JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Development of Hybrid Intrusion Detection System for Ubiquitous sensor networks

Mr. Yogesh S. Modhe, BHABHA University, Prof. Manish Rai, BHABHA University.

Abstract— With recent developments in electronics, the sensors nowadays are capable of performing multiple functions. The use of multi-function sensors has increased and hence dropped their prices down dramatically. Improvements in the design of sensors have lower power consumption. The sensors take input from the physical environment which is converted into electronic form and communicate with the network; some sensors may have data processing capability. The sensors are very useful in civil, medical and military applications, for collecting information from the physical environment where humans are having limitations. The sensors can be installed to access locations such as battlefield investigation, environment monitoring, etc. The ubiquitous sensors are generally deployed in open and unprotected environment hence become very easily accessible to be attacked by intruders. Thus, it becomes necessary to protect it. As Intrusion detection system is most promising defensive method against attacks on ubiquitous sensor network. In this paper we have proposed Hybrid Intrusion Detection System for ubiquitous Sensor Network. It combines the benefits of both anomaly detection and signature based detection mechanisms of intrusion detection.

Index Terms— Ubiquitous Sensor Networks, Anomaly detection, hybrid Intrusion Detection System and Signature based detection.

I. INTRODUCTION

Latest improvements in the micro-electronics and wireless communication technology have facilitated the development of multifunctional sensors with low priced and low-power consumption. These sensor nodes consist of data capturing device, data processing, and wireless communication devices.

A ubiquitous sensor network (USN) is formed by connecting number of sensor devices which operate independently and communicate with radio transmissions. In past few years security of Ubiquitous Sensor Networks has become burning issue, which attracts various researchers who have focused on USN attacks or malicious behaviors [1].

The various mechanisms used to provide security for the ubiquitous sensor network includes:

a) Cryptographic Techniques: These techniques are used to confirm authentication and integrity of data. It checks the source of the data to verify that it is not tampered or altered. The cryptographic techniques make use of hashing functions, encryption algorithms and public key cryptographic techniques [3] which has capability to protect the network from outside attacks. However cryptographic techniques fails to detect internal attacks where the attacker might know the keys and use them to encrypt or decrypt the data. The cryptographic techniques are used as first line of defense against the intruders.

b) Steganography Technique: The cryptography is said to be the art of keeping information secret. Using steganography one can hide or embed a message in another message or into a multimedia content like images, sound tracks, etc. However it requires large amount of processing power and hence become difficult to deploy in USN due to limited processing power of sensors.

c) Intrusion Detection System: This technique allows to detect normal and abnormal activities on the network nodes and activates an alarm when intrusion are detected. IDS also has high accuracy of intrusion detection. The cryptography cannot provide the necessary security in USN. This makes IDS very useful for both internal and external attacks. Many researches in IDS Technology for ubiquitous sensor networks were done, where very few topics were investigated because of limited energy and computing storage capacity of nodes.

In this context a hybrid intrusion detection system for USN is introduced. This approach uses the clustering algorithm to reduce the amount of information exchanged and decrease consumption of energy. A machine learning algorithm called support vector machine (SVM), that classifies data into normal and anomalous, in order to detect anomalies is used and applied misuse detection technique to determine known attack patterns (signatures). The combination of anomaly and misuse detection can achieve better detection rate with low false positive and false negative rate.

A) Basic Requirements of an IDS

To build powerful IDS, it is necessary to compute the needed characteristics. It must run continually. It must run in the background of the system being monitored. The security experts must always be able to monitor the status of system. Following are some requirements that must be considered while designing the IDS.

1. Fault tolerance – it is the ability to recover from system crashes and reinitializing the system. Crashes must not require retraining or relearning of rules/behavior.
2. Imperviousness to subversion - the IDS itself must not be vulnerable. The system must ideally be able to monitor itself to avoid subversion.
3. Scalability - the IDS must be able to handle the load as the network grows.
4. Adaptability - as the user behavior and system changes over time. Ex. A user may be assigned to a new work

shift causing the timestamps of his usage patterns to change sharply.

5. Minimal overhead - on systems\hosts running relevant programs. The more the overhead the less the possibility of acceptance. Host-based systems tend to be the worst affected by this. The overhead may be either by consuming too much memory (primary or secondary) or CPU cycles.
6. Configurability - the IDS must be able to be configured according to the desired Security policies, preferably dynamically.
7. Graceful degradation of service - if some component crashes the entire system must not crash.

II. LITERATURE SURVEY

Conventional signature based systems can detect known attacks with low false alarms. However, they cannot detect unknown attacks without any recollected signatures. Furthermore, signature matching yields good performance for single connection attacks. With the cleverness of attackers, more attacks involve multiple connections. This limits the detection by signature matching. Anomaly detection algorithms build models of normal behavior and automatically detect any deviation from it. A major limitation of anomaly detection systems is a possibly high false alarm rate.

Sensor networks have resource constraints such as lack of data storage and power [4]. According to Roman et al. [5] IDS solutions for ad hoc networks cannot be applied directly as it is to sensor networks. The intrusion detection system must meet the demands and restriction of USNs.

Kaplantzis [6] classified intrusions detection techniques into two categories:

A) Misuse detection: This technique involves the comparison of data captured and stored signatures of known attack, any matching patterns can be considered as an intrusion. The signatures are updated over time which is necessary to keep this technique effective. The only drawback of misuse detection systems is failure in detection of unknown attacks [7].

B)Anomaly detection: Anomaly detection builds a model of normal behavior of the nodes and then compare the captured data with the model, any activity that deviates can be said to be an anomaly. The advantage this technique is that it can detect attacks that are unknown [7]. On the other hand this technique requires a significant computation time which needs high energy consumption. Therefore, the anomaly detection algorithm in WSN must consider a detection accuracy and energy consumption as its development parameters. Various anomaly detection techniques proposed for the ubiquitous sensor networks in the literature includes: K-Nearest Neighbor, Rule based detection and support vector machine (SVM) [8].

Many researches use a combination of anomaly detection and misuse detection (hybrid model) to take advantages of these two techniques and try to detect a significant number of attacks. There are some hybrid intrusion detection systems for USN such as [10], [11] and [12].

In [10], Hai et al. proposed in USN cluster based and hybrid approach for IDS. Based on work undertaken by Roman et al. [5], they suggest that IDS agents are located in every node. The agent is divided into two modules: local IDS agent and global IDS agent. Because of energy and memory constraints of WSN, global agents are active only at a subset of nodes. For anomaly detection, the global agent IDS monitors the communication of its neighbors by using predefined rules with two-hop neighbor knowledge, then sends alarm to cluster-head (CH) when they detect malicious nodes. Each node has an internal malicious database, which contains a list of known attack patterns (signatures) computed and generated in the CH. The authors attempt to minimize the number of nodes where the global agents IDSs are deployed by evaluating their trustworthy based on trust priority. In order to reduce the collisions and avoid the waste of energy, they propose an over-hearing mechanism that reduces the sending message alerts. When the rate of collision and the number of malicious node is not very high the proposed scheme can detect the routing attacks such as selective forwarding, sinkhole, hello flood and wormhole attacks with a better energy saving. Nevertheless, the drawback of this scheme is the high rate of false positive that is generated when using the rule based-approach of anomaly detection. In addition, this method is well defined by experts and specialists in the area of wireless security by being dependent on manual rule updating.

Yan et al. [11] have focused on using clustering approach in WSN and embedded hybrid IDS in CH. the proposed IDS have three modules: misuse detection module, anomaly detection module and decision making module.

In the anomaly detection module, the rule-based method has been used to analyzed incoming packets and categorize the packet as normal or abnormal. For building misuse detection model, the supervised learning algorithm Back Propagation Network (BPN) is adopted. The abnormal packets, which are detected by anomaly detection model is used as input vectors of BPN. The algorithm trains this training dataset, then classifies the data into five classes (four types of attacks and one normal behavior), when the process of training is over, it integrates the model in the misuse detection module in order to classify the new data (testing dataset).

Finally the output of both models (anomaly detection and misuse detection models) is used as an input for the decision making module. The rule-based method is applied to determine if an incoming information is an intrusion or not, and determine the category of attack. In case of presence of an intrusion the module reports the results to the base station. The simulation results showed a high rate of detection and a lower false positive rate, but the major drawback of this proposed scheme is that IDS monitor run in a fixed cluster heads (the hot point). Therefore it's an attractive node for the intruder that uses all its capacity to attack this node. Another drawback is the number of features which is very important (twenty four features are used). Thus the cluster head consumes much more energy, which minimizes the life time of the node.

Hybrid Intrusion Detection System Integrated for Clustered Sensor Networks have been proposed by Hichem and Feham [1]. Thy have proposed hybridization between the SVM based anomaly detection and misuse detection. They used a distributed learning algorithm for SVM training and divided the sensor nodes to form cluster. Each cluster will have its cluster head. All the processing will be performed by this cluster head. The problem with this type of implementation is cluster head will consume more energy and hence require continuous source of energy. The authors have not defined efficient method for misuse detection.

III. ATTACKS IN USN'S

There exists a large variety of attacks against USNs. Two categories of attacks, DoS and Probe attack are discussed in this section.

Dos Attacks: Selective Forwarding and black holes attacks are classified as Dos attack [11].

Probe Attacks: Spoofed, Altered or Replayed Routing Information, Wormholes and Acknowledgment Spoofing are classified as Probe attack [11].

A) Selective forwarding:

Selective forwarding occurs when a anomalous node drops a packet that is intended for a particular destination. They can also forward a received packet along a wrong path, thus creating unfaithful routing information in the network [1].

B)Black holes:

In this attack, the intruder pretends to be as shortest path to the base station or cluster head (CH) by using a higher power transmission. The WSN are vulnerable to this kind of attacks because all nodes carry data to the single node, here, the CH.

C)Wormholes:

The attacker tunnels packets received at one location in the network (in this case, the cluster) to another location, where the packets are then replayed.

D) Spoofed, Altered or Replayed Routing Information:

The attacker monitors transmissions, intercepts packets, then altering or repelling traffic, this attack can also lead to create routing loops in networks [6].

E)Acknowledgment Spoofing:

In this attack, the intruder convincing the sender that a weak link is strong or that a dead node is alive [6]. This result in packet loss which is sent along such link or node.

IV. SVM FOR ANOMALY DETECTION

A) SUPPORT VECTOR MACHINE

Support vector machines are used for regression and classification. The SVM classifier determines support vector in order to construct a hyper plan in the feature spaces.

There are many researches based on the multiclass SVM for traditional network to separate data into n different classes, but this approach cannot be used with sensors network. So in this context a distributed binary classifier for anomaly detection is used to detect the abnormal packet.

Given the training datasets,

$$(x_i, y_i) \quad i = 1, \ldots . n, y_i \in \{-1, +1\}, x_i \in R^d$$

We want to find the hyperplane that have a maximum margin ω.x=b, Where ω represents a normal vector and b represents offset. To find the optimal hyperplane, solve the following convex optimization problem:

$$min\left\{\frac{||w||^2}{2} + C\sum_{i=1}^{n}\varepsilon_i\right\}$$

$$y_i(w.x_i + b) \geq 1 - \varepsilon_i, \varepsilon_i \geq 0, 1 \leq i \leq n \qquad (1)$$

$\sum_i^n \varepsilon_i$ relaxes the constraints on the learning vectors, and C is a constant that controls the trade-offs between number of misclassifications and the margin maximization.

The Eq. (1) can be deal by using the Lagrange multiplier [13]:

$$maximize\ L(\alpha) = \sum_{i=1}^{n}\alpha_i - \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}\alpha_i\alpha_j y_i y_j K(x_j, x_i)$$

Subject to

$$\sum_{i=1}^{n} y_i\alpha_i = 0, and\ 0 \leq \alpha_i \leq C\ for\ all\ 1 \leq i \leq n \quad (2)$$

Here is K(xj, xi) is the kernel function and α_i are the Langrange multipliers. According to the condition of Kuhn Tucker (KKT), the x is that corresponding to $\alpha_i \geq 0$ be called support vectors (SVs).

Once the solution to Eq. (2) is found, we can get [13]:

$$w = \sum_{i=1}^{n}\alpha_i y_i x_i \qquad (3)$$

Thus the decision function can be written as:

$$f(x, \alpha, b) = \{\pm 1\} = sgn(\sum_{i=1}^{n} y_i\alpha_i K(x, x_i) + b) \quad (4)$$

We choose SVM classifier for anomaly detection because it provides very good results with less training time compared to neural networks. In addition, it is more suitable for intrusion detection in case where new signature is detected. Another advantage of SVM is the low expected probability of generalization errors [13].

B) FEATURE SELECTION

Feature selection is an important factor to increase the classification accuracy, reduce the false positive and get a fast training time. In this research, the feature selection method proposed by Sung et al. [13] is adopted. Thus the most relevant features are selected.

V. PROPOSED FRAMEWORK AND ITS WORKING

This approach is using hybridization between anomaly detection based on SVM and misuse detection. The anomaly detection uses a distributed learning algorithm for the training of a SVM to distinguish between normal and anomalous activities. In addition, a hierarchical arrangement that divide the sensor network into clusters is used. The clusters have a cluster head (CH). This architecture saves the energy that allows the network life time extension. Each node in the network is equipped with IDS and has the ability to activate it. Our aim is to minimize number of nodes which run intrusion detection. The IDS will activate as and when necessary. Each IDS node monitors the neighboring nodes with no trust between each pair of agents (i.e. IDS also monitor its IDS neighbor) as illustrated in Figure 1.

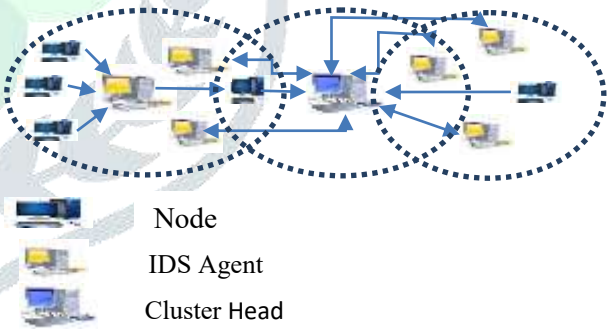

Figure 1.Placement of IDSs node in WSN

In proposed model, the sensor nodes are stationary and cluster head has more energy compared to the other ones. In the training phase, each IDS node receives the support vectors from the nearby IDS nodes. In the end, the selected training model is embedded into hybrid intrusion detection module (HIDMs) in order to obtain a lightweight and accurate detection system. The selected model is chosen according to the processes given below.

1. Train and test many SVMs according to selected features in a distributed fashion (delete one feature at a time)
2. Select SVM with the rate of accuracy >95%
3. Select the SVM with less input features.
4. Embed selected training model in the IDS nodes.

The IDS agent architecture

The proposed intrusion detection system (Figure 2) comprises three modules. First, the anomaly detection module is used to filter the normal or abnormal packet.

Then, the abnormal packets are judged through the misuse detection module for type detection. Finally, the results of the two detection module are integrated by the decision-making module to determine whether it is the intrusion and type of intrusion, and return to the manager to follow-up treatment, which are detailed as follow:

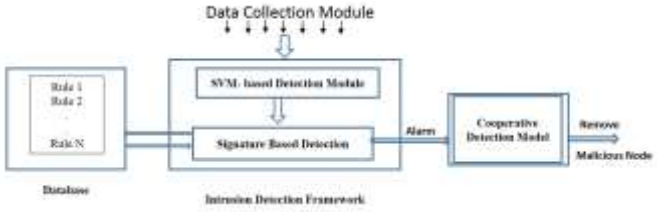

Figure 2: System architecture of Intrusion Detection System

1. Data Collection Module (DCM)

The data collection module collects data from sensors or may use standard dataset. Due to broadcast nature of wireless networks, monitor nodes gather the packets within their radio range [11] and pass it to the Hybrid Intrusion Detection Module.

2. Hybrid Intrusion Detection Module (HIDM)

The hybrid intrusion detection module involves anomaly and misuse detection techniques.

A. SVM-Based Anomaly Detection Engine

The anomaly detection procedure is divided into two stages:

Stage1: The training process.

Each IDS agent trains the SVM locally, then computes a set of data vectors called support vector (these set of data vectors are less in number than the input data vector used during the learning process). These later will be sent to an adjacent IDS node that is situated in the same cluster. Each monitor node that receives support vector from their IDS neighbours or cluster Head makes a combination between the union of received set and its own support vectors. These monitors update their support vector and compute the separating hyperplane. Afterward, they transmit the resulted set of support vector to the nearby IDS nodes. This process is continued until all IDS agents in the same cluster reach the same trained SVM (a complete pass through all IDSs within the same cluster). The communication activity within the cluster between IDS nodes are depicted in Figure 2. For each cluster, the selected IDS agent that depends on its residual energy, sends its support vector to the concerned cluster head; then, all the cluster heads exchange their data and communicate the computed set of support vector to their IDS nodes. Finally, when they all compute the global vector support the result is the same, after that, they can classify new captured packets as normal or anomalous. This algorithm reveals little communication overhead and less power consumption since the communication is performed only with a vector support rather than the whole data as in the case of the centralized approach. In addition, in order to save the energy, each IDS node sends back different values of support vector from the ones sent before.

Stage2: SVM testing process.

When the process of training is over each IDS node classifies the new data according to normal and anomaly patterns.

The selected training model (described above) is used for anomaly detection engine to classify the captured data that are delivered from data collection module. Any deviations from normal pattern are considered as an intrusion and delivered to misuse detection engine for further detection.

B. Signature Based Detection Engine:

When misuse detection engine receives the intrusion report (the suspected node, a set of features) from anomaly detection engine, it uses some predefined signs of intrusion that are stored in the signature database to check the occurrence of intrusion. If match occurs, the IDS node sends an alarm to cluster head that the analyzed node is an intruder. The cluster head removes the compromised node from the cluster and inform its IDS agents and all CHs over the network about the malicious node. If no match occurs, the process of cooperation is launched. Note that we stored at all nodes in the network a predefined rule about a set of intrusion signature.

3. Cooperative Detection Module (CDM)

If there are no matches between the intrusion detected by anomaly detection engine and some predefined signatures of attacker, the IDS agent sends the intrusion report to cluster head. That node performs a voting mechanism to make a better decision about the suspect nodes. If more than half of IDS nodes within the same cluster claim that the analyzed target is an attacker, the cluster head isolates the suspected nodes from the cluster and compute a new rule regarding the novel intrusion, then sends an alert message (that include a malicious node and novel intrusion signature) to their IDS agents and all CHs over the network. When the IDS agents receive this message they update their signature database.

VI. MATHEMATICAL MODELLING

After studding all the classes of problems. This topic "Hybrid Intrusion Detection System for USN" is of P Class because:

1) Problem can be solved in polynomial time.
2) This system always produces strong results.

Let S be the set of Datasets, Processes and Outputs

S : {I,P,O} where I represents the Standard Dataset in light SVM format which is input to HIDS, P represents the set of operations that are performed on the input. O is the Set of output. I1= Input Dataset

P1= Data Preprocessing

P2= SVM based Anomaly Detection

P3= Misuse Detection

P4= Co-operative Detection

O1= Normal

O2= Abnormal

I = {I1}

P= {P1, P2, P3, P4}

O={O1,O2}

Input is mapped to output which is shown in the following Venn diagram:

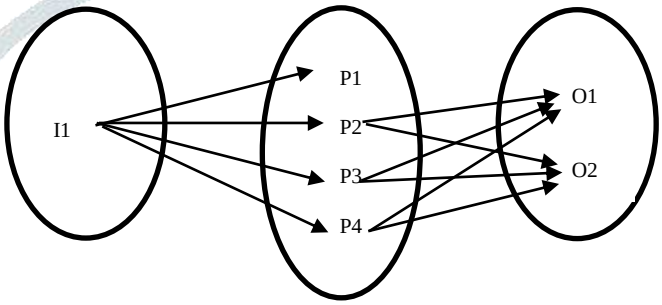

Figure 3: Venn Diagram.

VII. EXPERIMENTS AND RESULTS

In this section we evaluate the performance of the proposed hybrid IDSs. In our experiments, we have used the KDDcup'99 dataset [15] as the sample to verify the efficiency of the distributed anomaly detection algorithm and valid it in comparison with a centralized SVM-based classifier, which achieve a high level of accuracy detection. Also, we compare the distributed hybrid IDSs with one proposed by Yan et al. [11] in order to determine the effectiveness of this scheme.

1. Dataset

The KDD 99 intrusion detection dataset is developed by MIT Lincoln Lab in1998, each connection in the dataset has 41 features and it's categorized into five classes: normal and four attack behaviors (Dos, Probe, U2r, R2l).

Our analysis is performed on the "10% KDD" intrusion detection benchmark by using its samples as training and testing dataset. We focus only on two categories of attacks (Dos and Probe attacks), which are defined as anomalies behavior and are classified as (-1). A program written using C#.net is used to transform the standard KDD dataset in the form of SVM light input. The normal behavior is classified as (+1).

The training data used at each IDS comprises of 50 normal and 50 anomalous samples (include both Dos and Probe attacks). In order to evaluate the proposed algorithm, the amount of the data used in test process is equal to N*50, where N is the number of IDS nodes in the network, and the amount of both anomalous and normal samples is equal respectively to 42% and 68% of all test data. The test is performed at one among the IDSs, because all IDSs have the same trained SVM classifier.

2. Experiments results and discussion

The radial basis function (RBF) is used as the kernel function. The accuracy is used as performance measure to evaluate the algorithm. We also compute the detection rate, that represents the percentage of correctly detected intrusions, and false positive, that represents the percentage of normal connections that are incorrectly classified as anomalous.

The identification of the most relevant features is an important task, in our scenario we try to determine SVMs-based anomaly detection that achieve high classification accuracy by deleting the useless features. This task is performed by delete one feature at time according to the approach proposed by Sung et al. [13]. The increased number of features leads to high computational cost in the nodes, for that our aims is to obtain the SVM classifier with less number of features but able to provide high rate of accuracy, in order to save the memory storage and energy consuming in the sensor nodes. The results of the distributed SVMs binary classifier related to the most relevant features with N=10 are summarized as bellow.

Table 1. The performance evaluation of distributed IDSs based on SVM

# of Features	Accuracy (%)	Detection Rate (%)
13	87.50	83.33
9	90.80	89.66
7	93.90	91.86
5	92.53	90.21
4	93.75	91.65

From Table 1, we find out that, the binary SVM classifier with 7 features gives best results over those use (13, 9, 5, and 4) features. Thus, these 7 features represent the most significant features. However, the difference between detection rate of SVM with 7 features and 4 features is small and due to limited resources we use SVM with 4 features for anomaly detection engine. These features are:

Src_bytes: Number of bytes sent from source to destination

Dst_bytes: Number of bytes sent from destination to source

Count: Number of connection to same destination host

Srv_diff_host_rate: the percentage of connections to different host.

The centralized IDS (IDS located in base) based on SVM gives high performance but this requires all the data to be provided by each sensor. Thus it consumes much more energy. Our system is compared to centralized approach in terms of classification accuracy by using the selected 4 features. As shown in Figure 4 where N is number of IDS's and sensor nodes for both distributed and centralized approach.

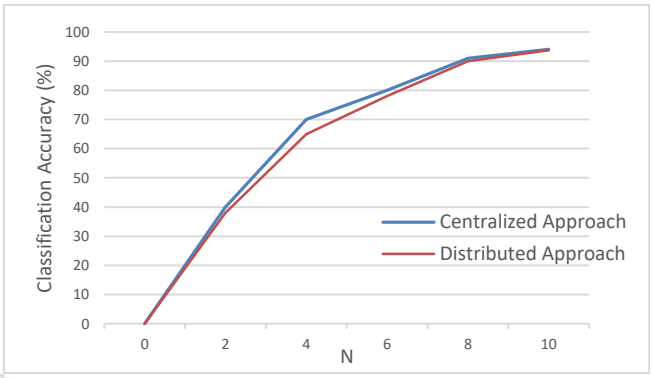

Figure 4: Classification accuracy of SVM for centralized and distributed approaches.

As can be seen in Figure 4, the curves for both approaches coincide almost exactly, and the rate of classification accuracy for centralized and distributed approaches increases with increase in number of IDS nodes. As a result distributed IDS's based on SVM deliver highly accurate performance, with less training data.

CONCLUSION

In this work, a distributed hybrid intrusion detection system (HIDSs) for clustered ubiquitous sensor networks is proposed. The proposed distributed learning algorithm for the training of SVM in USN reaches high accuracy for detecting the normal and anomalous behavior (accuracy rate over 90%). Also a combination between the SVM classifier and Signature Based Detection achieve a high detection rate with low false positive rate.

Communication in USN consumes a high energy. The training process is carried out with IDS nodes. These nodes need to compute and transmit only a set of data vector (support vector) between each other's, instead of transmitting all captured data to a centralized point, then train a SVM classifier. Thus this approach reduces energy consumption also

REFERENCES

[1] Hichem Sedjelmaci1 and Mohamed Feham," *Novel Hybrid Intrusion Detection System For Clustered Wireless Sensor Network*", In International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011

[2] T. H. Hai, F. khan, and E. N. Huh, "*Hybrid Intrusion Detection System for Wireless Sensor Networks*", In Proceeding of the ICCSA, LNCS 4706, pp. 383-396, 2007.

[3] R. Roman, C. Alcaraz, and J. Lopez, "*A Survey of Cryptographic Primitives and Implementations for Hardware-Constrained Sensor Network Nodes*", Mobile Networks and Applications, Springer. Vol.12, no 4, pp 231-244, 2007.

[4] J. P. Walters, Z.Liang, W.Shi, and V.Chaudhary, "*Wireless Sensor Network Security: A Survey*", Security in Distributed Grid and Pervasive Computing, Auerbach Publications, CRC Press, Vol.1, Issue.2, pp.1-50, 2006.

[5] R. Roman, J. Zhou, and J.Lopez, "*Applying Intrusion Detection Systems to Wireless Sensor Networks*", the 3rd IEEE Consumer Communications and Networking Conference, pp.640-644, 2006.

[6] S. Kaplantzis, "*Security Models for Wireless Sensor Networks*", PhD Conversion Report, Centre of Telecommunications and Information Engineering, Monash University, Australia, 2006.

[7] S. Rajasegarar, C. Leckie, and M. Palaniswami, "*Detecting Data Anomalies in Wireless Sensor Networks*", Security in Ad hoc and Sensor Network, Computer and Network Security , World Scientific Publishing Co, Vol. 3, pp.231-259, 2009.

[8] S. Kaplantzis, A. Shilton, N. Mani, and Y. A. Sekercioglu, "*Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines*", In 3rd International Conference on Intelligent Sensors, Sensor Networks and Information, IEEE, Melbourne, Australia, pp.335-340, 2007.

[9] K. Flouri, B. B.Lozano, and P. Tsakalides, "*Optimal Gossip Algorithm for Distributed Consensus SVM Training in Wireless Sensor Networks*", In Proc.16th International Conference on Digital Signal Processing, IEEE, Santorini, Greece, pp.1-6, 2009.

[10] T. H. Hai, E. N. Huh and M. Jo, "*A Lightweight Intrusion Detection Framework for Wireless Sensor Networks*", Wireless Communications and mobile computing, Vol.10, Issue.4, pp.559-572, 2010.

[11] K. Q. Yan, S. C. Wang, S. S. Wang, and C. W. Liu, "*Hybrid Intrusion Detection System for Enhancing the Security of a Cluster-based Wireless Sensor Network*",In Proc. 3rd IEEE International Conference on Computer Science and Information Technology, Chengdu, China, pp.114-118, 2010.

[12] G. Huo, and X. Wang, "*A Dynamic Model of Intrusion Detection System in Wireless Sensor Networks*", In Proc. International Conference on Information and Automation, IEEE, Zhangjiajie, China, pp.374-378, 2008.

[13] A. H. Sung, and S. Mukkamala, "*Identifying Important Features for Intrusion Detection using Support Vector Machines and Neural Networks*", Symposium on Applications and the Internet, IEEE, Orlando, USA, pp.209-216, 2003.

[14] M. S.Mamun, and A.F.M. Sultanul Kabir, "*Hierarchical Design Based Intrusion Detection System For Wireless Ad Hoc Sensor Network*", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2010

[15] http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[16] K. Vengatesan, A. Kumar, R. Naik and D. K. Verma, "Anomaly Based Novel Intrusion Detection System For Network Traffic Reduction," 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on, Palladam, India, 2018, pp. 688-690

[17] A.Stetsko, L.Folkman, and V.Matayáš, "*Neighbor-Based Intrusion Detection for Wireless Sensor Network*", 6th International Conference on Wireless and Mobile Communications, IEEE, Valencia, Spain, pp.420-425, 2010.

[18] Mr. Sachin B. Jadhav and Dr. A. B. Pawar "Design and Development of Hybrid Intrusion Detection System for Wireless Sensor Network " IJARIIE-ISSN(O)-2395-4396, Vol-3 Issue-1 2017.