Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Energy Efficient Layered Approach of Intrusion Detection System in Homogeneous and Heterogeneous WSN

N.Divya Bharathi,
M.Tech,
Dept. of Information Technology,
Institute of Aeronautical Engineering,
Dundigal, Hyderabad-43

Dr.N.Chandra Shekar Reddy
Proff & Head of the Dept.,
Computer Science & Engineering
Institute Of Aeronautical Engineering,
Dundigal, Hyderabad-43

N.Chaitanya Reddy
Assistant Professor,
Dept. of CSE,
Institute of Aeronautical Engineering,
Dundigal, Hyderabad-43

Abstract: Shielding data on the host systems or from the intruders on web is an extremely tedious task. The Intrusion Detection System is a technology for finding malicious behavior in a method or questionable activities from so-called intruders or the unauthorized customers. Alerts are produced during the intrusion task, but when more number of alarms is produced afterward managing of these alarms becomes not easy on IDS. In this paper, we propose a layered approach for IDS where the alarm information is represented dynamically in the shape of levels and we propose an alarm aggregation algorithm where an attack instance is developed for comparable kind of alerts generated and this is clustered to form a meta-alert which could reduce the quantity of alarms generated without losing any information. This technique has strategies like generative modeling, in this instance the beginning in addition to the end of strike properties and details can be discovered and it really is a data stream approach, where duplicate or the alarms which are discovered many number of times are processed only a few times. By implementing these techniques and alarm aggregation we can reduce quantity of alarms and the number of false alert rate. The project's aim will be to generate meta-alerts from the proposed alert aggregation algorithm and symbolize the intruder activity or all the alert advice on a dynamically symbolizing model. The alarm produced and the details of the alarm and the action taken are signified in the form of levels on a distinguishing layered model. The information on the alert are represented using further and these levels to make a meta-alert. Meta-alerts comprise all the useful information but the amount of data can be reduced progressively. Using the Info sets, it really is not impossible to reduce how many alarms produced while amount of missing meta-alarms is not incredibly high and signify all the information that is alert in the shape of layers on a design.

KEYWORDS: Wireless sensor networks (WSNs), Homogeneous WSNs, Heterogeneous WSNs, node density, Intrusion distance (ID).

I. INTRODUCTION

A WSN could be a extremely distributed network of wireless devices called sensing element nodes. Every sensing element node monitors some physical phenomenon's (e.g., humidity, temperature, pressure, light) within the realm of readying [1]. The monitored info is shipped to base station through wireless links. The communication vary of sensing element nodes is proscribed to tens of meters, thus knowledge square measure sent hop-by-hop from one sensing element node to a different till they reach the bottom station. WSNs square measure utilized in several applications wherever the sensors have physical interactions with the surroundings and square measure accessible by anyone build them additional liable to security threats. The constraints of WSNs in memory, energy and alternative resources build the utilization of existing security techniques impossible. Thus we want another psychoanalytic process "An Intrusion detection system" which will defend the network from attackers [2]. There square measure some possibilities of intrusion detection as, AN trespasser are often detected as presently because it enters within the network domain or once it covers a long way within the network domain. Detection likelihood is outlined because the likelihood that AN object is detected in bound observation period. Likelihood of intrusion detection heavily depends on the intrusion distance [5]. Intrusion distance denoted as D are often outlined because the distance between purpose wherever the trespasser enters the network and therefore the point wherever it gets detected by a sensing element. Some parameters that influence the probability of intrusion detection are:-

Node density: - It is defined as the total number of nodes present in the network.
Transmission range: - The maximum distance up to which a node can transmit is called transmission range.
Sensing range: - The distance up to which a sensor can detect the presence of intruder is called its sensing range. We consider these three parameters in our model. Depending on sensors capability there are two types of WSNs:-

Homogeneous WSNs

In homogeneous WSNs (Fig.1) all the sensors have same capabilities. They all have same battery energy, hardware complexity sensing range, and transmission range [3]. Homogeneous WSNs have simple network connectivity because of symmetrical wireless link.

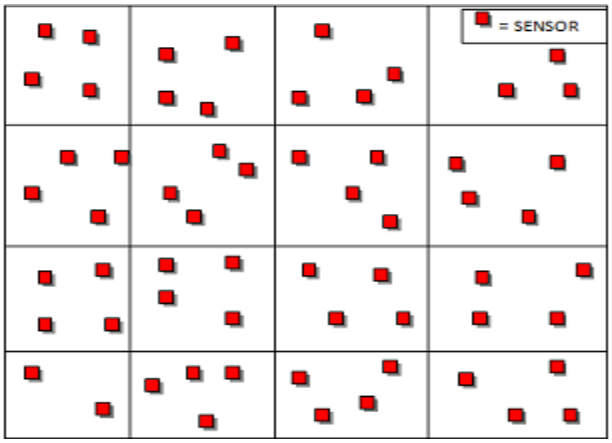

Fig 1 Homogeneous WSN

1.1 *Heterogeneous WSNs:* A heterogeneous WSNs (Fig. 2) consists different sensor nodes. In heterogeneous WSNs some sensors have larger capabilities than other sensors. In this network some sensors have larger sensing range, transmission range and have more battery power. Heterogeneous WSNs are most suitable for real life applications as compared to homogeneous. In heterogeneous WSNs a large no. of inexpensive nodes perform sensing, while a few nodes having comparatively more energy perform other tasks as data filtering, transport. Heterogeneous WSNs have comparatively difficult network connectivity because of asymmetrical wireless links. As packets from high capability nodes may reach the low capability nodes but low capability nodes may not be able to transmit information to high capability nodes. In real world the assumption of homogeneous sensors may not be practical because sensing application may require heterogeneous nodes in terms of sensing and communication capabilities in order to enhance network [4].

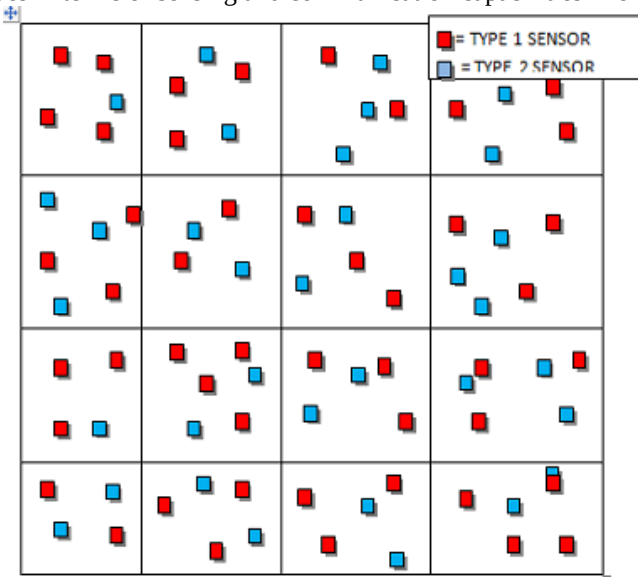

Fig 2 Heterogeneous WSN

we consider two sensing models:-

1.2 Single-sensing detection model: In single-sensing detection model an intruder is successfully detected by single sensor. But in some cases the information provided by singe sensor may not be correct as it can sense only a portion of the network domain. In that case we use multi-sensing detection model.

1.3 *Multi-sensing detection model:* In multi-sensing system an intruder is detected by multiple collaborating sensors. The no. of sensors depends upon specific applications. For example at least sensors are required to determine the location of intruder.

II. RELATED WORK

With relation to security, there are several tools I that are accustomed guarantee security in ID systems. The IDSs are vital tools since they will sight intrusions in networks. Several techniques that are results of analysis are bearing on network security generally. They are developed for the nodes that have heap of resources in situ. For this reason they can't be directly applied to WSN. That light-emitting diode to any analysis within the space of WSN for modifying techniques or inventing new ones those are best suited to WSN wherever nodes are energy unnatural. Among the researchers on WSN Zhang and Lee [1] are initial in researching on security problems with accidental networks. Their IDS that is distributed in nature works supported the detection techniques of applied mathematics anomaly. this system assumes a lot of traffic and therefore the time taken for detection of intrusion is high and therefore not economical. The price of this model can't be afforded by any WSN.

At times trespassers can be moving and detective work such intruder is additionally necessary in WSN. This has attracted analysis during this domain. Once nodes are in transit, the mechanisms and techniques are to be altered. The moving objects, their direction and chance of intrusion, detection etc. are to be thought-about. The intrusion detection during this setting conjointly must be considering energy economical approaches. Most of the analysis that has been drained this space focuses on detection of intrusions beneath assumptions and criteria. The detector coverage and sensing capabilities for detection of intrusions has impact are compact by quality in step with Liu et al. [9]. His work incontestable with the quality of detector will increase the coverage of network and provides quick detection of intrusions and targeted events. Sensing models are of 2 sorts. They're single sensing model and multi sensing model. Intrusion detection method in these 2 models is explored by Wang et al. [13].

In his work, the combination of detection probability and network Parameters such as transmission range, sensing range, and node density are considered for experiments under single sensing models. A security management model is proposed by [15] where intrusion detection in WSN assumes that the nodes in the network are self-organizing and the model is based on the layers in network. The cryptography used by WSN can only prevent external attacks while it can't do it with already compromised nodes.

III. LAYERED INTRUSION DETECTION SYSTEM ARCHITECTURE

The intrusion detection agent architecture consists of the following phases grouping Intrusion Detection Agents, Intrusion Detection and Alert Generation, Alert Format and Aggregation, Intrusion Prevention and Data Stream Alert Aggregation, Log File and Mobile Alert.

A. Intrusion Detection Agents: Intrusion Detection Agents acts because the agents for detection of suspicious actions from the entrant activity over the heterogeneous networks on a Distributed Intrusion Detection System. The agents area unit classified as User Level Agent, Packet Level Agent, and method Level Agent every playing the activities at completely different levels. The device layer acts because the layer to urge the small print of network systems similarly because the host systems wherever the agent resides. The devices within the sensor layer get all the small print i.e., data from each network system similarly because the host system. Info knowledge data contains probably valuable information that is required to perform any process activities. the knowledge embody the small print of the host system name and therefore the registered OS system, equally for the network systems wherever it check that network it's connected to, essentially it checks with TCP/IP connections, UDP connections and gets the small print of the network system connected with the Intrusion Detection System.

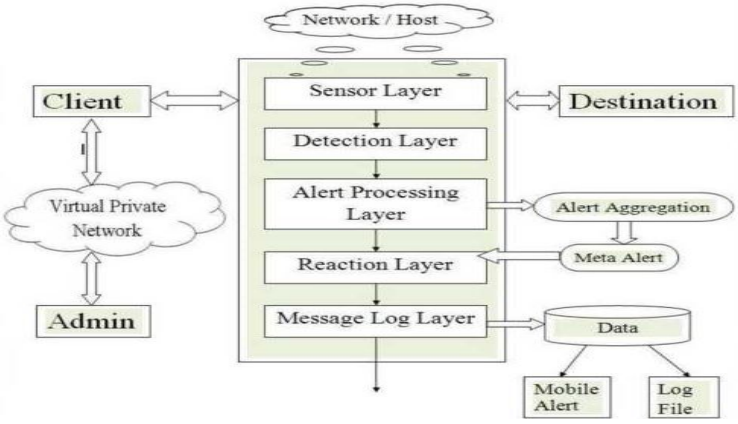

Figure 3: Layered Intrusion Detection System Architecture

Sensor Layer acts as the Sensors to get the details from host systems as well as the network systems. These raw data are sent for further processing to the detection layer. In the detection layer, the raw data are obtained as events. Detection layer acts as the protector from the intrusion activity by detecting what type of attack is going on using the detectors. These detectors using the data will search for any known suspicious behavior (anomaly detection), attack signatures (misuse detection) and other malicious activities. In the case of any suspicious activity or any intrusion activity, the detection layer produces alerts and forwards the details to the alert processing layers for further processing of these events. The alerts which are produced in the detection layer can be produced by installing FW in the detection layer. And the details are forwarded to alert processing layer for further processing. The Firewall software which is installed on a system is one of the systems which generate an alert during an intrusion activity.

B. Intrusion Detection and Alert Generation: The alert generated contains the information of the alert object aggregated and on their format. The attribute values are obtained from the data produced by the sensors which is used as the input for detectors and for alert aggregation. The details obtained from the sensors in the Sensor layer and the Detection layers are the attributes of the alert produced which are independent for each and every attack instance which are used for classification in Alert Processing layer. The Attack instances are distinguished between different attack types and the alerts produced based on the attributes obtained. These Attributes obtained are, might be dependent on the attack instance used in an alert aggregation process. To identify the attacker, the attributes which represent the information like source IP address and the destination IP address and the information destination port address which is 80 for the web based attacks are dependent on the alert information produced.

IV. HETEROGENEOUS WSN

A heterogeneous wireless sensor network (WSN) consists of several different types of sensor nodes (SNs). Various applications supporting different tasks, e.g., event detection, localization, and monitoring may run on these specialized sensor nodes. In addition, new applications have to be deployed as well as new configurations and bug fixes have to be applied during the lifetime. In a network with thousands of nodes, this is a very complex task .A heterogeneous node has more complex processor and memory so that they can perform sophisticated tasks compared to a normal node. A heterogeneous node possesses high bandwidth and long distant transceiver than a normal node proving reliable transmission.

4.1. Types of Heterogeneous resources: There are three common types of resource heterogeneity in sensor node:

*4.1.1. Computational Heterogeneity:*Computational heterogeneity means that the heterogeneous node has a more powerful microprocessor and more memory than the normal node. With the powerful computational resources, the heterogeneous nodes can provide complex data processing and longer term storage.

4.1.2. Link Heterogeneity: Link heterogeneity means that the heterogeneous node has high bandwidth and long-distance network transceiver than the normal node. It can provide more reliable data transmission.

4.1.3. Energy Heterogeneity: Energy heterogeneity means that the heterogeneous node is line powered, or its battery is replaceable.Among above three types of resource heterogeneity, the most important heterogeneity is the energy heterogeneity because both computational heterogeneity and link heterogeneity will consume more energy resource. If there is no energy heterogeneity, computational heterogeneity and link heterogeneity will bring negative impact to the whole sensor network, i.e., decreasing the network lifetime.

A heterogeneous node is line powered (its battery is replaceable).The heterogeneous WSN consists of different types of sensors with different sensing and transmission range. So while selecting the sensor nodes for intrusion detection, we need to consider these inequality of sensing and transmission range. For example, if two nodes have different transmission range it is better to select the one whose transmission range is higher. In this paper, we are considering N types of sensors. Here the sensing range and transmission range is high for Type 1 compared to Type2 and so on. The sensors are uniformly and independently deployed in a area A = LxL.

V. COMPARATIVE STUDY OF HETROGENEOUS WSN AND HOMOGENEOUS WSN

In consistent networks, all the device nodes are identical in terms of battery energy and hardware quality. Heterogeneous networks deliver the goods the previous and therefore the consistent networks deliver the goods the latter. In consistent network, single (uniform) platform is employed for per analysis cluster and every one node within the network share an equivalent practicality wherever as in heterogeneous network all the nodes treated otherwise. Within the universe, the idea of consistent sensors might not be sensible as a result of sensing applications might need heterogeneous sensors in terms of their sensing and communication capabilities so as to reinforce network dependableness and extend network time period. Also, although the sensors ar equipped with identical hardware, they'll not forever have an equivalent communication and sensing models. In fact, at the producing stage, there's no guarantee that 2 sensors exploitation an equivalent platform have precisely the same physical properties. This taxonomy focuses on heterogeneousness at the coming up with stage, once sensors are designed to possess non identical capabilities to satisfy the particular wants of sensing applications. In the heterogeneous wireless sensor network, the average energy consumption for forwarding a packet from the normal nodes to the sink in heterogeneous sensor networks will be much less than the energy consumed in homogeneous sensor network.

VI. SIMULATION AND RESULTS

In this section theoretical results are verified by using simulation tool. In this work ns2 is used for simulation and verification. The work is done on both homogeneous as well as heterogeneous WSNs.

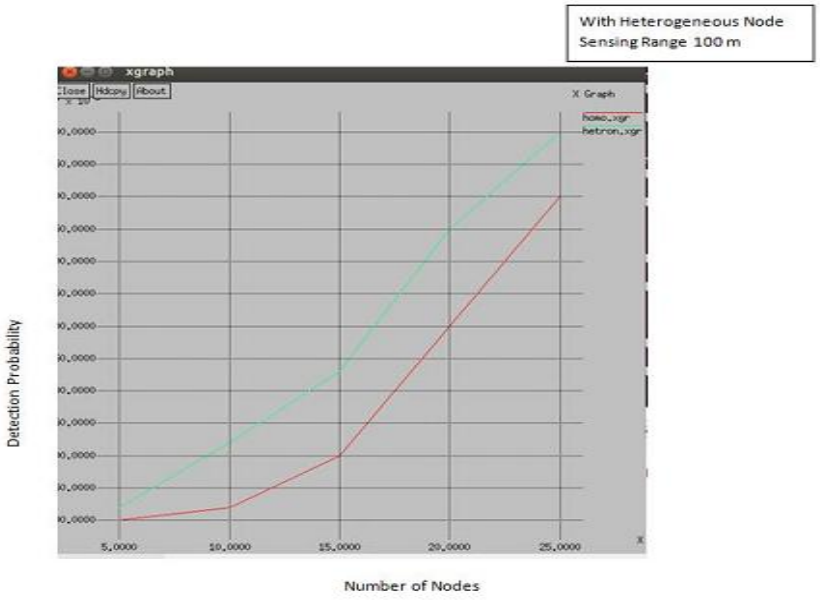

Fig 4 Graph between detection probability and no. of nodes with sensing range 100 m.

(Figure 4) shows the graph between detection probability and number of nodes for both homo and hetero network. In this graph the red line shows the detection probability for homogeneous WSN and green line is for heterogeneous WSNs. In this type1 heterogeneous nodes are considered with sensing range 100 m. As shown in figure as the no. of nodes is increasing from 5 to 25 detection probability is also increasing.

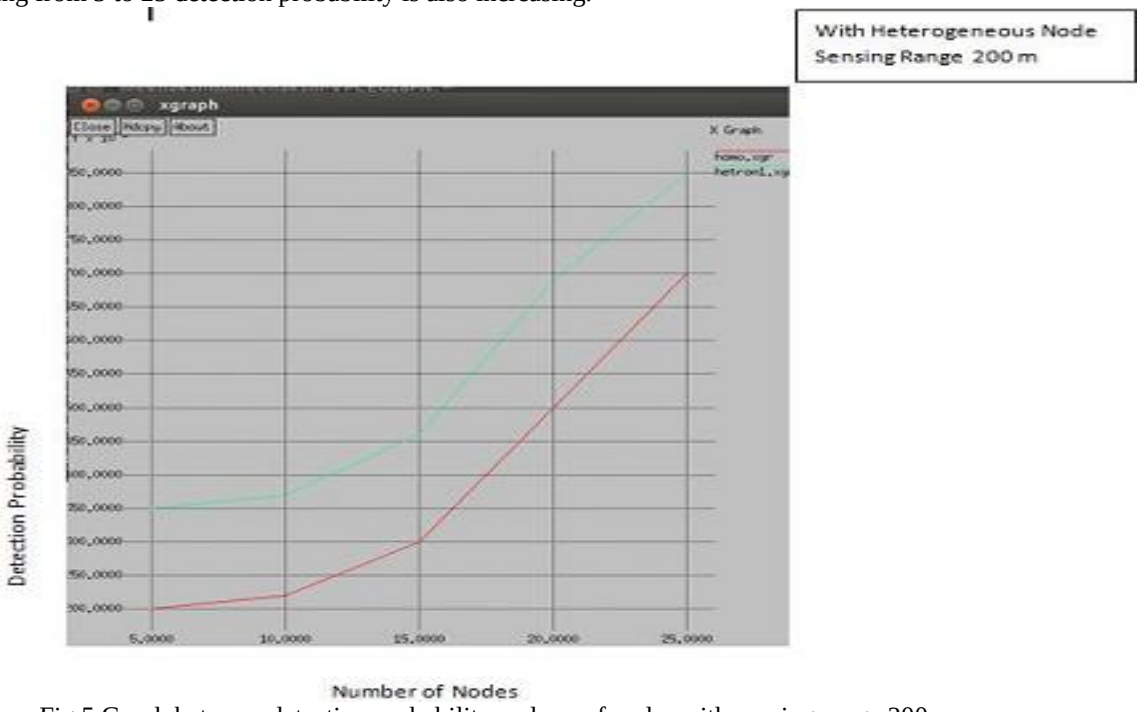

Fig 5 Graph between detection probability and no. of nodes with sensing range 200 m.

(Figure 5) shows the graph between detection probability and number of nodes for both homo and hetero network. In this graph the red line shows the detection probability for homogeneous WSN and green line is for heterogeneous WSNs. In this type2 heterogeneous nodes are considered with sensing range 200 m. As shown in figure as the no. of nodes is increasing from 5 to 25 detection probability is also increasing.

VII. CONCLUSION

The proposed method to cluster the alerts to make meta- alarms and the use DataStream approach and generative modeling demonstrated the quantity of alerts can be lowered without losing any advice that was important. The approach of the IDS developed, provided real time entry of the alarm generated and centered on the advice the actions is taken by the IDS on the intruders. The Projected algorithm speeds up in producing the clump of alerts i.e., meta-alerts which enhances the performance of the system without dropping any resource. The Projected IDS is regarded as scenario conscious and more foolproof. The bogus alarms which are produced can be considerably reduced by utilizing Data Stream Modeling where acquiring the experimental outcomes proves this. The testing conducted on three different data sets demonstrated that intruder advice can be obtained without losing any info where even firewalls may be used as manufacturers that were alert. Without losing any advice that was important in all of the cases, the quantity of data could be reduced significantly. The representation of alert information in the form of layers supplied a real time method of act on the alarms which are created during an intrusion task. The intruder details can be farther stored onto log file and can implement data mining to filter the information. An email which features the intruder advice on the mobile can be received by admin. The privilege is given to the client if he is regarded as the authentic and genuine time user.

REFERENCES

[1] Stetsko, A., L. Folkman and V. Matyas, 2010. "Neighbour-based intrusion detection for wireless sensor networks". Proceedings of the 6th International Conference on Wireless and Mobile Communications (ICWMC), Sept. 20-25, IEEE Xplore Press, Valencia, pp: 420-425.DOI:10.1109/ICWMC.2010.61.

[2] Krontiris, I., T. Dimitriou and F.C. Freiling, 2007. "Towards intrusion detection in wireless sensor networks". Proceeding of the 13 th European Wireless Conference, (EW' 07), CiteSeer.

[3] Jasvinder Singh, Er. Vivek Thapar, Er.Amit Kamra"Deployment Strategy of Homogeneous and Heterogeneous Wireless Sensor Network"Proceeding of International Journal of Computer Science and Communication Engineering Volume 1 Issue 2 (December 2012 Issue).

[4] Tapalina Bhattasali,Rituparna Chaki,2011. "Lightweight Hierarchical Model for HWSNET" Proceeding of the International Journal Of Advanced Smart Sensor Network Systems (Ijassn), Vol 1, No.2, October 2011.

[5] K.Suresh, A.Sarala Devi , Jammi Ashok "A Novel Approach Based Wireless Intrusion Detection System" Proceeding of the International Journal of Computer Science and Information Technologies, Vol. 3 (4) , 2012,4666 - 4669.

[6] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in Proceedings of ACM MobiCom, 2000, pp. 275-283.

[7] B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley, "Mobility improves coverage of sensor networks," in Proceedings of The Sixth ACM International Symposium on Mobile Ad Hoc Networking and Computing fMobiHoc^), 2005.

[8] Y. Wang, X. Wang, B. Xie, D. Wang, and D. P. Agrawal, "Intrusion detection in homogeneous and heterogeneous wireless sensor networks," in Proceedings of IEEE Transactions on Mobile Computing, vol. 7, no. 6, pp. 698-711, 2008.

[9] Xi Peng, Wuhan Zheng Wu, Debao Xiao, Yang Yu," Study on Security Management Architecture for Sensor Network Based on Intrusion Detection '" IEEE, Volume: 2,25-26 April 2009.

[10] Byunggil Lee, Seungjo Bae and Dong Won Han, "Design of network management platform and security frame work for WSN", IEEE International conference on signal image technology and internet based system, 2008.

[11] Qi Wang, Shu Wang, "Applying an Intrusion detection algorithm to wireless sensor networks", Second international workshop on Knowledge Discovery and Data Mining, 2009.

[12] K. Shaila, M. Sajitha, V. Tejaswi, S. H. Manjula, K. R. Venugopal, and L. M. Patnaik, "Secure and Energy Efficient Approach for Detection of an Intruder in Homogeneous Wireless Sensor Networks" , International Journal of Computer Theory and Engineering, Vol. 4, No. 6, December 2012.

