Intrusion Detection System in Wireless Sensor Networks: A Review

Anush Ananthakumar
Student of Electronics and Telecommunication Engineering
Thadomal Shahani Engineering College
Mumbai, India

Tanmay Ganediwal
Student of Electronics and Telecommunication Engineering
Thadomal Shahani Engineering College
Mumbai, India

Dr. Ashwini Kunte
HOD of Electronics and Telecommunication Engineering
Vice Principal of Thadomal Shahani Engineering College
Mumbai, India

***Abstract*—The security of wireless sensor networks is a topic that has been studied extensively in the literature. The intrusion detection system is used to detect various attacks occurring on sensor nodes of Wireless Sensor Networks that are placed in various hostile environments. As many innovative and efficient models have emerged in the last decade in this area, we mainly focus our work on Intrusion detection Systems. This paper reviews various intrusion detection systems which can be broadly classified based on certain traditional techniques, namely signature based, anomaly based and hybrid based. The models proposed by various researchers have been critically examined based on certain classification parameters, such as detection rate, false alarm, algorithms used, etc. This work contains a summarization study of various intrusion detection systems used particularly in Wireless Sensor Networks, and also highlights their distinct features.**

Keywords*—Wireless sensor networks; Intrusion Detction System; Signature based IDS; Anomaly based IDS; Hybrid based IDS; Algorithms

I. INTRODUCTION

Wireless Sensor Networks (WSN) are used for monitoring the environment or a given area by collection of data, such as temperature, sound, pressure, light, etc from various Sensor Nodes (SNs) and analyzing them at a Base Station [1, 2]. The WSN consists of hundreds of sensor nodes that are basically small sensors used for monitoring the environment. The advantage of these sensors is that they can be placed in any location where surveillance by humans is not possible, including harsh climatic conditions or underwater surveillance [3]. The WSNs are used in a variety of fields ranging from healthcare and area monitoring to environmental and industrial monitoring systems.

This paper focuses on one of the applications of Wireless Sensor Networks namely Intrusion Detection Systems (IDS) [5, 6]. Intrusion detection systems are used to detect intrusions in a certain network or an area under surveillance. Intrusion is defined as an unauthorized (unwanted) activity in a network. In [4], an efficient IDS has been proposed in the field of healthcare for prevention against intrusions. On the basis of detection methodology, IDS are traditionally classified into 3 models: Anomaly based, Signature based and Hybrid Based IDS. The signature based IDS have predefined set of rules that are designed on the basis of previously known security attacks and the signatures of the attacks are stored in a database. The signature is a kind of pattern that describes a known attack. The incoming information is compared and checked with the previously identified signatures and hence protect against well known attacks and also have the advantage of low false alarm rate (FAR). A preliminary rule based approach to detect intrusions is developed in [7] that is based on comparison of the incoming packets with known signatures. On the other hand as it has been pointed out in [8, 9], the signature based model is similar to an anti-virus system that has a database and can detect known attacks but has problems when unknown attacks whose signatures are unknown are to be detected. To eliminate this particular drawback, the anomaly based IDS are used which works on the basis of a threshold [10]. This type of IDS defines what is called as a normal behaviour and an abnormal behaviour. Any new inbound information packet is verified against this normal behaviour and determined if it is an intrusion or not. As the detection mechanism is based on a threshold for normal traffic pattern, it has the capability to detect new intrusions, but on the other hand, it has a major disadvantage of missing out on well known attacks. The anomaly based model has a high detection rate and seldom classifies an actual intrusion as a normal packet, but it has a large false positive rate (FPR) i.e normal packets are defined as abnormal. Also as suggested in [11], there could be attacks due to hybrid anomaly which consists of multiple anomaly attacks, for which he proposes a model which has a detection technique based on K-means clustering. To improve on the disadvantages of these two conventional methods, a hybrid of the two IDS is usually incorporated known as a Hybrid Intrusion Detection System (HIDS). In this system, both the IDS are present, with the anomaly based IDS usually functioning as a filter and the signature based IDS as a second level of intrusion detection as it has low false positives and can accurately detect the intrusions. For example, [12] has proposed a hybrid intrusion detection model that integrates anomaly based IDS based on support vector mechanism (SVM) with a misuse detection based IDS to achieve a high detection rate of 98% and a low false positive rate. Apart from these, a developing area of intrusion detection is the cross layered IDS that can detect attacks on different OSI layers. A cross layer based IDS that integrates the Mac and Physical layer has been proposed by [13]. However in this paper, we focus only on the signature, anomaly and hybrid based IDS. This paper attempts to review the work carried out by various

researchers in the broad area of intrusion detection systems, which are traditionally classified as signature, anomaly and hybrid based IDS. It is of interest to see how various models perform with respect to certain critical parameters that help us in understanding the robustness and effectiveness of these models against various security threats. This will also help in drawing certain important insights about the algorithms used and the preferred detection techniques incorporated in different conditions.

In Section 2, various models of Signature, Anomaly and Hybrid based IDS proposed by various researchers has been discussed. The subsequent section is on the analysis of these models based on eight parameters, namely the model used, algorithms used, the data set used for experiments and simulation, detection rate, false detection rate, attacks against which the IDS protects, adaptive/ learning nature of IDS and the distinct feature of the model. The last section is the conclusion.

II. Literature Survey

A. Anomaly based Intrusion Detection System:

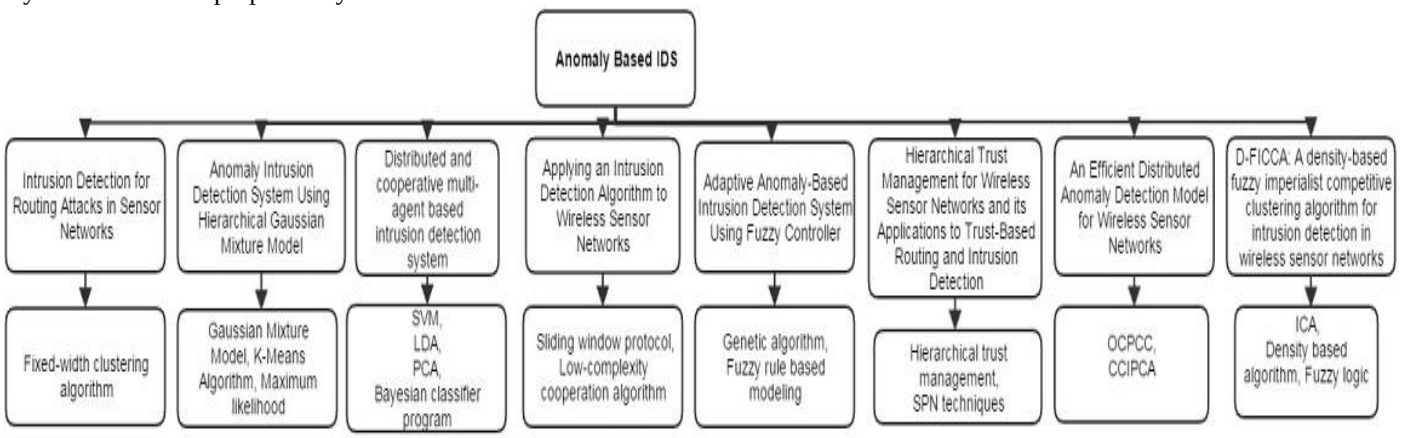

Fig. 1. Anomaly Based IDS

First the anomaly based intrusion detection systems have been discussed in detail. Chong eik loo et.al. [14] has designed an anomaly based IDS that collects information of normal traffic pattern which is then used to detect abnormal traffic patterns. In this technique no information is to be shared between the nodes and every node is equipped with an IDS which works independently without information from neighbouring nodes so as to conserve maximum energy. The anomaly based approach is based on a fixed width clustering algorithm which is used to model the distribution of training points. Using this model, 95% detection rate for a 5% false positive rate was achieved for periodic route attack. For passive sinkhole attack, the detection rate is 70% for a 5% false positive rate. For the active sinkhole (the most effective attack), detection rate is 100% with a 5% false positive rate. But in this method it is assumed that each node has sufficient power and resources so as to perform the computation required for proper functioning of the IDS. An anomaly based model incorporating Hierarchical Gaussian Mixture Model (HGMM) that classifies network attacks based on statistical pre-processing classification has been proposed in [15]. The normal and intrusive behaviours are learnt by Gaussian probability distribution functions and are used to classify observed system activities. The HGMM model proposed has also been compared with six other techniques: Gaussian Mixture, Radial Basis Function, Binary Tree Classifier, SOM, ART and LAMASTAR [34], and the results indicate that the proposed HGMM is able to achieve high accuracy, detection rate and low false positives. A major problem in WSNs is the availability of resources; hence the IDS must be resource efficient. The IDS presented in [16] uses mobile agents to collect data from the system and the classification of normal behaviour of the nodes is based on a SVM classifier. The mobile agent gathers information from the local agents before allowing the system to send data. Whenever information is sent in the network to any another system, the mobile agent gathers information from the neighbouring node and then calls the SVM to detect if an attack has occurred. If no suspicious behaviour is encountered, the information is then sent on the network.

This type of model is able to stop intrusion in the network level, and promises high levels of detection rate compared to traditional security measures. Another IDS using the information shared between neighbouring nodes is developed in [17], which is based on a simple and resource constrained WSN. This WSN consists of various static sensor nodes which create a statistical model of normal behaviour of their neighbouring nodes. Once this statistical model is created for each node, then the neighbouring nodes analyze the incoming packets on various layers and classifies whether an intrusion has occurred or not. The statistical model of the neighbouring nodes is used to determine a maximum and minimum threshold of the power consumption per packet, so that incoming packets having a receive power less than or greater than the minimum and maximum thresholds respectively, are classified as abnormal packets. The use of the low complexity algorithm improves the detection and containment process. Bao et. al [19] proposes a cluster based hierarchical trust management protocol for wireless sensor networks(WSNs). This IDS based on trust management protocol [35, 36] detects selfish or malicious sensor nodes for intrusion tolerance and can dynamically learn from the past experiences and adapt to the environment. It maintains two levels of trust management:

at the sensor level and other at the cluster head. The false positive and negative probabilities are dependent on the trust threshold and weight of social trust. A variety of methods exist for classification of intrusions, such as statistical techniques, which we have already observed in the two initial papers, data mining methods, etc. A method that is widely used for intrusion detection is based on fuzzy rules, as proposed by [18] which uses fuzzy controller to increase system performance and accuracy based on Adaptive anomaly. Here detection model generator is used for generating a detection model while IDS engine classifies test records and stores them in Buffer which are monitored and reports it to Fuzzy model tuner which updates the confidence prediction ratio. The proposed model gives accuracy of 15% higher than other machine learning methods and static models. Using the fuzzy rules, a density based fuzzy imperialist competitive clustering algorithm for intrusion detection in wireless sensor networks is proposed by [21]. It consists of the imperialist competitive algorithm (ICA) integrated with a density based algorithm and fuzzy logic for optimum clustering in WSNs. This proposed model increases the accuracy of security attack detection compared with KMICA, Kmean, and DBSCAN. The results demonstrate that the proposed framework achieves higher detection accuracy of 87% and clustering quality 0.99 compared to existing approaches. There have also been innovative algorithms and methods to reduce the energy consumption in WSNs such as the model used by Rassam et. al.[20]. This paper introduces a distributed anomaly detection model based on one class Principal component classifier (OCPCC) that uses the candid covariance free incremental principal component analysis (CCIPCA) algorithm so as to detect the intrusions as they occur. The sensor nodes classify every packet as either normal or abnormal according to the threshold specified in global normal model (GNM) that is formed during the training phase of the IDS. Various papers on anomaly based IDS that have been considered in this study are indicated in Fig I along with the respective algorithms used by each author.

B. Signature based Intrusion Detection System:

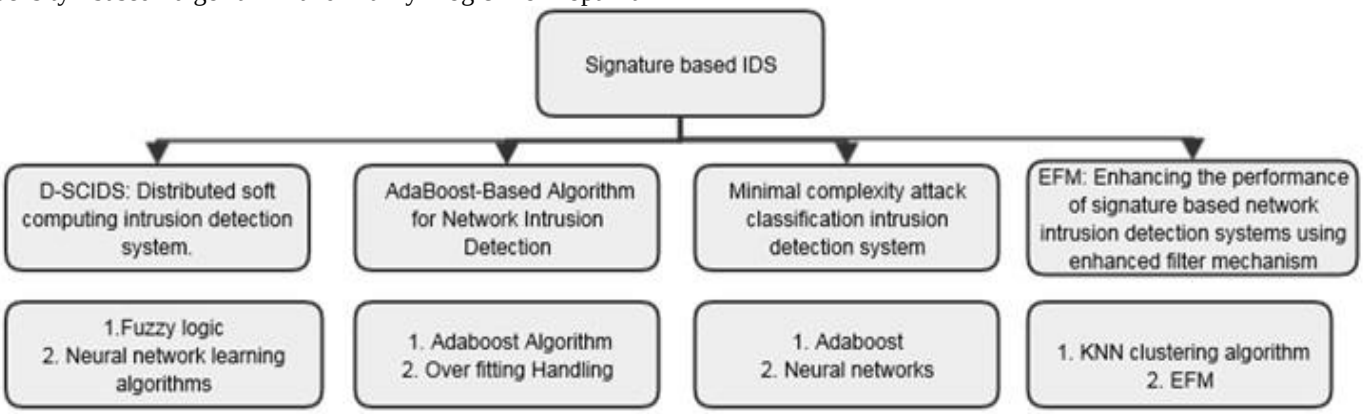

Fig. 2. Signature based IDS

The signature based IDS or misuse based IDS works on various set of rules and compares new information packets with already known signatures to detect intrusions. Abrahama et. al. [22] compared three fuzzy rule based approaches namely: 1:Rule generation based on the histogram of attribute values (FR1) 2:Rule generation based on partition of overlapping areas (FR2) 3:Neural learning of fuzzy rules (FR3). Since none of these approaches were able to single handedly get accurate results for all classes they proposed a new model which is a combination of different classifiers. The proposed heavy weight model was able to get 100% accuracy for all attacks and lightweight was able to get minimum accuracy of 94% for all attacks. A famous algorithm based on signature matching is the Adaboost algorithm and this algorithm has been incorporated in a network based IDS by [23]. The AdaBoost algorithm is a machine learning algorithm which corrects the misclassifications made by weak classifiers, which in this case are decision stumps [37].The decision rules are provided for both continuous and categorical features. Recognition performances of the AdaBoost based classifiers are fast and are generally encouraging. The following algorithm is compared against other algorithms such as SVM, SOM, RSSDSS, etc based on detection rate and false alarm rate. A simple overfitting handling is used to improve the learning results. But the following adaboost algorithm cannot be applied for incremental learning and does not support offline learning. Using the concept of adaboost and neural network method, an innovative design has been proposed by [24] to lower computational complexity by incorporating rules learnt from the behaviour of the network. The rules have been made according to the data set of KDD99, which is analysed in this case. The proposed IDS has been compared with the adaboost and neural network method. Even though classification by adaboost is better than neural network method, the proposed rule based method provides higher classification rate and lower computational time and also has the capability to learn rules from the behaviour of the network. Statistical methods such as KNN, are being widely used to improve the performance and speed of the signature matching. W. Meng et. al. [25] has used the concept of enhanced filter mechanism (EFM) on a network based IDS which improves the performance of a signature based IDS such as Snort [44] and consists of a context-aware blacklist-based packet filter, an exclusive signature matching component and a KNN-based false alarm filter. The blacklist based packet filter reduces the work of NIDS as it filters out intrusions based on IP address. The signature matching performs the important function of

identifying the intrusion based on signatures and the KNN-based filter is used to reduce the false positives i.e false alarms. The average detection accuracy of this IDS is about 86%, but this is based on the training set, with appropriate training a detection accuracy of over 90% is possible. Also it promises a great reduction in the false alarms. Fig II contains information about the various signature based IDS and algorithms which have been studied in this survey.

C. Hybrid based Intrusion Detection System:

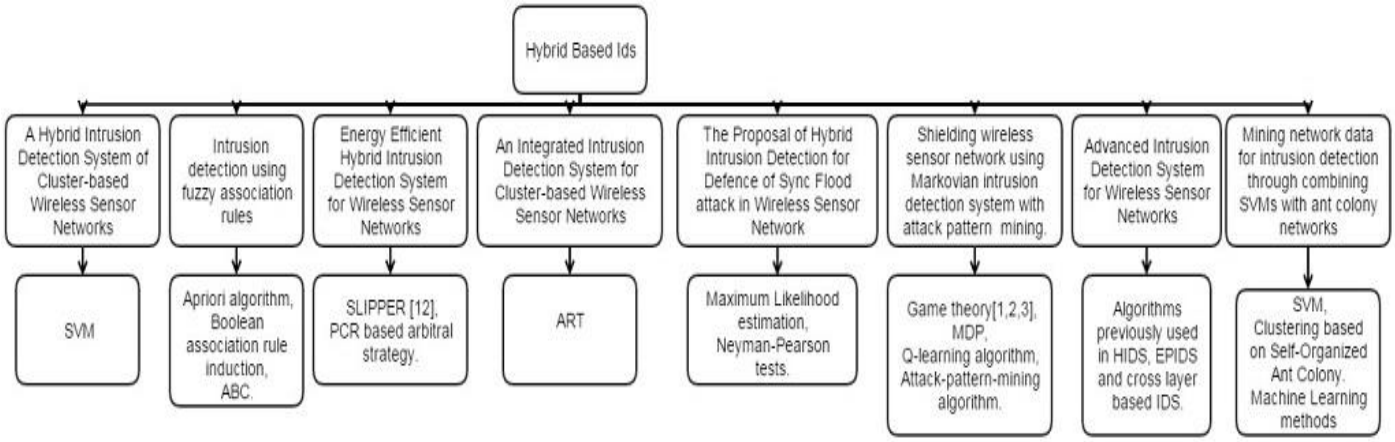

Fig. 3. Hybrid based IDS

The hybrid based IDS is a combination of both the signature based and anomaly based IDS and capitalizes on their advantages and results in a higher detection rate, false alarm, etc. Various data mining techniques like Association Based Classification (ABC) as incorporated by [27] are used to combine the two traditional detection methods. This paper was one of the early attempts that uses fuzzy association rulesets as descriptive models of different classes and combines anomaly based and signature based IDS using Association Based Classification (ABC) technique which is one of the well known approaches of data mining techniques. The fuzzy association rules are utilized to improve the time utilization of data mining technique. The performance of anomaly and misuse based IDS are evaluated separately and the proposed algorithm is shown to have a better performance than the two models independently. By combining the anomaly detection method with misuse detection method, the false positive error rate is very low and it also promises a good detection rate. Attacks on a WSN are usually on the Cluster Head (CH) as it collects data from different sensor nodes in a particular sensor and hence proper protection needs to be provided. K.Q. Yan [26] has proposed a hybrid based IDS for intrusion detection at the CH of a CWSN. The anomaly based model is used as a filter and a signature based IDS is used to detect the intrusion. It additionally consists of a decision making module that decides if an intrusion has occurred. The output of which is given to the administrator for the follow up work. In this model, the training sample must be sufficient to ensure high detection rates. A major difficulty in using Hybrid based models is the high consumption of resources and energy as indicated by Alrajeh [38]. To improve the energy efficiency, [28] has proposed a cluster based WSN (CWSN) so as to reduce communication costs and computational energy. CWSN helps to reduce the energy consumption and increase the lifetime of the model. The following eHIDS has been compared with HIDS and eHIP. In this scheme, each node of eHIP consumes on an average 2,91J and HIDS consumes 2,58J for the total packet transmission process, whereas eHIDS uses only 1,93J. This model achieves high accuracy, high detection rates, low energy consumption and low computational costs. The intrusive attacks in a network may be unknown to the IDS many a times and using a learning mechanism will help in storing a signature of the particular attack for future prevention, as is the case in the model incorporated by [29]. In this paper a model is proposed which has 3 separate IDS for sink, cluster head (CH) and Sensor node. The model is a cluster based WSN (CWSN). The 3 proposed IDS are: Intelligent Hybrid Intrusion Detection System (IHIDS) for the sink that has learning ability, Hybrid Intrusion Detection System (HIDS) for the cluster Head (CH) and a misuse based IDS for the sensor nodes. The first level of filter is done by anomaly detection and the identified intrusions are sent to misuse detection for further analysis. If the intrusions are not identified by the misuse detection then it is sent to the learning mechanism of IHIDS. IHIDS decreases the energy consumption and also reduces the information efficiently. The proposed IHIDS can achieve a high detection rate and low false positive rate and it also learns about new attacks on the IDS using ART [39]. Based on incorporating the learning mechanism in IDS, [31] has also proposed a new model that uses Markovian IDS to protect sensor nodes from attack. It integrates Anomaly based, Misuse based and game theory to prevent malicious attacks. The Markov decision process is used in the self learning process of the IDS and determines the weakest nodes to be protected. The system is able to reveal the patterns from which it predicts future points of attack and devises appropriate defence strategies, and also has a high detection rate.

TABLE I. ANOMALY BASED IDS

Authors	Algorithms Used	Data Set Source	Adaptive	Detection Accuracy (DA) and False Detection Rate (FDR)	Protection against Attacks	Distinct Features and type of WSN
[14] Loo et al. (2006)	Fixed-width clustering algorithm	1. NRL 2. NS-2	No	DA= 1. 95% for routing attacks. 2. 100% for active sinkhole attack. FDR=5% (FN)	Periodic route error attack, Active sinkhole attacks	Routing protocol is AODV. No information exchange between neighbouring nodes. Ad hoc placement of sensors.
[15] Behrololum and Khalegi (2008)	1. GMM 2. K-Means Algorithm 3. Maximum likelihood	MIT's Lincoln Lab[42]	No	DA=88.14% FDR=4.70	Probe, Dos, R2L, U2R	Uses statistical preprocessing classification. Classifies based on Gaussian probability distribution functions.
[16] Renjit and Shunmuganathan (2010)	1. SVM. 2. LDA. 3. PCA. 4. BCP	NA	Yes	DA=89%-98%. FDR= 5-9%(False Positive)	NA	Differentiates congestive packet loss from malicious packet loss. Anomaly detection result of neighbouring node is used.
[17] Wang et al. (2009)	1. SWP 2. Low-complexity cooperation algorithm	NA	No	DA > 90% FDR=Decreases with increase in intrusion buffer lengths.	Node Impersonation, Resource Depletion	Checks for anomalous packets from neighbouring nodes. Develops a statistical model of normal behaviour of these nodes.
[18] Abbaspour et al. (2012)	Genetic algorithm, Fuzzy rule based modeling	KDD Cup99	Yes	DA=86.71(TN) FDR= 13.29 (FN) 57.71(FP)	NA	Accuracy 78.6. Online Adaptation. CWSN
[19] Bao et al. (2012)	1.Hierarchical trust management 2. SPN	Self made	Yes	DA>90% when FP approaches zero FDR= Limited to 5%	BH,SH, Slandering attacks, Flooding-Based Routing	Hierarchical trust based IDS based on social trust and QoS trust. Learns from its past experiences and adapts to changes in network. CWSN
[20] Rassam et al. (2013)	1. OCPCC 2. CCIPCA	GSB	No	DA=96% FDR=7.2%	NA	High detection effectiveness. Utilizes network resources efficiently. Distributed online IDS.
[21] Shamshirband et al. (2014)	1. ICA 2. Density based algorithm. 3. Fuzzy logic.	1.IRL[41] 2.ARC[40]	Yes	DA> 87% FDR=15	DoS	Reinforces detection function against incoming DDoS attacks. Continuous self-learning from prior attacks. CWSN.

There have been IDS which are developed for protection against a specific attack, usually used for application specific IDS. One such model based on protection against sync flood attacks has been proposed by [30]. They propose a Hybrid Intrusion Detection System that works on Stream flow and state transition analysis by which the malicious nodes are effectively shut down. The main attack on which the model focusses is Sync Flood attack that establishes a number of TCP connections to use a large amount of resources on the affected nodes. The proposed hybrid detection approach is faster and effective in case of densely deployed sensor network and alarming the base station about the infected or abnormal behavior in the flow of the traffic.

To further improve on the range of attacks against which protection is provided and to enhance the detection rate considerably, Simenthy et.al. [32] proposes a new advanced intrusion detection system that consists of Hybrid Intrusion detection system(HIDS), Energy Prediction based Intrusion Detection System(EPIDS) and cross layer detection system in different stages to ensure maximum security. The Advanced intrusion Detection System has been compared with Energy Prediction Model, HIDS and Cross Layer Model, and it was analyzed that the proposed model gave better attack detection, less false positives and better detection probability compared to the other 3 models. Also in this system, the energy efficiency and lifetime of the system increases. A recent model that works on the principle of Clustering based on Self Organized Ant Colony Network (CSOACN) and SVM has been proposed by [33] to develop a hybrid based IDS. The SVM is used to find support vectors and to generate hyperplane that separates normal and abnormal data while a CSOACN is used to find data added to active SVM training set and to finally generate models for normal data as well as for each class of abnormal data. An important aspect of this paper is that the processes of training and testing are done parallelly. The detection rate of this model is 94.86%, False positive is 6.01% and False negative is 1.00%. The paper highlights that the proposed CSVAC (Combining Support Vectors with Ant Colony) performs better than SVM and CSOACN applied independently. Hybrid based IDS which have been studied in this survey are depicted in Fig III along with the algorithms used in each study.

This paper attempts to review these three important techniques, namely anomaly, signature and hybrid based IDS. The need of such a research is to provide an insight into the recent developments in the area of intrusion detection and provide details about the different types of IDS required according to varying requirements of the wireless sensor network.

III. COMPARISON

Various papers of anomaly, signature and hybrid have been analyzed in this survey. Certain parameters, such as, algorithms used, detection accuracy, false alarm rate (Both FN and FP), protection against attacks, adaptive/ learning and the distinct feature of each model have been investigated. A number of algorithms are incorporated which can be classified based on three traditional methods, namely statistical methods, machine learning and optimization techniques. Some algorithms have been tailor made for particular applications and have been classified as ad-hoc procedures. The models have also been classified based on whether the IDS is adaptive or not. Adaptive signifies that the proposed model is capable of learning from previous attacks that have already occurred, and hence can detect it the next time it occurs.

The most important aspect being considered is the attacks against which considerable protection is provided by the proposed IDS, as the work of an IDS is to eliminate security threats in the network. We have also touched upon the distinct features in each model and also included any other miscellaneous parameter that may prove useful.

The surveyed anomaly based IDS's indicate that it has a detection rate of >87% largely and can reach a high detection rate of about 95%-96% in certain cases. But the false alarms generated in the IDS are large, i.e about 4-6%. Whereas the false alarms in a signature based IDS are very less, generally around <1%. The hybrid based IDS ensures a high detection rate of >88%, and also has the advantage of low false alarms.

This indicates that the hybrid based IDS truly provides an improvement in terms of detection rate and false alarm reduction, than using signature and anomaly based IDS independently. A closer look on the various models proposed also suggests that the denial of service (DoS) attack is the most frequently detected intrusion, whereas the probe, U2R and R2L attacks have a lower detection rate. Hence there needs to be an improvement in detection of specifically the probe, R2L and U2R attacks.

A careful study of the comparison tables show that for the case of anomaly based IDS, statistical methods are preferred over the other algorithms. The statistical algorithms are being used in [14-16], [18-21], indicating that they are widely used in applications where a threshold has to be formed for the detection of intrusions in a network. The statistical algorithms used in various IDS include the fixed width clustering algorithm in [14], GMM, K-means and maximum likelihood algorithms in [15], Hierarchical trust management and SPN applied in [19] and OCPCC, CCIPCA incorporated in [20].

In [16], a mixture of both statistical and machine learning algorithms is incorporated that include SVM, LDA, PCA and BCP. The models proposed in [18, 21] incorporate statistical, machine learning and optimization algorithms simultaneously. They include genetic algorithms, fuzzy rule modeling, ICA and density based algorithm. The machine learning algorithm used in [17] includes SWP and low complexity cooperation algorithm. In the hybrid based IDS, a different scenario exists as the machine learning algorithms are the widely preferred methods, which includes ART, Q-learning, SVM, SLIPPER, CSOACN, etc.

TABLE II. SIGNATURE BASED IDS

Authors	Algorithms used	Data Set Source	Adaptive	Detection accuracy (DA) and False detection rate (FDR)	Protection against attacks	Distinct feature and types of WSN
[22] Abrahama et al (2007)	Fuzzy logic, Neural network learning algorithms	DARPA, 1998	Yes	DA= >94.11% FDR=NA	DoS, Probe, U2R, R2L	The detection accuracy can reach about 99.98 for R2L attack. Distributed IDS (DIDS).
[23] Hu et al. (2008)	Adaboost, Over fitting Handling	KDDCup99	Yes	DA= 90.04%-91%. FDR= 0.31%-1.79%	DoS, U2R, R2L, Probe	1.Decision stumps are used as weak classifiers, 2. Simple overfitting handling is used to improve the learning.
[24] Gowrisona et al (2013)	Adaboost [43], Neural networks	KDDCup99	Yes	DA= >99% FDR=0.1%	DoS, Probe, U2R, R2L	Can learn from network behaviour. High detection rate.
[25] Meng et al. (2014)	KNN clustering algorithm, Enhanced filter mechanism	1. DARPA, 1999 [49] 2.Real data set	No	DA= 86% - >90%. FDR= 85% less than snort.	IP Spoofing, Snort, algorithmic complexity attack	3 components: a context-aware blacklist-based packet filter, exclusive signature matching component and a KNN-based false alarm filter. Network based IDS

TABLE III. HYBRID BASED IDS

Authors	Algorithms used	Data Set Source	Adaptive	Detection accuracy (DR) and False detection rate (FDR)	Protection against attacks	Distinct Features and Type of WSN
[26] Yan et al.	SVM	KDDCup99	No	DA=99.81% FDR= 0.57% (FP)	DoS, U2R, R2L, Probe	High Accuracy of 99.75%. CWSN
[27] Tajbakhsh et al (2009)	1.Apriori algorithm 2.Boolean association rule induction[9]. 3.Association Based Classification(ABC)	KDDCup99	No	DA= 88.5% FDR=6.9% (FP)	DoS, Probe, U2R, R2L.	1. Handling symbolic (categorical) attributes. 2. Efficient classification of large datasets.
[28] Abduvaliyey et al. (2010)	1. SLIPPER [48]. 2. PCR based arbitral strategy.	Self made	No	DA= 96% FDR=0.05%	NA	Low energy consumption: 1.93J/node, Low computational costs. CWSN
[29] Wang et al. (2011)	ART	KDDCup99	Yes	DA=90.96% FDR= 2.06% (FP)	Spoofed/Altered/ Replayed Routing nformation, SF, SH, SY, WH, DoS,	1. Three IDS for Sink, CH and SN are proposed. 2. Learning mechanism. 3. Accuracy of 99.75%. CWSN
[30] Bhatnagar and Shankar (2012)	1. MLE. 2. Neyman-Pearson test.	Self made	No	DA= NA FDR= NA	DoS	1. Effective against SYNC flood attack. 2. Detection is faster & effective for densely deployed networks.
[31] Huang et al. (2013)	1. Game theory [45, 46, 47] 2. MDP. 3. Q-learning Algorithm. 4. Attack-pattern-mining algorithm.	Real world	Yes	DA= 1. 96.34% for high regularity attacks. 2. 79.75% for low regularity attacks. FDR= NA	Jamming, Blackhole, Flooding, De-synchronization capture attack	Reveals the patterns to predict future points of attack and devises defence strategies. Hierarchical clustered IDS.
[32] Simenthy et al. (2014)	Algorithms previously used in HIDS, EPIDS and cross layer based IDS.	Self made	Yes	DA >90% FP <0.175%	SF,WH,SY,SH,HF, DoS	Applicable to Small, medium and large sized networks. Integrates 3 types of IDS. CWSN.
[33] Feng et al. (2014)	1. SVM 2. CSOACN	KDDCup99	Yes	DA= 94.86% FDR= 6.01% (FP) 1.00% (FN)	DoS,U2R,R2L, Probe	1. The process of training & testing are done parallely. 2. Combines both SVM and CSOACN. CWSN.

The proposed models incorporating machine learning methods are [26, 28, 29, 31] and [33]. In papers [26, 33], SVM is used for detecting intrusions and in [33], CSOACN is used along with SVM to provide a dual layer of intrusion detection. Whereas in [29], adaptive resonance theory is used extensively. In [28], both machine learning algorithms such as SLIPPER and optimization algorithms such as PCR based arbitral strategy are incorporated.

A combination of all the 3 techniques is used in [31] which comprises of statistical machine learning and optimization algorithms. In the hybrid based IDS, purely statistical based algorithms such as MLE and Neyman Pearson test are applied by [30]. The model [27] uses an ad-hoc methodology for efficient performance.

From tables [1, 2 and 3] it is clear that the data set used for experimentation is mainly based on KDDCup-99 data set. In the anomaly based models a wide variety of data sets are used. A couple of models [18, 15] are based on KDDCup-99 set, whereas GSB, IRL, ARC NRL data sets have been scarcely used. The hybrid based IDS which have been reviewed in this paper, have majorly used only KDDCup-99. Four hybrid based models use KDDCup-99 and four hybrid models use the real data samples. On analyzing signature based IDS the KDDCup-99 is found to be the most widely used data set for training the sensor nodes.

A study of the literature reveals that the computation involved generally in an anomaly or signature based IDS is usually lower when compared to a hybrid based IDS. Also the energy consumption is higher in a hybrid based model than the signature or anomaly. But the higher consumption of resources by hybrid based IDS also ensures that the detection rate and protection against the attacks is enhanced and also the false alarms are greatly reduced in comparison to signature or anomaly based models.

This research provides an insight into the various recent developments in intrusion detection systems along with the types of algorithms which have been incorporated. It also provides the various merits and demerits of the models which

have been researched in this area by comparing them in a tabular format.

IV. CONCLUSION

This paper conclusively analyzes signature, anomaly and hybrid based intrusion detection systems. The models which have been proposed by various researchers, roughly in the past decade, have been reviewed on the basis of certain parameters. It indicates that the performance of IDS in detection of the attacks has been increasing consistently with time. There is an improvement in the detection rate, lesser false alarms generated and a considerable increase in the range of attacks being detected. It can be inferred from the analysis that the statistical algorithms are frequently used in anomaly based detection models and the machine learning algorithms are common in the hybrid based IDS. We have also observed that hybrid based models have a higher detection rate and lower false alarms compared to the two traditional methods namely, signature based and anomaly based IDS.

The protection against certain attacks such as R2L and U2R is usually low, and can be due to the skewed training data sets used, which contain fairly low number of data sets belonging to these attacks. Hence such attacks pose security concerns in some of the intrusion detection models. The presented information constitutes an important point for addressing future Research & Development in the field of IDS. As this paper essentially focuses on the traditional methods such as anomaly and signature based IDS, future work could include analysis of models based on cross layer or stack based IDS technologies. Techniques providing higher detection rate but utilising fewer resources are required so as to enhance WSNs. Countermeasures which are faster and more effective are needed to cope up with the ever-growing attacks to improve the protection of the networks under surveillance.

TABLE IV. ABBREVIATIONS

Name	Abbrevation	Name	Abbrevation
Cluster based WSN	CWSN	Adaptive Resistance Theory	ART
perialist competitive algorithm	ICA	Markov Decision Process	MDP
Intel Research Laboratories	IRL	Energy prediction based IDS	EPIDS
The Australian Research Council's research network	ARC	Clustering based on Self-Organised Ant Colony Network	CSOACN
Denial of Service	DoS	Maximum Likelihood Estimation	MLE
Stochastic Petri Net	SPN	Prediction Confidence Ratio	PCR
Support Vector Mechanism	SVM	Distributed Denial of Service	DDoS
Ad-hoc on demand distance vector	AODV	Black Hole	BH
Network Simulator-2	NS-2	Selective Forwarding Attack	SF
Naval Research Laboratories	NRL	Sink Hole Attack	SH
False Negative	FN	Sybil Attack	SY
False Positive	FP	Worm Hole Attack	WH
Gaussian Mixture Model	GMM	Hello Flood Attack	HF
Sliding window protocol	SWP	Linear discriminant analysis	LDA
Bayesian classifier program	BCP	Principal component analysis	PCA

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer Networks, vol. 38, no. 4, pp. 393–422, 2002.

[2] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey", Computer Networks, Vol. 52, Issue 12, pp. 2292-2330, August 2008.

[3] Muhammad Ayaz, Imran Baig, Azween Abdullah, Ibrahima Faye," A survey on routing techniques in underwater wireless sensor networks", Journal of Network and Computer Applications, Volume 34 Issue 6,pp.1908-1927,2011.

[4] Jelena Misic, Fereshteh Amini, Moazzam Khan,"Signature-based intrusion detection in healthcare wireless sensor networks implemented over IEEE 802.15.4 beacon enabled clusters".

[5] Nabil Ali Alrajeh, S. Khan, Bilal Shams," Intrusion Detection Systems in Wireless Sensor Networks: A Review", International Journal of Distributed Sensor Networks, Volume 2013 (2013), Article ID 167575, 7 pages.

[6] Robert Mitchell, Ing-Ray Chen," A survey of intrusion detection in wireless network applications", Elsevier, Computer Communications 42, pp.1-23,2014.

[7] S Jha, M Hassan," Building agents for rule-based intrusion detection system", Elsevier, Computer Communications, Volume 25, Issue 15, 2002, pp.1366–1373.

[8] T.S. Sobh, "Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art", Elsevier, J. Computer Standards and Interfaces, volume 28, number 6, pp.670-694, 2006.

[9] C. Borgelt, 2005, Association Rule Induction, Available: http://fuzzy.cs.uni-magdeburg.de/borgelt

[10] Miao Xie, Song Han, Biming Tian, Sazia Parvin," Anomaly detection in wireless sensor networks: A survey", Journal of Network and Computer Applications, Volume 34, Issue 4, July 2011, pp. 1302-1325.

[11] Mohammad Wazid," Hybrid Anomaly Detection using K-Means Clustering in Wireless Sensor Networks".

[12] Sedjelmaci, Hichem, Feham, Mohamed," Novel Hybrid Intrusion Detection System For Clustered Wireless Sensor Network", Academic

Journal, International Journal of Network Security & Its Applications; Jul2011, Vol. 3 Issue 4, p1.

[13] Djallel Eddine Boubiche and Azeddine Bilami," Cross Layer Intrusion Detection System For Wireless Sensor Network", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012,pp.35-52.

[14] Chong Eik Loo And Mun Yong Ng, Christopher Leckie, Marimuthu Palaniswami, "Intrusion Detection for Routing Attacks in Sensor Networks", International Journal of Distributed Sensor Networks, 2006, pp.313-332.

[15] M. Bahrololum and M. Khaleghi,"Anomaly Intrusion Detection System Using Hierarchical Gaussian Mixture Model", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.8, August 2008, pp.264-271.

[16] J. Arokia Renjit and K. L. Shunmuganathan," Distributed and cooperative multi-agent based intrusion detection system", Vol.3 No.10, Indian Journal of Science and Technology, 2010, ISSN: 0974- 6846, pp. 1070-1074.

[17] QiWang, ShuWang, ZhonglouMeng, "Applying an Intrusion Detection Algorithm to Wireless Sensor Networks", IEEE, Second International Workshop on Knowledge Discovery and Data Mining, 978-0-7695-3543-2/09 $25.00,2009, pp.284-287.

[18] Farzaneh Geramiraz, Amir Saman Memaripour, and Maghsoud Abbaspour(Corresponding author: Maghsoud Abbaspour),"Adaptive Anomaly-Based Intrusion Detection System Using Fuzzy Controller", International Journal of Network Security, Vol.14, No.6, Nov. 2012, pp.352-361.

[19] Fenye Bao, Ing-Ray Chen, Moon Jeong Chang, and Jin-Hee Cho," Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection", IEEE Transaction on network and service management, Vol. 9, No. 2, June 2012,pp.169-183.

[20] Murad A. Rassam, Anazida Zainala, Mohd Aizaini Maarof," An Efficient Distributed Anomaly Detection Model for Wireless Sensor Networks", Elsevier, AASRI Procedia 5, 2013, pp.9 – 14.

[21] Shahaboddin Shamshirband, Amineh Amini, Nor Badrul Anuar, Miss Laiha Mat Kiah, Ying Wah Teh, Steven Furnell, "D-FICCA: A density-based fuzzy imperialist competitive clustering algorithm for intrusion detection in wireless sensor networks", Elsevier, Measurement 55,2014,pp.212–226.

[22] Ajith Abrahama, Ravi Jain, Johnson Thomas, Sang Yong Hana," D-SCIDS: Distributed soft computing intrusion detection system", Elsevier, Journal of Network and Computer Applications 30, 2007, pp.81–98.

[23] Weiming Hu, Wei Hu and Steve Maybank," AdaBoost-Based Algorithm for Network Intrusion Detection", IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART B: CYBERNETICS, VOL. 38, NO. 2, APRIL 2008, 1083-4419/$25.00,pp.577-583.

[24] G. Gowrisona, K. Ramar, K. Muneeswaran, T. Revathi," Minimal complexity attack classification intrusion detection system", Elsevier, Applied Soft Computing 13, 2013, pp.921–927.

[25] Weizhi Meng, Wenjuan Li, Lam-For Kwok, "EFM: Enhancing the performance of signature-based network intrusion detection systems using enhanced filter mechanism", Elsevier, computers & security 43,2014,pp.189-204.

[26] K.Q. Yan, S.C. Wang, C.W. Liu," A Hybrid Intrusion Detection System of Cluster-based Wireless Sensor Networks", Proceedings of the International Multi Conference of Engineers and Computer Scientists 2009 Vol I, Hong Kong. ISBN: 978-988-17012-2-0

[27] Arman Tajbakhsh, Mohammad Rahmati, Abdolreza Mirzaei," Intrusion detection using fuzzy association rules", Elsevier, Applied Soft Computing 9,2009 , 1568-4946/$,pp.462–469.

[28] Abror Abduvaliyev, Sungyoung Lee, Young-Koo Lee," Energy Efficient Hybrid Intrusion Detection System for Wireless Sensor Networks", 2010 International Conference on Electronics and Information Engineering (ICEIE 2010).

[29] Shun-Sheng Wang, Kuo-Qin Yan, Shu-Ching Wang, Chia-Wei Liu," An Integrated Intrusion Detection System for Cluster-based Wireless Sensor Networks", Elsevier, Expert Systems with Applications 38,2011, pp.15234–15243.

[30] Ruchi Bhatnagar and Udai Shankar," The Proposal of Hybrid Intrusion Detection For Defence Of Sync Flood Attack In Wireless Sensor Network", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.3, No.2, April 2012.

[31] Jen-Yan Huang, I-En Liao, Yu-Fang Chung, Kuen-Tzung Chen," Shielding wireless sensor network using Markovian intrusion detection system with attack pattern mining ", Elsevier, Information Sciences 231 ,2013,pp.32–44.

[32] Joseph Rish Simenthy CEng ,AMIE, K. Vijayan," Advanced Intrusion Detection System for Wireless Sensor Networks", Vol. 3,Special Issue 3, International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14),April 2014.

[33] Wenying Feng, Qinglei Zhang, Gongzhu Hu, Jimmy Xiangji Huang," Mining network data for intrusion detection through combining SVMs with ant colony networks",Elsevier, Future Generation Computer Systems 37,2014,pp. 127–140.

[34] V. Venkatachalam, S. Selvan, "Intrusion Detection using Improved Competitive Learning Lamstar Neural Network", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.2, February 2007.

[35] J. H. Cho, A. Swami, and I. R. Chen, "A survey on trust management for mobile ad hoc networks," IEEE Commun. Surveys Tutorials, vol. 13, no. 4, pp. 562–583, 2011.

[36] E. M. Daly and M. Haahr, "Social network analysis for information flow in disconnected delay-tolerant MANETs," IEEE Trans. Mobile Computing, vol. 8, no. 5, pp. 606–621, May 2009.

[37] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," in Proc. Int. Conf. Comput. Vis. Pattern Recog., 2001, vol. 1, pp. I-511–I-518.

[38] Nabil Ali Alrajeh, S. Khan, Bilal Shams," Intrusion Detection Systems in Wireless Sensor Networks: A Review".

[39] Carpenter, G. A., & Grossberg, S.," The ART of adaptive pattern recognition by a self-organizing neural network". IEEE, Computer 21(3), 1988, pp.77–88.

[40] S. Suthaharan, M. Alzahrani, S. Rajasegarar, C. Leckie, M. Palaniswami," Labelled data collection for anomaly detection in wireless sensor networks", Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2010 Sixth International Conference on 2010,pp. 269–274.

[41] C. Guestrin, P. Bodik, R. Thibaux, M. Paskin, S. Madden, Intel lab data,

[42] Lincoln Laboratory, Massachusetts Institute of Technology (MIT), 1998-2000. DARPA Intrusion Detection Evaluation.

[43] Y. Freund, R.E. Schapire, "A short introduction to boosting", Journal of Japanese Society for Artificial Intelligence 14 (5), 1999, pp. 771–780.

[44] Snort, The Open Source Network Intrusion Detection System. http://www.snort.org/.

[45] A. Agah, S.K. Das, K. Basu," A Noncooperative Game Approach for Intrusion Detection in Sensor Networks (VTC 2004)", 2004, pp. 2902–2906.

[46] A. Agah, S.K. Das, K. Basu," Intrusion detection in sensor networks: A noncooperative game approach", 3rd IEEE International Symposium on Network Computing and Applications (IEEE NCA04),2004, pp. 1–4.

[47] A. Agah, M. Asadi, S.K. Das," Prevention of DoS attacks in sensor networks using repeated game theory", Proceedings of the International Conference on Wireless Networks, 2006.

[48] W. Cohen and Y. Singer, "A Simple, Fast, and Effective Rule Learner", Proceedings of 6th national Conference on Artificial Intelligence and 11th Conference on Innovative Applications of Artificial Intelligence, Orlando, Florida, pp.335342,July 1999.

[49] DARPA, 1999; McHugh, 2000 was produced by MIT Lincoln Laboratory and Air Force Research Laboratory.