J Intell Inf Syst (2016) 46:391–407
DOI 10.1007/s10844-015-0387-y

Machine learning for intrusion detection in MANET: a state-of-the-art survey

Lediona Nishani[1] · Marenglen Biba[1]

Received: 10 August 2015 / Accepted: 21 September 2015 /
Published online: 8 October 2015

Abstract Machine learning consists of algorithms that are first trained with reference input to "learn" its specifics and then used on unseen input for classification purposes. Mobile ad-hoc wireless networks (MANETs) have drawn much attention to research community due to their advantages and growing demand. However, they appear to be more susceptible to various attacks harming their performance than any other kind of network. Intrusion Detection Systems represent the second line of defense against malevolent behavior to MANETs, since they monitor network activities in order to detect any malicious attempt performed by intruders. Due to the inherent distributed architecture of MANET, traditional cryptography schemes cannot completely safeguard MANETs in terms of novel threats and vulnerabilities, thus by applying machine learning methods for IDS these challenges can be overcome. In this paper, we present the most prominent models for building intrusion detection systems by incorporating machine learning in the MANET scenario. We have structured our survey into four directions of machine learning methods: classification approaches, association rule mining techniques, neural networks and instance based learning approaches. We analyze the most well-known approaches and present notable achievements but also drawbacks or flaws that these methods have. Finally, in concluding our survey we provide some findings of paramount importance identifying open issues in the MANET field of interest.

Keywords Machine learning · Intrusion detection systems · MANETs · Classification · Association rule mining · Neural networks · Instance based learning

✉ Lediona Nishani
ledionanishani@gmail.com

Marenglen Biba
marenglenbiba@unyt.edu.al

[1] University of New York Tirana Kodra e Diellit Tirana, Tirana, Albania

1 Introduction

Machine learning algorithms are first trained with reference input to ”learn” its specifics and this process maybe supervised or unsupervised. Models are then deployed on unseen input for detection purposes. Machine learning methods (Deepika et al. 2012) enables systems to learn from experience. Usually the system starts with some prior corresponding knowledge that analyzes, and tests the data acquired. Machine learning techniques rely on explicit or implicit model that accommodate the analyzed patterns in order to be categorized. Machine learning based techniques can be divided into Genetic Algorithms, Fuzzy Logic, Neural Networks and Bayesian networks (Kaur et al. 2013).

Mobile Ad-Hoc Network (MANET) is a collection of autonomous nodes that establishes a dynamic, multi-hop radio network in decentralized and cooperative way (Panos et al. 2011). These nodes do not have an access point to be connected with; therefore, they can join and leave the network whenever they want. This makes MANET vulnerable to several kinds of threats and attacks. MANETs constitute a variety of mobile devices such as laptop, mobile phones, PDA (personal digital assistants), which introduce constraints in terms of computation memory, bandwidth, capability, etc. The absence of the access point connecting nodes as a central authority does not provide much trust between nodes, consequently individual nodes count on the dynamic establishment of connections with other MANETs. Their flexibility has expanded their usage in regards to military applications and emerging response circumstances. Due to their critical information infrastructure combined with distributed architecture, MANETs are being substantially a preferable target to various complex distributed threats, which mostly address the network and data link layer of the protocol stack.

For the aforementioned reasons, it is very important that an intrusion detection system is deployed in MANET as a second line of defense. Intrusion detection systems (IDS) represent a mechanism that monitors and investigates events that appear in a computer system. An IDS incorporates methods and complex techniques for modeling and discovering abnormal behaviors. They try to determine whether the network is experiencing any malicious activity or not. Usually, these are in the form of a process, a device or a combination of both that monitors the system and network activity against unauthorized malicious activity. The major goal of IDS is to detect the attempt before the attacker has already done any harm to the network. IDS are also responsible for monitoring network activity, auditing the network and system configuration for vulnerabilities, analyzing and interpreting data integrity. An IDS performs three major functions: monitoring, detecting and generating alarms. IDS must not be confused with firewalls. Firewalls protect the information flow and prevent intrusions, while IDS identifies whether the network is subject to any attack or if any vulnerability has penetrated the firewall security.

Intrusion detection processes can be categorized in two major methods namely misuse detection and anomaly detection methods. Misuse detection-based methods also known as signature-based, perform on databases containing known attack signatures; meaning that the system makes use of examples or patterns of prior known threats and then operates a comparison with the current behavior. The second most prominent method is anomaly detection method, which operates based on the reasoning that the intrusive behavior varies from the normal pattern data of users. Anomaly detection systems find out deviations from the prior existing activity. Therefore, abnormal activities show evidence of diverse properties from the normal usage. Anomaly detection approaches outperform the misuse detection system in terms of detecting new attacks that have not been observed in the existing patters before. However, their disadvantage consists of experiencing high false alarm rates due to their lack of discrimination capability.

Anomaly and misuse detection systems often have borrowed their schemes from the machine learning perspective respectively: information theory, neural networks, association rules, classification approaches, instance based-learning algorithms, artificial immune systems and many more. Machine learning algorithms are popular because they address many real world problems. They are based on explicit and implicit models facilitating the analysis of the pattern to be classified. Machine learning tools, which compose anomaly based detection systems, have demonstrated to achieve a significant increase of detection rate. This is due to the intrusion detection area, which operates with particular properties thus making the machine learning approach harder and onerously. Rather than finding similarities, machine-learning techniques perform better at identifying activities that do not pertain to the existing ones. The classic machine learning approach consists of a classification problem. Understanding and providing insights of what the system is doing, is the best way to enhance the performance of anomaly detection schemes. Intrusion detection domain does not benefit from studying the behavior of some previous combination of machine learning with particular feature set. In intrusion perspective, we can always discover a variation that performs slightly better in a specific context. However, in this domain, insights are of much more benefit than numbers.

Intrusion detection systems are deploying successfully machine-learning techniques in MANET.A lot of research is being conducted in this area focusing in IDS based-machine learning and data mining technologies. The model and the context in which they operate can differentiate the type of machine leaning algorithm that has to be employed in the first place. In MANET, we are interested in classifying activities in normal or abnormal. Machine learning helps to conduct easily data summarization and visualization. Therefore, aims to facilitate the security professionals at indicating weaknesses and flaws of the system. Due to the inherent distributed architecture of MANET, there some challenges in the deployment of these techniques in an IDS scenario. These difficulties are independent of actual learning algorithms employed by IDS and must be overcome by applying novel machine-learning methods.

In this paper, we present a thorough survey of machine learning techniques developed in the research community of both machine learning and computer security. To the best of our best knowledge, these are the latest works that have been discussed so far in this field of interest. We are going to compare these works and derive significant conclusions for new directions of research. In the remainder of this paper, first we provide a description in regards to intrusion detection systems; define what IDS represent and their classification based on data resource and system model. We have structured our survey into four directions of machine learning methods that correspond to the most well-known techniques employed in MANET respectively: classification approaches, association rules mining techniques, neural networks and instance based learning approaches. Hence, we deal and explore the most prominent approaches for each of aforementioned methods for IDS in MANET. We finally, we discuss the advantages and disadvantages of the four scenarios of machine learning. Finally, in concluding our review paper we draw significant conclusions for further works and identify some open issues for MANET.

2 Intrusion detection systems

In this section, we explore and categorize intrusion detection systems. We provide a general depiction of the most prominent IDS and their classification in terms of data resource and model of intrusion (Deepika et al. 2012).

Intrusion detection systems (IDS) encompass software or hardware systems, which are incorporated in a network in order to monitor the generated traffic and to flag out the compromised activities that might occur. An IDS employs techniques for modeling and analyzing intrusive behavior in a computer system (Engen 2010).We must make a difference between IDS and a firewall. While firewall filters all traffic between the internal network and the unreliable external network, IDS merely monitors and sniffs the network traffic. They cannot drop or ban the network packets (Fung and Boutaba 2013). In other words, IDSs property is to detect and to sniff the network for any network vulnerability. The IDS presents a second wall of defense and can be combined together with firewall to detect and prohibit suspicious computer activities entering and compromising the internal network.

An IDS is composed of its core element known as the sensor (engine that analyzes data). The sensor retrieves data from three major directions: Own IDS knowledge base, Syslog and Audit. The ultimate goal of the sensor is to filter the information retrieved from data and to drop any irrelevant data obtained from the event set associated with the protected system. In other words, it warns the system when suspicious activity occurs.

In terms of technology used for detection and identification of the suspicious activity, IDSs are classified in signature-based and anomaly-based types.

-Signature-Based IDSs are based on predefined set of patterns to detect attacks. Signature-based IDSs compare data packets with the signatures or attributes of known intrusions to decide whether or not the observed traffic is malicious (Fung and Boutaba 2010).This approach is employed only in known attacks. It utilizes a set of rules to indicate intrusions by observing known and documented events. This system is connected to large databases, which store prior attacks. Thus, if the database is not regularly up dated, there is risk of not capturing the attack. Signature definitions in database must be more specific so that variations of known attacks are not missed. This leads to a large database, which can grab much memory to the system. Signature-based IDSs are efficient in detecting known intrusions with monomorphic signatures. However, they are not efficient in detecting unknown intrusions or intrusions with polymorphic signatures.

-Anomaly-Based IDS operates on the concept that the attack behavior diverges from the normal profile behavior. Firstly, it identifies the baseline of normal profile, and then the new event is compared with the normal behavior. If the new activity deviates from the normal profile then it is regarded as anomalous by generating an alarm. The variations between the normal profile and the monitoring feature are analyzed by making use of various techniques like statistical analysis, machine learning and data mining techniques. Anomaly based IDS systems suffer from high rates of false positive alarms and can introduce heavy processing overheads on computation resources. Their main advantage is the detection of unknown attacks. Anomaly based detection has to be adaptive to be able to face the dynamic change of the network. Their normal profile should represent the normal network operation. The dynamic change must be incorporated immediately into the normal profile. Most current IDSs employ both techniques to achieve better detection capability. IDSs can be also classified in terms of data sources respectively in stack-based IDS, host-based IDS and network-based IDS.

-Stack based Intrusion Detection Systems (SIDS) works by integrating precisely with TCP/IP protocol stack, which enables the system to observe packets as they are distributed through the OSI layer. IDSs pull the packet when they identify any compromised behavior before the application can process the packet.

-Network Based Intrusion Detection Systems (NIDS) monitor network packets and detect network attacks. NIDS listen to the packets in a segment of the network allowing them to detect distributed attacks. NIDS monitor traffic of the network; it consists of sensors to detect packets, a data analyzer to make sense of data. It generates alarms when it encounters suspicious activity. Its major drawback is not being aware of the behavior in the internal environment.

-Host-based Intrusion Detection Systems (HIDS) detects intrusive activities and malevolent behavior on the host. It controls the privileged access of the host in order to monitor components of host that are not accessible to other systems. It monitors internal and external activity from the computer. It is viewed as an individual device; this approach is not aware of what is happening in the whole picture of network environment. Its major disadvantage is that HIDS cannot detect attacks targeted to the host that does not have HIDS installed.

With the development of Internet, hackers are developing novel malware every day. While new malware is developed, IDSs are also evolving and becoming more sophisticated. They need to be a step ahead compared to hackers, with regard to improving and being able to detect the dramatic growth of attacks. IDSs detect fraudulent behavior by looking for known weaknesses and known attack patters (signature-based) or normal behavior (anomaly-based). Therefore, it is difficult to indicate all potential attacks because IDSs need to know all probable attacks in order to achieve a satisfying protection. Whenever IDSs encounters novel attacks, IDS manufacturers develop rules and signature for that novel threat. In practice, some manufactures may not be aware of new attacks distributed in the network. Another pitfall of IDS is the management of its sensitivity. Many IDSs generate high false alarm rates, in other word they flag out many intrusion alerts, which do not consist of any malevolent behavior. This leads to hurdles on handling and inspecting alerts from security professionals. On the other hand, if we lower the sensitivity of IDS we might encounter the problem of missing attacks of paramount importance, which can lead to insecure networks and hosts. A major challenge in this case is to determine the optimal sensitivity of IDS.

3 Classification approaches

Classification is the process of learning a function that maps data objects to a subset of a given class set. Therefore, a classifier is trained with a labeled set of training objects, specifying each class. The two major objectives of classification are to find a good general mapping predicting the class of previously unknown data with significant efficiency and the second one is to discover an understandable class model for each of the classes. In this section, we review the most interesting body of work that has been carried out so far in regards to classification approaches for IDS in MANET. Here we focus on intrusion detection systems based on classification algorithms.

A simple technique to employ intrusion detection is to make use of a classifier so that IDS can determine if data investigated is ”normal” or ”abnormal”. Classification algorithms have been largely used for intrusion detection in wired computer networks. However if we compare the body of knowledge that community researchers have explored for MANET with the works in classification for MANET, we must say that MANETS field combined with classification is quite limited and not so expanded in the research community.

Zhang and Lee (2003) proposed the first significant Intrusion Detection System for wireless networks. They described a new model for intrusion detection and response for MANET's environment. Their contribution was the design of distributed and cooperative anomaly-based IDS. This work has served as a guide to the subsequent research in the area. They specifically focused on anomaly detection approach-based in routing updates of Media Access Control (MAC) layer and mobile application layer. They have advocated that intrusion detection architecture in mobile computing environments should be distributed and cooperative. Intrusion detection should comprise all the networking layers in an integrated cross-layer manner. This paper emphasized anomaly detection constructed by information available from routing protocols. They pointed out that protocols with strong correlation among changes of different types of information have the tendency to better detect intrusive behavior.

Huang and Lee (2003) presented another interesting approach concerning classification techniques in MANET. They provided detailed information about intrusions from anomaly detection. They stated that for several known attacks, a rule can be applied to identify the type of attack after an anomaly is reported. The second important point clearly stated in that paper was that intrusion detection in MANET must be carried out in a distributed way because of the absence of the infrastructure and wired topology. They proposed a novel architecture when a detection agent runs on each monitoring node to detect local intrusions and collaborates with the other agent so that they can investigate where intrusion came from and manage the response. Since, MANET nodes have limited battery power; it is not efficient to make each MANET node always a monitoring node, especially when the threat level is low, and therefore authors proposed a cluster-based detection scheme. A cluster of neighboring MANET nodes can randomly select a monitoring node for all nodes. They made use of a set of statistical features resulting from routing tables and then they applied the classification decision-tree induction algorithm to detecting "normal" versus "abnormal" behavior.

Deng et al. (2003) presented two novel intrusion detection frameworks; one consisting of a hierarchical architecture and the other of a distributed based architecture. Both approaches focused on the network layer and are based on the SVM Support Vector Machines classification algorithm. Their main contribution was that a hierarchical distributed approach might be a better approach compared to a thoroughly distributed framework.

An interesting line of research in the classification algorithm employed in IDS for MANET is the work proposed by Huang et al. (2003). The authors have developed a novel technique based on cross-feature analysis. They have derived the conclusion that a strong feature correlation exists in normal behavior patterns that can be utilized to identify the deviations from the normal behavior. Researchers have observed that the number of dropped packets increase rapidly without any change of the network. This flags out a suspicious activity. The relationship of packets being dropped and routed entries can be detected by analyzing normal patterns. Regarding cross-feature analysis approach, the paper has investigated correlations between each feature and the entire features. Researchers have turned the anomaly detection issue into a set of classification sub-problems. The outcome of each classifier is combined in order to create the detector. They have demonstrated through experiments results that the intrusion detection models trained by employing this cross-feature analysis approach can outperform in capturing routing abnormal activities. Finally, the authors provide insights on some drawbacks of this method including computation cost and the generality of this model, which at the same time can be an advantage in terms of exploring and implementing this framework in different datasets.

Bose et al. (2007) developed a Bayesian classifier for MANET. They developed a new anomaly detection system for each node of the network. Each node has respectively a detection subsystem for the MAC, routing and application layer. Then data collected for each layer are elected from normal transactions. This body of work has implemented the Bayesian classification algorithm, Markov chain construction algorithm and association rules mining algorithm. Data from detection subsystems of MAC routing and applications layers respectively are integrated at the local integration module and collection of this data is processed in the global integration module.

In classification approaches, building ensembles from single classifiers is a field of interest that has encountered a rich tradition and strong-grounded theoretical framework. The major outcome of employing ensemble classification algorithms is raising the effectiveness and outperforming the single classifiers. Researchers, while examining ensembles, have come up with two strong criteria: accuracy and diversity in order to build a better ensemble than single classifiers.

With regard to building ensemble classifiers for intrusion detection purposes, Cabrera et al. (2008) described a three-level hierarchical system for collecting and processing data by employing ensembles classification approach. Throughout that paper clustering algorithms for processing the anomaly indexes are examined. The complete ensemble of classification algorithms is tested under two types of routing protocol and two kinds of attacks. Finally, researchers derived interesting conclusions regarding benefits of averaging with detection accuracy, which can enhance when moving up in the node-cluster hierarchy.

Ghodratnama et al. (2010) disseminated a nearest neighbor-based classifier model for cost-sensitive issues. They have determined the distance function in a parametric form, which is used for tuning the NN classifiers. They introduced feature and instance weighting algorithms attempting to lower the average cost. The contribution of this work is in demonstrating the novel model of being successful in reducing the average cost of classification comparing to baseline of NN. It can reduce the time of classification of basic NN when eliminating excessive features and instances. The authors made use of KDD datasets while examining the cost sensitive problem of classification for IDS in wired networks.

An interesting line of research is related to classification decisions having the minimum expected cost. Regarding authentication systems, the cost of unauthorized access is larger than denying the wrong access to users. Analogically to IDS, generating false alarms has a substantial lower cost than missing a dangerous intrusion. A considerable body of work has been explored in the line of cost-sensitive intrusion detection systems.

Mitrokotsa and Dimitrakakis (2012) investigated this direction in the MANET area. They discussed five well-known supervised classifiers over a number of metrics to measure their performance in the dataset. The major objective of this paper is to explore the relationship between classification performance and the cost matrix; how these properties correlate with each other. Another scope of this paper is to discuss techniques for tuning classifiers while previously unseen attacks may occur during the testing procedure. Subsequently, they have designed a sequential cross-validation procedure in order to raise the classifiers' robustness. Authors claimed that weighted cost matrices could be more beneficial with more statistical classifiers. In addition, sequential classifiers can have a substantial effect for some kinds of classifiers. An open issue in this paper would be implementing this approach on real-world data or validating these results in simulators whose metrics and parameter can be derived from real data.

A growing body of work has been focused on feature-selection techniques for intrusion detection system in MANET. Feature-selection is the technique of selecting a subset of relevant features from the dataset for building robust IDS (Mukkamala and Sung 2006). Feature-selection can be assessed as a substantial asset to build classification models. Another major advantage that this algorithm provides is the elimination of useless features, which contributes to enhancing detection accuracy, thus enhancing the entire performance of the detection framework.

We have deemed appropriate to thoroughly present herein the research work of Visumathi and Shunmunganathan (2012). The authors have developed an efficient Forward Feature Selection and Enhanced Decision Tree Support Vector Machine classifier, which have been applied to the KDD 99 Cup dataset and addresses. The aforementioned algorithm selects important features from KDD Cup Dataset in order to reduce classification time. These features are used in Enhanced Decision Tree Support Vector Machine (EDTSVM) classifier to develop an intrusion detection system.

Related work proposed an architecture for IDS in MANET which consists of six components: KDD cup dataset, User interface module, Preprocessing module (FFS algorithm), Classification Module (EDTSVM), Decision making Module. Preprocessing Module comprises Forward Feature Selection algorithm utilized for effective preprocessing of dataset. This mechanism selects only the valuable attributes from the dataset using the projection operation of relational algebra. Data cleaning, data integration and data transformation are carried out on the selected data for performing effective preprocessing. The classification module is represented by Enhanced Decision Tree Support Vector Machine (EDTSVM), which is based on genetic algorithms. DTSVM is a binary tree with m-1 inner nodes; each node is SVM binary classifier. One point to highlight herein is that if the classification performance is not good at the upper nodes then the overall performance might be affected. The enhanced DTSVM algorithm provides an effective classification. The classification consists of three steps respectively decision tree formation, application of Enhanced Multiclass SVM for classification leading to intrusion detection and intrusion prevention.

Regarding the experimental phase, EDTSVM provides better detection accuracy when compared to other methods and mechanisms. Another experiment is conducted for EDSCM to be tested under three kinds of dataset attacks: Probe attack, DoS attack or others. In all cases, EDTSVM outperforms the DTSVM algorithm; it provides better accuracy and higher detection rate. This is due to the preprocessing properly data using information gain ratio and hence only necessary attributes having been selected. This approach improves accuracy when compared to other methods.

4 Association rule mining algorithms

Association rules have drawn a lot of attention in the data mining community. This technique is very useful for discovering relevant relationships between variables that might be hidden in large data sets. It intends to identify strong rules discovered in databases using different measures of interestingness (Piatetsky-Shapiro and Frawley 1991). Association-rule mining algorithms have been used to find correlations between services of one session and can forecast the future (Cliftom and Gengo 2000). Association-rule mining identifies associations (patterns or relations) among database attributes and their values. It is a pattern-discovery technique, which does not serve to solve classification problems (it does not classify samples into some target classes) nor prediction problems (it does not predict the development of the attribute values). Association-rule mining generally searches for any association among any attributes present in the database (Maheshwar and Singh 2013). In association-rule mining, efficiency is of paramount importance.

MANET are very susceptible to malevolent behavior, while authentication and encryption techniques may protect in some term like reducing the number of intrusions, however these cryptography techniques cannot perform well in unseen or novel attacks. The following body of work reviewed below is related to cross-layer detection technology incorporated with association-rule mining algorithms.

Shrestha et al. (2010) have introduced a new IDS framework based on cross layer which act jointly with all the layers of OSI Protocol Stack approach in order to capture weaknesses in MANET. Furthermore, they have employed association module to perform the leakage between OSI and IDS module. After association-rules are released from multiple segments of training data set, then they are aggregated into a rule set. This helps in lowering the overhead of data collection. Fixed-width algorithm is implemented to enhance the detection rate. The proposed cross-layer based intrusion detection is appropriate to detect DoS attacks and sinkhole attacks. One drawback is that this mechanism lacks of IDS robustness and needs to perform further simulation results with broader semantic information. To the authors' perspective, many traditional intrusion detection systems are limited in terms of collecting training data from real world and the process of manually deciding whether normal or abnormal behavior is deemed very time consuming. The association algorithm Apriori provides traffic feature and subsequently is followed by a clustering algorithm. Both they are used as a root to help in anomaly detection.

Anjana-Devi and Bhuvaneswaran (2011a) have proposed a cross-layer intrusion detection system in order to disclose different types of DoS attacks. In addition, they have made use of clustering and data mining techniques for detecting the frequency of intrusive behavior. Authors have pointed out an IDS architecture composed of several modules: local data collection, local detection, and cooperative detection and alert management module. This approach is undertaken by utilizing various layers of protocol stack; it incorporates fixed clustering algorithm for anomaly detection and it makes use of Adaptive Association Rule Mining for the association process in order to achieve traffic features. Subsequently, it follows up with the clustering fixed width algorithm. This algorithm is responsible for helping the increase of detection rate. The fixed-width algorithm helps in finding out and capturing DoS and sinkhole attacks at different layers. This approach leads to an increasing speed in detecting illegal activity when compared to other conventional models. The major contribution of this paper is that they have achieved some significant results regarding the novel technique, which carries out lesser traffic when intrusion is included in the system compared to the prior intrusion detection system that has been developed so far.

Another interesting work, which follows up the direction of association-rule mining for IDS in MANET, is presented by Anjana and Bhuvaneswaran (Anjana-Devi and Bhuvaneswaran 2011b). They have disseminated an efficient cross-layer based intrusion detection framework to detect malicious node and various types of DoS attacks. The proposed framework helps in identifying weaknesses in wireless networks. This approach engages a fixed width-clustering algorithm for accurately capturing of malicious activity in MANET. The association algorithm carries out the connection between OSI protocol stack and IDS architecture. Additionally, they have made use of the association rule mining techniques dubbed as the Fast Apriori algorithm for the association process aiming to raise the detection efficiency and to perform the association algorithm faster.

Ponsam and Srinivasan (2014) presented another approach recently. Previous scientific works have focused on cross-layer based intrusion detection system. Hence, this work is following the approach focusing on multilayer-based intrusion detections systems. Many intrusion detection systems have received a great attention from the research community; however still they face weaknesses and abnormal activities due to the multilayer attacks. This work attempts to fill this gap in the body of knowledge. They have disseminated a multilayer-intrusion based detection system by incorporating the fixed-width algorithm combined with the Apriori association rule mining algorithm. In the intrusion detection phase it is utilized the Apriori algorithm, then subsequently it is followed by the fixed-width algorithm in order to capture various vulnerability that might appear. The two algorithms comprise the base of anomaly detection in MANET. Authors have justified their findings in the experimenting phase deriving in significant conclusions that Multilayer IDS outperform the Single Layer IDS.

One interesting piece of paper relevant to this section of association-rule mining for intrusion detection system in MANET is presented in Mabu et al. (2011). The paper explores new fuzzy class-association-rule mining method based on genetic network programming (GNP) aiming to detect network intrusions. GNP used directed graph structures instead of strings in genetic algorithms. The introduced model can handle mixed databases containing discrete and continuous attributes and at the same time can build significant class-association rules deliberately raising the detection proficiency. This method is relevant to both misuse and anomaly detection. Experimental evaluations provide interesting findings that this novel approach has achieved significant growth in detection rates when compared to other machine learning techniques.

Another interesting piece of work was discussed in Changguo et al. (2009). The research work examines an association-rule mining based intrusion detection algorithm in wireless networks. A comparative analysis with classification approach has been explored through conducting experiments based on adopting Apriori and fuzzy association rule-mining algorithms. They have improved the performance of intrusion detection systems in terms of accuracy, detection rate, comparison evaluation and analysis of experiment outcome. This paper provides meaningful findings regarding wireless networks intrusion detection system. Incorporating fuzzy association rules is without no doubt an applicable and efficient method.

The previous association-rule mining techniques have extracted the association that may occur only between data that satisfy the minimum support confidence set by users. Nevertheless, they do not take into consideration the interval of time in which the rules are valid. Hence, Somasundaram and Lakshmana (2013) have represented an interesting study research that covers this gap. The researchers have developed a new intrusion detection system based on Conditional Random Field (CRF). In addition, deploying the aforementioned algorithm helps in enhancing the accuracy of IDS. Authors have proposed a new temporal association rule-mining algorithm, which is an extension of Apriori algorithms with new temporal conditions. Moreover, the CRF based feature algorithm is useful to select valuable attributes from the dataset. Finally, experimental findings conclude that the proposed approach captures abnormalities with low false alarm rate and significantly high detection rate.

5 Artificial neural network approaches

An Artificial Neural Network is a collection of treatments, which provides the desired output by doing certain simple processing on the set of input. ANNs comprise a family of statistical learning algorithms encouraged by the neural networks in the biological domain. Additionally, they are used to determine approximate functions depending on considerable number of inputs. Processing of ANNs is benchmarked from natural neurons and are developed the same to make a learning process. Moreover, ANNs provide a general, practical method for learning real-valued, discrete-valued, and vector-valued functions from examples. In the hidden layer it is performed the processing phase. In addition, the hidden layer is positioned among input and the output set of the application. The major goal of neural networks is to learn and retrain coefficient in the neural networks according to the data input and data outputs. The major advantages of ANN are high computation rate, learning ability through pattern presentation and prediction of unknown pattern flexibility to deal with noisy patterns. They provide a significant tool for detecting compromised nodes in MANET. When it comes to involve and apply artificial neural networks approach in the intrusion detection domain, firstly NN must be exposed to normal data formats and to known attacks in order to regulate and arrange coefficients accordingly throughout the training part.

Mitrokotsa and Kominos (2007) proposed an efficient detection approach combined with an Intrusion Detection Engine based on neural networks (NN) and an authenticated intrusion response, which relies on the innovation key agreement protocol. Intrusion detection engine is based on neural networks known as emergent Self Organizing Maps (eSOMs). This work has combined machine learning techniques, information visualization and key agreement protocol. Each node of ad-hoc network creates a map that reproduces its security state and disseminates this map to all neighboring nodes. Each node knows the security status of its neighbor by generating a global map. The paper provides a visual depiction of the normal-attack state on each node of the ad-hoc network. Then, key agreement protocol is combined with eSOMs in order to make sure the exploitation of information visualization will not be harmed by any malicious activity. Using key agreement protocol makes the approach capable to generate local key and global key. The proposed IDS architecture is made of multiple local IDS agents, which are locally responsible on detecting potential vulnerabilities. All local IDS together create the entire IDS system. The best matches of the trained dataset and thus the corresponding dataset are manually divided into groups representing normal and abnormal behavior. Then, it is identified the region of the map that represents the cluster that can be used for the classification on normal dataset.

One of the disadvantages of this method is high false alarm rate, which is caused due to the difficulty that the classifier eSOM faces in order to discriminate the changes in the behavior of the node.

The main advantage of the Intrusion Detection Engine and Intrusion Response Engine is the visual representation of the normal-attack state in mobile ad-hoc network. It has the capability to respond immediately in case an attack occurs by selecting the most secure node, as U-Matrix Map indicates for forwarding information. The key agreement protocol is used to verify the reliability and alteration of the maps.

The following-up work of Mitrokotsa and Kominos consisted of Neural Networks based intrusion detection systems and watermarking techniques for MANET (Mitrokotsa et al. 2007). In this paper, they presented an intrusion detection engine based on neural networks combined simultaneously with a protection method based on watermarking techniques. Throughout their paper, they have explored the strength of information visualization in order to better safeguard MANETs in terms of detecting flaws. Furthermore, they authenticate maps provided from intelligent techniques applications by implementing a novel watermarking embedded method. Results show and justify from various evaluation metrics that this novel framework leads to a high efficiency and accuracy in the detection process. The contribution of this paper is to first use the combination of neural networks and watermarking approach for MANET IDS. NN provides information visualization for achieving response of intrusion. Some open issues that arise in this context are that IDSs, which incorporate eSom, need to go through training in regular intervals. This may cause overheads] and affect efficiency and accuracy of the algorithms. Another major shortcoming of this method is not detecting different kinds of attacks.

One particular approach was proposed in Shao et al. (2010). They attempt to build a fruitful intrusion detection based on cooperative framework combining clustering techniques and Back Propagation Network (BPN). In one hand, clustering architecture ensures network scalability and fault tolerance, on the other hand, back-propagation neural network is appropriate tool for anomaly detection. The contribution of this research paper is in exploring the comparison between BPN and finite state machine (FSM), therefore adding another method to the anomaly based detection approach for MANET. In the implementation domain, this paper focuses on few attacks namely packet drop attack and changing serial number attack. The issue that packet related feature is too limited constitutes a substantial shortcoming of this proposed architecture.

One research work with regard to ANNs employed in the MANET perspective is introduced in Moradi et al. (2011). They discussed a mechanism of intrusion detection in MANET based on neural networks aiming to detect DoS attacks. Experimental phase is performed in a simulated MANET environment while inspecting the results of ANN modeling in the purpose of capturing DoS attack. This body of work provides significant evidence that the employed approach can effectively achieve high detection rate regarding the DoS attacks. Contribution of this paper to the field of IDS for MANET comprises successful employment of ANN modeling in order to detect a specific DoS attack. However, there are some gaps to be filled in the future work just like improving the limited feature selected for data collection. Furthermore, another drawback to overcome in future research is the concentration of one specific attack. This approach must be employed in other attacks rather than DoS attack.

Cannady (1998) illustrated a new design aiming to improve and better safeguard mobile ad-hoc networks. This body of work comprises the incorporation of the learning vector quantization neural networks that enables the identification attacks pattern in a distributed landscape. The goal of this study research was to demonstrate that can be designed an intrusion detection mechanism able to detect distributed attacks demanding multiple nodes data for accurate performance of analysis. This ongoing research carries out facilitation regarding complex attacks, which deliberates to exploit MANETS. This mechanism attempts to fill the gaps in the inherent MANET limitation by empowering the NN in the MANET landscape. This approach makes use of the Learning Vector Quantization algorithm (LQV) which aims to discover distributed attacks' instances and patterns. LQV comprises a self-organizing map (SOM) algorithm in regards to classification process and a competitive multilayer neural network. Furthermore, SOM outcome serves as input for the multilayer NN concerning pattern recognition. The significant contribution this paper provides to the body of knowledge is the presentation, development of a new approach and extending the current research in detecting MANET's malicious events. This piece of work has given strong evidence of obtaining good results encompassing the decentralized domain and the low bandwidth of MANET.

However, this mechanism poses limitation to identifying relatively straightforward attacks, for instance routing protocols.

In concluding to this section, we summarize that ANN provide the appropriate properties for intrusion detection. Due to their ability to learn patterns in the data sets and generalizing known patterns to new ones, ANNs are an effective and efficient approach for both misuse and anomaly detection. Intrusion detection scheme benefits of ANN flexibility regarding noisy/missing data (Cannady 1998) and some networks dispose the capability of continuously learning during run time. However, ANN are stated to be less sensitive to the selected input data. Additionally, whether features appears to be irrelevant ANN is not able to learn to neglect it. Two ANN drawbacks are being emphasized in Cannady (1998): the first comprises the training requirements; large amounts of training data are needed and the second flaw constitutes the difficulty when defining the topology of the ANN, which is deemed significantly time-consuming.

6 Instance-based learning approaches

In this section, we present the most relevant instance-based learning techniques that have been explored in the landscape of intrusion detection for MANET. Instance-Based Learning (IBL) encompasses techniques of obtaining a more flexible system when compared with the most expert systems, specifically concerning dynamic networks. IBL find out the solution based on prior solved instances and cases. Hence, they do not require knowledge engineering to figure out rules. Instances can be updated automatically and the system can learn by its own experience throughout its performance.

The most prominent approach pertained to Instance-based learning methods is certainly the nearest neighbor, which is conceptually a straightforward approach and operates to approximating real-valued or discrete-valued target functions. The learning process constitutes mainly storing the actual training data. When discovering a new query instance, a set of related instance is retrieved from memory, moreover is performed the classification of the above-mentioned new instances.

The k-NN algorithm classifies an instance by applying the criteria of majority vote among labels of the k-nearest neighbors. Abdel-Fattah and Dahalin (2010) proposed one promising strategy based on classification algorithms in order to detect compromised activity. They have introduced a novel IDS model, which consists of a combination of Conformal Predictor K-Nearest Neighbor algorithm and Distance based Outlier Detection algorithm dubbed as CPDoD algorithm. This approach employs two different parameters to enhance the detection performance. Firstly, the nonconformity metric measures, if the unknown instance is more similar to the normal instance or to the abnormal one and the second parameter are represented from the outlier factor LFOD. LFOD algorithm identifies the similarity to the normal class thereby detects the malicious activity. This algorithm utilizes machine learning and data mining techniques. It pertains to the transductive machine learning techniques. This work proposes a detection framework, which deploys the combined Anomaly and Signature detection in order to detect intrusion more efficiently. This algorithm works as follows: CP-kNN computes the nonconformity score of the query point and provides a sequence of p-value. This algorithm predicts when the points with the largest p-value belong to the class. The nonconformity score estimates that how much suitable is the new example to the one class compared to the other classes. Moreover, the Outlier Factor LDoF estimates the absolute deviation from the class of interest. The event, which is significantly far from the nonconformity score of the normal data, is dubbed as malicious. Authors implemented and tested the detection framework over three types of attacks dataset: Black Hole attack, resource consumption attack and dropping packet attack. It appears this algorithm performs better than the two other algorithms under three common dataset attacks, and achieves a high detection performance with low false positive rate.

Similarly, another application to IBL in the area of IDS for MANET is described in Abdel-Fattah et al. (2010). Although, traditional mechanisms have experienced difficulties in gathering real time attacks, hence researchers have been triggered to dig into and overcome it by designing a novel intrusion scheme to accurately detect malicious attempts in MANET. This research paper introduces a distributed and cooperative model combining the flexibility of anomaly detection with the signature-based detection accuracy. The novel approach employs a cooperative anomaly detection combined with machine learning techniques in order to improve the suggested model. Specifically this body of work focuses on Conformal Prediction K-Nearest Neighbor (CP-KNN) and Distance-Based Outlier Detection (DOD).Subsequently, they give evidence of new details and information attacks. They have categorized attacks in strong and weak ones and additionally, they have put special treatment for all of them. They have applied the proposed algorithm under three common attacks respectively resource consumption attack, dropping routing traffic attack and black hole attack in order to evaluate the performance of cooperative and distributed intrusion detection architecture. According to experimental results, the paper demonstrates that the novel approach can significantly detect abnormal activities with low positive rates while achieving higher detection rate.

Lalli and Palanisamy (2014) explored further the K-NN approach in MANET. The paper attempts to project a unique intrusion detection model for MANET. This model operates with the CP-KNN (Conformal Prediction K-Nearest Neighbor) algorithmic rule to classify the audit prior knowledge for anomaly detection. The non-conformity score value is utilized to lower the classification duration for multilevel iteration. This novel work accurately detects abnormalities with high true positive rate and low false positive rate. Authors highlight that the method is robust and at the same time remains a good performance of IDS even after the employment of the feature section. However, Conformal Prediction for k-nearest neighbor (CP-KNN) was utilized to estimate the resemblance between new instance and other samples undertaking the K-nearest neighbor method. The novel work demonstrates accurate detection of several abnormalities with high true positive rates, low false positive rates, and a high confidence rate. When introducing noisy data to the proposed method, it retains its good detection performance.

As a summary of IBL, we can emphasize that this artificial intelligent approach is efficient and effective in developing event correlation and has high memory requirements (Hanemann 2006) as it is necessary to store a large number of cases (Lane and Brodley 1999). Furthermore, the main advantage is that instead of providing a decision function for the entire input space, here is likely to be generated locally and differently for each of the examples. One major shortcoming of instance-based approaches is the high cost of classifying new instances. This happens because the computation process is carried out at the classification time instead of the time when training examples are encountered for the first time. In addition, another weakness of IBL approach is the fact that it considers all attributes of the instances in the process of retrieving the similar stored training example. However, in regards to MANET where the networks changes dynamically, it faces difficulties for determining general rules for the entire network activity. This is why IBL are applicable and of significant relevance for intrusion detection system in MANET because they overcome these challenges.

7 Conclusions

MANETs are being substantially a preferable target to various complex distributed threats, which mostly address the network and data link layer of the protocol stack. For this reason, it is very important an intrusion detection system to be deployed in MANETs as a second line of defense. While authentication and encryption techniques may protect in some terms like reducing the number of intrusions, however these cryptography techniques cannot perform well in unseen or novel attacks. In this case, machine-learning approach helps in detecting the unknown intrusive behavior.

In this paper, we have reviewed machine learning based detection systems for MANETs by categorizing them in four specific approaches.

Classification approaches for MANET is quite a limited field. It is not so rich when compared to the body of knowledge that researchers have been explored in other domains. Therefore, we suggest this field to be further investigated in order to enhance classification-based intrusion detection system in MANET.

Many traditional intrusion detection systems are limited in terms of collecting training data from real world. Deciding manually whether it is normal or abnormal behavior makes this process very time consuming. In association-rule mining, the efficiency is of paramount importance. The most prominent algorithm of the association rule mining approach is the Apriori algorithm, which is used as a fundamental method for anomaly detection. Association-rules mining algorithms employ lesser traffic when intrusion is included in the system compared to the prior intrusion detection systems that have been developed so far. However, Association-rule mining approach lacks robustness.

While ANNs provide the appropriate properties for intrusion detection due to their ability to learn patterns in the data sets and capability of generalizing known patterns to new ones. This leads to making ANN approach effective and efficient for both misuse and anomaly detection. Intrusion detection scheme can benefit of ANN flexibility regarding noisy data. However, ANNs are less sensitive to the selected input data; when features appears to be irrelevant ANN is not able to learn to neglect it. In addition, ANN needs large amounts of training data and it faces difficulties when defining the topology of the ANN, which is deemed significantly time-consuming.

IBLs are efficient and effective in developing event correlation and have high memory requirements, as it is necessary to store a large number of cases. The main advantage of IBL is that instead of providing a decision function for the entire input space, it generates locally and differently for each of the examples. One major shortcoming of instance-based approaches is the high cost of classifying new instances. In addition, another weakness of IBL approach is considering all attributes of the instances in the process of retrieving the similar stored training example.

Compliance with Ethical Standards

Conflict of interests L. Nishani and M. Biba state that there are no conflicts of interest.

Research involving Human Participants and/or Animals This article does not contain any studies with human or animal subjects.

Informed consent Informed consent is not required for the information referred in this research.

References

Abdel-Fattah, F., & Dahalin, F. (2010). Dynamic intrusion detection method for mobile ad hoc network using CPDOD algorithm. In *IJCA Special Issue on Mobile Ad-hoc Networks MANETs*.

Abdel-Fattah, F., Dahalin, F., & Jusoh, Sh. (2010). Distributed and cooperative hierarchical intrusion detection on MANETs. *International Journal of Computer Applications*, *12*(5).

Anjana-Devi, V., & Bhuvaneswaran, R.S. (2011a). Adaptive association rule mining based on cross layer intrusion detection system for MANET. *International Journal of Network Security & Its Applications (IJNSA), 3*(510.5121/ijnsa.2011.3519), 243.

Anjana-Devi, V., & Bhuvaneswaran, R.S. (2011b). Agent based cross layer intrusion detection system for MANET. In *Advances in Network Security and Applications Communications in Computer and Information Science*, (Vol. 196 pp. 427–440).

Bose, S., Bharathimurugan, S., & Kannan, A. (2007). Multi-layer intergraded anomaly intrusion detection for mobile ad hoc networks. In *Proceedings of the IEEE International Conference on Signal Processing Communications and Networking (ICSCN 2007)* (pp. 360–365).

Cabrera, J.B.D., Gutirrez, C., & Mehra, R.K. (2008). Ensemble methods for anomaly detection and distributed intrusion detection in mobile ad hoc networks. *Information Fusion*, *9*, 96–119.

Cannady, J. (1998). Artificial neural networks for misuse detection. In *Artificial Neural Networks - ICANN: International Conference Vienna*.

Changguo, Y., Qin, Zh., Jingwei, Zh., Nianzhong, W., Xiaorong, Zh., & Tailei, W. (2009). Improvement of association rules mining algorithm in wireless network intrusion detection. In *Computational Intelligence and Natural Computing International Conference*.

Cliftom, C., & Gengo, G. (2000). *Developing custom intrusion detection filters using data mining.* Military communications International LosAngeles.

Deepika, T., Vinchurkar, P., & Reshamwala, A. (2012). A review of intrusion detection system using neural network and machine learning. *ISSN: 2319-5967 ISO 9001:2008 (IJESIT)*, *1*(2).

Deng, H., Zeng, Q., & Agrawal, D.P. (2003). SVM-based intrusion detection system for wireless ad hoc networks. In *Proceedings of the 58thIEEE Vehicular Technology Conference (VTC03)*, (Vol. 3, pp. 2147–2151).

Engen, V. (2010). *Machine learning for network based intrusion detection. An investigation into Discrepancies in Findings with the KDD Cup 99 Data Set and Multi-Objective Evolution of Neural Network Classifier Ensembles for Imbalanced Data, Dissertation.* Bournemouth University.

Fung, C., & Boutaba, R. (2010). *Cooperation in Intrusion Detection Networks.* Cooperative Networks.

Fung, C., & Boutaba, R. (2013). *Design and Management of Collaborative Intrusion Detection Networks*. Ghent Belgium: IFIP/IEEE Integrated Network Management Symposium (IM).

Ghodratnama, S., Moosavi, M., Taheri, M., & Zolghadri, M. (2010). A cost sensitive learning algorithm for intrusion detection. In *Proceedings of the 18th Iranian Conference on Electrical Engineering (ICEE)* (pp. 559–565).

Hanemann, A. (2006). A hybrid rule-based/case-based reasoning approach for service fault Diagnosis. In *Proceedings of the 2006 International Symposium on Frontiers in Networking with Applications*.

Huang, Y., & Lee, W. (2003). A Cooperative Intrusion Detection System for Ad Hoc Networks. In *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks* (pp. 135–147).

Huang, Y., Lee, W., & Yu, P. (2003). Cross-feature analysis for detecting ad-hoc routing anomalies. In *Proceedings of the 23rd International Conference on Distributed Computing Systems* (p. 478).

Kaur, H., Singh, G., & Minhas, J. (2013). A review of machine learning based anomaly detection techniques. *International Journal of Computer Applications Technology and Research*, *2*(2), 185–187.

Lalli, M., & Palanisamy, V. (2014). A novel intrusion detection model for mobile ad-hoc networks using CP-KNN. *International Journal of Computer Networks & Communications (IJCNC)*, *6*(5). doi:10.5121/ijcnc.2014.6515_193.

Lane, T., & Brodley, C.E. (1999). Temporal sequence learning and data reduction for anomaly detection, ACM Transactions on Information and System Security, 295331.

Mabu, S., Chen, C., Lu, N., & Shimada, K. (2011). An intrusion-detection model based on fuzzy class-association-rule mining using genetic network programming. *IEEE Transactions on Systems Man and Cybernetics Part C*, *41*(1), 130–139.

Maheshwar, K., & Singh, D. (2013). A review of data mining based intrusion detection techniques. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, *2*(2), 2319–4847.

Mitrokotsa, A., & Kominos, N. (2007). Intrusion detection and response in ad hoc networks. In *International Journal of Computer Research*.

Mitrokotsa, A., Komninos, N., & Douligeris, Ch. (2007). Intrusion detection with neural networks and watermarking techniques for MANET. In *Proceedings of IEEE International Conference on Pervasive Services* (pp. 118–127).

Mitrokotsa, A., & Dimitrakakis, C. (2012). Intrusion detection in MANET using classification algorithms: The effects of cost and model selection ad-hoc Networks, Retrieved from doi:10.1016/j.adhoc.2012.05.006.

Moradi, Z., Teshnehlab, M., & Rahmani, A. (2011). Implementation of neural networks for intrusion detection in MANET. In *International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT)*.

Mukkamala, S., & Sung, A. (2006). *Significant feature selection using computational intelligent techniques for intrusion detection.* Berlin Heidelber: Springer.

Panos, Ch., Xenakis, Ch., & Stavrakakis, I. (2011). An evaluation of anomaly-based intrusion detection engines for mobile ad hoc networks. *Trust Privacy and Security in Digital Business Lecture Notes in Computer Science*, *6863*, 150–160.

Piatetsky-Shapiro, G., & Frawley, J. (1991). *Discovery analysis and presentation of strong rules.* Knowledge Discovery in Databases AAAI/MIT Press.

Ponsam, J., & Srinivasan, J. (2014). Multilayer intrusion detection in MANET. *International Journal of Computer Applications*, *98*(20).

Shao, M., Lin, J., & Lee, Y. (2010). Cluster-based cooperative back propagation network approach for intrusion detection in MANET. In *IEEE 10th International Conference on Computer an Information Technology (CIT)*.

Shrestha, R., Han, K., Choi, D., & Han, S. (2010). A cross layer intrusion detection system in MANET. In *24th IEEE International Conference on Advanced Information Networking and Applications*.

Somasundaram, R.M., & Lakshmana, K. (2013). An intrusion detection system for MANET using CRF based Feature Selection and Temporal Association Rules. In *International Journal of Soft Computing*.

Visumathi, J., & Shunmunganathan, K.S. (2012). An effective IDS using feature selection and classification algorithm. *International Conference on Modeling Optimization and computing, Procedia Enginnering*, (pp. 2816–2823).

Zhang, Y., & Lee, W. (2003). A cooperative intrusion detection system for ad-hoc networks. In *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, SASN03* (p. 135147).