Volume: 07 Issue: 02 Pages: 2674-2681 (2015) ISSN: 0975-0290

Hybrid Technique for Detection of Denial of Service (DOS) Attack in Wireless Sensor Network

S.Sumitha Pandit[1]
[1] Research Scholar, Department Of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, TamilNadu, India
Email: sumitha975@gmail.com
Dr.B.Kalpana[2]
[2] Professor, Department Of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, TamilNadu, India
Email: kalpanacsekar@gmail.com

----------**ABSTRACT**----------
Wireless Sensor Network (WSNs) are deployed at aggressive environments which are vulnerable to various security attacks such as Wormholes, Denial of Attacks and Sybil Attacks. There are various intrusion detection techniques that are used to identify attacks in a network with high accuracy level. This paper has focused on Denial of Service attack, since it is the most common attack that affects the environment severely. Therefore a new hybrid technique combining Hidden Markov Model with Ant Colony Optimization (HMM+ACO) has been proposed that gives improved performance than the other techniques.
Keywords – **ACO, Denial of Service, HMM ,Intrusion Detection,Wireless Sensor Network**

Date of Submission: Sep 17, 2015 Date of Acceptance: Oct 09, 2015

1.INTRODUCTION

1.1 Wireless Sensor Network (WSN)

Wireless Sensor Networks have been widely applied in various fields such as environmental monitoring, healthcare management, battlefield surveillance and industry control. Wireless Sensor Networks (WSNs) is one of the most important technologies for the twenty-first century. Wireless sensor network (WSN) connects the distributed autonomous sensors for collecting the data from sensors or distribute the data into sensors. Wireless sensor networks (WSNs) consist of a large number of low-cost, low-power, and multi-functional sensor nodes. These sensor nodes are small in size, equipped with sensors, embedded microprocessors, and radio transceivers [12]. They communicate over a short distance and collaborate to accomplish any task. The aim of security mechanism in WSN is to guard the information from attacks. This security mechanism which is provided for wireless sensor network makes sure that network services are available in presence of any vulnerability. There are security mechanism is based on five principles [17] confidentiality, authenticity, Integrity, availability and data freshness.

To cope up with the attacks, the concept of Intrusion detection was invented by James Anderson in 1980 and a method based on this was introduced by Denning in 1987.Intrusion Detection System (IDS) is a device or software application that monitors the activities to identify malicious behavior or suspicious event in different environment. Intrusion Detection System is a type of sensor that raise the alarm when specific event occurs and it produces the log report to the management system. Intrusions are caused by inside attackers and authorized users attempting to gain and misuse unauthorized privileges [9]. The various causes of intrusions include incorrect algorithms, architectures, vulnerabilities/flaws, implementation mistakes, component defects and external disturbances [2]. There are different security attacks in WSN are as follows,

- Denial-of-Service (DoS) attacks
- Sinkhole/Black hole attacks
- Selective forwarding attack
- Node Replication attacks
- HELLO Flood attacks
- Wormhole attacks
- Sybil attack

1.2 Denial of Service

The Denial of Service (DoS) attack frequently sends unwanted packets and it tries to utilize the bandwidth of network. It legitimates the network user from accessing the system or resources when required. The DoS attack can present itself in physical layer, link layer, network layer and transport layer. DoS attack can be prevented by strong authentication and identification built into the intrusion detection system. Other DoS attacks are very harsh and it reacts in two ways such as jamming and tampering.

Jamming is the deliberate interference on the wireless communication channel. This attack is a

Volume: 07 Issue: 02 Pages: 2674-2681 (2015) ISSN: 0975-0290

common one in which the attacker tries to disrupt the operations of entire network or a particular small portion of it. Jamming may be consistent or irregular. To handle jamming at network layer deals with mapping jamming area in the network or in neighboring routing area. The attack is simple and effective when the network is based on single frequency otherwise the attack should be eliminated since it uses various forms of spread spectrum.

Tampering is one of the physical attacks, which targets the hardware of the sensor nodes. Tampering attack is not feasible to manage hundreds of nodes extend over an area of several kilometers. Tampering attackers may dig out the sensitive information like cryptographic key from node by damaging it to get access to higher level of communication. The only security mechanism against tempering is to temper-proof physical packaging. But it costs additional. [1]

2. RELATED WORK

Shi-Jinn Horng *et al* [26] have designed a new flow for intrusion detection system using SVM technique. The famous KDD Cup 1999 dataset was used to evaluate the proposed system. Compared with other intrusion detection systems that are based on the same dataset, this system showed better performance in the detection of DoS and Probe attacks, and the best performance in overall accuracy.

Hayoung Oh *et al* [5] have proposed a real-time intrusion and anomaly detection system using SOM. This system labels the map produced by SOM using correlations between features. It classifies neurons as normal or attacks. In the case of attack neurons, they have classified them again into the types of attacks. When a malicious behavior is caught, this system detects the intrusion as previously known attack or a new untrained attack.

Mohammad Wazid [10] has used hybrid anomaly detection technique with the k-means clustering. WSN are simulated using OPNET simulator and the resultant dataset consists of traffic data with end to end delay data which has been clustered using WEKA 3.6. In this experiment, it has been observed that two types of anomalies (misdirection and black hole attacks) are activated in the network.

Shun-Sheng Wang e*t al* [18] have designed an integrated intrusion detection system using intrusion dataset from UCI repository .The dataset trained well using BPN and the output is used as an important parameter in ART model to cluster the data. Finally the outputs received from both techniques are compared and the ART model provides the best accuracy rate and overall performance.

Mohit Malik *et al* [11] have applied the rule based technique for detecting the security attack in WSN. They have discovered ten important security attack type in their work and the parameters of those attack have been developed fuzzy rule based system for calculating the impact of security attack on the wireless sensor network. Once the system has been executed it shows the impact of attack in the network.

Reda M. Elbasiony *et al* [14] have proposed a hybrid detection framework i.e. in anomaly detection, k-means clustering algorithm is used to detect novel intrusions by clustering the network connection's data to collect the most of intrusions together in one or more clusters. In this proposed hybrid framework, the anomaly part are improved by replacing the k-means algorithm with another one called weighted k-means algorithm, In this approaches Knowledge Discovery and Data Mining (KDD'99) datasets are used.

LeventKoc *et al* [7] have proposed a new technique HNB model which exhibits a superior overall performance in terms of accuracy, error rate and misclassification cost .In early stages the traditional Naïve Bayes model are used but the result produced by HNB is better than traditional Naïve Bayes. The results they have produced indicate that this model significantly improves the accuracy of detecting denial-of-services (DoS) attacks.

WenyingFenga *et al* [22] have introduced a new way of combining algorithm for the better result in detecting intrusions. They have classified the network activities into normal or abnormal by reducing the misclassification rate. In this work the author combined Support Vector Machine method and the Clustering based on Self-Organized Ant Colony Network to take the advantages by avoiding their weaknesses. This Experiments show that CSVAC (Combining Support Vectors with Ant Colony) outperforms better the SVM or CSOACN in terms of both classification rate and run-time efficiency.

MeghaBandgar*et al* [8] have described a novel approach using Hidden Markov Models (HMM) to detect Internet attacks and they have described about an intrusion detection system for detecting a signature based attack. They have performed single and multiple HMM model for source separation both on IP and port information of source and destination. In this approach they have reduced the false positive rate.

Dat Tran *et al* [3] have proposed Fuzzy Gaussian mixture modeling method for network anomaly detection. In this work a mixture of Gaussian distributions are used to represent the network data in multi-dimensional feature space. Using fuzzy C-means estimation, Gaussian parameters were estimated and the whole work is carried out with the KDD Cup data set. The proposed method produced here is more effective than the vector quantization method.

VahidGolmah [19] has been developed a hybrid technique using C5.0 and SVM algorithm and they have investigated and evaluate the performance of this hybrid technique with DARPA dataset. The motivation for using this hybrid approach is to improve the accuracy of the intrusion detection system when compared to using individual SVM and C50. By combining the SVM and C5.0 this technique took less of execution time.

PunamMulak [13] has used hybrid technique by combining Boundary cutting algorithm and clustering algorithm. The motivation for using this hybrid approach is to improve the accuracy of the intrusion detection system and to provide better result than other clustering.

Volume: 07 Issue: 02 Pages: 2674-2681 (2015) ISSN: 0975-0290

VenkataSuneethaTakkellapati [21] has proposed a new system where Information Gain (IG) and Triangle Area based KNN algorithm are used for selecting more discriminative features. Then Greedy k-means clustering algorithm is combined with SVM classifier to detect Network attacks. This system achieves with high accuracy detection rate and less error rate .All this work are carried out in KDD CUP 1999 training data set.

Vaishali Kosamkar [20] has followed same technique of combining C4.5 Decision Tree and Support Vector Machine (SVM) algorithm in order to achieve high accuracy and diminish the false alarm rate. In feature selection stage, Correlation- Based Feature Selection (CFS) algorithm is used for better accuracy result.

HarmeetKaurl [7] has designed their work to reduce the delay in the network and to produce end to end data in good speed. So in order to achieve, they have simulated WSN using SPEED protocol. They have used two performance parameters throughput and energy consumption for analysis. BCO (Bee Colony Optimization) algorithm is used to give better results with high throughput and low energy consumption. All the simulations are carried out in MATLAB.

3. METHODOLOGY

This research work aims at detecting DoS attack in WSN using Hybrid technique. The objective is to improve accuracy level and reduce misclassification and false positive rate. The steps involved in this proposed research design are shown in fig1.

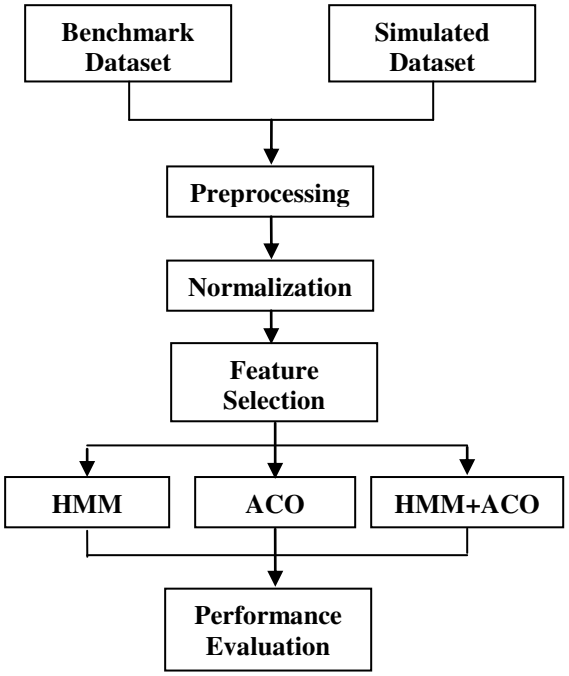

Figure 1. Overview of Methodology

3.1 Pre-processing

It is the main step in improve the data quality. Data from the dump area or from real-time environment consists of noise, inconsistent, incomplete, missing value, numeric and non-numeric data. Such type of data must be cleaned using preprocessing techniques. Since in this work both TCP dump and simulated dataset are used, probability method is used to convert all non-numeric values into numeric values in both datasets.

3.2 Normalization

Data normalization is a method to convert the data vector into a new data vector where numeric values fall within a specified range, such as scaling values between [0,1]. This allows better comparisons or visualizations of attributes that are of different units. There are many types of normalization such as min-max, z-score and decimal scaling normalization. The normalization method used for this data is Min-Max Method. It transforms all feature value to fall between specified range [0, 1], since each value has different ranges. The normalized value of e_i for variable E in the i^{th} row is calculated as:

$$\boldsymbol{Normalization}\,(\boldsymbol{e_i}) \;=\; \frac{\boldsymbol{e_i - E_{min}}}{\boldsymbol{E_{max} - E_{min}}}$$

Where,

E_{min} = the minimum value for variable E

E_{max} = the maximum value for variable E

If E_{max} is equal to E_{min} then Normalized (e_i) is set to 0.5.

3.3 Feature Selection

Using Feature Selection technique it selects specific subset of features to achieve the target output. The main aim of feature selection is to remove the redundant and irrelevant attributes (features), it is also named as attribute subset selection [15].Through this selection, the level of accuracy increases, with a reduction on dimensionality and over fitting. **Principal Component Analysis** approach monitors the variables and their relationship to one another. It reduces the number of variables in regression and clustering, for example. Each principal component in **Principal Component Analysis** is the linear combination of the variables which gives a maximized variance. The steps in PCA are as follows:-

i) it assign scoring to each feature and based on the scoring the features are either kept or removed from dataset to achieve the target output and

ii) It finds a linear projection in high dimensional data and converts them into lower dimensional subspace that helps to minimize the reconstruction error.

- Subtract the mean from the dataset in all the n-dimensions
- Calculate the covariance matrix of this mean subtracted dataset.
- Calculated the eigenvalues and eigenvectors of the covariance matrix found in step2.
- Forming a feature vector by selecting the eigenvector with the largest eigenvalues

Finally Results are produced.

Figure 2. Procedure for PCA

Volume: 07 Issue: 02 Pages: 2674-2681 (2015) ISSN: 0975-0290

3.4 Techniques

3.4.1 Hidden Markov Model (HMM)

In this work, HMM perform a generative model that can model data sequentially in nature. HMM is used to model data by assuming Markov property .Suppose a system with N states and at discrete time intervals transition take place among states. Let these instances be t, t = 1, 2, 3 ... .any process is said to be a Markovian, if only if the conditional probability of future states, depend only upon the present state. The identification and equations of HMM consists of 5tuples i.e. [N,M,A,B,π] [20].

Where,

N denotes the number of states $Q = \{Q_1, Q_2, ...Q_n\}$.

M, number of observation symbols, $V= \{V_1, V_2 ... V_M\}$.

Hidden Markov Model use two different algorithms which perform different task, they are Baum- Welch and Forward –Backward algorithm. Baum-Welch algorithm learns only the parameter of the model {A, B, π} and Forward-Backward algorithm learns the probability of occurrence of an observation sequence from the given model, P|O|λ. Here HMM algorithm learn the parameter, and compute the probability of an output sequence on both dataset using Forward-Backward technique.

Iterate the following stages until the termination condition is met:

Forward stage

- Initialize $alpha_0$(start state) = 1, and $alpha_0(s)$ = 0 \\ for all other states 's'.
- Repeat for each i from 0 up to k-1:For each state s: $alpha_{i+1}(s) = sum_{all\ states\ s'} alpha_i(s')*p_{s,s'}*q(y_{i+1} \mid s <-- s')$

Backward stage

- Initialize $beta_k(s) = 1$ for all states s
- Repeat for each i from k down to 1:For each state s: $beta_{i-1}(s) = sum_{all\ states\ s'} p_{s',s}*q(y_i \mid s' <-- s)*beta_i(s')$

Figure 3. Pseudocode for HMM

3.4.2 Ant Colony Optimization (ACO)

Ant colony optimization is a probabilistic technique initially used for solving computational problem, later it was used for finding good path through graph. ACO algorithm belongs to the class of swarm intelligence methods, it constitutes some novel optimizations. To achieve the goal of finding an optimal path in a graph, ACO algorithm follows the behavior of an ant in seeking its food in its own colony. When an ant runs for food into an object automatically it measures 'colony similarity' within its local range. This run decides whether to pick up or drop the object according to the value of probability. That finally diversified to solve a wider class of numerical problems, and as a result, several problems have emerged, drawing on various aspects of the behavior of ants.

Initialization

for i=1 to I (I=cycle number)

If i=1 then generate m random ant within range

else reduce FS within range $[x_{t-1}^{best} + \beta; x_{t-1}^{best} - \beta]$

end if

for i =1 to m

Determine f (x_t^{best})

Save x_t^{best}

end

Pheromone Update

Pheromone evaporation

Update Pheromone trail

Solution phase

Determine search direction

Generate the values of α vector

for i= 1 to m

Determine the values of new colony

Determine new f (x_t^{best})

Save x_t^{best}

end

If $f(x_t^{best})^{new} \leq (x_t^{best})^{old}$ then $x^{globalmin} = (x_t^{best})^{new}$

else $x^{globalmin} = (x_t^{best})^{old}$

end if

end

Figure 4. Pseudo code for ACO

A definition of colony similarity is the similarity between an un-clustering object and other objects within its local range [9] .It possesses properties like flexibility, robustness, decentralization, and self-organization; it can suggest very interesting heuristics and it is used in both dataset.

3.4.3 Hidden Markov Model combined with Ant Colony Optimization (HMM+ACO)

Combination of techniques is the best way to improve the overall performance in intrusion detecting system .Here new hybrid algorithm is developed by combining the two existing algorithm that is discussed above (HMM and ACO).In this algorithm, both HMM and ACO are two interactive phase which multiples the

Volume: 07 Issue: 02 Pages: 2674-2681 (2015) ISSN: 0975-0290

iteration and executing time. HMM generates 'pState' value as output whereas ACO produce 'GlobalMin' value as output .To enhance the result of HMM and ACO, both values are hybridized to give a new optimization structure and a better result.

```
Input: A new data item x.
Input: GlobalMin (ACO) and pStates (HMM)
from Individual algorithm.
Output: L – the label of x.
  Begin
  LH ←performance of x with HMM;
  LA ← performance of x with ACO;
  if LH = LA = normal  then
 L ← normal;
  else if LH<>LA then
 L ← amphibious;
  else
 L ← LA;
 (Generate new optimization iteration)
  (A sub-class of abnormal is detected by the
 HMM+ACO abnormal algorithm.)
 end
 end
```

Figure 5.Pseudocode for ACO

4. RESULTS AND DISSCUSSION

4.1. Experimental Setup

In this work, two different types of dataset i.e. i) Benchmark Dataset and ii) Simulated Dataset are used and performance is evaluated using MATLAB13b.

4.1.1 Benchmark Dataset

This experiment uses Intrusion Detection Evaluation dataset which was first used in "The Third International Knowledge Discovery and Data Mining Tools Competition". This dataset contains TCP dump generated data over a nine week periods of simulated network traffic in a hypothetical military LAN. It includes 7 million TCP connection records which have 21 types of attacks in that only DoS attacks are considered such as Back, Neptune, Pod, Smurf, Teardrop and normal attack and it has 41 features which is categorized as follow:

- Basic TCP features (1-9) are derived from packet headers without inspecting the payload.
- Time- and Host-Based Traffic features (10-28) capture both present and historical data
- Content features (29-41) are domain knowledge which is used to assess the payload of the TCP packets. i.e. no of failed login attempts.

4.1.2 Simulated Dataset

In this experiment, MATLAB software is used to simulate a WSN based on LEACH protocol with and without attack .Initially nodes are distributed randomly in the network topology in a square area of 100m*100m. Various parameters used for simulation are shown in Table 1

Table. 1 Simulation Parameters

Simulation Parameters	Value
Field Dimensions(in meters)	100 *100m
Packet size	4000 bits
Number of Nodes	50,100,150, 200
Optimal Election Probability of a node to become cluster head(p)	0.1
Tx& Rx Antenna gain (Gt=Gr)	50j/energy
Tx& Rx Antenna heights (in m)	1
Percentage of attack node	Upto 1%
Maximum number of rounds (r)	250

Simulated dataset are based on different scenarios i.e. normal mode and attack mode. Initially in normal mode, an event occurs in network and sensor nodes transmit packets to the base station in each round of simulation. In attack mode, once DoS attack is detected at any node, the service passing through that particular node automatically stops during simulation of 'n' no of nodes where n is varied from 50-200 nodes. From the experimental setup, the extracted features are extracted and it is given as input for pre-processing and then normalized using min-max normalization. Then principal component analysis (PCA) is applied to reduce the dimensionality of the normalized features. Finally a hybrid technique is applied to classify it as normal or abnormal and the performance is evaluated.

4.2 Performance Evaluation

The parameters used to evaluate the performance of proposed approach are Accuracy, False Positive Rate (FAR), and Misclassification Rate. They are defined as follows,

1) Accuracy

The Accuracy is defined as the number of intrusion instances detected divided by the total number of intrusion instances present in the data set. The formula to estimate the Accuracy is,

$$\text{Accuracy} = \frac{\text{Number of Intrusions detected}}{\text{Total Number of Intrusions Present}} \text{ X } 100$$

2) False Positive Rate (FPR)

False positive rate (FPR) is defined as the ratio of the numbers of abnormal measurements that are incorrectly misclassified as normal to the total number of normal measurements.

Volume: 07 Issue: 02 Pages: 2674-2681 (2015) ISSN: 0975-0290

$$FPR = \frac{\text{Number of misclassified abnormal measurements}}{\text{Total Number of normal measurements}} \text{ X } 100$$

3) Misclassification Rate

It is defined as the degree of errors encountered during data transmission over a communications or network connection. It is also denoted as "Error Rate".

$$\text{Misclassification Rate} = 1 - \frac{\text{Number of corrected classified connections}}{\text{Total Number of connections}} \text{ X } 100$$

The performance results are obtained and the proposed method of HMM+ACO is compared with HMM, ACO are tabulated in the following table. From the tables it is observed that hybrid technique (HMM+ACO) gives improved results when compared to HMM and ACO in all metrics.

4.3 Results:

A sample results for 150 nodes with DOS attacks is shown in the following figures 6, 7 and 8.

Table .2 Comparison of HMM, ACO and HMM+ACO on Benchmark dataset

Benchmark Dataset			
Metrics	**HMM**	**ACO**	**HMM+ACO**
Accuracy	79.5	73.4	**84.39**
False Positive Rate (FPR)	0.905	0.423	**0.074**
Misclassification Rate	0.204	0.265	**0.166**

Table .3 Comparison of HMM, ACO and HMM+ACO on Simulated dataset.

Simulated Dataset			
Metrics	**HMM**	**ACO**	**HMM+ACO**
Accuracy	89.55	82.66	**93.83**
False Positive Rate (FPR)	0.100	0.452	**0.077**
Misclassification Rate	0.104	0.173	**0.061**

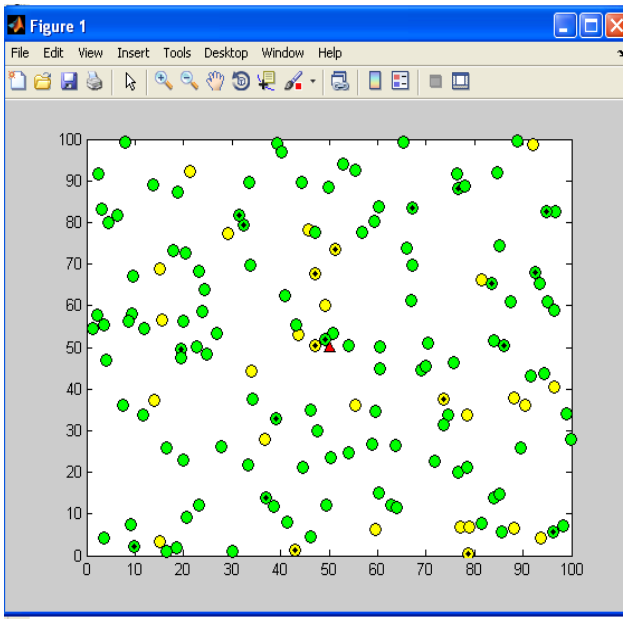

Figure 6. Detection of Attacker Nodes using 150 nodes

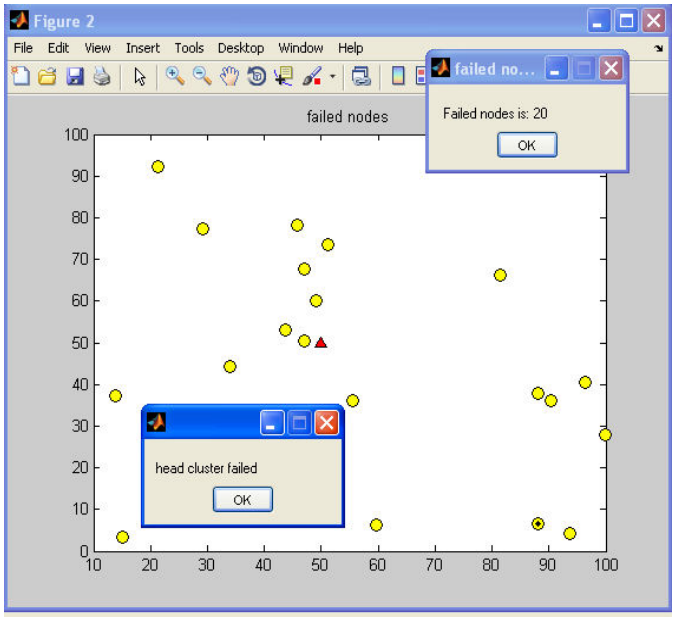

Figure 7. DOS attack occur at 20th node using 150 nodes

Volume: 07 Issue: 02 Pages: 2674-2681 (2015) ISSN: 0975-0290

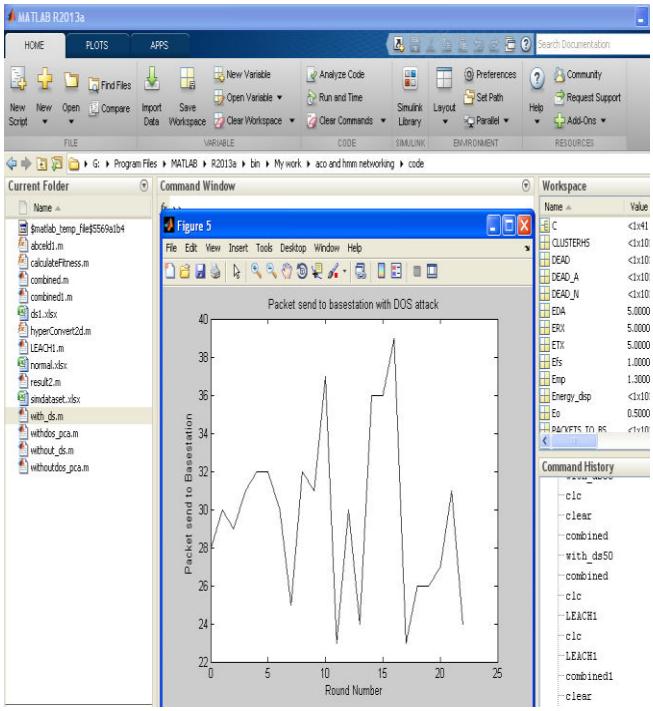

Figure 8. Packets sent to Base Station using 150 nodes.

From the experimental results, it is concluded that hybrid technique gives improved results than HMM and ACO. Accuracy result has been increased almost 10% in the case of both datasets. False Positive Rate and Misclassification rate has decreased by 2% almost using the both datasets.

5. CONCLUSION AND FUTURE ENHNCEMENT

There are different intrusion detection mechanisms available in the literature. There are many intrusions that affect the network day to day life but DoS is the most common attack that affects the environment. Therefore, the work has focused on detecting DoS attack using hybrid technique in WSN. The experimental results showed that the proposed technique achieves better Accuracy when compared to existing algorithms. The proposed hybrid technique (HMM+ACO) results are compared with earlier algorithms such as HMM and ACO.

Following are identified as the scope for future enhancement,

- In the future, Candid-Covariance free Incremental Principal Component Analysis (CCIPCA) can be operated instead of Principal Component Analysis (PCA) for dimensionality reduction .It can be used in the incremental mode to simulate the real time applications.
- The simulated data set can be further analyzed for classifying of other different type of attacks (i.e. Sink attack, Hello attack etc) where proposed technique can be used.

REFERENCES

[1] Amit Kumar Mishra, Sunil Ghildiyal, Ashish Gupta, Neha Garg ," *Analysis Of Denial Of Service (Dos) Attacks In Wireless Sensor Networks",* IJRET: International Journal of Research in Engineering and Technology, Volume: 03 Special Issue: 10 | NCCOTII 2014 | Jun-2014.

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

[3] Dat Tran, Wanli Ma, and Dharmendra Sharma," *Network Anomaly Detection using Fuzzy Gaussian Mixture Models*", International Journal of Future Generation Communication and Networking, pp.37-42, 2012.

[4] Harmeet Kaur , Ravneet Kaur, " *Crossbreed Routing Protocol for SPEED Terminology in Wireless Sensor Networks",* International Journal of Advance Research in Computer Science and management Studies, Volume 2, Issue 7, ISSN: 2321-7782, July 2014.

[5] Hayoung Oh," *Attack Classification based on Data Mining Technique and its application for Reliable Medical Sensor Communication*", International Journal of Computer Science and Applications, Vol. 6, No. 3, pp 20 – 32, 2009.

[6] Jue Lu, Rongqiang Hu, *"A new hybrid clustering algorithm based on K-means and ant colony algorithm",* Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013).

[7] Levent Koc , Thomas A. Mazzuchi, Shahram Sarkani, "*A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier"*, Elsevier, pp.13492–13500, 2012.

[8] Megha Bandgar, Komal dhurve, Sneha Jadhav,Vicky Kayastha,Prof. T.J Parvat, " *Intrusion Detection System using Hidden Markov Model (HMM)*", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 3, pp.66-70, (Mar. - Apr. 2013).

[9] Miao Xie, SongHan, BimingTian and, SaziaParvin," *Anomaly detection in wireless sensor networks: A survey",* Elsevier Journal of Network and Computer Applications, Vol.34, pp. 1302-1325, 2011.

[10] Mohammad Wazid , " *Hybrid Anomaly Detection using K-Means Clustering in Wireless Sensor*

Volume: 07 Issue: 02 Pages: 2674-2681 (2015) ISSN: 0975-0290

Networks" , Center for Security, Theory and Algorithmic Research, pp. 1-17.

[11] Mohit Malik, Namarta kapoor, Esh naryan, Aman Preet Singh," *Rule Based Technique detecting Security attack for Wireless Sensor network using fuzzy logic",* International Journal of Advanced Research in Computer Engineering & Technology ,Volume 1, Issue 4, , ISSN: 2278 – 1323, June 2012.

[12] Murad A.Rassam, Anazida Zainal and Mohd Aizaini Maarof,"*An Efficient distributed anomaly detection model for wireless sensor networks",* Elsevier AASRI Procedia, No.5, pp. 9-14, 2013.

[13] Punam Mulak, Nitin R. Talhar, "*Novel Intrusion Detection System Using Hybrid Approach*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 11, ISSN: 2277 128X, November 2014.

[14] Reda M. Elbasiony , Elsayed A. Sallam , Tarek E. Eltobely ,Mahmoud M. Fahmy ," *A hybrid network intrusion detection framework based on random forests and weighted k-means"* Ain Shams Engineering Journal", vol 4, pp.753–762,2013.

[15] Revathi, T. S. (2013). "*Survey: Effective Feature Subset Selection Methods and Algorithms for High Dimensional Data*". International Journal of Advanced Research in Computer Engineering & Technology (IJARCET).

[16] Shi-Jinn Horng , Ming-Yang Su , Yuan-Hsin Chen , Tzong-Wann Kao, Rong-Jian Chen, Jui- Lin Lai , Citra Dwi Perkasa *," A novel intrusion detection system based on hierarchical clustering and support vector machines"* , Elsevier Computer Network pp.306–313, 2010.

[17] Kumar Singh 1, M P Singh 2, and D K Singh, "*A Survey on Network Security and Attack Defense Mechanism for Wireless Sensor Networks",* International Journal of Computer Trends and Technology- May to June Issue 2011.

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

[19] Vahid Golmah, " *An Efficient Hybrid Intrusion Detection System based on C5.0 and SVM***",** International Journal of Database Theory and Application Vol.7, No.2 ,pp.59-70, (2014).

[20] Vaishali Kosamkar, Sangita S Chaudhari," *Improved Intrusion Detection System using C4.5Decision Tree and Support Vector Machine*", International Journal of Computer Science and Information Technologies, Vol. 5 (2) , pp. 1463-1467, 2014

[21] Venkata Suneetha Takkellapati1 , G.V.S.N.R.V Prasad," *Network Intrusion Detection system based on Feature Selection and Triangle area Support Vector Machine*", International Journal of Engineering Trends and Technology-Volume3Issue4- 2012

[22] Wenying Fenga, Qinglei Zhangc, Gongzhu Hud, Jimmy Xiangji Huange, "*Mining network data for intrusion detection through combining SVMs with ant colony networks*", Elsevier , pp. 127-140, 2013

BIODATA OF THE AUTHORS

Ms.S.Sumitha Pandit has received her MCA degree in 2014 from Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, TamilNadu, India. She is now completed her M.Phil in 2015 in Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, TamilNadu, India. Her areas of interest are Wireless Sensor Networks and Data Mining.

Dr.B.Kalpana Professor in Computer Science, Avinashilingam University for Women, Coimbatore, has around 25 years of teaching and research experience. Her areas of interest include Data mining and Wireless sensor networks. She has served as a reviewer for several journals in computer science. She has been the Principal Investigator for a project funded by the NRB in the area of wireless sensor networks. She has to her credit research papers and book chapters in several reputed national and international journals/books.