". Anatolian Journal of Computer Science Volume: 4 No:2 2019 © Anatolian Science ISSN:2548-1304. pp 96-116

[18] 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/. pp 1-2.

[19] Cybersecurity IDS Dataset (2020): "Cybersecurity Intrusion Detection System Dataset". Retrieved 25th February 2020, from URL: http://www.cybersecurity.unsw.adfa.edu.au/ADFA%20IDS%20Datasets/.