ISSN No. 0976-5697

Volume 8, No. 3, March – April 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Hybrid Framework for Intrusion Detection in Wireless Sensor Networks

D. P. Mishra
Research Scholar CSVTU Bhilai
Department of Computer Science & Engineering
Durg,Chhattisgarh, India

Ramesh Kumar
Professor, Department of Computer Science & Engineering
CSVTU Bhilai
Bhilai, Chhattisgarh , India

Abstract: Wireless Sensor Networks (WSN) possess vulnerable characteristics such as outdoor unattended operations for transmission and self-organized behaviour without a fixed infrastructure leads them to suffer from various challenges including lower processing power, low battery life, small memory and wireless communication channel. Security of a communication channel is the major concern to handle such kind of networks. Due to well-known and accepted limitations, overall security of WSN becomes the main concern to deal with. Intrusion Detection Systems (IDSs) can play an important role in detection and prevention of security attacks. In this paper, we propose a hybrid framework for intrusion detection system for wireless sensor networks that would take advantage of cluster-based architecture to optimize energy consumption. Proposed hybrid model uses anomaly detection based on support vector machine (SVM) algorithm and a set of signature rules to detect malicious behaviours and provide and ideal hybrid framework for IDS in WSN. Simulation result shows that the proposed hybrid model can detect abnormal events with higher and efficient detection rate with lower false alarm.

Keywords: Wireless Sensor Network, Hybrid Intrusion Detection System, Support vector machine, Signature attacks, false alarm, detection rate, Frameworks.

I. INTRODUCTION

Wireless sensor networks (WSNs) is one of the most interesting research areas over the past few years. Characteristics of wireless sensor networks (energy limited, low-power computing, use of radio waves, etc...) exposes it for several security threats and challenges. Cryptography tools and techniques provides first line of defense, but it is ineffective when the attacker is located inside the network. Intrusion detection system (IDS) will provide the second line of defense that allows intrusion detection and prevention from internal and external attacks. Existing IDSs system designed for wired, wireless and ad hoc networks cannot be supported or implemented directly in the WSN. Considering fact and limitations of existing IDS systems, it is highly needed to design a hybrid intrusion detection system for wireless sensor network, which takes in consideration the limitations of WSNs.

In literature reviewed, there is little works that aims to combine between anomaly-based approach and signature based approach (hybrid model) to benefit from the advantages of both detection techniques. Yan et al. [1] proposed hierarchical IDS based on clusters. The authors took advantage of this approach by installing IDS agent (core defense) on each cluster-head. This agent has three modules: a supervised learning module, anomaly detection module based on rules and decision-making module. The simulation results show that this model has a high detection rate and lower false positive rate. However, the main disadvantages of this scheme is: The IDS node is static (runs only in the cluster-head), in this case the intruder uses all his strength to attack this hot spot (hot point) and subsequently disrupts the network. The implementation of this detection mechanism requires many calculations in cluster-heads, which can decrease the network lifetime.

Hai et al. [2] proposed a hybrid, lightweight IDS for sensor networks, based on the model proposed by Roman et al. [3]. IDS system takes advantage of cluster-based protocol to build a hierarchical network and provides IDS framework based on anomaly and misuse techniques. In their scheme, IDS agent consists of two detection modules, local agent and global agent. An approach that works on a process of cooperation between two agents will effectively detects an attack with greater accuracy (since both agents are in the same node). However, the disadvantage of this scheme is the sharp increase in signatures, may cause overload of the node memory.

In recent work, Coppolino and al. [5] presented a hybrid, lightweight, distributed IDS for WSN. This IDS uses both misuse-based and anomaly-based detection techniques. It is composed of a Central Agent (CA), which is very accurate intrusion detection that uses data mining techniques, and several LA (Local Agents) which are running lighter anomaly-based detection techniques on the motes.

Considering these hybrid models our contribution in this paper is to propose and implement an efficient and lightweight intrusion detection system that combines the advantages of both techniques i.e. anomaly based model and signature-based model in cluster wireless sensor environment and surpassing other hybrid models proposed in the literature.

II. IDS BACKGROUND AND RELATED WORK

WSN inherit all the properties and aspects of wireless networks, along with they have their own distinct characteristics and features, which make the design of a security model for WSNs far different from that of Ad hoc networks. R. Roman et al. [3] showed in his work that IDS proposed for wireless ad-hoc networks cannot be directly applied to WSNs. So, it is highly needed to have a novel and lightweight design of IDS for WSN. There are three main techniques that IDS can use to classify the attacks [2, 3, 4]:

Misuse detection: In this case, the behavior of WSN node is compared with available well-known attack patterns, where attack patterns must be defined and given to the system. The disadvantages of this technique is – need to have the knowledge to build attack patterns in addition, always someone has to update the attack signatures database.

Anomaly detection: It compares the behavior of WSN nodes under observation with normal behavior of WSN nodes rather than attack patterns. This model describes normal behaviors, which is established by automated training, and then flags as intrusions any activities varying from these behaviors. The disadvantages of these methods is system can exhibit legitimate but unseen behavior may leads to a substantial false alarm rate. In addition, an intrusion that does not exhibit anomalous behavior may not be detected, resulting in false negatives.

Specification-based detection: this technique combines the aims of misuse and anomaly detection. It is based on deviations from normal behaviors, which is defined by neither machine learning techniques nor training data. The attack specifications are defined manually that describe what normal behavior is and monitor any action with respect to these specifications. The drawback of this model is manual development of attack specifications, which is too time-consuming process for human beings. We consider proposing hybrid system; there are some proposed hybrid schemes such as HIDS [7] and eHIP [8].

In recent work [8], Yan et al. proposed a hybrid approach for IDS. The algorithm contains detection model, anomaly detection, and decision-making modules. The uniqueness of the model is the use of back propagation network (BPN) for anomaly detection module. First, the packet records are given to anomaly detection model to check for abnormal activities. If the activity is determined as abnormal then it will be forwarded to both misuse detection model and decision-making module. Then, the misuse detection model analysis received data with the help of BPN and sends them to the decision-making module. Finally, the decision-making module combines the outputs of both models to determine whether an output is an intrusion and the category of attack. In a case of intrusion, the module reports to the base station. Analysis of simulation shows that the scheme performs well for energy efficiency and computation cost of WSNs. The limitation is obtaining training data for determining the intrusion. Our work is motivated by this work and improves it in terms of completeness and reliability.

In [8], Su et al. proposed energy efficient hybrid intrusion prohibition system for WSNs. They use both intrusion detection and intrusion prevention techniques in order to have hybrid security solution. Their system contains collaboration-based intrusion detection subsystem, which uses cluster head monitoring and member node monitoring. In this scheme, member nodes monitor the cluster heads and the cluster heads monitor their own cluster members by using alarm table and HMAC. This scheme successfully detects the intruder in case of member nodes are monitors, but when cluster-nodes are monitors, the scheme lacks the detection problem because of considering the only shared key between cluster head and member node. It is the fact that the shared key can be easily accessed by the attacker and used during the data transmission. In our scheme, cluster head has full capability of detecting the attacks by using hybrid IDS scheme [9]. This approach has high accuracy and detection rate, also prolongs the network lifetime and scale of the network

III. PROPOSEED HYBRID MODEL

The Hybrid Intrusion Detection System (HIDS) meets desired goal of high detection and low false positive rate. The proposed model uses anomaly detection based on SVM technique and a set of attacks represented by fixed rules signatures, which are designed to validate the malicious behavior of a target identified by anomaly detection technique. Detection method is integrated into a cluster-based topology to increase the network lifetime. This is achieved by designating one known node as a leader of the group (cluster-head), that forwards nodes packets (data aggregated) to the base station (BS) instead of sending their (nodes) collected data to a remote location (base station). Cluster head work as local base station sensor, and then clusters select or elects themselves to be a CH at any given time with a certain probability. We propose a cluster-based architecture that divides the array of sensors into a plurality of groups, each of which comprises a cluster-head (CH). In specified architecture, all the node belongs to only one of the clusters, which are distributed across the whole network. Cluster head is used to reduce network energy consumption and to increase its lifetime. As shown in Figure 1, the architecture of proposed hybrid IDS, where info or data packet record is passed to anomaly detector(SVM based) and signature-based detector that takes decision based on polling and report to admin model and base station about intrusion

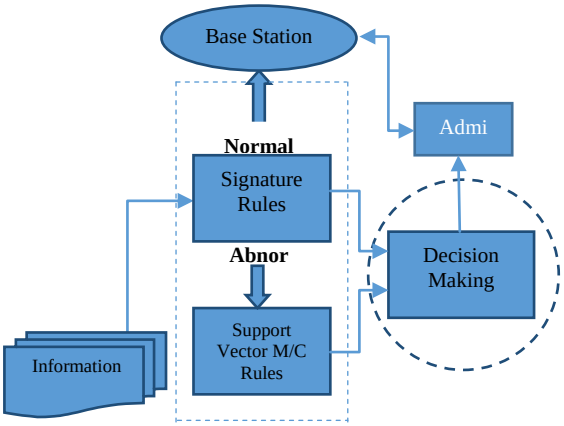

Figure 1. The architecture of proposed hybrid IDS.

A. Cluster election and strategy location of IDS

CH is elected dynamically based on energy f the node. The BS announces the process of CH election, the CHs calculate residual energy by equation Vi(t) = [Initial – Ei(t)] / r, where Initial is the initial energy, Ei(t) is the residual energy and r is the current round of CH selection. BS calculates the average value and average deviation, according to obtained values. CH announces the CH election procedure for nodes. Old CH broadcasts a message about the withdrawal of authority. New CH sends alert messages to the sensors nodes. CH is responsible for authentication of the other members of the cluster, and the base station (BS) is responsible for CH

authentication. Because of limited battery life and resources, each agent is only active when needed.

- ***Local agent:*** Local agent is responsible for monitoring the information sent and received by the sensor. The node stores in his internal database specific malicious network nodes attacks. When the network first organized, WSN nodes are not having any information or knowledge specific to malicious nodes. After the deployment of WSNs, the signature database is constructed gradually. The entry in the malicious node database is created and propagated to every node by a CH.

- ***Global agent:*** The global agent monitors the communication of its neighbor nodes. Because the broadcast nature of the wireless network, every node can receive all the packets going through its radio range. The global agent must have the information of its neighbor nodes to monitor the packets. We use local monitoring mechanism and pre-defined rules to monitor the packets if the monitor nodes discover a possible breach of security in of their neighbor nodes; they create and send an alert to the CHs. The CHs receive the alert and make the decision of a suspicious node through the threshold X. Both agents are built on the application layer.

B. Strategic location of IDS agent

Intrusion detection and response mechanism must be distributed and cooperative one in order to meet the needs of sensor networks. In our scheme, IDS agent is located in every sensor node. All the sensor node have an intrusion module known as local IDS agent. The cluster head executes a global IDS agent. Because of limited battery life and resources, each agent is only active when needed. The local agent is responsible for monitoring the information sent and received by the sensor, and forward it to the cluster head. The global agent is responsible for making a decision. Because the broadcast nature of the wireless network, every node can receive all the packets going through its radio range. Figure 2. below describes the strategy location of IDS.

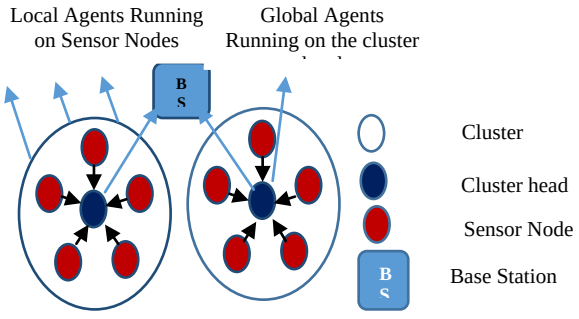

Figure 2. Describes the strategy location of IDS in network.

In our scheme, every node belongs to a single cluster among the clusters; it is geographically distributed across the whole network. Our objective is to make use of cluster-based protocols in energy saving, inorder to minimize the use of computational resources and data transmission redundancy, an intrusion framework for information sharing, which utilizes hierarchical architecture to improve intrusion detection capability for all participating nodes

IV. SUPPORT VECTOR MACHINE

Support vector machines (SVMs) are a class of machine learning algorithms, due originally to Vapnik [10]. It is originally devised for binary classification; it has been extended to include (amongst others) regression, density estimation, and one-class classification. Over the last decade, SVMs have gained popularity due to their ability to tackle complex and nonlinear problems in a structured & reliable manner, while simultaneously avoiding problems of overfitting on simpler problems. For further details on the attributes of SVMs, [10], [11] can be referred.

In the present context, we will be using one-class SVMs to detect selective forwarding attacks in a sensor network. We have chosen the one-class approach because we are unlikely to know the form of any attack prior, and hence if we construct attack training set it may unlikely provide an accurate representation of actual attack on the network.

SVM is a design method based on the small sample study and it is best suited for the classification of small sample data. Therefore, the SVM method is used to classify the high-dimension data in IDS[12],[13]. During the training phase, which takes place offline at a system with abundant resources, data are collected from the physical, MAC (medium access control) and network layers. Later on, the collected training data is pre-processed using a data reduction process, which aims to reduce their size in order to be processed by SVM.

As shown in Figure 3 classification of hyperplanes, thee solid points and the hollow points express the two classes training sample respectively. Hy is the class line which divides the two classes without mistake, Hy1 and Hy2 are the line that pass through the points which are the nearest to the class line in each class's samples and parallel to the class line. The distance between Hy1 and Hy2 is called the separating margin of the two classes[14]. We want the optimal class line which may separate the two classes correctly as well ensure the experience risk minimization, and have the maximum separating margin of the two classes to ensure the real risk minimization.

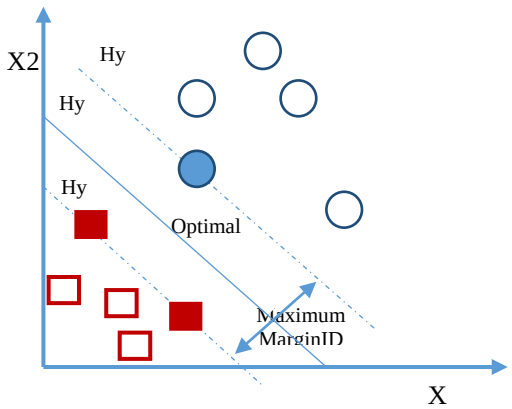

Figure. 3. Classification of hyperplane

Classification hyperplane of training data may be divided by linear classification plane noy by mapping the training data vector to higher dimensional space with some function and transferring the respective problem to a linear classification problem in that space. After the mapping procedure, SVM finds linear separating hyperplane with the maximum margin

in the space. In [15] [16], described the problem as finding a solution of convex optimization problem

V. ATTACK MODEL & DETECTION SCHEME

We have simulated an application in which the goal of the deployed sensor network is to report the presence of a mobile intruder to the base station as quickly as possible. This is done by having each node initiate a packet destined to the base station when its sensors sense the intruder in its vicinity. From these packets, the base station is able to analyze the movement pattern of the mobile intruder and its status. However, in our scenario we suppose that an intelligent adversary has included herself in the position of maximum node degree, so that he or she can intercept the maximum number of data flow paths. The nodes use MTE to forward the packets to the base station. At any given time, the base station records incoming bandwidth utilization and number of hops each message took to reach it. Simulation parameters are as follows: We use field size of 100 x 100 m2, where 50 nodes have been deployed randomly[17]. There is a single base station located on the far left end of the network. Each node has a maximum signal strength of 30m. The detection range of each sensor is 10m. Sensors are activated in 1 sec intervals. Each node has an initial energy of 400 Joules and AMP = 10pJ/bit/m2 and Eelec = 50nJ/bit. The simulated packet size is 26 bytes.

Detection algorithms

We assume that when a sensor node is first deployed in the environmental field there is no malicious node since an adversary requires a particular period to deploy an attack.

The monitor nodes use the watchdog monitoring mechanism and predefined rules with two-hop neighbor knowledge to detect anomalies within their transmission ranges. In watchdog approach, wireless packets are captured and stored in a buffer, which contains information including the packet identification and type, source and destination, etc. Monitor node entry in the buffer is time stamped. This expires after a timeout or after the entry in the buffer is examined by monitor nodes.

Intrusion Detection Model

This module uses a discovery protocol based on the specifications to detect malicious nodes and prevent network disruptions by these nodes. The purpose of this protocol is to classify the behavior of a target as normal or abnormal based on a set of rules. We have used four rules for each attacks.

Rule-1: for hello flood attack: The rule for detecting the Hello flood attack is the received signal strength (ISSR) at the IDS agent, it is greater than a certain threshold (δissrh).

1. {
2. If (ISSR >δissrhf)
3. Then {
4. Create (alert);
5. Send (alert, node_ID, ISSR);}
6. Else receive (packetp)}

Rule-2: for selective forwarding attack: The rule for detecting the number of packets defines the attack Selective forwarding dropped (PDR) and a node that is above a certain threshold δsf).

1. {
2. if(PDR >δbh && ISSR>δissrbh)
3. Then {
4. Create (alert);
5. Send(alert, node_ID, PDR, ISSR);}
6. Else receive(packetp)}

Rule-3: for Wormholes attack: the rule for detecting the attack excess wormholes is the signal power (above the threshold δissrhwh) and none of the neighboring nodes malicious node makes the retransmission of packets received from this opponent (PDR threshold the threshold δwh).

1. {
2. if (ISSR >δissrwh && (PDR >δwh)
3. Then {
4. Create (alert);
5. Send(alert, node_ID,ISSR); }
6. Else receive(packetp) }

Rule-4: Global IDS agent: Once the receipt of alerts from the IDS agents, Cluster head takes the decision from its malicious nodes database, creates and propagates the rule (code snippet for Global detection on Cluster head)

1. Repeat
2. If Looking(alert, malicious node's database)
3. then {
4. Drop (packetp);
5. Create(rule);
6. Propagate(rule);

7. } }

Decision making model

If more than half of IDS nodes says the suspected target is malicious, CH ejects node and calculates the appropriate rule of this new intrusion detected. CH sends a message to all IDSs, so they proceed to update their table of signatures.

Finally, the CH will be excluded from the network and a new CH will be elected. Note that for each cluster, this threshold is equal to N/2 where N is the number of IDS agents in each cluster. Figure 4. below illustrates Structure of the proposed intrusion detection model.

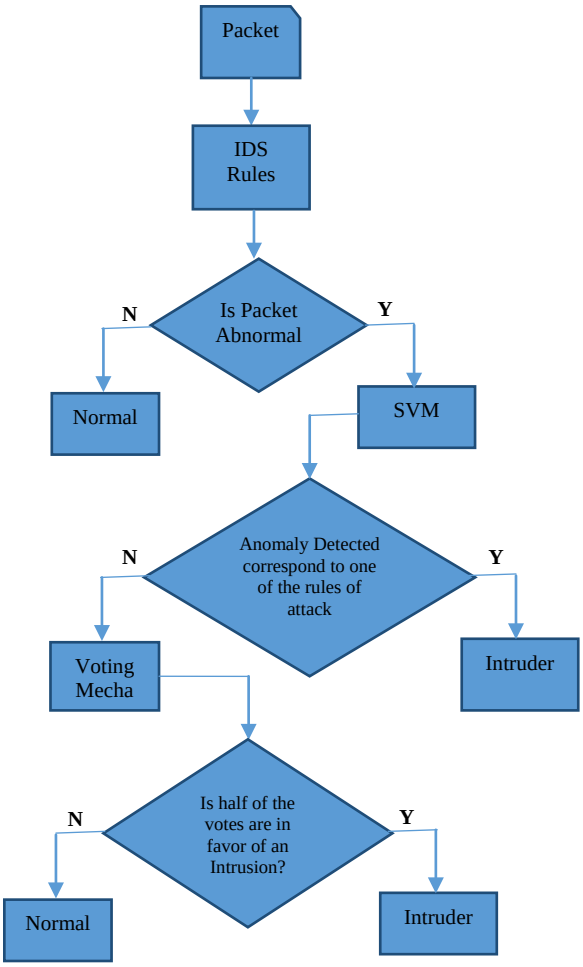

Figure 4. Logical Structure of Intrusion

VI. DATA STRUCTURE

Sensor nodes maintain two databases: malicious nodes and neighbor knowledge.

Two-hop neighbor knowledge: Two-hop neighbor knowledge: Two-hop neighbor knowledge is generally used in broadcasting protocols to reduce the number of transmissions, such as Source-based Protocol, Dominant Pruning, etc [18]. As we mentioned in Related Work, IssaKhail et al. Applied two-hop neighbor knowledge for detecting wormhole attacks in WSNs and Ad Hoc networks (Khalil et al., 2005; 2008). We do have applied two-hop neighbor knowledge as a component in detection technique. Unlike the two-phase setup in Khalil's work, we have prepared two-hop neighbor list in each sensor node via a single phase, by modifying the Hello packet. When the sensor nodes are initially deployed in the sensing environment, each node must build its direct neighbor list and a list of two-hop neighbors accessible to these one-hop neighbors.

To accomplish this, each node broadcasts its Hello message; fields contain information about source node ID, immediate node, and the hop counter is set to two. In case of the source node, and immediate node have the same node ID when a node receives a two-hop Hello packet, it changes the immediate node as its node ID, decrements the hop count to one and re-broadcasts it. WSN node receiving Hello message assigns the immediate node as its direct neighbor, and the source node as its two-hop neighbor. This process is performed once, after the deployment of sensor nodes. We assume that the neighbor node knowledge is secure and confidential within the deployment period.

Malicious node database/ blacklist:

The internal database is computed and generated in the CH by using anomaly detection in the global detection algorithms of monitor nodes. Once a monitor node identifies or suspects an anomalous event within its neighborhood, it forwards an alert to its CH. If the malicious counter from a suspicious node stored in a CH crosses a threshold X, the CHs provide an update of a new rule to every sensor node in the cluster. The sensor nodes update the entry to its malicious database with new rules. The malicious node is isolated from the cluster and not involved in communication in the network.

VII. PERFORMANCE ANALYSIS

For evaluating the performance of our intrusion detection model using KDDcup'99, database [20]. We have analyzed the variations intrusion detection and false positiveness when the number of IDS increases in the network. Finally, we compare the performance of proposed model with existing hybrid models. To evaluate and verify the effectiveness of proposed approach, we have adopted set of metrics to determine the most efficient intrusion detection model.

- Detection Rate: Shows the percentage of detected attacks on the total number of attacks.
- False positive rate (false alarms): It is ratio between the numbers classified as an anomaly on the total number of normal connections.

The combination of anomaly detection based on SVM and attack signatures allows the Intrusion detection model to achieve a high rate of intrusion detection (almost 98%) with a number very reduces false alarms (near 2%) as shown in Table I below.

Table 1. Detection and false positive rate under four attacks.

Sr.No.	*Attack*	*Detection rate*	*False positive*
1	Selective forwarding attack	98,40%	5,13%
2	Hello flood attack	97,20%	2,24%
3	Black Hole attack	96,80%	3,50%
4	Worm Hole attack	98,20%	4,54%

To determine the effectiveness of our approach, we have compared our model with others hybrid models proposed by authors Bin et al. [21], Khanum et al. [22], Yuan et al. [23] and Hai et al. [24], analyzing in particular the detection rate and false alarms and generated by IDS agents. Figure 5. below shows the performance comparison of some existing intrusion detection models with proposed one based on detection rate whereas Figure 6. Shows that proposed model is better in terms of lower false positive rate.

Figure 5. Shows hybrid model is better in detection rate

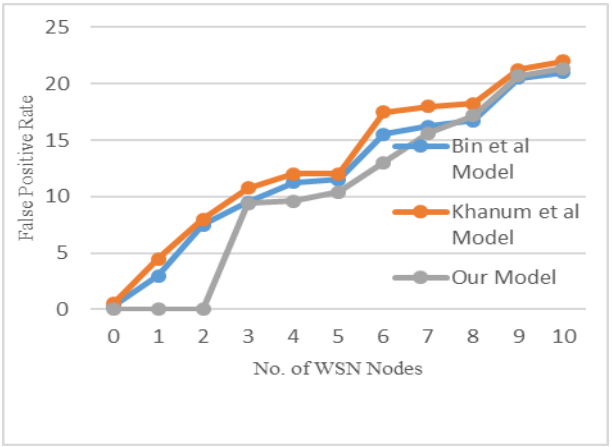

Figure 6. Proposed hybrid model is having lower false positives rate

VIII. CONCLUSION AND FUTURE WORK

Proposed hybrid IDS for WSN is based on anomaly, signature and SVM. The combination of these techniques offer an intrusion detection system with a higher Intrusion Detection and low false positive rate. Proposed approach is integrated in a cluster-based topology in-order to reduce communication costs, which leads to improve the lifetime of the network. For future, more research work needs to be undertaken for supplementing Intrusion detection to achieve a high level of security.

IX. REFERENCES

[1]. K. Q. Yan, S. C. Wang, S. S. Wang, C. W. Liu, "Hybrid intrusion detection system for enhancing the security of a cluster-based wireless sensor network", Proceedings of 3rd IEEE International Conference on Computer Science and Information Technology, China, pp. 114-118, 2010.

[2]. T. H. Hai, E. N. Huh and M. Jo, "A lightweight intrusion detection framework for wireless sensor networks", Wireless Communications and Mobile Computing, 10(4): 559-572, 2010.

[3]. R. Roman, J. Zhou, J. Lopez, "Applying intrusion detection systems to wireless sensor networks ", in: 3rd IEEE Consumer Communications and Networking Conference, pp.640-644, 2006.

[4]. Mishra, D. P., & Kumar, R. (2015). "Vision of Hybrid Security Framework for Wireless Sensor Network", Indian Journal of Applied Research, 5, 167.

[5]. L. Coppolino, S. D'Antonio, A. Gafalo, L. Romano, "Applying Data Mining Techniques to Intrusion Detection in Wireless Sensor Networks", Eighth IEEE International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2013.

[6]. Mishra, D. P., & Kumar, R "IDS Foundation for Wireless Sensor Network", GJRA-Global Journal for Research Analysis, Vol.5, Issue 11, pp.453-459,Nov 2016.

[7]. C. Haiguang, W. Huafeng, X. Zhou , G. Chuanshan, "Key Feature and Rule-based Intrusion Detection for Wireless Sensor Networks", IFIP International Conference on Network and Parallel Computing – Workshops, 2007.

[8]. Da Silva, A. Loureiro, M.H.T Martins, L.B Ruiz, H.Wong, "Decentralized Intrusion Detection in Wireless Sensor Networks". International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems, October 2005

[9]. Mishra, D. P., & Kumar, R. (2016). Analysis of Wireless Sensor Networks Security Solutions and Countermeasures. Journal of Scientific and Technical Research, 8, 10.

[10]. C. Cortes and V. Vapnik, "Support vector networks," Machine Learning, vol. 20, no. 3, pp. 273–297, 1995.

[11]. C. J. C. Burges, "A tutorial on support vector machines for pattern recognition," Knowledge Discovery and Data Mining, vol. 2, no. 2, pp. 121–167, 1998.

[12]. L. M. Manevitz and M. Yousef, "One-class SVMs for document classification," Journal of Machine Learning Research, vol. 2, pp. 139–154, 2001

[13]. J. Schray and C. A. Manogue, "Octonionic representations of Clifford algebras and triality," Foundations of Physics, vol. 26, pp. 17–70, 1996

[14]. B. E. Boser, I. M. Guyon, and V. N. Vapnik, "A Training Algorithm for Optimal Margin Classifiers", The 5th Annual ACM Workshop on Computational Learning Theory, Vol. 1, pp. 144-152, July 1992.

[15]. I. Nurtanio, E. R. Astuti, I. K. Purnama, M. Hariadi, "Classifying Cyst and Tumor Lesion Using Support Vector Machine Based on Dental Panoramic Images Texture Features," IAENG International Journal of Computer Science, Vol. 40, No. 1, pp. 29-37, 2013.

[16]. J. M. Yang, Z. Y. Liu, Z. Y. Qu, "Clustering of Words Based on Relative Contribution for Text Categorization", IAENG International Journal of Computer Science, Vol. 40, No. 3, pp. 207-219, 2013.

[17]. Mishra, D. P., & Kumar, R (2015) "Qualitative Analysis of Wireless Sensor Network Simulator" International Journal of Computer Applications (0975 – 8887) National Conference on Knowledge, Innovation in Technology and Engineering (NCKITE 2015)

[18]. Vapnik, "V.N.: Statistical study theory essential", Qinghua University publishing press, 1995.

[19]. Khalil, I., Bagchi, S. & Shroff, N. B. (2008). Mobiworp: Mitigation of the wormhole attack in mobile

multihop wireless networks, *Ad Hoc Netw.* 6(3): 344–362

[20]. KDD Cup 1999 Data, http://kdd.ics.uci.edu/databases/kddcup99/task.html; 1999.

[21]. W. H. Bin, Y. Zheng, W. C. Dong, "Intrusion detection for wireless sensor networks based on multi-agent and refined clustering", International Conference on Communications and Mobile Computing, IEEE, Yunnan, China, pp. 450-454, 2009.

[22]. S. Khanum, M. Usman, K. Hussain. "Energy-efficient intrusion detection system for wireless sensor network based on MUSK architecture", Second International Conference on High Performance Computing and Applications, Springer, Shanghai, China, pp.212-217, 2009.

[23]. L. Yuan, L.E Parker, "Intruder detection using a wireless sensor network with an intelligent mobile robot response", IEEE Southeastcon, 2008.

[24]. T. H. Hai, E. N. Huh and M. Jo, "A lightweight intrusion detection framework for wireless sensor networks", Wireless Communications and Mobile Computing, 10(4): 559-572, 2010.