TECH-CHRONICLE
AN INTERNATIONAL E-JOURNAL ON
EMERGING TRENDS IN SCIENCE, TECHNOLOGY AND MANAGEMENT

Defense degree Evaluation in IDS for ZigBee based WSN by PSO

Madhav G.Raut
Associate Professor, Department of Electronics,
Hislop College,Nagpur
madhavraut63@gmail.com

Abstract—: As Wireless Sensor Networks are becoming popular as a simple means of collecting data by public utilities, motor vehicle manufacturers and other organizations. Unfortunately the devices on such networks are often insecure by default, which presents problems in terms of the integrity of the data provided across those networks. This paper explores a range of attacks that were successful on a network consisting of nodes using the ZigBee protocol stack and evaluates the degree of defenses for IDS by means of swarmly optimized networks. System proposes here can be put in place to circumvent these attacks thus leading to more secure systems and increasing user confidence.

Keywords - IDS, ZigBee, accepted indicator quality evidence (RSSI), WSN, Swarm

I.INTRODUCTION

Quick development of framework, scaling down the attacks, remote association, and on-chip sign transforming has pushed the advancement of remote sensor mastery, which has enriched its wide submissions from condition established upkeep to created framework observing and biological feeling. The amount of remote sensors, which are ordinarily prompted as a remote sensor network(wsn), made for genuine applications has immediately expanded in most recent years, and this pattern is required to much more help in the one years from now . The security issues that ZigBee suffer from are not something newly introduced, but inherent in the protocol stack. However, its widespread use in smart grid networks and home area networks (HANs) exert a serious threat. Attackers can simply redirect the traffic, dump the network or inject some data in the packets in order to alter the network. This can result in serious disaster, if an attacker locked all the doors in case of a fire, or alters the data being sent back and forth to the smart grid. Several attacks on WSNs are already known, including multiple attacks migrated from the TCP/IP world to WSNs. Attacks on WSNs can be classified in several categories: (i) sybil, (ii) wormhole, (iii) DoS, (iv) node replication, and (v) node compromise. The resources of sensor nodes in a WSN are limited, thus a detection of attacks on the WSN communication infrastructure is a non-easy task. An intrusion detection system (IDS) which monitors all sensor nodes and gives controller and gateway nodes enough information to build a kind of an early warning system is a needed but challenging task. The idea is that sensor nodes monitor their neighborhood, detect and report abnormal network traffic, and respond by certain countermeasures like isolation of malicious nodes in the network. In this work we have broadly focused on node replication and node compromise attacks, system developed here is meant for defending the attacks by means of PSO optimized IDS & hence evaluates the degree of defense.

Among the latest events of the wireless revolution, the increasing importance of ZigBee as a standard for WSN is certainly one of these. ZigBee and IEEE 802.15.4 had been proving in the last years that they can achieve the same results as Wi-Fi had achieved for high bit-rate wireless LANs and some large reliable deployments are now in place implementing ad-hoc WSN in critical applications, like environment monitoring, asset tracking, and also military scenarios. The first release of the ZigBee standard was in 2004, followed by two revisions in 2006 and 2007 (ZigBee 2006v and ZigBee-Pro 2007v). The main differences between the first ZigBee revision and the latest ZigBee-Pro release are stochastic addressing, mesh data management, packet fragmentation, dynamic best channel choice, optional asymmetric connections and security improvements. Improvements concerning the security are made by optional provided header and/or data cryptography with AES-128. In ZigBee-2006 a global network key is used to create secure communication. ZigBee-Pro offers a more complex system which adds a peer-to-peer encryption layer. Each couple of nodes has its own key which allows a peer-to-peer encryption. However, we will focus on the ZigBee standard since ZigBee-Pro is today almost not used on WSN platforms. The ZigBee standard for short-range wireless networking is targeted mainly for battery-powered applications where low costs and low power consumption are the main requirements. Technically, the ZigBee standard is based on IEEE 802.15.4 PHY/MAC standard. The ZigBee Alliance is only promoting technology, like stack protocol development, interoperability guarantee and application profile, and certification for home automation, industry automation, automatic metering infrastructure, telecommunication value-added services, personal health care, etc. The IEEE 802.15.4 MAC layer implements several features which are used by the ZigBee protocol in network and application layers. The security services are one of these features. The underlying IEEE 802.15.4 protocol defines the encryption algorithm to use when transmitted data should be ciphered. However, IEEE 802.15.4 does not specify the key management or what kind of authentication policies has to be applied. These issues are treated in the upper layers which are managed by protocols such as ZigBee. The ZigBee standard implements two extra security layers on top of the IEEE802.15.4 protocol, namely the network and the application security layer. Most IDS that will be examined in this section fall into the broad category of anomaly detection IDS. Bear in mind that systems of this type do not rely on a base of signatures of

known attacks for their detection and thus are destined to recognize novel malicious behavior. Also, it is a common ground that intrusion detection problems in general and anomaly detection IDS in particular have to cope with huge volume and high dimensional datasets, the need for real time detection, and with diverse and constantly changing behavior. This is where computation intelligence comes into play and converges with the

IDS realm. In a step known as training, a number of records that is already gathered from the sensing components of the system (in the form of network connection data or log file data) is fed to the analysis engine. After the training step the IDS goes online to protect the system in real time. A classification or clustering algorithm is applied in this component to categorize the behavior into normal or abnormal. So, in a sense, the intrusion detection problem is reduced to a classification or clustering problem. In this context researchers have always been seeking
easy-to implement methods that provide high quality results in a fast and efficient manner.

The unique characteristics of SI make it ideal for this purpose. More specifically, SI techniques aim at solving complex problems by the employment of multiple but simple agents without the need of any form of supervision to exist. Every agent collaborates with others toward finding the optimal solution. This happens via direct or indirect communications (interactions) while the agents constantly roam in the search space. In this respect, agents can be used for several hard tasks like finding classification rules for misuse detection, discover clusters for anomaly detection, keep track of intruder trails etc. Indeed, these self-organizing and distributed attributes are highly appreciable by offering the means to break down a difficult IDS problem into multiple simple ones assigned to agents. This potentially makes the IDS autonomous, highly adaptive, parallel, self-organizing and cost efficient. The system consists of four sensor nodes .First one is configured as co-ordinater,Second one is as a router third and fourth are the end devices as shown in the block diagram below.The co-ordinator will be connected to the CMU i.e. central monitoring unit and it will collect the data from another sensor nodes and will give that data to the CMU.The co-ordinator is also designed to send the data to other sensor nodes.The Second sensor node which is configured as a router transmits the data to the end devices and vice a versa. There are several components in IDS to construct multiple attacks and defend the network over the discovered attacks. The performance gains of the optimized defense protocols are highly dependent on the ability of the proposed protocol to construct high quality, reliable discovering the networks. We describe these components in details

II. EXPERIMENTAL DETAILS

METHODOLOGY:

The Particle Swarm Optimization (PSO) algorithm was proposed by Kennedy and Eberhart in 1995. It can be defined as an Evolutionary Computation (EC) technique that simulates the social behavior of the swarm in nature such as schools of fish or flocks of birds where they find food together in a specific area. In other words, PSO is an iterative algorithm that searches the space to determine the optimal solution for an objective function (fitness function). The PSO algorithm evaluates itself based on the movement of each particle as well as the swarm collaboration. Each particle starts to move randomly based on its own best knowledge and the swarm's experience. It is also attracted toward the location of the current global best position Xgbest and its own best position Xpbest. The basic rules of the PSO algorithm can be explained in three main stages:

1) Evaluating the fitness value of each particle.
2) Updating local and global best fitness and positions.
3) Updating the velocity and the position of each particle.

Mathematically, the search process can be expressed by simple equations using the position vector Xi = [xi1;xi2; :::; xin] and the velocity vector Vi = [vi1; vi2; :::; vin] in the specific dimensional search space. In addition, the optimality of the solution in the PSO algorithm depends on each particle position and velocity update using the following equations

$$V_i^{k+1} = w.V_i^k + c_1.r_1[X_{pbest}^k - X_i^k] + c_2.r_2[X_{gbest}^k - X_i^k]$$

$$X_i^{k+1} = X_i^k + V_i^{k+1}$$

where i is the index of the particle; V ki , Xki are the velocity and position of particle i at iteration k, respectively; w is the inertia constant and is often in the range [0 1]; c1 and c2 are coefficients which are usually between [0 2]; r1 and r2 are random values which are generated for each velocity update; Xgbest and Xpbest are the global best position that is achieved so far, based on the swarm's experience, and local best position of each particle that is achieved so far, based on its own best position, respectively. A confined search space is the main limitation of the PSO algorithm. Limited search space provides a fast solution, but it influences the optimality of the solution if the global optimum value is located outside the boundaries. However, extended boundaries allow finding global optimum results, but need more time to determine the global optimal value in the search space. Therefore, more information about the limits of the parameters will help to determine the search boundaries. Fig. below shows the flowchart of the applied PSO algorithm.

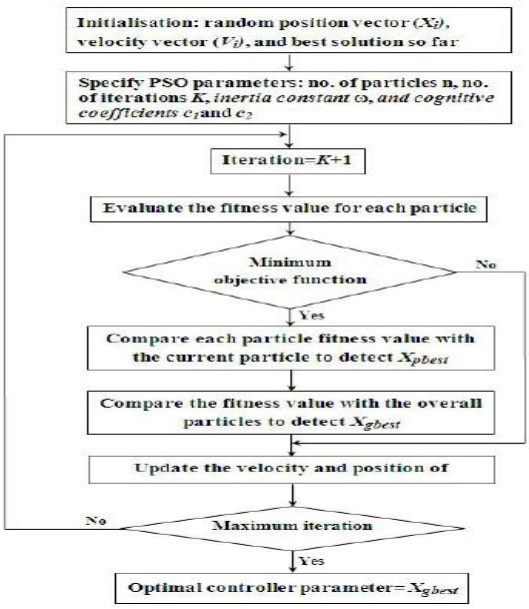


Fig No.1 Flowchart for PSO

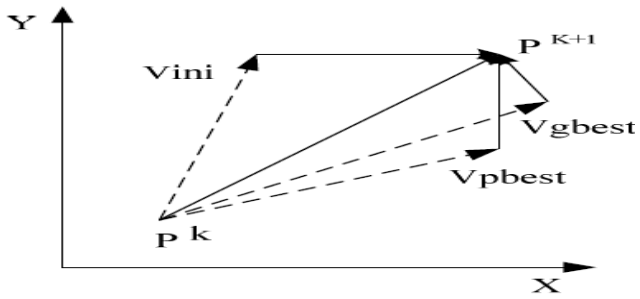
III.OBJECTIVE FUNCTION

The objective function is a particular criterion that is used to evaluate the particle's positions. In this work, the

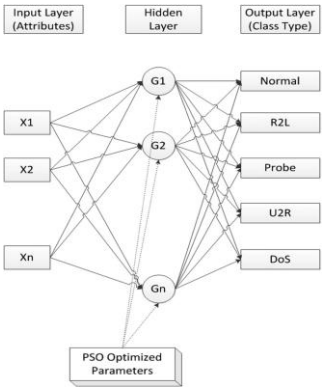
controller's fitness function is based on ITAE which is calculated using The mathematical expression of the ITAE performance index is defined by the following expression :

$$ITAE = \int_0^{\infty} t|e(t)|dt$$

where t is the time and e(t) is the difference between the reference set point and the controlled signal.



In PSO each particle adjusts its flight according to its own and its companion's flying experience. The best position in the course of flight of each particle(s) is called Xpbest, and the solution associated with it is denoted by Jpbest. Initially Jgbest (global best) is set to Jpbest and the particle(s) associated with it is denoted by Xgbest. Later on as the particle(s) is updated, Jgbest represents the best solution attained by the whole population and Xgbest denotes the corresponding best position. Every particle(s) updates itself through the above mentioned best positions. The basic concept of PSO technique lies in accelerating each particle towards its pbest and the gbest locations at each time step. Acceleration has random weights for both pbest and gbest locations. Fig. above illustrates briefly the concept of PSO, where Pk is current position, Pk+1 is modified position, Vini is initial velocity, Vmod is modified velocity, Vpbest is velocity
considering pbest and Vgbest is velocity considering gbest. In general, the termination criteria of a PSO algorithm can be either when the algorithm completes the maximum number of iterations or achieves an acceptable fitness value. In this work, the minimization of the objective function is considered with the maximum number of iterations to find optimum IDS control parameters. The acquired results can dynamically help the IDS reconfigure on-the-fly in order to be more effective.



IV. EXPERIMENTAL TEST

In this paper, the optimization strategy that we designed on the sensor platform consists of two parts: node-level attacks and network-level attacks. The node-level attacks are achieved by adaptive transmission power setting and by the periodic sleep/wake-up scheme. The network-level attacks are achieved by adaptive network configuration. In the experimental test, we first investigate the performance of node-level attacks. Then, the performance of network level attacks is investigated by comparing the energy consumption of fixed network configuration with that of adaptive network configuration.

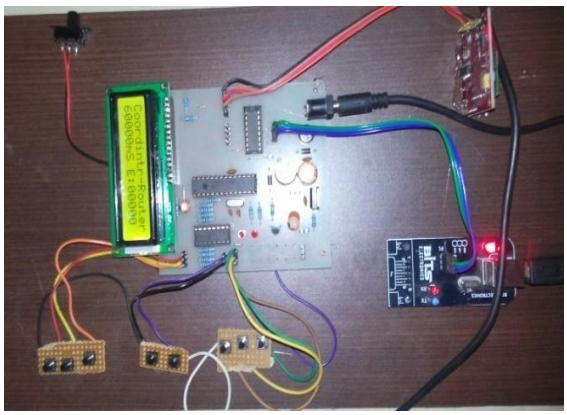
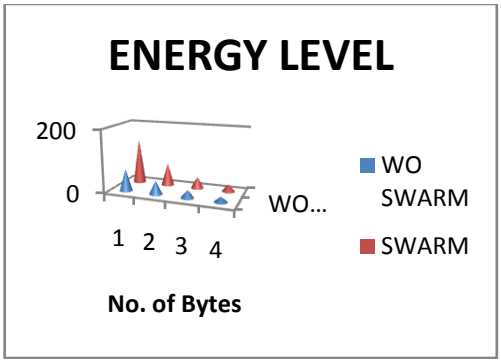


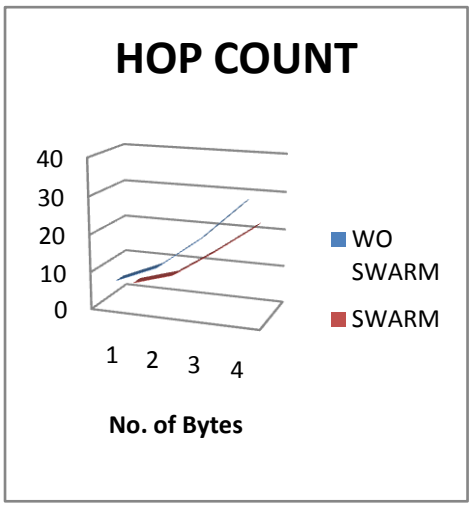
Fig No. 2:Experimental Set-up

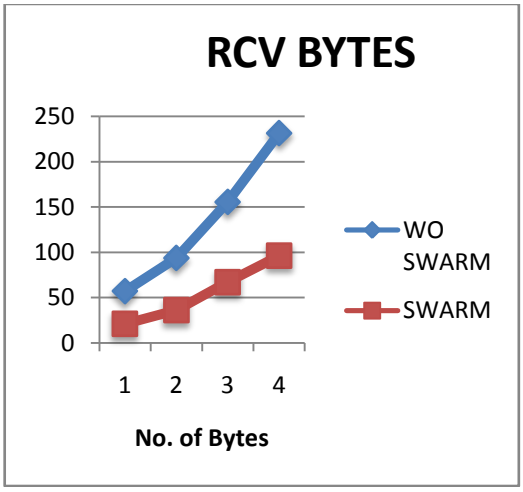
V. RESULT ANAYLAYSIS

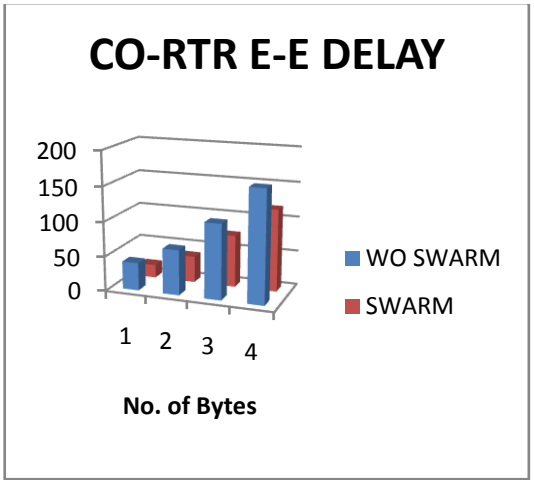
As described above we have recorded the values for different data length in order to verify the system efficiency as accord with increase in data length. It shows that with the increase in data length system is going to be more efficient with optimization which further improvises the degree of % of defended attacks..

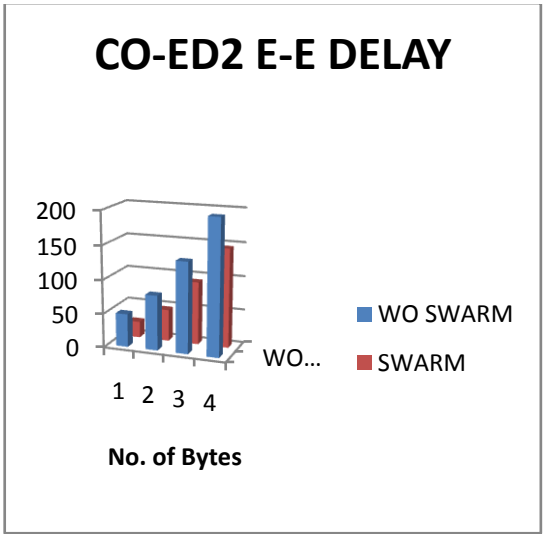


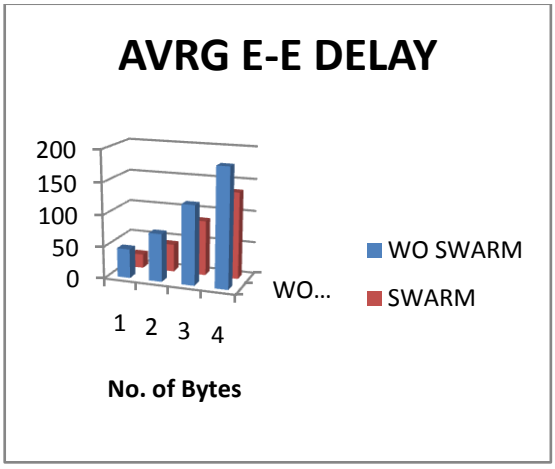
Graphs above shows that with the application of PSO to system there is highly increase in energy restoration in node & hence it increases the systems offensive nature to malicious network activities. Again it reduces the hop count also.

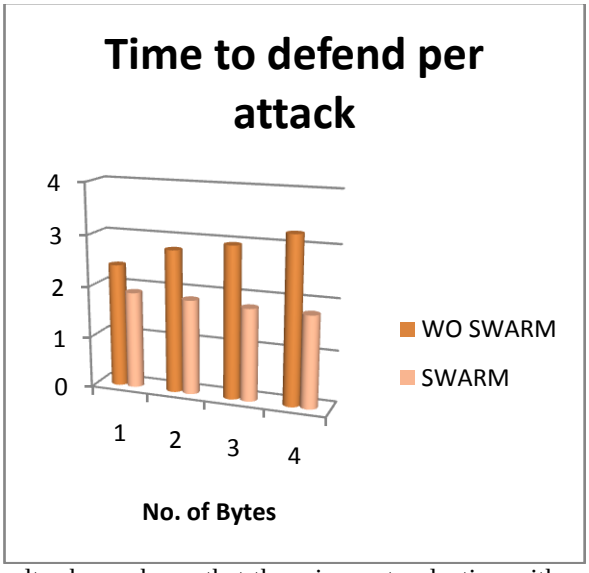












Results above shows that there is great reduction with swarm in average time to defend per attack.

As far time of communication is concerned, system will more prone to attack with more delays. As seen from in the simulations with Optimizations , the number of packets to travel in air reduces & hence there is direct reduction in time of communication & hence system will be more defendable to the malicious network activities.

VI. CONCLUSION

CONCLUSION AND FUTURE WORK Intrusion Detection is a process of detection Intrusion in a computer system in order to increase the security. Intrusion detection is an area in which more and more sensitive data are stored and processed in networked system. We Proposed a Hybrid PSO-SVM approach for building IDS. In SVM parameters C, ε and σ are selected by SPSO. Here we are using two feature reduction technique: Information Gain and BPSO. We analyze that there are several technique which provide good detection rate in case of Denial of Service (DoS) attack. But fail to achieve good detection rate in case of U2R and R2L attack. Many of the algorithm does not perform well in detecting the attacks like U2R and R2L. We perform series of experiment on KDD Cup 99 for acquiring more accuracy. We have used Confusion matrices for evaluation of our proposed technique and the result are obtained on the basis of evaluation metrics namely, Sensitivity, Specificity and Accuracy. As we saw we got the best result as compared to the previous algorithm and it is clear our technique perform well.

VII.REFERENCES

[1] FengGuorui, ZouXinguo , Wu Jian, "Intrusion Detection Based on the Semi Supervised Fuzzy C-Means clustering Algorithm", Department of information Science and Technology, ShandongUniversity,china , pp. 2667- 2670,2012

[2] Mr. Suresh kashyap ,Ms. Pooja Agrawal, Mr.Vikas Chandra Pandey, Mr. Suraj Prasad Keshri," Soft Computing Based Classification Technique Using KDD 99 Data Set for Intrusion Detection System" in International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering,Vol.2,Issue4,April2013.

[3] R.Durst, T.champion, B.witten, E.Miller, and L.Spagnuolo, "Testing and valuating computer intrusion detection system" communications of ACM, Vo1.42, no.7, pp 53-61, 1999

. [4] Erbacher R F, Walker K L, Frincke D A. Intrusion and Misuse Detection in Large-scale Systems. IEEE Computer Graphics andApplications, 2002, 2(1), pp.38-47.

[5] A.Sung & S.Mukkamala, "Identifying important features for intrusion detection using SVM and neural networks," in symposium on application and the Internet, pp 209-216, 2003.

[6] A.M Chandrasekhar, K.Raghuveer,"Intrusion detection technique by using K-means, Fuzzy Neural Network and SVM classifiers", proceedings of ICCCI, pp1-7, 2013.

[7] Jirapummin, C., Wattanapongsakorn, N., & Kanthamanon, P."Hybrid neural networks for intrusion detection system". Proceedings of ITCCSCC, pp 928-931, 2002.

[8]Horeis, T "Intrusion detection with neural network – Combination of self-organization maps and radial basis function networks for human expert integration", a Research report 2003.

[9] Han, S J & Cho, S. B. "Evolutionary neural networks for anomaly detection based on the behavior of a program", IEEE Transaction on System, Man and Cybernetics, pp 559-570, 2005.

[10] Chen, Y. H., Abraham, A., & Yang, B, "Hybrid flexible neural tree- based intrusion detection systems", International Journal of Intelligent Systems, pp. 337- 352,2007.

[11] S. Axelsson, "The base rate fallacy and its implications for the difficulty of Intrusion detection", Proc. Of 6th.ACM conference on computer and communication security 1999.

[12] R.Puttini, Z.marrakchi, and L. Me, "Bayesian classification model for Real time intrusion detection", Proc. of 22nd. International workshop on Bayesian inference and maximum entropy methods in science and engineering, 2002