Computer and Information Science; Vol. 11, No. 3; 2018
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Machine Learning Approach to Combat False Alarms in Wireless Intrusion Detection System

D. Sudaroli Vijayakumar[1] & S. Ganapathy[2]

[1] Alliance College of Engineering and Design, Alliance University, Bengaluru, India

[2] School of Computing Science and Engineering, VIT university-Chennai Campus, Chennai, India

Correspondence: D. Sudaroli Vijayakumar, Alliance College of Engineering and Design, Alliance University, Bengaluru, India. Tel: 91-988-604-1664. E-mail: oli.sudar@gmail.com

Received: June 27, 2018 Accepted: July 6, 2018 Online Published: July 28, 2018

doi:10.5539/cis.v11n3p67 URL: https://doi.org/10.5539/cis.v11n3p67

Abstract

Wireless Networks facilitate the ease of communication for sharing the crucial information. Recently, most of the small and large-scale companies, educational institutions, government organizations, medical sectors, military and banking sectors are using the wireless networks. Security threats, a common term found both in wired as well as in wireless networks. However, it holds lot of importance in wireless networks because of its susceptible nature to threats. Security concerns in WLAN are studied and many organizations concluded that Wireless Intrusion Detection Systems (WIDS) is an essential element in network security infrastructure to monitor wireless activity for signs of attacks. However, it is an indisputable fact that the art of detecting attacks remains in its infancy. WIDS generally collect the activities within the protected network and analyze them to detect intrusions and generates an intrusion alarm. Irrespective of the different types of Intrusion Detection Systems, the major problems arising with WIDS is its inability to handle large volumes of alarms and more prone to false alarm attacks. Reducing the false alarms can improve the overall efficiency of the WIDS. Many techniques have been proposed in the literature to reduce the false alarm rates. However, most of the existing techniques are failed to provide desirable result and the high complexity to achieve high detection rate with less false alarm rates. This is the right time to propose a new technique for providing high detection accuracy with less false alarm rate. This paper made an extensive survey about the role of machine learning techniques to reduce the false alarm rate in WLAN IEEE 802.11. This survey proved that the substantial improvement has been achieved by reducing false alarm rate through machine learning algorithms. In addition to that, advancements specific to machine learning approaches is studied meticulously and a filtration technique is proposed.

Keywords: WLAN 802.11, Intrusion Detection System (IDS), False Alarm Rate, Security, Access Point (AP), Machine Learning Approaches, Wireless IDS (WIDS).

1. Introduction

Wireless networks one of the promising developments in this decade have changed the way we live and work. Current world is accessible anywhere and everywhere is the best analogy that can describe the efficiency and usage of wireless networks. Wi-Fi proved the significance of the wireless networks in terms of mobility, cost effectiveness, resource sharing and its presence where wired networks are impossible. Despite of its tremendous benefits, the major pitfall that is creating havoc in this technology is its lack of well-defined security control measures. Since the transmission medium chosen for the wireless networks is air, anybody can tune it into the specific network and gain access to it with the aid of simple wireless devices and powerful operating system. The traditional security standard that was introduced along with IEEE 802.11 standard in 1999 was the WEP encryption method where a shared key is used for both encryption and decryption. This technology failed drastically with the simple brute force attacking tools like Air snort and WEP crack. The next standard WAP was introduced in the year 2003 that provided encryption by mixing up the key and named as Temporal Key Integrity Protocol (TKIP). Cisco's LEAP was the next standard that allowed authenticated data to pass between the Access Point (AP) and the RADIUS [1].

Despite the efforts taken to identify the suitable security standard, it failed majorly with access point potential threats, weakness in application layer and encryption methodologies. Not only this, the basic component in Wireless Local Area Network (WLAN) is the access point that contributes lot of security breaches in the form of

its authorized signal range. The necessary signal range for listening to the network is much lower than that of the one necessary to make a connection, thus providing the hackers an opportunity to listen to the network without many efforts. The other form of security attacks in accordance with AP can happen due to its poor configuration or unauthorized Rogue AP. Other security vulnerability apart from AP also exists and one such comes in the form of frames [2]. WLAN can produce three types of frames like management, data and control frames at the Medium Access Control (MAC) layer. Currently available WEP,WPA, WPA-2 standards can protect only Data frames. This opens up lot of oppurtunities for the hackers to perform efficient spoof attacks especially termed as Denial of Service (DoS) attacks that can be invoked in almost every layer of the WLAN. Typical DoS attacks involve flooding the network with traffic choking the transmission lines and preventing other legitimate users from accessing services on the network. This clearly gives us an idea that the weakness exist in network, application as well as in Link layer. To combat these types of attacks and to protect the network, a system that can basically work well on unencrypted data, that has complete knowledge about the network in the form of the users, APS and Rogue and the actions to take if we detect an unauthorized access point. With this information in hand, it becomes easy for the administrators or for the underlying system to protect the network from unnecessary attacks. Such a system is being coined as Wireless Intrusion Detection System (WIDS).

An intrusion detection system can informally be in analogy with the security camera installed in an organization that can basically monitor and track all the activities happening in an organization. Like a security camera an IDS can monitor the wired and wireless networks for intruders and create an alarm. WIDS dynamically monitors the events of a host or a network, analyze and report on possible unauthorized attempts. These unauthorized attempts typically termed as alarms and they are generated whenever the detection system come across any event that can directly or indirectly harm the network. The general form of attacks that the WIDS can identify are AS leap attack, Association frame flooding, authentication frame flooding, broadcasting de-authentication, EAPOL packet flooding, Invalid MAC OUI, Null SSID probe response, spoofed De-authentication, long duration attack and weak WEP detection. Identifying and isolating the real alarms from false alarms remains as an unsolved problem because of the reasons listed [5]:

1. False alarms differ only slightly to an extent that only the context can say that the alarm generated is false.
2. Alarms are generated which varies depending on the environment. i.e., actions that are normal in some environments may be malicious in other environment and that can ultimately raise a false alarm.
3. It is completely unmeasurable to identify and describe the number of signatures to discriminate the false and real alarms.

In real world scenarios, despite the efforts taken to intelligently identify the true alarms with the predefined classification, it becomes impractical to separate the alarms that are harmful. To combat the false alarms, a solid understandability of the different types of false alarms and the primary reasons for generation should be studied so as when it comes to reduction it becomes easy for us to distinguish true and false alarms. Further studies revealed that the contributing factors for false alarms are network protocol, network architecture and inherent challenging issues. Depending on these factors, the more meaningful and specific categories of false alarms are as follows:

Reactionary Traffic alarms: Traffic that is caused by another network event, often non-malicious.

Equipment-related alarms: Attack alerts that are triggered by odd, unrecognized packets generated by certain network equipment.

Protocol Violations: Alerts that are caused by unrecognized network traffic often caused by poorly or oddly written client software.

True False Positives: Alarms that are generated by an IDS for no apparent reason. These are often caused by IDS software bugs.

Non-Malicious alarms: Generated through some real occurrence that is non-malicious in nature.

Along with this, understandability of the major triggering mechanisms used in WIDS is essential so that the intelligent techniques employed to isolate the real alarms from false alarms to be more accurate. The most common form of triggering mechanism used are anomaly-based detection otherwise referred to as profile-based detection, in which every user who is using the WLAN is created with a profile and their normal activities are monitored. At any instant if the WIDS come across any activity which is deviated from their normal activities then an alarm is produced from the WIDS. This method serves as an efficient technique to detect insider attacks as well as account theft. However, the obvious disadvantage with this technique is the system should be trained to create appropriate user profiles. This method is more prone to false alarms. Misuse based detection or

signature-based IDS are generated based on specific attack signatures. This methodology provides some very less false alarms. However, it becomes highly impossible to update the signature frequently. The complete analysis gave us an idea that false alarms remains as a contributing factor that can reduce the overall efficiency of the Wireless Intrusion Detection System.

To mitigate the problem of false alarms and to improve the performance of detection system, we are trying to design a machine learning based intelligent filter that can identify and analyze the false alarms accurately so that there is a drastic reduction in the rate of false alarms. The contributions of this extensive survey are summarized as follows:

This paper presents a survey regarding the existing methodologies to solve the problem of false alarms in four aspects namely ontology-based approaches, Mining Approaches, heuristic and machine learning based approaches.

This paper proposes a machine learning based false alarm filter that follows the traditional steps of reducing features and in filtration process, our focus mainly concentrates in finding out the suitability of traditional machine learning algorithms in wireless intrusion detection system.

Another proposal of this work is to use the AWID dataset, where meagre amount of work is done using this dataset compared to the DARPA, KDD and Trace Dataset. Here, it listed the relevancy of this dataset especially in wireless networks.

This paper is organized as follows: In section 2, we discuss the different approaches followed traditionally to decrease the false alarm rate with the conclusion of machine learning approach and its importance in wireless intrusion detection system. In section 3, the features of AWID dataset and its relevancy in designing the filter is discussed. In section 4, we present the machine learning based false alarm filter. In section 5, we suggest some suitable machine learning algorithms and the way to improve the performance in wireless networks. Finally, we conclude our paper in section 6 with highlighting the features of this work.

2. Traditional Techniques to Reduce the False Alarms

Computer network has two major classification namely wired (infrastructure) and wireless (infrastructure less) networks which are based on the topology. Similarly, the different IDSs are used separately for these different networks namely wired intrusion Detection system with wireless Intrusion Detection system. Here, the only difference is network topology and the requirement to scan air than wire [1]. The above said point ponders that the methodologies tried generally for reducing the false positives in wired network can help us to arrive at a more efficient methodology to minimize the number of false positives. Traditionally, the network intrusion detection system false alarms are reduced by dealing the problem by following any of the four approaches namely ontology-based approaches, mining, heuristics and machine learning based approaches. Moreover, wireless intrusion detection system is no exception to this.

This section discusses briefly about all the work that revolves around these categories. This entire survey considers only the anomaly-based detection mechanism as they are more prone to false alarms as this method completely takes decision depending on the behaviour of a user. Moreover, it is always not essential that the user must follow the same pattern of behaviour when the user is trying to access the network. Certain unexpected behaviour from a legitimate user always persists and this unusualness should not be identified as malicious and that ultimately triggers a false alarm. The above-mentioned methodologies are provided some noteworthy research on solving the false alarm problem. However, we can't ignore the fact that these techniques have its root with some of the preliminary approaches like fine tuning procedure that worked by adapting a signature policy. Even though this technique opened its doors towards handling the false alarms it was a trade-off between the reduction and security level. Manual assistance in examining, updating the environment and the concept of acknowledging the alarms depending on the operating system [18] reported this procedure to be less effective. However, there was a clear understanding about the number of false alarms on an average generated in any intrusion detection system for a day motivated for further research.

Another major research issue is claimed that the false positives are arises in any intrusion detection system because of the lack of correlation between the input and output [19] termed as APHRODITE. This system is defined with two components: output anomaly detector that refers to the predefined statistical model which holds all the possible normal behaviour and any deviation was flagged as an attack generally used to monitor the output of the system. Correlation engine specific purpose was to correlate the input to the output. The process of the identification of the threats was made by tracking and combining the input and output traffic. Bolzoni and Etalle [19] shows the similar research stressing in their work on a very simple concept of generating as many

number of alarms as they are and then compare this alarm with statistical model, monitor the input and output traffic, if a match is found in the statistical model report as a false alarm. This survey clearly denotes that this was the starting point for dealing the false positives problem using the modernized artificial intelligence technique.

An alternative to the traditional alarming technique can be performed by modelling a specification-based Model [5]. This model primarily uses a wireless sensor that can monitor the spectrum and construct a state transition model for each AP and STA in that spectrum. The state transition model denotes the series of actions that must be taken for the association of STA and AP. Anomalous transition is something that is observed with the frames in the state transition table. Every frame is evaluated against the specification which is configured in the sensor and if it results in a security constraint, alarm is generated. This model was analysed using the snort-based tool and monitored for the changes in transition model, and this generated low rate of false positives. Since this methodology is completely based on the state behaviour, threshold tuning would be helpful to provide a better solution. With these preliminary approaches, the research towards false alarm rate reduction narrowed down to the below categories.

2.1 Data Mining Approaches

Lot of valuable research is done for the creation of effective intrusion detection system using data mining approaches, which basically extracts knowledge from larger database and using that knowledge to build a concept, rule, law or model. Then we try to find a relationship from extracted knowledge that will help largely in decision making. Interestingly most of the researches performed using the date mining concepts concludes that the accurate detection methodologies can reduce the number of false alarms in intrusion detection system. The beauty of mining is most appropriately used in the alert processing technique [20]. Detection phase and alert processing techniques was dealt differently by many people but common idea behind every research lies with the statistical modelling, decision tree classification. In most of the mining approaches, alert correlation analysis is performed by the usage of clustering and merging functions to recognize alerts that corresponds to the same occurrence of an attack and then creating a new alert by combining the data from similar alerts. One very important work with respect to data mining is to find alarm clusters and generalised forms of false alarms to analyse the root causes [21]. This cluster-based study identified that more than 90% of the false alarms are generated from a very small subset of root causes. Despite the idea looked very promising, this could reduce only a percent of the false alarms.

Rupinder Gill et al [6] derives the conceptual understanding from the age-old data mining concepts as it possesses the feature of describing behaviour from a given large data set. They demonstrate that the implementation of WIDS based on statistics. Combining these concepts an algorithm that can statistically measure the similarity of management traffic clusters between a long term and short-term performance is presented. The methodology presented in their work concentrated on the management frames which is generally created whenever the stations tries to associate a connection, i.e., the stations create management frame and send it to AP for its association. The activities that are associated with the frames are scanning, joining, leaving are grouped into a cluster which results in a different cluster pattern for every event. This management cluster frames if analysed systematically, WIDS can tell the type of event occurring. This work has created a test bed with five clients, one attacker and one sniffer to observe the traffic. Considering window size and sample interval as parameters this algorithm tried to identify the patterns of every cluster and report any unnecessary events. This methodology kept in mind that the false alarms are better than missing events, so more emphasis is kept for not any missing events which practically put a barrier on the prediction in real time analysis.

Another work [48] has dealt the correlation phase as duplicate removal and consequence correlation. As the name signifies, duplicate removal looks for specific configuration file and identify the instances of the same attack using the rules. Consequence correlation includes five functions alert base management, alert clustering, alert merging, alert correlation and intention recognition function. Management receives the alerts generated from WIDS in IDMEF format and stores it in relational database for further analysis. Alert cluster and merging function accesses the database, uses a similarity function to cluster and merge the alert. A pure statistical causality analysis doesn't require predefined knowledge about attack scenarios but uses causality analysis to correlate alerts and constructs attack scenarios. This work was helpful in identifying new attack scenarios.

Despite the tremendous research performed in this category there are some open problems and disadvantages related to the studied techniques.

- Most of the proposed techniques act in an off-line mode.
- Some of these techniques are depended to human analyst for training phase or developing filtering rules.

- Another problem associated to some of the proposed techniques is the lack of accuracy.

This extensive study on the datamining approaches gave us a clear idea that most of the approaches revolved around the alert processing technique which can be used as a starting point for dealing the false alarms problem without human dependence especially in machine learning approaches.

2.2 Heuristic Approaches

The growth of technology is massive, and we are all living in a situation where we try to identify a heuristic methodology for every concept under study. False Alarm rate detection is no exception to this and the idea of designing a heuristic approach to reduce the false alarm is proposed by Wenche chow et al [7]. Even though, the specification model tried to identify the solution for giving a novel understandable solution for making the system to learn by itself. The viable difference lies in heuristic approach, which concentrated on identifying the intrusive behaviour of a node rather than the specific attack. The technique proposed is simply by sniffing the packets of 802.11 whatever packet captured is checked for its owner and its origin by just converting the frame from its hexadecimal format to decimal format and a comparison is performed between the MAC and 802.11 frame. Signatures are basically verified, and this process is repeated for every upload file so that an alarm is generated which showed some promising results. This approach showed promising results, however the testing was done for 20 values and the efficiency of this approach with the more signature can be studied. The concept of studying the framework for a distributed intrusion response engine based on alarm confidence, attack frequency, accessed risks are estimated and produced a response matrix for detecting attacks is proposed by Lim et al [9].

Danziger et al [13] conduct a thorough study about the different types of attacks existing in WLAN 802.11 is given and then the idea of blending the 802.11 with WIDS and identifying the false alarm is implemented. The most common form of attack identified in wireless networks is DoS, the SSID from where the attack originated is identified and the corresponding management frames are studied. This frame value is compared with the existing threshold value and the identification of alarms is generated. The same principle applies to the other types of attacks as well. This model failed to explain about on what factors the threshold limit can be set [14]. This factor is one essential component that should be identified and set in a proper format in the problem statement.

Borsc and Shinde [15] developed a Wi-Fi-EWS model in which the methodology is implemented as two level defenses. First level looks for anomalies, and a systematic learning mechanism is used to track the timings of wireless transmissions. At the second level, a state transition model is built and then querying the historical data is performed. Results evaluated in this methodology are quite the same proposed by Tade and Timothy [5]. Elankayer Sithirasenan and Vallipuram Muthukkumarasamy [16] tried to match sequences of audit records to the expected audit trials and the usage of various tools is clearly identified and studied.

2.3 Ontology Based WIDS

Semantic Web techniques and methods like concept of “content” and “ontology” can be used in many fields of computer science. Classification tools for unlimited events can be obtained using ontology and it can analyze user behavior, system activities and abnormal behavior. With this basic idea of ontology, it tried to extract semantic relations between computer attacks and intrusions. Ontology constructions are done based on the computer attacks and every method incorporated consists of some agents and master agent. Every time the agents come across a suspected condition, they send a report to master agent and the master agent verifies its ontology and takes relevant action [32]. Research in this area is very minimalistic and most of the work revolved around these four aspects: target centric ontology, relationship between features, hybrid ontology and master IDS agent model. The target centric ontology is characterized by system component, Means of Attack, Consequences of Attack and Location of attacker. The simple taxonomies are replaced by ontologies and an initial ontology construction for intrusion detection system is proposed [50]. Hybrid ontology tries to combine the syntactic and semantic features as it believed that the syntactic match alone is not sufficient as they are based on prefix substring and suffix matching. Most of the work reused the ontology with older set of attacks. Ontology is an iterative process. Because of these drawbacks, very few research works are performed in this area.

To summarize, this survey gave us an idea about the different approaches that can be thought of to deal the false alarm problem in intrusion detection system. Some of the common problems which was observed in these approaches are

1. Analytical module uses a limited portion of source information, so the detection capability is limited.
2. Continuous scanning of the network traffic affects adversely the performance.

3. Inability to handle encrypted data packets.
4. Upgradation to newer standards is difficult.
5. Some requires alteration in the 802.11 protocol.

We need a human independent solution that can process millions of data points each minute and automatically identify anomalous behaviour. The most notable difference between machine learning and statistical approaches is that the latter in general is based on understanding the process behind the generation of the observed data. Machine learning in contrast focuses on a system that can improve the detection rate by learning from previous results, therefore being able to adapt their strategy over time.

2.4 Machine Learning Based WIDS

Machine learning based intrusion detection can be viewed in two perspectives as approaches based on artificial Intelligence and Computation Intelligence. There is a strong bonding between the artificial intelligence and Machine learning which can be well explained as writing a very clever program which has human like behaviour can be artificial intelligence, if the program's parameters are automatically learned from data, it is machine learning. This strong relationship between these led us to do a further research in the role of artificial intelligence in intrusion detection system. Artificial Intelligence techniques revolve around some well-known concepts like statistical modelling while computational intelligence concentrates on evolutionary computation, fuzzy logic, artificial neural networks and artificial Immune System. Computational Intelligence differs from artificial intelligence with the underlying representation. Generally artificial intelligence uses symbolic representation whereas Computational Intelligence uses numeric representation.

Most of the approaches under the artificial intelligence concentrate on the development of cognitive models that can perform the activities of clustering, correlation and prioritization under single roof. Mansour et al [23] tried to discover the structural relationship using the interference technique in fuzzy cognitive modelling. Alert clustering refers to simple grouping of common attack patterns, correlation concentrates on finding the relationship between patterns, common feature values between two alerts are compared for a perfect match to develop a unified alert fusion model that can reduce the number of false alarms. This work by long [24] have suggested a clustering algorithm for discriminating the IDS true alerts from the false positives. In this work, he understood that one major problem raised when they tried to analyze the alarms was the diversity of formats used by different vendor, so a unified framework for IDS alerts was essential to handle the alarms efficiently and came to the existence of IDMEF. The proposed clustering algorithm worked with this measure. Along with this a combination of mining and fuzzy came in this technique proposed by Long et al [25] which followed mining concepts to build the clustering algorithm and the same old root cause analysis was done to provide a cognitive model.

One of the works that is going to be used as a starting point for our proposal is well described in [50]. This work of generating a filter-based feature selection method, one of the preliminary approaches of reducing the number of features in the dataset to identify the best features that can be suited for prediction. This work already showed some comparative results that can be used as a conclusive benchmark for our feature selection. KDD cup dataset consists of nearly five million training samples and two million testing samples that not only contributed in terms of computational complexity but can also reduce the efficiency with more number of redundant samples. Here the data pre-processing is performed by following the traditional steps of transferring and normalization. Feature selection is performed by using the appropriate mutual information and linear correlation co-efficient algorithm and the classification is based on support vector machines. With this information, the points that is still unexplored in this work is that the feature selection methodology wasn't been tested for network specific data and the suitability of these algorithms in wireless networks remains as a question mark. Thus, in our proposal we are going to test the adaptability of these feature selection algorithms in wireless networks by considering the network specific data as well.

Another interesting work in which a specific machine learning based wireless intrusion detection system was created for detecting and recovering from DoS attacks. This work believed that the accuracy of any intrusion detection system depends on the classifier and the classification was carried out as a two-step process with the training phase to build the classifier and the performance of several classification algorithms is analysed. Major algorithms like Bayesian, Ad boost, SVM, RIDOR are all tested for its detection rate and false alarm rate. An approach named as Additional Localization Approach mentioned in [32] can be applied to both open as well as encrypted networks, which used RSSI and AoA localization approaches for detecting the existence of flooding-based DoS attacks in a Wireless network. This research tried to cover up some of the drawbacks which we mentioned earlier, and the architecture consisted of knowledge base, intrusion Detection system and

Localization Module. Here they concentrated to decide the best classifier algorithm for accuracy and detection. The comparison results are mentioned in table 1:

Table 1. Comparison of Various Classification Techniques

Classifier	Accuracy	Detection Rate
Naïve Bayes	0.683	0.934
BayesNet	0.954	0.88
SVM	0.987	0.578
Ridor	0.955	0.903
ADTree	0.96	0.922
AdaBoostM1	0.954	0.957

The above results prove that the AdaBoostM1 classifier algorithm showed promising results for achieving better accuracy and detection if the type of attacks is Denial of Service (DoS). From this work, we decided to try on the other attacks as well and use the classification algorithm that can yield promising results irrespective of the type of attacks. As mentioned, this work tried to build a WIDS that can handle the DoS attacks, however it failed to address MAC layer attacks and they have used 18 features to identify the attack, reducibility of features is what we need to concentrate. The ideas derived from this work can be used as a base for building our dataset and selecting the features, however more emphasize is to be given for recent machine learning classifiers.

Another interesting work that concentrated to study specifically the MAC layer attacks in which the feature selection dataset followed the traditional methodology, however the feature selected consisted of the MAC address. They have tried to explore the impact of MAC address mapping schemes on the cross-platform robustness of machine learning based intrusion detection system. This work can also be used as a base for understanding that the same methodology of feature selection, formatting and classification can very well be used not only for DoS but also for other forms of Wi-Fi attacks. Another well-known attack with respect to wireless networks is probe request attacks and an intelligent approach to deal with these attacks is presented in [3]. Here, they have built a prototype to detect the probe request attacks using neural networks is trained using MATLAB and the network was trained using the back-propagation algorithm to detect an external attacker. With this approach, they have successfully discriminated a rogue frame than a genuine frame and with this approach we can justify that even the probe request attacks can be detected efficiently by using the machine learning approach. Another common type of attack found in WLAN is the man in the middle attack (MITM) that can be detected MITM by observing abnormal variation of network measurements with its empirical data such as delay and signal strength. Here they have proposed a novel method to identify MITM by analyzing and obtaining the mean and deviations of the round-trip time and received signal strength. Presence of attacks is identified by using the longer delay and larger standard deviation in round-trip time. To locate the Man-in-the-Middle attacker, they have the traditional machine learning algorithms like Naïve Bayes, Support Vector machine learning algorithms and concluded that Gaussian naïve base shows better results for MITM [35].

One of the notable research that used a novel approach using machine learning technique to identify true positive is presented in [35] as Adaptive Learner for Alert Classification. Here they have constructed a classifier that gets instant updates from the analyst which helps the system to update the classifier automatically. This continuous updating builds up the system knowledge base so that it can minimize the number of false alarms. This method offered a great efficiency in terms of operation that failed as it completely dependent on the analyst accuracy and faced lot of difficulties when it was tried in real time analysis. ALAC was designed to operate in two modes: a recommender mode, in which all alerts are labelled and passed onto the analyst, and an agent mode, in which some alerts are processed automatically. In recommender mode, where it adaptively learns the classification from the analyst, false negative and false positive were obtained. Where in the agent mode, some alerts are autonomously processed (e.g., false positives classified with high confidence are discarded). In this system, a fast and effective rule learner was used that is RIPPER. It can build a set of rules discriminating between classes (i.e. false and true alerts). The number of false alerts is reduced by more than 30%. This system has a disadvantage that is during a system's lifetime the size of the training set grows infinitely.

Later, he extended his previous work in [27] and presented two complementary approaches for false positives reduction: CLARAty which is based on alert post processing by data mining and root-cause analysis and ALAC which is based on machine learning. CLARAty is an alert-clustering approach using data mining with a modified version of attribute-oriented induction [27]. Using this system, the number of alerts to be handled has been

reduced by more than 50%. He has released a complete document of his work in 2006 [28]. Another promising ability of artificial intelligent technique is its pattern recognition ability. Several studies have been undertaken to improve the alert correlation mechanism by artificial intelligent technique. In this work [36] alert fusion is a process of interpretation, combination and analysis of alerts to determine and provide a quantitative view of the status of the system is being monitored. This method uses the cause and effect events to interpret the data which could lead to the identification of attacks. This technique was not able to discover the casual relationship among alerts or it required large number of pre-defined rules in correlating new alerts. Siraj and Vaughn [37] considered some of the well-known algorithms like decision trees, k-nearest neighbour, multi-layer protection and support vector machines to perform a comparative analysis if the system follows a classification approach and clustering approach. This analysis gave us an insight these algorithms can reduce false alarms if clustering is employed. This study gave us an idea that machine learning is better for finding variations of known attacks rather than previously known malicious activity.

Computational intelligence-based approaches use genetic algorithms [38] that can create rules for an expert system and the training sets are generally created by the analyst for rule development and decision support. Support Vector Machines belongs to a set of classifiers that simultaneously minimize the empirical classification error and maximize the geometric margin. The process involves creating a hyperplane in N-dimensional space that would separate two data sets with highest margin [39]. Support Vector Machines classify data by determining a set of support vectors which are members of the set of training inputs that outline a hyperplane in the feature space. Support vector machine using a kernel function provides a mechanism to fit the surface of the hyperplane to the data. Their method offered a great efficiency in terms of operation. However, the system working procedure without an analyst role is unexplored. The ideas derived from their work can help us to conclude that alert processing technique can be well used in our proposal.

This work [9] is quite interesting as they used the computational intelligence techniques that can be deployed easily in network security [10, 11]. Associating the danger theory and Artificial Immune system produced an intelligent system that are the key components of multi agent systems and tried to identify the active and passive attacks in 802.11. This work is an extension of the model proposed in [12] in which the anomalies are detected using the Immune Based Agents. The methodology followed in this scheme is a test bed is created using five workstations, one server and one AP. JADE is used as a framework air crack ng was the tool for attack and the experiment was conducted based on attack. The results analyzed in this methodology showed very less number of false alarms. This methodology can be further improvised by performing the analysis for both active and passive attacks. Mayank Agarwal and Sukumar Nandi [33] concentrate in genetic programming and artificial neural networks that can help the system to decide on untrained attack with its trained ability. We tried to evaluate all the algorithms that fall under the machine learning approach that can help us to build a resilient intrusion detection system that eventually reduces the false alarms.

Later, Law and Kwok [50] proposed a method using KNN classifier that works by using the Euclidean distances. They created a model that shows the sequence of incoming alarms which are normal and any deviations from this model was identified as anomalies. Initially lot of machine learning work concentrated on applying supervised learning algorithms that requires number of labelled instances for training phase. As far as the intrusion detection system it's better to avoid human intervention so the necessity for semi supervised learning increased. The idea of using the semi supervised learning can make the false alarm rate more realistic. Another concept of active learning is a form of supervised machine learning that has the capability of interactively querying the user for information by using the classifier and query function. By combining the active learning and semi supervised learning the unlabelled data can be used effectively in intrusion detection system.

With these meticulous studies, we can explore few of the points that remain unaddressed and if it is addressed effectively can help us to achieve better results. Most of the researches in machine learning tried and achieved the results using the KDD 1999 Cup dataset, the problem of evaluating the robustness of machine learning techniques in real networks is still unexplored. In terms of attacks, most of the machine learning approaches concentrated on DoS and very few works considering other wireless attacks. Alert verification and correlation techniques showed promising results, however it failed when it comes to the methodology to collect and determine the appropriate contextual information. Many WIDS approaches using machine learning to combat false alarms are unable to detect recent unknown attacks and others were not able to provide a real-time solution. In the next section, we will try to address the issues that were commonly found in the machine learning approaches and come up with a solution that can effectively reduce the false alarm rate.

2.5 Data Pre-processing and Filtering

Filtering and pre-processing is an essential step if we must perform any operations related to the intrusion detection system as even for a very small network large amount of data is generated. The larger number of attributes in dataset produces will increase the computation complexity and decreases the redundancy. In pre-processing the raw intrusion alarms are formatted to a standard format in which the processing using the machine language algorithm becomes easier. Once the standard format is acquired, it becomes easy to identify the redundant alerts that in turn can decrease the computation complexity. The standard procedure for performing the pre-processing is formatting, cleaning and sampling. Formatting is a process that converts the standard format in which we acquired the data into the one that can be used for further processing. Cleaning is generally carried out to remove the incomplete data instances that may not be useful for processing. Sampling reduces the number of data instances by grouping similar alerts with the available techniques like clustering and aggregation that can make the analysis process easy. Filtration process should be carefully done as wrong filtration might remove the alerts that are necessary. In most of the situations, depending on the machine learning tools we use, pre-processing can be iterative. Filtration process are generally performed by using any of the approaches like human expert analysis, WEKA, R machine learning package, MAO, ELKI, Rapid Miner etc.

2.6 Wrapper Based Feature Selection

Feature selection becomes unavoidable in performing the analyses of intrusion detection alarms as some of the features may be redundant and some feature may not useful for our analyses. So, consistency should be maintained to select the best features for our analyses. As known, there are two types of feature selection method: filter based and wrapper based. Both the methods hold goodness in terms of certain factors, the wrapper method is best in terms of accuracy. So, if we employ the wrapper method it goes undoubtedly the best feature set is generated. A suitable algorithm will be used to perform the feature selection. Once the appropriate feature set is obtained, combining the alerts with same attributes is performed and the relationship that existing among the similar alerts also analysed so that we can obtain a complete minimalistic dataset for further processing.

2.7 Machine Learning Algorithm based Feature Selection

In this section, we are trying to identify the best machine learning algorithm from the pool of algorithms by evaluating some of the well-known algorithms like OneR, Adaboost, J48, decision tree, Random Forest and Random Tree. The Waikato Environment for Knowledge Analysis (WEKA) toolkit can be used for performing the same. We will be using a decision value that can possibly predict the accurate number of false alarms. With our proposed method, we are trying to achieve the double filtration process that can effectively reduce the number of false alarms.

3. Results and Discussion

Some of the results that are derived from some works can be used as some parameters that can aid us in the development of false alarm filter. Some of the earlier results obtained in terms of evaluating the performance of machine learning algorithms from various sources are presented here. Most of the algorithms provided 90% classification accuracy with random tree acquiring the top position. Another point that was observed with respect to the network intrusion detection system using the AWID dataset indicated removal of low rank features didn't improve the classification accuracy and it can only be achieved by following different feature reduction levels. So, it becomes unavoidable that continuous evaluation of datasets is extremely important to achieve the highest accuracy. This result evaluated can be taken as a benchmark for our false alarm filter.

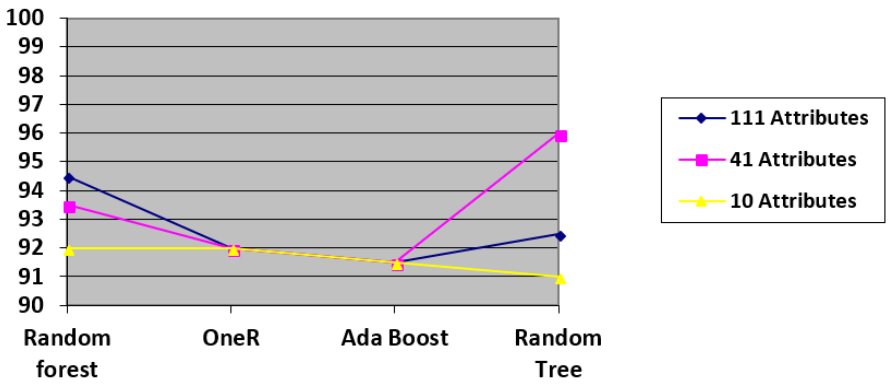

Figure 1. Performance evaluation of various machine learning algorithms

Another interesting result obtained from based on snort alarms that took 8 features description, classification, priority, packet type, source IP address, source port number, destination IP address and destination port number. Conversion of snort alarms to standard alarms is depicted in table 2:

Table 2. Snort Alarms Feature Selection

Features		
Description	ICMP PING	Attack Responses Invalid URL
Classification	Misc Activity	Attempted Information Leak
Priority	3	2
Packet Type	ICMP	TCP
Source IP address	194.7.248.153	207.200.75.201
Source Port Number	0	80
Destination IP address	172.16.113.204	172.16.117.103
Destination Port Number	0	12624

After the feature reduction process, they have derived one very important equation of using the decision value to identify the false alarms effectively. This looks promising and the idea of adaptively selecting the machine learning algorithm is also discussed. This feature set can be used as a benchmark for our false alarm filter.

4. Suggestion Proposed

The end of this survey provides us a solid research conclusion that machine learning technique is able to produce better or more concise rule if the background knowledge is used appropriately for the classification. We have also understood that the anomalies fall under these three categories namely:

1. *Point Anomalies:* If an individual data instance lies outside the boundaries of normal region of data.
2. *Contextual Anomalies:* If an information occurrence is anomalous in a precise context.
3. *Collective Anomalies:* If collection of data instances is anomalous with respect to the entire data set.

The mentioned anomalies are concentrating on only one thing i.e., to gain knowledge about the network infrastructure internals. Many WIDS approaches using machine learning to combat false alarms are unable to detect recent unknown attacks and others were not able to provide a real-time solution. This section helps to understand about the primary reasons for false alarm generation and with the help of false alarm filter and also try to reduce the false alarm rate considerably.

Current machine learning algorithms are not suitable to use in real time network as it might require some changes in the protocol itself. So, if a standalone filter is created that doesn't require any alterations in the protocol would be satisfactory. And the filter if it undergoes double filtration process can reduce the false alarm rate considerably. The intelligent filter that is proposed by us is not going to perform something which is not mentioned in the traditional methodology. However, this survey guides the researchers to follow different algorithms that can perform the double filtration process. Constructing a false alarm filter offers some merits in terms of flexibility, adaptation and scalability. The alarm filter doesn't affect the structure of the intrusion detection system as it is deployed behind an intrusion detection system and can work both online as well as offline. One gap that is still unexplored in terms of intrusion detection system is the semantic needs, so the alarm filter effectively uses the contextual information for filtering process. We are also aiming to provide the accuracy of the filtration rate to maximum and stable by selecting the most appropriate machine learning algorithm. The architecture for false alarm filter is described in the below figure:

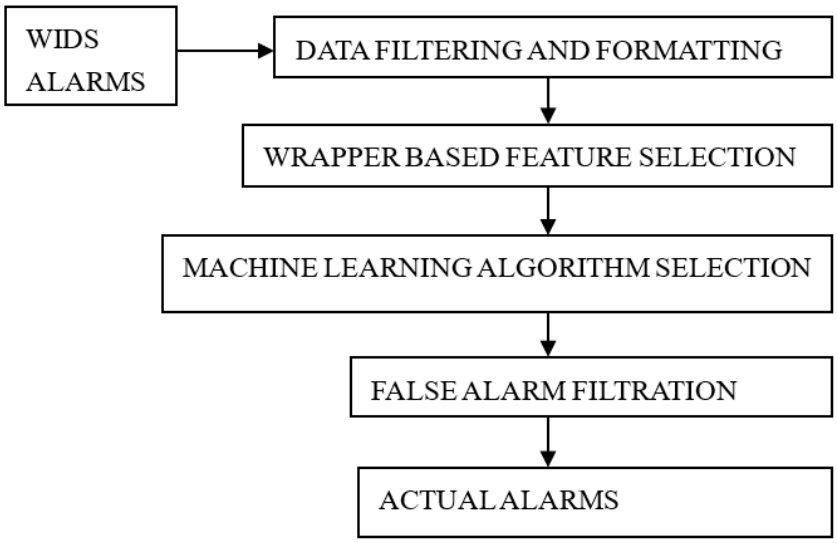

Figure 2. Architecture of False Alarm Filter

As mentioned earlier, the alarm filter is going to follow the standard procedure of formatting, feature selection, prediction phases. However, the idea of using wrapper-based feature selection and its suitability in IEEE 802.11 is something unexplored. The process of identifying the best prediction algorithm is been done for specific attacks, here we are going to do the same considering all the possible attacks possible. The prediction itself will identify the type of alarm, and in the next filtration process again we are performing the filtration to rule out the rate of false alarms. Thus, the objective of double filtration can be achieved by the proposed architecture. Starting off with the process of pre-processing we will try to achieve the standard process of formatting, cleaning and sampling to obtain the most relevant information for analysis. Massive Online Analysis can be considered for carrying out this work due to its suitability over demanding problems and its widest support of algorithms covering different concepts of machine learning.

The next process of feature reduction using the wrapper method generates different training data sets from the given training data set. Ensemble learning algorithms like the Bagging and ad boost can be used to generate the feature subset. The obtained reduced subset undergoes the process of classification and the performance evaluation of various machine learning algorithms are carried out. The performance of the algorithm is measured by evaluating some of the standardized metrics such as classification accuracy and the false alarm detection accuracy. The algorithm that is coming out with the best classification accuracy rate and false alarm detection accuracy can be selected from the pool of several machine learning algorithms. Some of the algorithms that will be tested are Decision Tree, Random forest, Random tree, one R and J48. The objective of double filtration can be achieved by using the false alarm filtration component that once again will make use of the best learning algorithm to boost the detection accuracy of false alarms.

The Aegean Wi-Fi Intrusion Dataset (AWID) is the dataset chosen by us for this evaluation as this contains 155 attributes. Even though this dataset consists of simulated attack, the higher number of attributes allows us to identify higher number of intrusion types so that different types of attacks can be addressed. The Aegean Wi-Fi Intrusion Dataset (AWID) is a publicly available labeled dataset which was developed based on real traces of both normal and intrusion activities of an 802.11. Wi-Fi network is under the supervision of University of the Aegean and George Mason University. The AWID dataset is comprised from a large set of packets (F) and a smaller one (R). These two versions are not related i.e., the smaller one has not been produced from the larger. They have been captured at different times, with different equipment and in different environments. Each version has a training set (denoted as Trn) and a test set (denoted as Tst). The test version has not been produced from the corresponding training set. Finally, a version where labels that correspond to different attacks (ATK), as well as a version where the attack labels are organized into 3 major classes (CLS) are provided. In that case, the datasets only differ in the label.

Table 2 lists the intrusion types which are available in the standard AWID Dataset. It has 17 intrusions with description.

Table 2. Intrusion Types in AWID Dataset

Intrusion	Description
Amok	An Increased number of 802.11 Authentication Requests is noticed in Amok
Arp	It may be used as a first step for any of the Key cracking attacks
Authentication request	802.11 DoS Attack
Beacon	802.11 DoS Attack
Cafe latte	802.11 Keystream Retrieving Attacks
Chop chop	802.11 Keystream Retrieving Attacks
Cts	802.11 DoS Attack
Deauthentication	802.11 DoS Attack
Disassociation	802.11 DoS Attack
Evil twin	802.11 Man-in-the-Middle
Fragmentation	802.11 Keystream Retrieving Attacks
Hirte	802.11 Keystream Retrieving Attacks
Power saving	802.11 DoS Attack
Probe request	802.11 DoS Attack
Probe response	802.11 DoS Attack
Rts	802.11 DoS Attack

From table 2, it can be observed that the availability of DoS attacks is high when it is compared with other types of attacks which are listed in the table. In this 802.11 WLAN, authentication, power saving, probe request, probe response and Rts named attacks comes under the category DoS attack. By using this information, we can frame fuzzy IF…THEN rules for identifying the attacks exactly. This paper is also suggested to prepare new fuzzy rules for enhancing the detection accuracy and also reduces the false alarm. Moreover, it concludes the uses of computational intelligence techniques are useful to reduce the computational complexity, increase the detection accuracy and it also able to reduce the false alarm rate by using conditional probability. In addition, intelligent agents can be introduced for the effective communication and it also helps to improve the decision-making accuracy. Soft computing techniques can be used with intelligent agents for improving the machine learning algorithm performance in terms of detection accuracy.

5. Conclusion

False alarms remain as a big challenging issue in intrusion detection system and this serves as a limiting factor for its construction. Constructing a false alarm filter appears to be a promising method in reducing the false alarms. In this survey, we explained in detail about the usage of data mining techniques, preprocessing techniques such as filter approach and wrapper approach, ontology-based approaches and heuristic search-based approaches for enhancing the detection accuracy, reducing the false alarm rate and computation complexity. The comparative analysis made by the end of the discussion. After the comparative analysis, it recommends the suitable idea for enhancing the detection accuracy by reducing the false alarm rate and computation complexity. Finally, it recommended that to introduce an intelligent agent based false alarm filter that undergoes double filtration process for enhance the performance in terms reduction of false alarm rate. Moreover, most of the best machine learning algorithms are studied to obtain the best feature set and to obtain the best prediction. End of the discussion, it suggested that to design new machine learning algorithms with the introduction of intelligent agents, soft computing techniques and fuzzy rules for better prediction accuracy on WLAN 802.11 attacks.

References

Adetokunbo, M., Zincer-Haywood, E., & Milios, E. (2011). Robust Learning Intrusion Detection for Attacks on Wireless Networks. *Journal of Intelligent Data Analysis, 15*(5), 801-823.

Alexandros, T., Georgios, K., & Stefanos, G. V. (2007). Towards effective Wireless Intrusion Detection in IEEE 802.11i", Third International Workshop on Security Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2007), pp.1-6.

Alicherry, M., & Keromytis, A. D. (2009). Doublecheck: Multi-Path Verification Against Man-in-the-Middle Attacks", IEEE Symposium on Computers and Communications, pp. 557-563.

Al-Mamory, S. O., & Zhang, H. (2008). IDS Alarm Reduction using Data Mining. IEEE International Conference on Neural Networks, pp. 12-22.

Al-Mamory, S. O., & Zhang, H. (2009). Intrusion Detection Alarms Reduction using Root Cause Analysis and

Clustering. *Computer Communications, 32*(2), 419-430.

Al-Mamory, S. O., & Zhang, H. (2010). New Data Mining Technique to Enhance IDS Alarms Quality. *Journal in Computer Virology, 6*(1), 43-55.

Anita, P., & Sunita, G. (2013). Analysis for improving intrusion detection system in wireless network. *International Journal of Advanced Research in computer science and software Engineering, 3*, 85-91.

Bolzoni, D., & Etalle, S. (2006). APHRODITE: an Anomaly-based Architecture for False Positive Reduction. Retrieved from http://arxiv.org/PScache/cs/pdf/0604/0604026.pdf

Borsc, M., & Shinde, H. (2005). *Wireless Security & Privacy.* In proc. of IEEE International Conference on Personal Wireless (ICPWC '05), pp. 424-428.

Chris, S., Lyn, P., & Sara, M. (1999). *An Application of Machine Learning to Network Intrusion Detection.* In Proceedings of the 15th Annual Computer Security Applications Conference, ACSAC '99, Washington, DC, USA, pp. 1-7, 1999.

Cuff, A. (2003). Intrusion Detection Terminology (Part One). Retrieved from http://www.securityfocus.com/infocus/1728

Danziger, M., Lacerda, M., & de Lima, N. (2009). Danger Theory and Multi-agents Applied for Addressing the Deny of Service Detection Problem in IEEE 802.11 Networks. ISDA, 2009 Ninth International Conference on Intelligent Systems Design and Applications, 695-702.

Deborah, L., Guinness, M. (2003). *Ontologies Come of Age.* In Dieter Fensel, Jim Hendler, Henry Lieberman, and Wolfgang Wahlster, editors. The Semantic Web: Why, What, and How, MIT Press, 2003.

Deepthi, N. R., Hassan, B. K., Syed, A. Y., & Azween, B. A. (2011). An Intelligent Approach to detect probe request attacks in IEEE 802.11 networks. *IFIP Advances in Information and Communication Technology, 363*, 372-381. Retrieved from http://ciscopress.com/articles/aticle id =25334

Doukas, C., Maglogiannis, I., Tragas, P., Liapis, D., & Yovanof, G. (2007). Patient Fall Detection using Support Vector Machines. *IFIP The international federation for Information Processing, 247*, 147-156.

Du, Y., Wang. H., & Pang, Y. (2004). Design of a Distributed Intrusion Detection System based on Independent Agents. Proceedings of International Conference on Intelligent Sensing and Information Processing, pp. 1-14.

Elankayer, S., & Vallipuram, M. (2006). *An early warning system for 802.11 I wireless networks.* 1st International Conference on Wireless Broadband and Ultra Wideband Communications, pp.1-6.

Giacinto, G., Perdisci, R., & Roli, F. (2005). Alarm Clustering for Intrusion Detection Systems in Computer Networks. *Lecture Notes in Computer Science, 3587*, 184-193.

Greensmith, J., & Aickelin, U. (2007). Dendritic cells for SYN scan detection", Proceedings of the IEEE Genetic and Evolutionary Computation Conference (GECCO-07), London.UK. pp. 49-56.

Greensmith, J., Twicross, J., & Aickelin, U. (2010). Dentritic cells for anomaly detection. In IEEE Congress on Evolutionary Computation, pp. 1-8.

Hutchinson, K. (June 2004). SANS GSEC. Whitepaper in GIAC security Essentials, London.

Ilgun, K., Kemmerer, R., & Porras, P. (January 1995). State transition analysis: A rule-based intrusion detection approach. *IEEE Transactions on Software Engineering, 21*(3), 181-199.

Julisch, K., & Dacier, M. (2002). Mining Intrusion Detection Alarms for Actionable Knowledge. Proceedings of the 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 266-375.

KDD Cup Data. (n.d.). http://kdd.ics.uci.edu/databases/kddcup99/ kddcup99.html.

Law, K. H., & Kwok, L. F. (2004). IDS false alarm Filtering using KNN classifer. *Lecture Notes in Computer Science, 33*(25), 114-121.

Law, K. H., & Kwok, L. F. (2004). IDS false alarmfiltering using KNN classifier. In Proceedings of the 5th International Workshop on Information Security Applications, pp. 114-121.

Lim, Y. X., Yer, T. S., Levine, J., Owen, H. L. (2003). Wireless Intrusion Detection and Response. *IEEE Systems, Man and Cybernetics Society Information Assurance Workshop, 20*, 883-884.

Lippmann, R., Cunningham, R. K., Fried, D. J., Graf, I., Kendall, K. R., Webster, S. E., & Zissman, M. A. (1999). Results of the 1998 DARPA Offline Intrusion Detection Evaluation," in Proc. Recent Advances in Intrusion

Detection, pp.1-29.

Lippmann, R., Fried, D., Graf, I., Haines, J., Kendall, K., McClung, D., Weber, D., Webster, S., Wyschogrod, D., Cunningham, R., & Zissman, M. (January 2000). Evaluating Intrusion Detection Systems: The 1998 DARPA Off-Line Intrusion Detection Evaluation. In Proceedings of the DARPA Information Survivability Conference and Exposition, pp. 12-26.

Lippmann, R., Haines, J. W., Fried, D. J., Korba, J., & Das, K. (October 2000.). The 1999 DARPA Off-line Intrusion Detection Evaluation. *Computer Networks, 34*(4), 579-595.

Long, J., Schwartz, D., & Stoecklin, S. (2006). Distinguishing False From True Alerts in Snort by Data Mining Patterns of Alerts. Proc. SPIE 6241. *Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security, 6241*, 1-10.

Mahoney, M. V., & Chan, P. K. (2003). *An Analysis of the 1999 DARPA/Lincoln Laboratory Evaluation Data for Network Anomaly Detection*. In Proc. Recent Advances in Intrusion Detection, pp. 220-237.

Mansour, N., Chehab, M. I., & Faour, A. (2010). Filtering Intrusion Detection Alarms. *Cluster Computing, Springer, 13*(1), 19-29.

Mayank, A., Sukumar, N. (2016). Machine Learning Approach for Detection of Flooding DoS Attacks in 802.11 Networks and Attacker Localization. *International Journal of Machine Learning and Cybernetics, 7*(6), 1035-1051.

McHugh, J. (2000). Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 Darpaoff-Line Intrusion Detection System Evaluation as Performed by Lincoln Laboratory. *ACM Transactionson Information and System Security, 3*(4), 262-294.

McHugh, J. (November 2000). Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Performed by Lincoln Laboratories. *ACM Transactions on Information and System Security, 3*(4), 262-294.

Meng, Y. X., & Lam-For, K. (2014). Enhancing Intrusion Detection Systems using Intelligent False Alarm Filter, pp. 1-23, IGI Global Publisher. Retrieved from http://www.igi-global.com/chapter/enhancing-intrusion-detection-systems-using-intelligent-false-alarm-filter/78873.

Mohammed, A. A., He, X. J., Nanda, P., & Tan, Z. Y. (2016). Building an Intrusion Detection System using a filter Based Feature Selection Algorithm. *IEEE Transactions on Computers, 65*(10), 2986-2998.

Moises, D., Fernando, B., & de Lima, N. (2010). A hybrid approach for IEEE 802.11 based on AIS,MAS and Naïve Bayes", 10th International conference on Hybrid Intelligent Systems, pp. 201-204.

N. B. Anuar, H. Sallehudin, A. Gani, O. Zakari, (2008). Identifying False Alarm for Network Intrusion Detection System using Hybrid Data Mining and Decision Tree. *Malaysian Journal of Computer Science, 21*(2), 101-115.

Pavel, L., Patrick, D., Christin, S., & Konrad, R. (2005). Learning intrusion detection: Supervised or unsupervised? In Image Analysis and Processing, *Lecture Notes in Computer Science, 3617*, 50-57.

Perdisci, R., Giacinto, G., & Roli, F. (2006). Alarm Clustering for Intrusion Detection Systems in Computer Networks. *Engineering Applications of Artificial Intelligence, 19*(4), 429-438.

Pietraszek, T. (2004). *Using Adaptive Alert Classification to Reduce False Positives in Intrusion.* Proc. 7th Symposium on Recent Advances in Intrusion Detection Cogres, 32(24), 102-124.

Rupinder, G., Jason, S., & Andrew, C. (2006). *Specification Based Intrusion Detection in WLAN*. Proceedings of the 22nd Annual Security Applications, 1-10.

Shika, G., Vijendra, K., & Suruchi, G. (2013). Spoofing Detection Methods in Wireless LAN - A Study with pros and cons. Proc. of Int. Conf. on Emerging Trends in Engineering and Technology, pp. 1-8.

Siraj, A., & Vaughn, R. B. (2005). Multi-Level Alert Clustering for Intrusion Detection Sensor Data. Fuzzy Information Processing Society, 1-6.

Siraj, A., Vaughn, R. (2005). A Cognitive Model for Alert Correlation in a Distributed Environment. *Lecture Notes in Computer Science, 3495*, 218-230.

Tade, T., Ptacek, H., & Timothy, N. N. (1998). Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection. Technical Report, Secure Networks Inc., 1-63.

Van Beusekom, J., Shafait, F., & Breuel, T. M. (2008). Automated OCR Ground Truth Generation. Proceeding DAS '08 Proceedings of the 2008 The Eighth IAPR International Workshop on Document Analysis Systems, pp. 111-117.

Wenche, C., Allen, M., & Qu, Q. (2006). A sliding window based management traffic clustering algorithm for 802.11", In Chapter Network control and engineering for QoS, Security and Mobility. *IFIP International Federation for Information Processing, 213*, 55-64.