Volume: 6 Issue: 4 Pages: 2414-2421 (2015) ISSN: 0975-0290

A Brief Study on Different Intrusions and Machine Learning-based Anomaly Detection Methods in Wireless Sensor Networks

J. Saranya[1]
Research Scholar
Dept. of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, India
Email: jsaranyam.philcs@gmail.com
Dr.G.Padmavathi[2]
Professor and Head
Dept. of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, India
Email: ganapathi.padmavathi@gmail.com

----------**ABSTRACT**----------
Wireless Sensor Networks (WSN) consist of a number of resource constrained sensors to collect and monitor data from unattended environments. Hence, security is a crucial task as the nodes are not provided with tamper-resistance hardware. Provision for secured communication in WSN is a challenging task especially due to the environment in which they are deployed. One of the main challenges is detection of intrusions. Intrusion detection system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches. Different intrusion detection methods have been proposed in the literature to identify attacks in the network. Out of these detection methods, machine-learning based methods are observed to be efficient in terms of detection accuracy and alert generations for the system to act immediately. A brief study on different intrusions along with the machine learning based anomaly detection methods are reviewed in this work. The study also classifies the machine learning algorithms into supervised, unsupervised and semi-supervised learning–based anomaly detection. The performances of the algorithms are compared and efficient methods are identified.

Keywords—**Anomaly Detection, Intrusions, Intrusion Detection System, Machine-learning algorithms**

Date of Submission: August 25, 2014 Date of Acceptance: November 5, 2014

1. Introduction

Wireless sensor networks (WSNs) are composed of a number of limited, battery-powered and multi-utilitarian devices called sensors which are obtusely arranged to collect data from untended environments. It offers numerous advantages over conventional networking in terms of lower cost, scalability, flexibility, reliability and ease of deployment. The constrained sensor resources in terms of memory, processing, transmission and power make WSNs vulnerable to a variety of malignant attacks. This provides the way for the attackers to launch attacks in these protocols. Modeling a stable security protocol is a difficult task and more expensive that leads to enforcement degradation. Intrusions are the set of actions by the intruders that attempt to compromise the principles of security. An Intruder attempts to gain illegitimate entry to a system/network [4]. It is built on many patterns such as refusing the services by inundating system resources, speedily inseminating a virus or worm, and gaining authorization of root users to perform malignant behavior. Network intruders enter the hosts through Enumeration, Viruses, Trojan horse, E-mail infection, password cracking, and router attacks [8]. Intrusions are caused by insiders and authorized users also while they attempt to gain and try to misuse unauthorized privileges. The various causes of intrusions include erroneous innovation, planning, hardware/software model and susceptibility, applications, component, operational defects and external disturbances.

The main objective of this paper is to provide a brief description of the classification of different intrusions and anomaly-based detection mechanisms using machine learning algorithms in WSN. The rest of the paper is organized as follows: Section 2 describes literature study. Section 3 and 4 discuss about the different intrusions and intrusion detection systems in WSN. Classification of anomaly-based detections in WSN is presented in Section 5. Machine learning-based anomaly detection is discussed in Section 6. Supervised, unsupervised and semi-supervised learning-based anomaly detections are discussed in Section

Volume: 6 Issue: 4 Pages: 2414-2421 (2015) ISSN: 0975-0290

6.1, 6.2 and 6.3. Section 7 and 8 give the conclusion and references.

2. Literature Study

Abror et.al [1] and Vijay Daniel et.al [7] surveyed on the various intrusions in WSN. To detect the attacks in WSN, three different types of intrusion handling mechanisms are used namely, i)Misuse detection ii) Anomaly detection and iii) Specification detection. Animesh patcha and Jung-Min Park [3] surveyed on different anomaly detection techniques. The techniques include statistical, machine-learning, data-mining based anomaly detection. Miao et.al [9] surveyed on the anomaly detection based on flat and hierarchical WSN. In the flat WSN, different techniques used are statistical, graph-based detection, data-mining and computational intelligence-based techniques. In hierarchical WSN, different approaches used to handle attacks are statistical, data-mining and game-theory based detection approach. Islam et.al [6] surveyed on various attacks in WSN and classified anomaly based intrusion detection system into OSI layer-based detection, sliding window, rule-based detection and delta grouping algorithm.

The present study classifies the anomaly-based detection using machine learning algorithms into supervised, unsupervised and semi-supervised learning algorithms.

3. Intrusions in Wireless Sensor Networks

Several attacks are launched on WSN. Handling the attacks are challenging due to limited resources. Some of the significant attacks are denial-of-service attacks, sinkhole attack, selective forwarding, node replication, wormhole and Sybil attacks [1]. The classification of intrusions in WSN is shown in Fig.1.

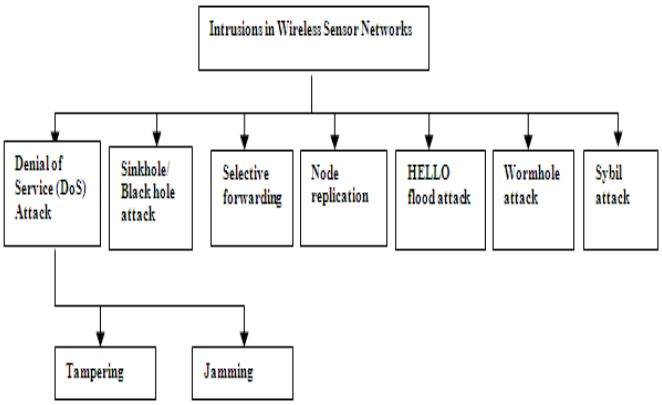

Fig.1 Intrusions in WSN

3.1 Denial of Service (DoS) Attacks

DoS attacks target the network resources and try to overburden them. It can be categorized into three types as consumption of scarce resources, destruction of configuration data or modification of computer/network resources. Jamming attack produces an intervention in the communication channel. Tampering attack tries to compromise the hardware of the sensor nodes.

3.2 Sinkhole/Black hole Attacks

A malicious node moves as a black hole and tries to spate the traffic in the network. It is very difficult to detect when the nodes are extended far from the base station.

3.3 Selective Forwarding

In this attack, a malicious node performs like a normal node by forwarding messages and selectively drops the messages, which are hard to detect by the system.

3.4 Node Replication Attacks

An attacker arrests and excerpts the data, tries to add one or more nodes in a network and starts performing similar cryptographic functions like genuine nodes which results in severe consequences.

3.5 HELLO Flood Attacks

In this case, the attack broadcasts HELLO packets to explore one-hop neighbors and the attacker makes use of such packets to engage broad number of sensor nodes by inundation the traffic in the network.

3.6 Wormhole Attacks

In this attack, an attacker reports the data at one location in the network to another location with the help of a long-range wireless channel.

3.7 Sybil Attacks

In this attack, a malicious node impersonates to be expanded than the normal node using the integrity of other legitimate nodes to prevent the collusion.

The next section discusses the different intrusion detection systems in wireless sensor networks.

4. Intrusion Detection Systems in WSN

An intrusion detection system (IDS) is a frame of reference used to detect illegitimate intrusions in a computer system/network [13]. There are three types of IDS [9] in WSN. They are Misuse detection, anomaly detection and specification detection. Fig.2 shows the classification of intrusion detection systems in WSN.

Volume: 6 Issue: 4 Pages: 2414-2421 (2015) ISSN: 0975-0290

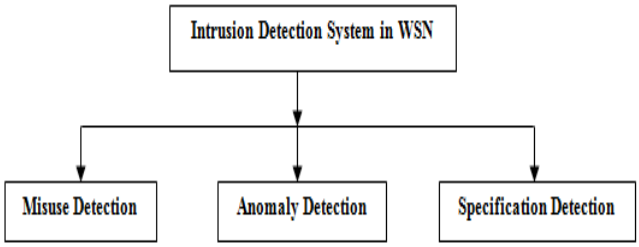

Fig.2 Classification of IDS in WSN

4.1. Misuse Detection

In misuse detection, the attitude of sensor nodes is correlated with infamous attack patterns. This technique requires knowledge to build attack patterns and difficult to detect novel attacks. The patterns must be well-defined.

4.1.1Limitation

This technique requires familiarity to build attack models and fail to detect unusual attacks.

4.2. Anomaly Detection

Anomaly detection analyses and the classifies the behavior of sensor nodes as normal or abnormal according to certain metrics such as changes made in payload of packet and retransmission of packet in specified threshold. This technique is used to detect uncommon attacks.

4.2.1 Limitation

This leads to an increase in substantial amount of false alarm rate.

4.3. Specification Detection

Specification detection incorporates misuse and anomaly detection and it targets on detecting the variations from usual observations.

4.3.1 Limitation

It requires manual development of all specifications.

Out of three detection methods, the anomaly based detection techniques are studied in this paper. The next section presents the various anomaly based detections in WSN.

5. Anomaly-Based Detections in WSN

An anomaly detection system is one of the intrusion detection systems available to model the normal system/network behavior which is effective in identifying both common as well as uncommon attacks. It is built on a normal system that studies the network or program activity. There are a number of different architectures and methods used for anomaly detection. They are statistical approach, clustering approach, centralized approach, artificial immune system, isolation table, machine learning approach and game-theory approach. Table 1 shows the overall comparison of IDS in terms of accuracy, energy efficiency, memory requirements and network structure. The classification of anomaly-based detection in WSN is shown in Fig.3.

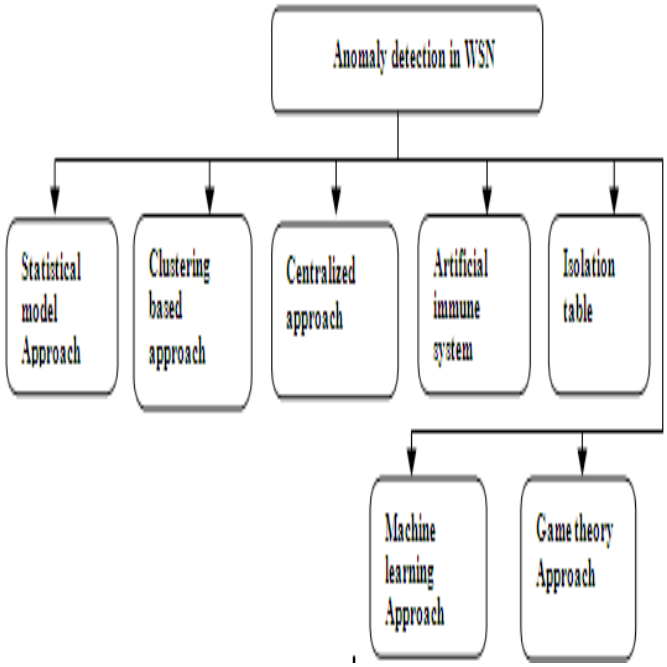

Fig.3 Classification of anomaly-based detection in WSN

5.1 Statistical Model-based approach

These approaches are based on statistical models built on each sensor node to classify the packets as normal or abnormal. At every node, end packets from each neighboring nodes are used to calculate the statistical metrics. Each arriving packet is compared with statistical model to classify it as normal or anomaly.

5.2 Clustering Model-based approach

This model uses unsupervised learning algorithms for routing attacks to build a model of normal behavior. The traffic samples are considered as a group of clusters. The clusters that contain less training traffic samples than a certain threshold are considered as anomaly. This model is used to detect anomaly in the traffic patterns.

Volume: 6 Issue: 4 Pages: 2414-2421 (2015) ISSN: 0975-0290

Table.1 Comparison of anomaly based IDS in WSN

IDS	Accuracy	Energy efficiency	Memory requirements	Network structure
Statistical model Based approach	Better accuracy is achieved	Minimum energy consumption	Minimum memory consumption	Normal
Clustering algorithm based approach	Achieves high detection rate	Energy efficiency is not discussed	High memory usage for computation	Cluster
Centralized approach	Achieves high detection rate	Energy efficiency is not discussed	Minimum memory consumption	Normal
Artificial immune system	Achieves high detection rate	Energy efficiency is not discussed	Minimum memory consumption	Normal
Isolation table	Minimum accuracy is achieved	High energy consumption	Minimum memory consumption	Cluster
Game theory based approach	Better accuracy is achieved	High energy consumption	Minimum memory consumption	Normal
Machine learning based approach	Achieves high detection rate	Achieved minimum consumption of energy	Minimum memory consumption	Normal

5.3 Centralized approach

A centralized anomaly detection system known as ANDES is available in the literature. In this approach, a detection agent is positioned in the base station and information are cascaded and scrutinized to identify network anomaly. It collects application data, management information and the node status information to detect intrusions.

5.4 Artificial Immune System-based approach

Artificial Immune System is very efficient and effective to detect node misbehaviors in WSN. Dendritic Cell algorithm is modeled to detect the cache poisoning attacks. Sensor nodes build two tables namely, interest cache table and data cache table. When a node receives a packet, necessary updates are performed in two cache tables. The signals and antigens are excerpted from each packet and moved to dendritic cell where the antigens are classified as benign or malicious.

5.5 Machine learning-based approach

Machine learning and automaton-based learning approaches are used for anomaly detection in WSN. These approaches are based on packet sampling, where a capacity of the packets roam in the network is fragmented to identify the malicious nodes. It makes use of hidden markov model to detect the affair to be out of range and raises a horror.

5.6 Isolation Table

Isolation table registers the anomaly information and detection table isolates the nodes in the network. The tables are generated by cluster head and forwarded to the base station. Out of the different anomaly based IDS, machine learning based methods are discussed in the next section.

6. Machine Learning-Based Anomaly Detection

Different techniques have been used for anomaly detection. Existing intrusion detections are not sufficient in detecting the novel attacks. Therefore, some anomaly detection approaches work on the available normal data and model them to identify the deviations. To solve the detection systems that rely on human intervention, machine-learning based anomaly detections are discussed. Machine learning deals with ability of a program to train and enhance the performance on a certain task [3]. The classification of Machine-learning based anomaly detection is as follows:

6.1 Supervised-learning based anomaly detection
6.2 Unsupervised-learning based anomaly detection
6.3 Semi-Supervised-learning based anomaly detection

Fig.4 shows the classification of Machine-learning based anomaly detection

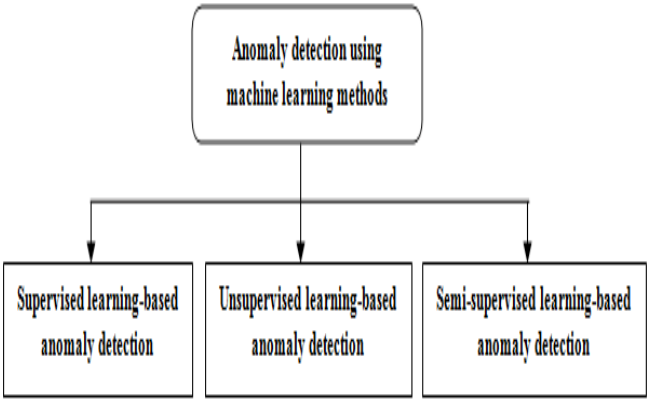

Fig.4 Different types of machine-learning based anomaly detection

6.1 Supervised Learning-based Anomaly Detection

In the supervised anomaly detection, the learning comes from the labeled examples in the training data set and mostly used for classification. Some of the supervised learning algorithms that are used for anomaly detection are designed based on support vector machine (SVM). They are also combined with principal component analysis (PCA), particle swarm optimization (PSO), AdaBoost-based classifier, and K-Means algorithm with C4.5 Decision trees to classify the network behaviors as either normal or

Volume: 6 Issue: 4 Pages: 2414-2421 (2015) ISSN: 0975-0290

abnormal behavior. Some examples of supervised machine learning algorithms are shown in Fig.5.

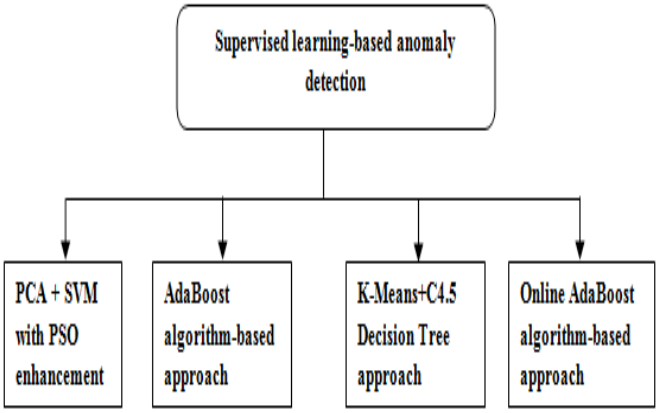

Fig.5 Example Supervised learning based anomaly detection methods

6.1.1 PCA+SVM with PSO Enhancement

The detection model based on SVM [16] combines PCA and PSO for anomaly detection. Principal Component Analysis (PCA) is used to reduce the dimensions of data. Particle Swarm Optimization algorithm is used to optimize the factors in SVM. PSO performs searches using a population called a swarm. Each particle moves in the direction of the previously best position and the best global position is used to find the optimal solution. The fitness of each particle is compared with its fitness value to update the particles best value.

6.1.2 AdaBoost algorithm-based approach

The detection model based on AdaBoost algorithm is used for anomaly detection. The decision stumps are used as weak classifier [17], and rules are provided for both categorical and continuous features. The data are classified for training that contains both normal data and attacks. The normal data is classified as "+1" and attack data is classified as "-1". A decision stump is built for each feature of the data. Strong classifier is attained by cascading the weak classifiers for the classification of network attacks.

6.1.3 K-Means + C4.5 Decision Tree-based Detection

The detection model using K-Means and C4.5 is used for distinguishing the normal and anomalous activities in a computer network [2]. Network intrusion detection system (NIDS) allows detecting the security policy violations. The process of cascading the K-Means and C4.5 method includes two phases: i) Selection phase ii) Classification phase. In the selection phase, Euclidean distance is measured to identify the closest cluster and C4.5 decision tree is employed to handle the neighbor cluster, whereas in the classification phase, C4.5 decision tree are computed on the test instance to classify it as normal one or anomalous one.

6.1.4 Online AdaBoost-based Intrusion Detection approach

In the online AdaBoost classifier, for each network connection, weak classifiers are constructed for both the continuous and categorical features [18]. Local intrusion detection models are designed using two algorithms: i) AdaBoost algorithm and decision stumps ii) Online AdaBoost classifier and online Gaussian Mixture Models (GMM). These are considered as weak classifiers. The local parametric models for intrusion detection are shared between the nodes of the network. Particle swarm optimization and support vector machine are used to cascade the local detection models into a global detection model. Table.2 shows performance comparison of supervised anomaly detection in terms of detection rate and false alarm rate.

Table.2 Comparison of supervised anomaly detection

S.No	IDS	Detection Rate (%)	False Alarm Rate (%)
1.	PCA+SVM with PSO Enhancement	97.75	Not discussed
2.	AdaBoost Algorithm-based Detection	90.88	1.7
3.	K-Means + C4.5 Decision Tree-based Detection	99.6	0.1
4.	Online AdaBoost-based Intrusion Detection approach	99.99	0.39

From the comparison, it can be noted that online AdaBoost-based intrusion detection approach is a well suited supervised learning algorithm due to higher detection rate and lower false alarm rate.

6.2 Unsupervised Learning-based Anomaly Detection

In the unsupervised learning algorithm, the learning process is unsupervised. The input data are not class labeled and mostly clustering algorithms are used to discover classes within the data. Some of the unsupervised-learning based algorithms are hyper spherical cluster-based approach and principal component classifier based detection approach. They operate in both the centralized and distributed manner. Unsupervised machine learning algorithms are shown in Fig.6.

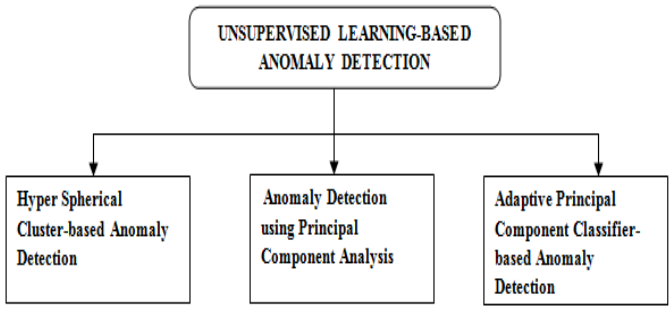

Fig.6 Example methods on unsupervised anomaly detection

Volume: 6 Issue: 4 Pages: 2414-2421 (2015) ISSN: 0975-0290

6.2.1 Hyper Spherical Cluster-based Anomaly Detection

A hyper spherical cluster based detection algorithm is used for identifying anomaly in WSN [14]. In the centralized approach, each sensor node sends all its data to the gateway node and combines all data to form a combined dataset. The fixed-width clustering algorithms are used for anomaly detection. They randomly choose data points as centroid and Euclidean distance is measured between the centroid and next remaining data vector. If the distance to the closest centroid from a data is less than radius, then the data is added to that cluster, otherwise a new cluster is formed. In the distributed approach, the model is scattered to all sensor nodes. The local anomalies are detected and clusters are classified as normal or anomalous using K-NN classifier. Fig.7 shows centralized and distributed approach.

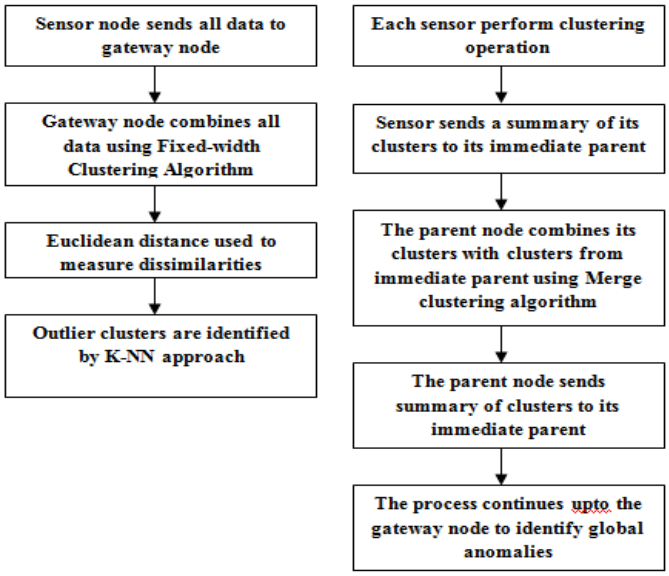

Fig.7 Centralized and Distributed approaches

6.2.2 Anomaly Detection using Principal Component Analysis

A new distributed online anomaly detection model is designed to measure the dissimilarities of sensor observations in WSN [11]. The candid-covariance free principal component analysis is utilized for data reduction in WSN. It includes two main stages. They are: i) Training stage ii) Detection stage. In the training stage, the observations are gathered at every sensor node to find the local normal model and sent it to the cluster head to create a global normal model. The detection threshold that represents the local normal model is chosen as the maximum and minimum range, whereas in the detection stage, every sensor observation is classified as normal or anomalous by analyzing the detection threshold from global normal model. This algorithm is based on the distance similarity to find the global anomalies in WSN.

6.2.3 Adaptive Principal Component Classifier-based Anomaly Detection

The principal component classifier-based anomaly detection model is designed to detect anomalous sensor measurements to track dynamic changes [10]. The model has three phases: i) Training phase, ii) online detection phase and iii) update phase. In the training phase, the standard data analysis is collected at each sensor node to frame normal model. The detection phase compares each data with normal model framed in the training phase to classify the data as normal or anomalous. In the update phase, the normal model is retrained to produce a new normal reference model. The performance comparison of unsupervised anomaly detection algorithms in terms of detection rate (DR) and false alarm rate (FAR) are shown in Table.3.

Table.3 Comparison of unsupervised anomaly detection

S.No	IDS	Detection Rate (%)	False Alarm Rate (%)
1.	Hyper-spherical Cluster-based Anomaly Detection	85.47	1.48
2.	Anomaly Detection using Principal Component Analysis (PCA)	82.86	13.3
3.	Adaptive Principal Component Classifier-based Anomaly Detection	97.84	1.10

From the comparison, it can be noted that the adaptive principal component classifier is good under supervised learning algorithm in terms of detection rate and false alarm rate.

6.3 Semi-Supervised Learning-Based Anomaly Detection

Semi-supervised learning-based anomaly detection is a class of machine-learning techniques that make use of both the classified and unclassified data for training. Fig.8 shows the classification of semi-supervised anomaly detection. Some of the semi-supervised learning anomaly detections are fuzzy-rough semi supervised outlier approach, triangle area-based nearest neighbors approach, twin support vector machine and hybrid machine learning detection approach.

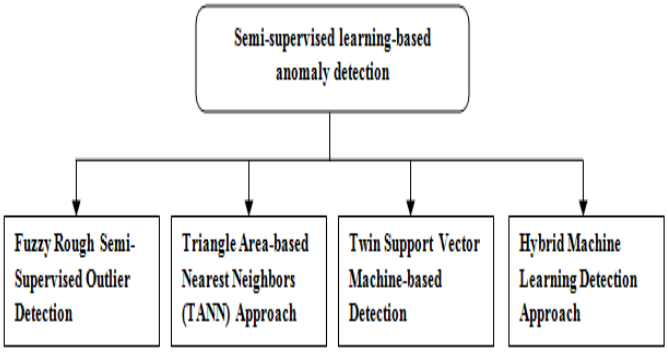

Fig.8 Examples of Semi-supervised anomaly detection

Volume: 6 Issue: 4 Pages: 2414-2421 (2015) ISSN: 0975-0290

6.3.1 Fuzzy Rough Semi-Supervised Outlier Detection

The semi-supervised outlier detection makes use of both the labeled and unlabeled data. The Fuzzy-rough semi-supervised outlier detection algorithm merges the fuzzy theory, rough theory and semi-supervised learning model to detect the anomaly [19]. The Fuzzy C-Means clustering model dissolves data into clusters with a fuzzy membership function in the range 0 to 1. Rough C-Means classifies the data into three parts as follows: i) lower similarity ii) Boundary and iii) weak range. The data in lower similarity returns the similar weight and form a cluster, where the objects in the boundary fit to a cluster to some limit. Finally, the new cluster center is computed.

6.3.2 Triangle Area-based Nearest Neighbors (TANN) Approach

The model based on hybrid machine learning identifies unusual access in the network to secure internal networks [5]. The mode is composed of three stages as follows: i) cluster centers extraction ii) New data formation iii) K-NN training and testing. The K-means clustering algorithms are used to identify five centroids of each category as data points. The formation of new data is obtained from three data points. Two data points are taken for K-means clustering centroid. Euclidean distance formula is used to calculate the distance between two points, and final data point is selected from the data to form a triangle area. The Heron's formula is used to calculate triangle area. K-NN classifier is used to classify attacks based on the new feature formed by triangle area.

6.3.3 Twin Support Vector Machine-based Detection

The detection system based on static reference model and twin support vector machines are designed to detect intrusions [12]. The intrusion detection system architecture consists of three parts. The data preprocessing model acquires and scrutinizes the network traffic features. This phase excerpt network traffic features and drives the features into feature static reference model.

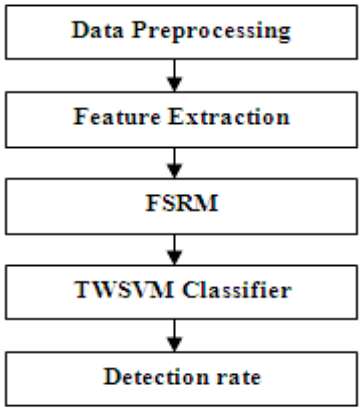

Fig.9 Framework of Twin Support Vector Machine

The FSRM is a reference model that exercise a probability density function (PDF) to consider the effect of each feature. The TWSVM classifier catches two hyper planes and classifies it according to the neighbor. The experiments are conducted on KDD'99 dataset and results of detection rate of FSRM with TWSVM show improvements when compared to traditional SVM with FSRM. *Limitations*: It is not good enough in detecting new attack types, where the model is constructed with the known attack features.

6.3.4 Hybrid Machine Learning Detection Approach

Hybrid machine learning approaches are used for network anomaly detection [15]. The normal packet is constructed using Self-Organized feature Map (SOFM) for SVM learning. A packet filtering approach based on passive TCP/IP fingerprinting is used to filter incomplete network traffic. Feature selection techniques using genetic algorithm (GA) are used to extract optimized features. The SVM model combines two kinds of machine learning methods: i) Soft-margin SVM and ii) one-class SVM. M-cross validation test is used to verify the approach and compared with the real world NIDS.

Table.3 Comparison of semi-supervised anomaly detection

S.No	IDS	Detection Rate (%)	False Alarm Rate (%)
1.	Fuzzy Rough Semi-Supervised Outlier Detection	87.89	0.80
2.	Triangle Area-based Nearest Neighbors (TANN) Approach	98.95	3.83
3.	Twin Support Vector Machine-based Detection	97.94	Not discussed
4.	Hybrid Machine Learning Detection Approach	95.63	4.37

The performance comparison of semi-supervised anomaly detection algorithms in terms of detection rate (DR) and false alarm rate (FAR) are shown in Table.3. From the comparison, it can be noted that Triangle area-based nearest neighbor intrusion detection approach is well suited under supervised learning algorithm in terms of the detection rate and false alarm rate in WSN.

7. Conclusion

Wireless Sensor Networks (WSN) is progressively used as an important terrace to aggregate and observe data from untended environments. The deployment of constrained sensor resources in such environment is susceptible to a variety of potential attacks. There are various intrusion detection mechanisms that are used to identify the attacks in a network with high detection rate. Anomaly detection approaches are modeled to identify the deviations in the system due to unknown attacks. To handle the detection systems that rely on human intervention, machine-learning

Volume: 6 Issue: 4 Pages: 2414-2421 (2015) ISSN: 0975-0290

based anomaly detections are designed that are capable of detecting novel attacks. Compared with classification of machine-learning-based anomaly detections, it is observed that unsupervised-learning based anomaly detection is efficient in unknown attack detection.

References

[1]. Abror Abduvaliyev, Al-Sakib Khan Pathan et.al, On the vital Areas of Intrusion Detection System in wireless Sensor Networks, *IEEE, Vol.15, No.3*, 2013.

[2]. Amuthan Prabakar Muniyandi, R. Rajeshwari and R.Rajaram, Network Anomaly Detection by Cascading K-Means Clustering and C4.5 Decision Tree algorithm, *Elsevier, Vol.30*, 2012.

[3]. Animesh Patcha and Jung-Min Park, An overview of anomaly detection techniques: Existing solutions and latest technological trends, *Elsevier Computer Networks, Vol. 51*, 2007.

[4]. P Charles, P. Fleeger, Shari Lawrence Fleeter, *Security in Computing (*10th Edition, Pearson Education Inc, 2009).

[5]. Chih-Fong Tsai and Chia-Ying Lin, A Triangle area based nearest neighbors approach to intrusion detection, *Elsevier Pattern Recognition, Vol. 43*, 2010.

[6]. M. S. Islam, and S. AshiqurRahmal, Anomaly Intrusion Detection System in Wireless Sensor Networks, *Security Threats and Existing Approaches, International Journal of Advanced Science and Technology, vol. 36*, November 2011.

[7]. J. Vijay Daniel, S. Joshna, and P. Manjula, A Survey of Various Intrusion Detection Techniques in Wireless Sensor Network, *International Journal of Computer Science and Mobile Computing, Vol. 2*, Issue. 9, 2013.

[8]. S. Maxwell Drive, *Computer Forensics Investigating Network Intrusions & Cybercrime*, (Engages Learning, 2010).

[9]. Miao Xie, SongHan, BimingTian and, SaziaParvin, Anomaly detection in wireless sensor networks: A survey, *Elsevier Journal of Network and Computer Applications, Vol.34*, 2011.

[10]. Murad A. Rassam, Mohd Aizaini Maarof and Anazida Zainal, Adaptive and online data anomaly detection for wireless sensor systems, *Elsevier*, 2014.

[11]. Murad A.Rassam, Anazida Zainal and Mohd Aizaini Maarof, An Efficient distributed anomaly detection model for wireless sensor networks, *Elsevier*, 2013.

[12]. Nie Wei and He Di, A Probability Approach to Anomaly Detection with Twin Support Vector Machines, *Journal of Shanghai Jiaotong University Vol.15*, 2010.

[13]. Roman R, Zhou J, and Lopez J, Applying Intrusion Detection Systems to Wireless Sensor Networks, *Proc. Conf. on Consumer Communications and Networking*, 2006, pp. 640-644.

[14]. Sutharshan Rajasegarar, Christopher Leckie and Marimuthu Palaniswami, Hyper spherical cluster based distributed anomaly detection in wireless sensor networks, *Elsevier Journal of Distributed Computing, Vol.74*, 2014.

[15]. Taeshik Shon and Jongsub Moon, A hybrid machine learning approach to network anomaly detection, *Elsevier, Vol.177*, 2007.

[16]. Wang Hui, Zhang Guiling *et.al*, A Novel Intrusion Detection Method Based on Improved SVM by Combining PCA and PSO, *Journal of Natural Sciences, Vol.16, No.5*, 2011.

[17]. Weiming Hu and Steve Maybank, AdaBoost-Based Algorithm for Network Intrusion Detection, *IEEE, Vol.8, No.32*, 2008.

[18]. Weiming Hu, Jun Gao, Yanguo Wang, Ou Wu and Steve Maybank, Online AdaBoost-Based Parameterized Methods for Dynamic Distributed Network Intrusion Detection, *IEEE, Vol.44, No.1*, 2014.

[19]. Zhenxia Xue, Youlin Shang and Aifen Feng, "Semi-supervised outlier detection based on fuzzy rough C-means clustering", *Elsevier, Vol. 80*, 2010.

Authors Biography

J.Saranya received her MCA degree from Avinashilingam Institute for Home Science and Higher Education for Women University, Coimbatore in 2013. She completed her M.Phil at Avinashilingam Institute for Home Science and Higher Education for Women University, Coimbatore in 2014. Her areas of interest are Network Security, Wireless Sensor Networks and Mobile Ad-hoc Networks.

Dr.G.Padmavathi is the Professor and Head of computer science Department of Avinashilingam Institute for Home Science and Higher Education for Women University, Coimbatore. She has 25 years of teaching experience and one year of industrial experience. Her areas of interest include Real Time Communication, Network Security and Cryptography. She has significant number of publications in peer reviewed International and National Journals. Life member of CSI, ISTE, WSEAS, AACE and ACRS.