DESIGN AND DEVELOPMENT OF HYBRID INTRUSION DETECTION SYSTEM FOR WIRELESS SENSOR NETWORK

Sachin B. Jadhav[1], Dr. A.B. Pawar[2]

[1]*Student, Department of Computer Engineering,SRES COE, Kopargaon, Maharashtra, India*
[2] *Professor, Department of Computer Engineering,SRES COE, Kopargaon, Maharashtra, India*

ABSTRACT

With evolution in electronic and wireless communication the cost of sensors having multi-function capability has dropped down dramatically. Also the power consumption by these sensors also came down. The sensors consists of wireless communication and capturing devices with data processing capability. The sensors are very useful for many military and civil applications, in collecting and processing information from unfriendly environment and difficult to access locations such as battlefield investigation, environment monitoring, etc. Thus the WSN's are point of attraction for the attackers as they are deployed in open and unprotected environment. The characteristics of wireless infrastructure and characteristics of WSNs cause potential risks of attacks on the network. Numerous studies have attempted to address vulnerabilities in WSNs. Current research on security in sensor networks generally focuses on secure routing protocols, key management and prevention techniques for specific attacks. Although research on security (related to) issues in WSN is productive, the need for a security framework for WSNs still exists. Intrusion Detection System (IDS) is a common prevention mechanism which protects the network from intrusion. Here we study the problem of intrusion detection in WSNs, and propose a hybrid intrusion detection framework for clustered sensor networks.In this paper we have proposed Hybrid Intrusion Detection System for Wireless Sensor Network. It combines the benefits of both anomaly detection and signature based detection of intrusions. The anomaly detection is based on Support Vector Machine (SVM) which then forwards the result to misuse detection algorithm for further necessary action. The work together as Hybrid system for intrusion detection.

Keyword: - *Wireless Sensor Network, Hybrid IDS, Anomaly detection, Signature based detection*.

1. INTRODUCTION

Recent advances that deal with the technology of micro-electronics and wireless communication have enabled the development of multifunctional sensor with low-cost and low-power. These sensor nodes consist of data processing, wireless communication and capture device.

A wireless sensor network (WSN) consists of a large number of devices operating independently and communicating with radio transmissions. Many researchers have focused on the security of WSN against attacks or malicious behaviors.

The security mechanisms used to protect the wireless sensor network against intruders are:

- Cryptographic techniques: These technics are used to ensure authentication and data integrity. It checks the source of the data and to verify that it is not altered or tampered. The cryptographic techniques make use of hashing functions, symmetric encryption algorithms and public key cryptography [3] which has capability to protect WSN from external attacks. However cryptographic techniques fails to detect internal attacks where the attacker might know the keys and uses them to perform encryption/decryption. This technique is defined as the first line of defense.
- Steganography: The cryptography is said to be the art of secrecy, steganography called the art of concealment. The main objective of steganography is to hide or embed a message in another message or into a multimedia data

like images, sound, etc. However this technique requires substantial processing resources and also is hard to implement in WSN because of the constraints of these sensors.

- IDS: An intrusion detection system is the second line of defense, it can protect with high accuracy against internal attacks. This mechanism allows detecting abnormal or suspicious activities on the analyzed target and activates an alarm when intrusion are detected. The cryptography cannot provide the necessary security in WSN. This makes IDS very useful for both internal and external attacks. Many researches in the application of the IDS technology in ad-hoc networks were done, in comparison with wireless sensor networks where few subjects were investigated because of its limited energy and computing storage capacity.

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

1.1 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

2. RELATED WORK

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 WSNs.

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 possible high false alarm rate.

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

A) Misuse detection: this technique involves the comparison between captured data and known attack signatures, any corresponding pattern can be considered as an intrusion. The signatures are updated over time which is necessary to keep this technique effective. However, the major drawback of misuse detection systems is their inability to detect unknown attacks [7].

B) Anomaly detection: is based on modelling the normal conduct of the nodes and then compare the captured data with the model, any activity that deviates from normal model 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 implies high energy consumption. Therefore, the anomaly detection algorithm in WSN must consider a detection accuracy and energy consumption. Among anomaly detection techniques proposed for the wireless sensor networks are: Rule Based, K-Nearest Neighbor and support vector machine (SVM) [8].

Hybrid Intrusion Detection System Integrated For Clustered Sensor Networks. There are some researches that use a combination between anomaly detection and misuse detection (hybrid model) in order to leverage the advantages of these two techniques and try to detect a significant number of attacks. There are some hybrid intrusion detection systems for WSN such as [10], [11] and [12].

In [10], Hai et al. proposed in WSN 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 higher 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 leads to minimize the life time of the node, also the names of this features are not mentioned.

3. SVM FOR ANOMALY DETECTION

A) Support Vector Machine

Support vector machines are a set of supervised learning techniques used for regression and classification .The aim of SVM classifier is to determine a set of vector called support vector to construct a hyper plan in the feature spaces.

There are several researches that use SVM based on multi-class for traditional network to classify a data into n-classes, but this approach don't meet the requirement of sensors network and remains as an open research question. In our context a distributed binary classifier (anomaly or normal) for anomaly detection is performed to detect the abnormal packet.

Given the training datasets,

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

We want to find the hyper plane that have a maximum margin: ω.x=b Where ω is a normal vector and the parameter b is offset. In order to find the optimal hyper plane, we must solve the following convex optimization problem:

$$min\left\{\frac{||w||^2}{2} + C\sum_{i=1}^{n}\varepsilon_i\right\}$$
$$y_i(w.x_i + b) \geq 1 - \varepsilon_i, \varepsilon_i \geq 0, 1 \leq i \leq n \qquad (1)$$

$\sum_i^n \varepsilon_i$ relax 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 $\sum_{i=1}^{n} y_i \alpha_i = 0, and\ 0 \leq \alpha_i \leq C\ for\ all\ 1 \leq i \leq n$ (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]: $w = \sum_{i=1}^{n} \alpha_i y_i x_i$ (3)
Thus the decision function can be written as: $f(x, \alpha, b) = \{\pm 1\} = sgn(\sum_{i=1}^{n} y_i \alpha_i K(x, x_i) + b)$ (4)

We choose SVM classifier for anomaly detection because it's provide 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.

4. PROPOSED FRAMEWORK AND ITS WORKING

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 illustrated in Fig-1.

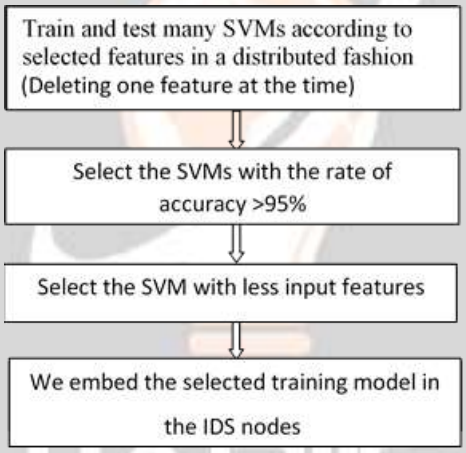

Fig- 1: Optimal distributed SVM selection process

The IDS agent architecture

The proposed intrusion detection system comprises three modules, which are detailed as follow:

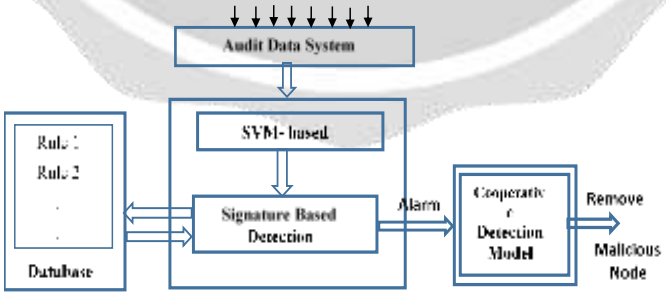

Fig-2: System architecture of Intrusion Detection System

1. Data Collection Module (DCM)

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 hyper plane. 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). 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 suspect 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.

5. 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] and Hai et al. [10] according to the false positive rate (false alarm) in order to determine the effectiveness of this scheme.

- 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). 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*60, 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 58% of all test data. The test will perform at one among the IDSs, because all IDSs have the same trained SVM classifier.

- Experiments results and discussion

The radial basis function (RBF) is used as the kernel function: $F_{RBF} = \exp(-\|x_1 - x_2\|/2.\sigma^2), \text{where } 1/2.\sigma^2 > 0$

The accuracy measure is used as performance metric to evaluate our 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 led a 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=18 are summarized in Table 1.

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

# of Features	Accuracy (%)	Detection Rate (%)
9	**97.80**	**93.66**
7	**98.47**	**95.61**
5	**96.95**	**91.21**
4	**98.39**	**95.37**

From Table 1, we find out that, the binary SVM classifier with 7 features outperforms the SVMs that use (9, 5, 4) features, respectively, in terms of accuracy and detection rate. Thus these 7 features represent the most significant features. However, the difference of accuracy between both SVM with 7 and 4 features is small, and due to the resource constraints at sensor nodes, 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 based on SVM (IDS located in the base station) exhibits high performance for solving a problem of 2-class, but this approach requires all the data to be provided by each sensor. Thus it's consuming much energy. The proposed algorithm is compared to centralized approach in term of classification accuracy by using the selected features (Src_bytes, Dst_bytes, Count, Srv_diff_host_rate)

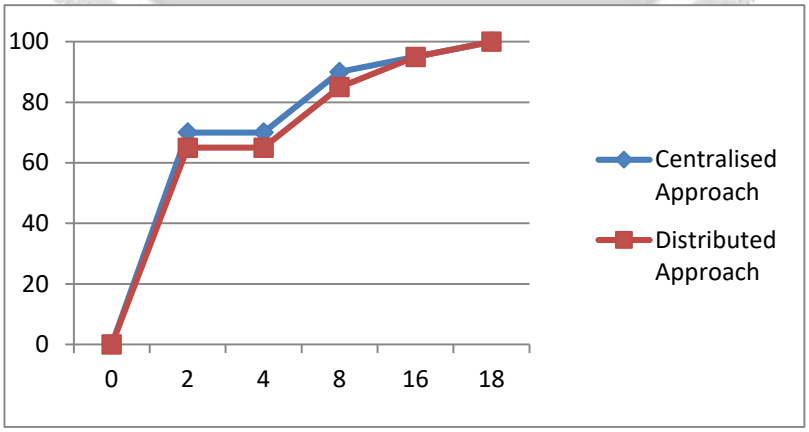

Chart -1: Classification accuracy of SVM for centralized and distributed approaches

As shown in chart-1, the curves for both approaches coincide almost exactly, and the rate of classification accuracy for centralized and distributed approaches increases when the number of IDSs and sensor nodes increase

respectively. Specifically when the number is important (in our case N=18) the rate is close to 100%, 99.07% for centralized approach and 98.39 % for distributed approach. As a result distributed IDSs based on SVM deliver highly-accurate performance, with less training data.

6. CONCLUSION

In this work, a distributed hybrid intrusion detection system (HIDSs) for clustered wireless sensor networks is proposed. The proposed distributed learning algorithm for the training of SVM in WSN reaches high accuracy for detecting the normal and anomalous behavior (accuracy rate over 98%). Also a combination between the SVM classifier and Signature Based Detection achieve a high detection rate with low false positive rate.
Conclusion related your research work Conclusion related your research work Conclusion related your research work Conclusion related your research work Conclusion related your research work Conclusion related your research work Conclusion related your research work Conclusion related your research work Conclusion related your research work Conclusion related your research work Conclusion related your research work

7. REFERENCES

[1] Hichem Sedjelmaci1& Mohamed Feham,"*Novel Hybrid Intrusion Detection System For Clustered Wireless Sensor Network*", In International Journal of Network Security & 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, 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] 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.