Distributed and Cooperative Hierarchical Intrusion Detection on MANETs

Farhan Abdel-Fattah
Graduate Dept. of Computer Science
College of Arts and Sciences
Universiti Utara Malaysia
Sintok 06010 Kedah, Malaysia

Zulkhairi Md. Dahalin
Graduate Dept. of Computer Science
College of Arts and Sciences
Universiti Utara Malaysia
Sintok 06010 Kedah, Malaysia

Shaidah Jusoh
Graduate Dept. of Computer Science
College of Arts and Sciences
Universiti Utara Malaysia
Sintok 06010 Kedah, Malaysia

ABSTRACT

The wireless links between the nodes together with the dynamic-network nature of ad hoc network, increases the challenges of design and implement intrusion detection to detect the attacks. Traditional intrusion detection techniques have had trouble dealing with dynamic environments. In particular, issues such as collects real time attack related audit data and cooperative global detection. Therefore, we are motivated to design a new intrusion detection architecture which involves new detection technique to efficiently detect the abnormalities in the ad hoc networks. In this paper we present the architecture and operation of an intrusion detection technique in Mobile Ad hoc NETwork (MANET). The proposed model has distributed and cooperative architecture. The proposed intrusion detection technique combines the flexibility of anomaly detection with the accuracy of a signature-based detection method. In particular, we exploit machine learning techniques in order to achieve efficient and effective intrusion detection. A series of simulation and experimental results demonstrate that the proposed intrusion detection can effectively detect anomalies with low false positive rate, high detection rate and achieve higher detection accuracy.

General Terms

Intrusion detection, mobile Ad hoc Network Security, k-Nearest Neighbors.

Keywords

MANET Intrusion detection, CPDOD, CP-KNN, distributed and cooperative architecture intrusion detection, Conformal Prediction.

1. INTRODUCTION

Wireless network is seen as one of the fastest growing trends in technology. The flexibility that this network offers has attracted many people. However, its security issues have somehow distracted internet users from adopting this network freely. It is a responsibility of the network developer to ensure and enforce a secured network. Intrusion detection system (IDS) [1] plays a very important role in detecting different types of attacks. The main function of intrusion detection is to protect the network, analyze and find out intrusions among normal audit data. Although there is a number of intrusion detection techniques designed for traditional wired networks, they may not be suitable if applied to mobile ad hoc network due to the differences in their characteristics. Therefore, those techniques must be modified or new techniques must be developed to make intrusion detection work effectively in MANETs [2].

In this study, we investigate intrusion detection architecture suitable to the dynamic and distributed environments to meet the requirements of Intrusion detection for ad hoc network. Two intrusion detection architectures are considered in this research: local detection and hierarchical architecture. Distributed and cooperative hierarchical intrusion detection architecture, where nodes communicate with their region gateway node to make decisions, is proposed. The need for the cooperative and distributed intrusion detection arises because ad hoc networks are dynamic and they naturally lack a central administration or wired infrastructure. In comparison to local intrusion detection, the collaborative intrusion detection presents the possibility of improvement in detection time and detection accuracy, by sharing intrusion information between local intrusion detection in the same region or across regions. We have used cooperative anomaly intrusion detection with machine learning technique to enhance the proposed architecture. In our previous work [3] we proposed an efficient intrusion detection method based on the combination of two anomaly methods, namely Conformal Predictor k-nearest neighbor and Distance-based Outlier Detection (CPDOD). We investigate our proposed model by employing combined intrusion detection model and feature selection techniques and compared it with the performance of local detection.

The rest of the paper is organized as follows. Section 2 provides background knowledge of the intrusion detection models in MANET. We review some related work in Section 3. Section 4 and 5 present the Distributed and cooperative hierarchical intrusion detection model. Section 6 illustrates the experiments and presents the results with some discussion. Finally, we summarize our work in Section 7.

2. RELATED WORK

In the discussion of intrusion detection in ad hoc network, we have to distinguish between two concepts: intrusion detection architecture and intrusion detection methods [11]. Intrusion detection methods refer to the anomaly and misuse detection. While Intrusion detection architecture utilizes and employs intrusion detection methods as one of its modules, such as collaboration module and data collection module. Therefore, intrusion detection architecture deals with problems on a larger scale. Intrusion detection architecture defines the functions of network mobile nodes and the way they collect the data and the form of communication they utilize. A number of possible architectures of intrusion detection techniques in MANET have been proposed. These include stand-along intrusion detection, distributed and cooperative intrusion detection, and hierarchical intrusion detection [4, 5]. The intrusion detection proposed by Zhang and Lee [6] in 2000, was the first discussion about the intrusion detection techniques in MANET. This model uses distributed and cooperative decision making with anomaly detection. Patrick and Camp [7] proposed a distributed and collaborative architecture for MANET intrusion detection system, using mobile agent technology. In this architecture each node runs a Local IDS (LIDS) for local concern. Each LIDS detects intrusion on its node and uses external information that is derived from other LIDS on additional machines to confirm the detection.

Hierarchical intrusion detection architecture was proposed by Huang and Lee [8]. This model extends the distributed and cooperative IDS proposed by [7]. In this model the network is divided into clusters. A clusterhead is elected by a collection of nodes in a neighborhood or citizen nodes. Cluster size is defined as the number of mobile nodes in the cluster .When the cluster head is elected, all the nodes in the cluster have to transmit the data they obtain locally to the cluster head. A clusterhead is responsible for its node in addition to its cluster, e.g. monitoring and observing network packets and starting a global response when intrusion is detected [4]. A multisensor intrusion detection system based on mobile agent was proposed by Kachirski and Guha [9]. The intrusion system is composed of three major models: monitoring, decision-making and action agent (response agent). The ad hoc network is divided into clusters; each cluster has only one clusterhead. The workload is distributed by dividing IDS tasks into classes and assigning each task to a different agent. A Specificationbased Intrusion Detection System for Ad hoc On-Demand Distance Vector Routing (AODV) was proposed by Tseng et al. [10]. The normal behavior for important features in the ad hoc network is constructed in the first stage. Then the actual activity of the system is compared to the profiles of normal behavior of systems. This model uses Network Monitor (NM), Cooperative Network Monitors Architecture to trace the request-reply RREP flow in the MANET routing protocol.

2.1 Conformal Prediction

Gammerman et al. [11] use Transduction to present confidence measures for the decision of classifying an example point as belonging to a set of pre-defined classes. The recently introduced Conformal Predictor (CP) [12, 18] uses past experience to determine precise levels of confidence in predictions. CP introduced the computation of the confidence using Algorithmic Randomness Theory. Transaction confidence machine is a prediction technique that computes a p-value for the new example *v* of any predefined class *c*. The definition of p-value is the probability of observing an example in the sample space that can be considered more extreme than a sample of data. The p-value measure how well the data (examples of a class) supports a null hypothesis that the query point belongs to a certain class. The smaller the p-value, the greater is the evidence against the null hypothesis.

The Conformal Prediction for k-nearest neighbor (CP-KNN) algorithm computes the similarity between new individual and other examples in the class using the K-nearest neighbor distances method. The important step when applying transductive confidence is to calculate a nonconformity score value for each example. And estimates how likely it is that a new example belongs to this class with p-values. The main idea is that the nonconformity score corresponds to the uncertainty of the point being measured with respect to all the other classified examples of a class: the higher the nonconformity score, the higher the uncertainty [12, 13].

The CP-KNN nonconformity score is calculated using the Euclidean distances between points. Let us define $D_i^{\,y}$ as the sorted sequence of the Euclidean distances of point *i* from other points with the same classification *y*. The distance between *i* and the *jth* shortest examples in the sequence is $D_{ji}^{\;y}$ similarly let D_i^{-y} define the distances of example *i* from the other example with different classification, then D_{ji}^{-y} as the distance between *i* and the *jth* shortest examples in the sequence. α is an individual nonconformity score assign to every example. The nonconformity score for example *i* with classification *y* is α_{ij} .

$$\alpha_{ij} = \frac{\sum_{i=1}^{k} D_{ij}^{y}}{\sum_{i=1}^{k} D_{ij}^{-y}} \qquad (1)$$

Therefore, this measure of nonconformity is the ratio of the sum of the k nearest distances from the same class (y) to the sum of the k nearest distances from all other classes (-y). When there are several classes in the feature space, nonconformity score the fitness of the query example to class y with respect to all others classes in the features space. The nonconformity score of a example raises when the sum of the k nearest distances from the points of the same class becomes bigger or when the sum of the k nearest distances from the other classes becomes smaller.

Nonconformity score can be used in intrusion detection to measure the strangeness of an activity *i* belonging to the normal class *y* with respect to the abnormal class *-y*. The CP-KNN algorithm computes the nonconformity score of *m* training examples in class *y* and sorts their nonconformity score values in descending order { $\alpha_1, \alpha_2, \ldots, \alpha_m$ }. Based on Equation (1), the algorithm can also calculate the nonconformity score of the new query example *v* if it is classified as normal class *y*. Then, the p-value of the query point can be computed using Equation (2), where α_v is the nonconformity score of the new unknown example *v*.

$$p(\alpha_v) = \frac{\#\{i = (1,\ldots,m) : \alpha_i \geq \alpha_v\}}{m+1} \qquad (2)$$

As all training points are independent random samples, the strength of the evidence against *v* belonging to the class *y* is quantified by $p(\alpha_v)$, where *i* is the number of class members with nonconformity score larger than α_v . The *p*-value shows how likely the query point is to be classified as *y* by referring to the distribution of all points in the same class. The smaller the *p*-value the more unlikely the query point belongs to class *y*.

2.2 Distance-based Outlier Detection (DOD)

Recently, Zhang et al. [14] proposed Local Distance-based Outlier Factor (LDOF) to measure the outlier-ness of a point in the feature space. LDOF uses the relative location of a point to its neighbors to determining whether a point is an outlier with respect to all clusters. LDOF is the distance ratio representing and indicating how far the point x lies outside its neighborhood system. Formal definition of the Local Distance-based Outlier Factor:

Definition 1 (KNN distance of x_p) *Let N_p be the set of the k-nearest neighbours of object x_p (excluding x). The k-nearest neighbours distance of x_p equals the average distance from x_p to all objects in N_p. More formally, let dist(x , x') $\geq$ 0 be a distance measure between objects x and x'. The k-nearest neighbours distance of object x_p is defined as:*

$$\overline{d_{x_p}} = \frac{1}{k} \sum_{x_i \in N_p}^{k} dist(x_i, x_p).$$

Definition 2 (KNN inner distance of x_p) *Given the k-nearest neighbours set N_p of object x_p, the k-nearest neighbours inner distance of x_p is defined as the average distance among objects in N_p :*

$$\overline{D_{x_p}} = \frac{1}{k(k-1)} \sum_{x_i, x_{i'} \in N_p, i \neq i'} dist(x_i, x_{i'})$$

Definition 3 (LDOF of x_p) *The local distance-based outlier factor of x_p is defined as:*

$$LDOF_k(x_p) := \frac{\overline{d_{x_p}}}{\overline{D_{x_p}}}$$

When the Outlier Factor LDOF ≤ 1, it means that new example x_p is inside the class and surrounded by a class data. In contrast, when Outlier Factor LDOF $\geq$ 1, it means that new example x_p is outside the whole class. We use Outlier Factor LDOF to distinguish between normal and abnormal examples. It is easy to see that in any datasets, an example is outlier if Outlier Factor LDOF > 1.

3. INTRUSION DETECTION MODEL

Intrusion detection models on ad hoc networks can be classified into three groups: stand-alone, distributed and cooperative, and hierarchical intrusion detection. In stand-alone detection, every mobile node in the ad hoc network has an intrusion detection agent and makes the detection process on their own machine without collaborating with other mobile nodes. In a distributed and cooperative architecture, each node has intrusion detection agents as in the stand-alone detection architecture, at the same time they communicate with other mobile nodes to exchange attack data and helpful information, to make one global decisions and to agree on responses. The nodes in hierarchical intrusion detection are generally divided into small groups such as clusters, and zones where some mobile nodes have more responsibility than other mobile nodes in the same group.

In this research, we explore intrusion detection architecture and propose a region-based intrusion detection framework because of the following considerations. Flat architecture is unwanted in managing alerts. In this architecture all nodes are supposed to participate in the cooperative intrusion detection process [15]. When the ad hoc network becomes very large, huge power is consumed and scalability issues become a major problem [16]. It is also unrealistic to have a centralized manage point in MANETs to control all of the alerts because of the complicated mobility management and the network reliability problem caused by single point of failure [9, 16]. However, the existing clustering techniques [8, 9, 16, 17, 18] for MANET intrusion detection are simple adaptations of ones used in Ad-Hoc Network routing protocols and still have the similar problem of duplicate nodes and fragmented cluster [19], where the duplicate nodes are the nodes belonging to more than one cluster at the same time and fragmented clusters are the clusters with only one or two mobile node. Fragmented clusters are created because the clustering algorithm prefers a group of well-connected nodes as a cluster and tends to keep boundary nodes not belonging to any cluster as one node clusters. Duplicate nodes exist in the overlapped area between two neighboring clusters. Duplicate nodes and cluster fragments increase unnecessary monitoring and overhead on cluster heads [19]. Another major weakness of the clustered approach is the single point of failure; the failure of the cluster head. If a compromised node happens to be selected as the cluster head, it can initiate attacks without being detected [4, 23]. In addition, The biggest drawback with clustering techniques in MANET is the high cost of creating and maintaining the clusters and hierarchy in highly dynamic environment [20].

3.1 Assumptions

We assume a distributed and cooperative intrusion detection architecture that allows promiscuously monitoring of all Hello and TC messages. The intrusion detection models are supposed to have access to internal routing components, such as routing table. Intrusion detection model must also have the ability of intercepting messages transmitted between the mobile nodes, such as control packets, data packets and routing packets. We assume that the ad hoc network can be divided into geographic region. For instance, each node can use a Global Positioning System to find its physical geographic location and determine its region identity by mapping its physical geographic location to a predefined region map [20, 21]. The division of the ad hoc network could be based on geographic partitioning or other clustering algorithms. We assume that the region dividing method is accurate and safe. In addition, we assume that message transmitted between intrusion detection models cannot be altered or modified by an attacker and will not be compromised.

3.2 Intrusion Detection Framework

The proposed Intrusion Detection is a distributed detection method, in which two levels of hierarchical structure are defined; it is designed using region-based framework. The whole network is divided into non overlapping regions as shown in Figure 1. It is assumed that the existence of such a framework could be done without difficulty, based on techniques such as geographic partitioning [4]. There are two categories of nodes in our model: region member nodes and gateway nodes. The node is called a gateway if it has connection to a node in the neighboring region; otherwise, it is called a region node.

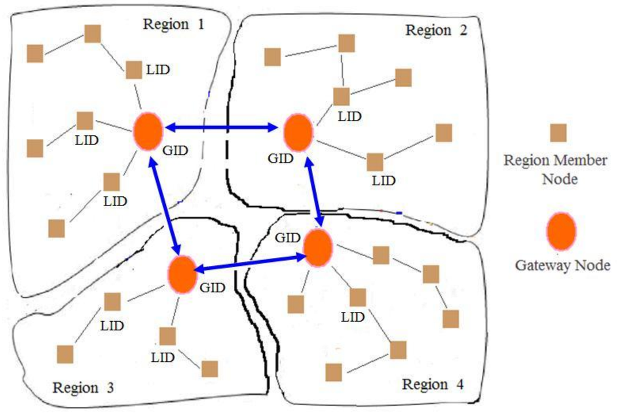

Figure 1: Intrusion Detection Framework

The proposed intrusion detection system intends to completely automate intrusion detection in a hierarchical and distributed way. The structure of our proposed intrusion detection model consists of two major components that is, Gateway Intrusion Detection (GID) and Local Intrusion Detection (LID). In this new hierarchical architecture, every mobile node runs a LID locally to perform local data collection and anomaly detection and initiate local response , and only a subset of the nodes (gateway nods) will run GID and such nodes are organized in multiple layers.

Local alarms are used to indicate a potential security attack recognized by local intrusion detection agents, while global alarms are finalized decisions made by GID. When a node locally detects an intrusion with strong evidence, depending on some threshold value, the node can initiate a Local Alarm by sending an alarm message to the nearest gateway node GID, which in turn triggers local and global response process. This actually starts local response module and global response module. Then, the GID stores this alarm in the long term memory (LTM). However, if a node detects intrusion with weak or inconclusive evidence and low confident prediction measure, the node initiates Local Alert to the nearest gateway node GID, which directly starts local and global cooperative intrusion detection procedure, as well as global detection module GDM, to search for new evidence and if any strong evidence is discovered, it initiates global response module. The global alarm communications among regions is accomplished through global response module and cooperation module, which share information among different security GID in network's regions.

Since we work in wireless network, the attack can come to the node by one of two ways: directly to the node by external attack or by its neighbors (internal attacks). For that, the attacks' evidences will be in the same node or with its neighbors. For that reason, the global detection process starts from the gateway node in the central region, then this region will grow by adding its neighbors, and every region add its neighbors until we get strong evidence with high confidant measures. At the same time, any region which does not have evidence will not participate in the global cooperation decision making process. By using growing region framework, we can minimize MANET bandwidth and energy consumption for intrusion detection purpose.

4. INTRUSION DETECTION ARCHITECTURE DESIGN

The proposed intrusion detection model consists of two major components that is, Gateway Intrusion Detection (GID) and Local Intrusion Detection (LID). Gateway Intrusion Detection is shown in Figure 2 and comprises of three components: Global Detection Model (GDM), Global Response Module (GRM) and Cooperation Module (CM). In the proposed intrusion detection, a gateway node can optimize energy use by scheduling only a subset of region members who will activate their monitoring sensors agents at one time. Other region members can minimize their energy consumption at the same time. LID is shown in Figure 2, and is mainly divided into: Data Collection module (DCM), Pre-process Module (PM), Local Detection Module (LDM) and Local Response Module (LRM).

The DCM collects audits data from various ad hoc network sources and pass it to the PM. PM selects informative feature from all features set, then pass these features to the LDM. The LDM analyzes the collected local data using CP-KNN and DOD classification algorithms, and identifies malicious nodes in the ad hoc network. From Figure 3 we can see that our proposed ad hoc intrusion detection system, based on the machine learning approaches, includes several modules which we will now introduce briefly and separately.

4.1 Data Collection Module

The data collection module collects attack related audit data from more than one source. This attack related data can include user and system data, network routing and data traffic and activity within the radio range of the data collection module. Collecting the correct and related set of features is an important step when formulating the prediction tasks. A node on an ad hoc network can only monitor a part of the network: the packets in its radio range and the packets which it sends or receives. The types of attacks we want to detect depend on the data source in addition to the selection of features. More than one data collection module can be utilized by local intrusion detection to collect a variety of environment state information. Each data collection module is in charge of gathering data from a particular data source.

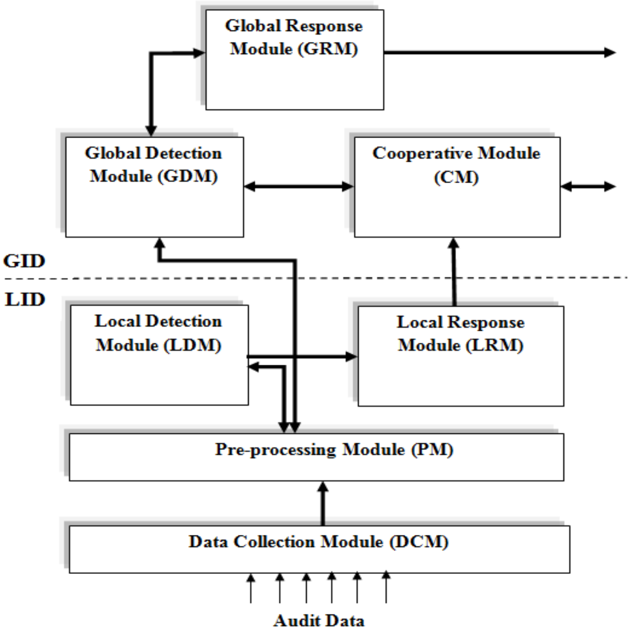
Global Response Module (GRM)
Global Detection Module (GDM)
Cooperative Module (CM)
GID
LID
Local Detection Module (LDM)
Local Response Module (LRM)
Pre-processing Module (PM)
Data Collection Module (DCM)
Audit Data

Figure 2: Intrusion Detection Components

4.2 Pre-processing Module

The data collection module of intrusion detection provides data of network activity. Not all network activity is important for intrusion detection task and if the detection module was presented with unrelated network activity, the intrusion detection task would be hard. Therefore, a number of features need to be selected to represent ad hoc network activity so that those features can be used to detect attacks. This initial subset features selection is part of the pre-processing in the domain of machine learning. In pre-processing module, we implement a feature selection algorithm. Different types of attack correspond to different feature selection. Higher performance may result if irrelevant features are removed.

Designing intrusion detection in ad hoc networks needs to define new features, as ad hoc networks are a new communication paradigm. Due to the distributed and dynamic nature of ad hoc networks, these features should also be locally collected. That is, they should be collected within the node itself or its communication activities by overheard transmissions to and from the nodes. In this thesis, the selected features are determined by the type of attacks we would like to detect. Therefore, pre-processing module runs several feature selection agent.

4.3 Local and Global Detection Module

Detection unite is the key component of the intrusion detection system. The function of detection module is to analyze the network activities and to draw a conclusion whether normal or anomalous. Different detection methods can be implemented in different detection models in order to improve the detection performance. The two main intrusion detection methods are anomaly methods and signature based methods: anomaly detection can detect unknown intrusion, but usually has a high positive false alarm rate while signature based detection is unable to detect new, unseen before attack that has no matched patterns stored in the signature data base. The major advantage of signature based method is that it can accurately detect known attacks with very low false alarm ratio. Therefore, we combine signature based detection and anomaly detection in order to detect unknown intrusion which achieves better positive false rate and detection rate. The research done in [22] suggests that a typical attacking process can be divided into three main phases: a learning phase, a standard attack phase, and an innovative attack phase. During the first phase, an inexpert new attacker learns about the limitation and vulnerabilities of the target system, to train himself for the second phase. A professional attacker directly moves into the standard attack phase and in this phase the attackers try out all attack methods they may know of previously. When all known attack methods tested fail, the attacker would be forced to go into the third phase (innovative attack phase) and try to find out and utilize vulnerabilities that may be new and unknown to system managers of the target system. It is expected that the attack launch during standard attack phase have high chances of success. Therefore, the well updated signature based detection model should be used to detect most of the attacks, and anomaly detection model is used to detect the innovative and unseen before attacks.

The detection module illustrated in Figure 3, integrates the flexibility of anomaly detection with the accuracy of a signature-based detection method. In detection module operations, observed activities are fed to the anomaly detection unit and misuse detection unit in parallel. Anomaly detection unit uses the CP-KNN as a main classifier to analyze the collected data. In this step, if the data is sufficient to find the class of activity (depending on the two labeled classes), the system initiates an intrusion alarm if the classification result is anomalous. On the other hand, if the result is normal, the system does not do any action. But if the CP-KNN predicts the class with confidence score less than a pre-defined threshold, then the system goes to the next step by using DOD algorithm, which uses only normal data to make the decision. The signature based unit applies the string matching to detect known attacks. Signature based unit raises an alarm to the response module if any activates matches an intrusion pattern. The signature generation unit describes the detected anomalies and extracts their signatures, then store the result in the attack signature database.

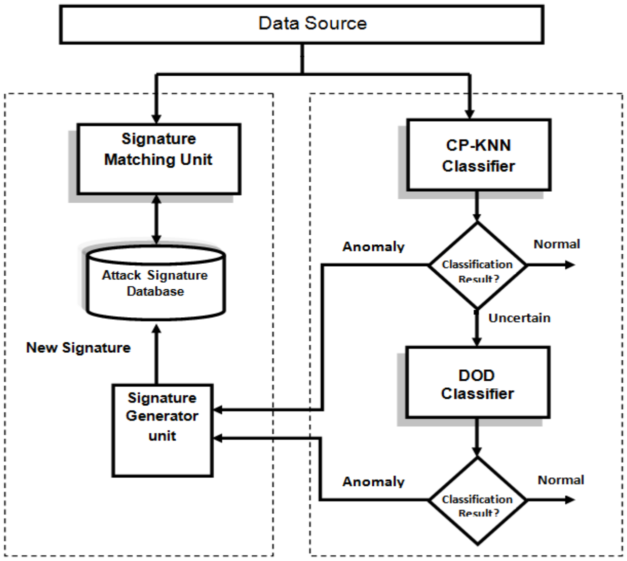

Figure 3: Detection Module

4.4 Cooperative Module

When local response module generates local alarm with conformal prediction score less than pre-defined thresholds, this local alarm moves from node detection level to region level. Cooperation Module identifies local alarms that belong to the same occurrence of an attack and create a global alarm that combines information contained in these different local alarms. The main process of Cooperation Module is to combine and analyze the information of all available sources such as local intrusion detection or neighbors' gateway intrusion detection to make accurate prediction. Cooperation Module allows us to reduce the number of not true alarms (false positive) transmitted to the security administrator, generated by response module and at the same time increases the detection rate of attacks.

4.5 Attack Signature Database

The long term memory or attack signature database is used to store attack signatures generated by detection module with high conformal prediction score. This memory will be updated periodically. In order to save network resources, we use this data in attack signature verification (signature matching) in detection model.

4.6 Local and Global Response Module

Local response module reports the detection result to its gateway intrusion detection (in the same region) if the detection result is less than some pre-define thresholds, and at the same time does not have enough evidence to make a decision. But if the detection result (conformal prediction score) is greater than some threshold, the module broadcasts the result. The global response module handles the generated alarms from LDM or GDM and sends the global alarms to the whole ad hoc network to notify the nodes of the network about the occurrence of an intrusion.

5. EXPERIMENTS AND EVALUATION

5.1 Simulation Environment

Simulators are the most common tools used for testing MANET intrusion detection systems [23, 24]. Simulators help researchers to study the performance and the reliability of their proposed IDS without using real mobile nodes. In order to evaluate our technique we simulated MANET by using Global Mobile information systems Simulation library (GloMoSim) [25]. It builds a scalable simulation environment for wireless and wired network systems. Parsec, a C-based simulation language based on parallel discrete-event simulation, is used to design GIoMoSim. We have taken Ad hoc On Demand Distance Vector (AODV) [26], one of the popular MANET routing algorithms [27], as a network routing protocol. Specifically, in the simulation are nodes having the same transmission range of 200 meters with the channel capacity of 2000 bps. We use the Distributed Coordination Function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. In this simulation, 30 mobile nodes were set to move in the area of 1000 meters x 1000 meters. To simulate the nodes' mobility, a Random Waypoint model (RW) is used. All nodes were set to move independently with the same average speed.

Wireless ad hoc network routing protocols are designed based on the concept that all the nodes must participate in the routing process. These protocols assume a trusted and cooperative network environment. Many researchers [28, 29] discussed various types of attacks that can be performed easily against the ad hoc network routing protocols. We choose to implement three common attacks to evaluate the performance of our Dynamic Intrusion Detection algorithm: Black Hole Attack, Resource Consumption Attack and Dropping Routing Traffic Attack.

In this work, 10 source nodes and 10 destination nodes are selected randomly to generate Constant Bit Rate (CBR) traffic as the background traffic. The transmission rate is 2 packets per second with the packet size of 512 bytes. In our simulation, in order to give the nodes enough time to finish the network initialization process, we collect the traffic data after a warm up time of 400 seconds. In our experiments, the data is sampled in three sampling periods: 10 seconds, 30 seconds, and 60 seconds. Selecting the correct set of features is an important step when formulating the classification tasks. We mainly consider the features which have been commonly used in the MANET intrusion detection research [16, 29]. The feature will be selected as a sensitive feature based on the confidence measure during CPDOD algorithm training phase, when some features give high confidence for normal prediction or anomaly prediction. Therefore, the features will depend on the region and type of attack. Because this research is focused on the routing attacks, the features' source mainly consists of the routing activities, Route table changes and Data packet transmission.

Table 1: Description of the datasets

Data set	Attack	Examples	sampling period
BHAT10	Black Hole	3000	10 seconds
BHAT30	Black Hole	1000	30 seconds
BHAT60	Black Hole	500	one minute
RCAT10	Resource Consumption	3000	10 seconds
RCAT30	Resource Consumption	1000	30 seconds
RCAT60	Resource Consumption	500	one minute
DRAT10	Dropping Routing Traffic	3000	10 seconds
DRAT30	Dropping Routing Traffic	1000	30 seconds
DRAT60	Dropping Routing Traffic	500	one minute
BRDAT	Three attacks	3000	10 seconds

5.2 Performance of Intrusion Detection Model

Intrusion detection systems are often evaluated on data containing attacks as well as normal traffic. The data may be simulated or collected from real networks. One of the most important problems facing MANET intrusion detection is the high false alarms rate or False Positive Rate (FPR), generated during intrusion detection process [18, 24]. The researcher in MANET intrusion detection focuses on ether to minimize false alarms rate or to maximize detection rate (the rate of attacks detected successfully). High detection rate and low false positive rate are required for any good intrusion detection system. In order to determine the relationship between false alarms rate and detection rate we used Receiver Operating Characteristic (ROC) curve as a performance evaluation metric to evaluate our intrusion detection algorithm. In intrusion detection, the ROC curve is usually used to measure the performance of the detection model [18, 24].

Table 2: Confusion Matrix

	Predicted Class positive	Predicted Class Negative
Actual Class Positive	TP	FN
Actual Class Negative	FP	TN

When a classifier predicts a class label for a certain example, this can have four possible results, a so-called confusion matrix, as shown in table 5.4. A negative prediction for negative example is called True negatives (TN), while positive prediction for negative examples is false positives (FP). A negative prediction for a positive example is labeled as false negative (FN), while a positive prediction for a positive example is called a true positive (TP). On the basis of this confusion matrix, a number of performance metrics can be calculated, and are described below.

True Positive Rate (TPR) measures the number of correctly classified examples relative to the total number of positive examples. This measure is also called Recall.

$$TPR = \frac{TP}{TP + FN} = \frac{\#\text{correct intrusions}}{\#\text{intrusions}} \qquad (3)$$

False Positive Rate (FPR) measures the number of misclassified positive instances in relative to the total number of misclassified instances.

$$FPR = \frac{FP}{FP + TN} = \frac{\#\text{normal as intrusions}}{\#\text{normal}} \qquad (4)$$

Classification accuracy (ACC) is the most essential measure of the performance of a classifier. It determines the proportion of correctly classified examples in relation to the total number of examples of the test set i.e. the ratio of true positives and true negatives to the total number of examples. From the confusion matrix, we can say that:

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} \qquad (5)$$

With 10 folds cross validation method [30], the data set is split randomly into 10 equal sized folds. We use one fold as a testing set and use the remaining fold to form a training set. We run an algorithm to the training set and evaluate the resulting model on the testing set. The process of evaluation is repeated 10 times, each time a different fold (10% of the data) is used as the test data and remaining folds (90% of the data) is used to form training set. The averaged accuracy of the classifiers from the 10 runs is reported.

Tables 3, 4, 5 and 6 show the results of the Cooperative intrusion Detection model, and the local intrusion detection model using both classifiers CP-KNN and DOD using the same metrics. It shows that the Cooperative detection model achieves a higher detection rate than local intrusion detection model. The false positive rate is also decreased. Moreover, the prediction accuracy of the Cooperative intrusion Detection model is higher than the model using local intrusion detection.

Table 3: Experimental results on Comparison of Local and Cooperative Intrusion Detection Model for Detection of Ad Hoc Resource Consumption Attack

	Local Detection			Cooperative Detection		
Data set	TPR	FPR	ACC	TPR	FPR	ACC
RCAT10	0.9620	0.041	0.9522	0.9960	0.0019	0.9976
RCAT30	0.9644	0.051	0.9355	0.9644	0.0116	0.9787
RCAT60	0.951	0.042	0.9300	0.9916	0.0086	0.9913

Table 4: Comparison of Local and Cooperative Intrusion Detection Model for Detection of Ad Hoc Black Hole Attack

	Local Detection			Cooperative Detection		
Data set	TPR	FPR	ACC	TPR	FPR	ACC
BHAT10	0.963	0.043	0.951	0.9943	0.0019	0.9973
BHAT30	0.95	0.026	0.965	0.9700	0.0115	0.9797
BHAT60	0.942	0.051	0.95	0.9802	0.0066	0.9887

Table 5: Comparison of Local and Cooperative Intrusion Detection Model for Detection of Ad Hoc Resource Dropping Routing Traffic Attack

	Local Detection			Cooperative Detection		
Data set	TPR	FPR	ACC	TPR	FPR	ACC
DRAT10	0.97	0.069	0.952	0.9922	0.0019	0.9968
DRAT30	0.971	0.044	0.965	0.9747	0.0156	0.9804
DRAT60	0.951	0.064	0.951	0.9720	0.0149	0.9797

Table 6: Comparison of Local and Cooperative Intrusion Detection Model for Detection the three Attacks

	Local Detection			Cooperative Detection		
Data set	TPR	FPR	ACC	TPR	FPR	ACC
BRDAT	0.9701	0.071	0.961	0.9885	0.0114	0.980

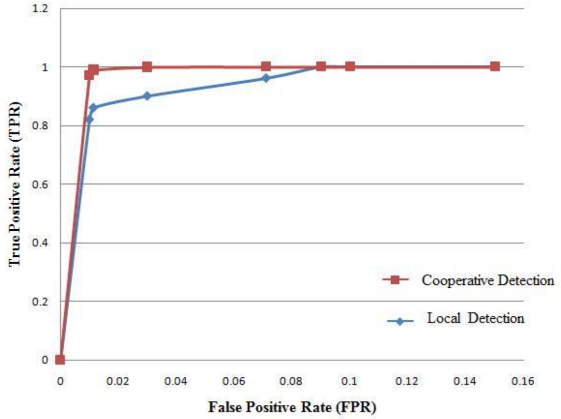

Figure 4: RCO curves showing the performance of Local and Cooperative Intrusion Detection Model over three Attacks dataset

Figure 4 shows the ROC curves of the performance of Local and Cooperative Intrusion Detection Model over three Attacks dataset (Black Hole Attack, Resource Consumption Attack and Dropping Routing Traffic Attack). It has been seen that the Cooperative intrusion Detection model achieves a higher detection performance.

6. CONCLUSION

We have presented the architecture and operation of cooperative and distributed intrusion detection for ad hoc networks, in non-overlapping region framework. This intrusion detection method uses machine learning techniques in order to achieve efficient and effective intrusion detection. This fits the distributed nature of MANET. Our proposed model combines the flexibility of anomaly detection with the accuracy of a signature-based detection method. In particular, we exploit two anomaly methods Conformal Predictor K-Nearest Neighbor (CP-KNN) and Distance-based Outlier Detection (DOD). By using cooperative and distributed system, we improve the intrusion detection approach to provide new details and information on attack types and sources. We classify the detected attacks into two types: strong and weak attack. And then gave a special treatment for each of them, the local alarm goes in three levels of processing which is the node, region and global, or network level to generate one global alarm. We implemented our detection algorithm and tested the detection approach over three common attacks dataset (resource consumption attack, dropping routing traffic Attack and black hole attack) to evaluate the performance of our cooperative and distributed Intrusion detection model. A series of experimental results demonstrate that the proposed model can effectively detect anomalies with low false positive rate, high detection rate and achieve higher detection accuracy.

7. REFERENCES

[1] N.J. Puketza, K. Zhang, M. Chung, B. Mukherjee, and R.A. Olsson. A methodology for testing intrusion detection systems. Software Engineering, IEEE Transactions on, 22(10):719 –729, October 1996.

[2] Y. Xiao, X. Shen, Tiranuch Anantvalee, and Jie Wu. Chapter 7 a survey on intrusion detection in mobile ad hoc networks, 2006.

[3] Farhan Abdel-Fattah, Zulkhairi Md. Dahalin, and Shaidah Jusoh. Dynamic intrusion detection method for mobile ad hoc network using cpdod algorithm. IJCA Special Issue on MANETs, (1):22–29, 2010. Published by Foundation of Computer Science, USA.

[4] Li, Y and J Wei. Guidelines on Selecting Intrusion Detection Methods in MANET. In *The Proceedings of the Information Systems Education Conference 2004*, v 21 (Newport): §3233. ISSN: 1542-7382.

[5] Paul Brutch and Calvin Ko. Challenges in intrusion detection for wireless ad-hoc networks. In Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), SAINT-W'03, pages 368–, Washington, DC, USA, 2003. IEEE Computer Society.

[6] Yongguang Zhang and Wenke Lee. Intrusion detection in wireless adhoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking, MobiCom '00, pages 275–283, New York, NY, USA, 2000. ACM.

[7] Patrick Albers, Olivier Camp, Jean marc Percher, Bernard Jouga, and Ricardo Puttini. Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches. In In Proceedings of the First International Workshop on Wireless Information Systems (WIS-2002, pages 1–12, 2002.

[8] Yi-an Huang and Wenke Lee. A cooperative intrusion detection system for ad hoc networks. In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, SASN '03, pages 135–147, New York, NY, USA, 2003. ACM.

[9] Oleg Kachirski and Ratan Guha. Intrusion detection using mobile agents in wireless ad hoc networks. In Proceedings of the IEEE Workshop on Knowledge Media Networking, pages 153–, Washington, DC, USA, 2002. IEEE Computer Society.

[10] Chin-Yang Tseng, Poornima Balasubramanyam, Calvin Ko, Rattapon Limprasittiporn, Jeff Rowe, and Karl Levitt. A specification-based intrusion detection system for aodv. In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, SASN '03, pages 125–134, New York, NY, USA, 2003. ACM.

[11] Alex Gammerman and Volodya Vovk. Prediction algorithms and con_dence measures based on algorithmic randomness theory. Theor. Comput. Sci., 287(1):209_217, 2002.

[12] Glenn Shafer and Vladimir Vovk. A tutorial on conformal prediction. J. Mach. Learn. Res., 9:371–421, 2008.

[13] Yang Li, Binxing Fang, Li Guo, and You Chen. Network anomaly detection based on tcm-knn algorithm. In ASIACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security, pages 13_19, New York, NY, USA, 2007. ACM.

[14] Ke Zhang, Marcus Hutter, and Huidong Jin. A new local distancebased outlier detection approach for scattered real-world data. CoRR, abs/0903.3257, 2009.

[15] A. Mishra, K. Nadkarni, and A. Patcha. Intrusion detection in wireless ad hoc networks. Wireless Communications, IEEE, 11(1):48 – 60, February 2004.

[16] Yi-an Huang, Wei Fan, Wenke Lee, and Philip S. Yu. Cross-feature analysis for detecting ad-hoc routing anomalies. In ICDCS '03: Proceedings of the 23rd International Conference on Distributed Computing Systems, page 478, Washington, DC, USA, 2003. IEEE Computer Society.

[17] D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C y. Tseng, T. Bowen, K. Levitt, and J. Rowe. A general cooperative intrusion detection architecture for manets. In In IWIA 05: Proceedings of the Third IEEE International Workshop on Information Assurance (IWIA05, pages 57–70. IEEE Computer Society, 2005.

[18] W J Ulivla. Evaluation of intrusion detection system. J. J. Res. Natl. Inst. Stand. Technol., 108(6):453–473, 2003.

[19] C.V. Zhou, S. Karunasekera, and C. Leckie. Evaluation of a decentralized architecture for large scale collaborative intrusion detection. In Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium on, 21 2007.

[20] Bo Sun, Kui Wu, and Udo W. Pooch. Alert aggregation in mobile ad hoc networks. In Proceedings of the 2nd ACM workshop on Wireless security, WiSe '03, pages 69–78, New York, NY, USA, 2003. ACM.

[21] Farhan A.F, Zulkhairi. D, and M.T. Hatim. Mobile agent intrusion detection system for mobile ad hoc networks: A non-overlapping zone approach. In Internet, 2008. ICI 2008. 4th IEEE/IFIP International Conference on, pages 1 –5, 2008.

[22] Erland Jonsson and Tomas Olovsson. A quantitative model of the security intrusion process based on attacker behavior. IEEE Trans. Softw. Eng., 23:235–245, April 1997.

[23] A. Karygiannis, E. Antonakakis, and A. Apostolopoulos. Host-based network monitoring tools for manets. In PE-WASUN '06: Proceedings of the 3rd ACM international workshop on Performance evaluation of wireless ad hoc, sensor and ubiquitous networks, pages 153–157, New York, NY, USA, 2006. ACM.

[24] Hadi Otrok, Joey Paquet, Mourad Debbabi, and Prabir Bhattacharya. Testing intrusion detection systems in manet: A comprehensive study. Communication Networks and Services Research, Annual Conference on, 0:364–371, 2007.

[25] GloMoSim. Glomosim website, June 2007.

[26] Charles Perkins and Elizabeth Royer. Ad-hoc on-demand distance vector routing. In In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pages 90–100, 1997.

[27] C. Siva Ram Murthy and B.S. Manoj. Ad Hoc Wireless Networks: Architectures and Protocols. Prentice Hall PTR, Upper Saddle River, NJ, USA, 2004.

[28] Varun Chandola, Arindam Banerjee, and Vipin Kumar. Anomaly detection: A survey. ACM Comput. Surv., 41(3):1–58, 2009.

[29] Hongmei Deng, Roger Xu, Jason Li, Frank Zhang, Renato Levy, and Wenke Lee. Agent-based cooperative anomaly detection for wireless ad hoc networks. In ICPADS '06: Proceedings of the 12th International Conference on Parallel and Distributed Systems, pages 613–620,

[30] Marcus A. Maloof. Machine Learning and Data Mining for Computer Security: Methods and Applications (Advanced Information and Knowledge Processing). Springer-Verlag New York, Inc., Secaucus, NJ, USA,2005.