ISSN: 2277-9655
Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

DETECTION OF MALICIOUS NODE IN WIRELESS SENSOR NETWORK

Bhushan A. Khaire*, Prof. Pragati Patil
* WCC DEPT. A.G.P.C.O.E, NAGPUR
WCC DEPT. A.G.P.C.O.E, NAGPUR

DOI: 10.5281/zenodo.51460

ABSTRACT

The intrusion detection in Wireless Sensor Network (WSN) is of practical interest in many applications such as detecting an intruder in a field. The intrusion detection is defined as a system for a WSN to detect the existence of inappropriate, wrong or anomalous moving attackers. In this paper, I consider this issue according to heterogeneous WSN models. Furthermore, I consider two sensing detection models: single-sensing detection and multiple-sensing detection... our results show the advantage of multiple sensor heterogeneous WSNs. In this system we assume an using single as well as multiple wireless sensor network.

KEYWORDS: Homogeneous Network, Intrusion Detection, Node Density, Node Heterogeneity ,Range Sensing , Wireless Sensor Network.

INTRODUCTION

A wireless Sensor Network is a collection of particularly arrange wireless sensors to monitor various changes of environmental conditions by using these sensors. A sensor hardware and network architecture have been made by number of research effort in order to effectively deploy WSNs for a variety of applications. Because of a wide range of diversity of WSN application requirements, however, a general-purpose WSN design cannot fulfill the requirement of all applications. By taking reference of certain application few network such as sensing range , transmission range and node density have to be taken in account at network design stage. To achieve this, it is difficult to capture the impacts of network parameters on network performance with respect to application specifications.

The application of intrusion detection depend on fastness of the wireless sensor network to detect intruder. If the quantity of sensor applied with very large quantity hence it can cover very large area, once it approaches the network area it can detect the intruder in short time. However, such a large quantity deployment policy increases the network investment and may be even very costly for a large area. In true sense, it is not mandatory to apply so many sensors to take the entire WSN area in many applications , therefore a network with small and spread areas will also be able to detect a moving object

What is wireless sensor network?

Wireless sensor network is also called as wireless sensor and actuator network . it consist of nodes a few to several hundred all are connected to each other

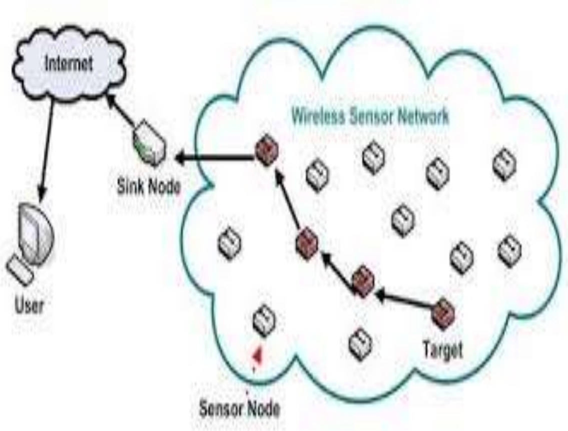


Figure1. wireless sensor network

What Characteristics and Benefits?

Area monitoring

It is use to monitoring small and large area by using various topologies. It is used in military areas to detect enemy intrusion.

Air pollution monitoring

It is use in monitoring air pollution by deploying wireless sensor network in several cities.

Forest fire detection

wireless sensor network is use in detection of fire in forest by installing sensor node in forest to measure temperature rise and fire can be detected.

Natural disaster monitoring

It also use in monitoring disaster by deploying several nodes in particular area.

Industrial monitoring

It is use to monitoring machine health as well as data logging it is also use in water waste monitoring by checking quantity of underground surface water.

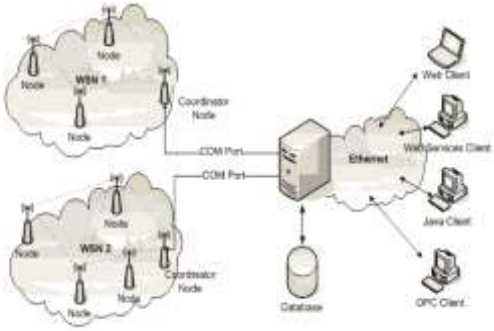


Figure: Overview of wireless sensor network

LITERATURE SURVEY

Yun Wang [1] , In wireless sensor networks (WSNs) intrusion detection is one of the main application. Few applications require different detection abilities at different areas in the deployment field. Gaussian distributed WSNs can fulfil such requirements and are widely deployed in practical., Plus the presence of some high capability sensors leads to performance increase the improvement in value in term of intrusion detection probability. This helps to make it explore the detection of intrusion problem in heterogeneous wireless sensor network. Theoretically and experimentally this work is to confirm the intrusion detection problem in a heterogeneous Gaussian distributed WSN. A heterogeneous WSN system model with different types of Gaussian distributed sensors is proposed, where both single-sensing detection and k-sensing detection models are employed. relied on this network model, the intrusion detection possibilities under various application programme are theoretically derived and experimentally validated by extensive simulations. The given work is to provide guidelines in designing heterogeneous WSNs for intrusion detection in given system.

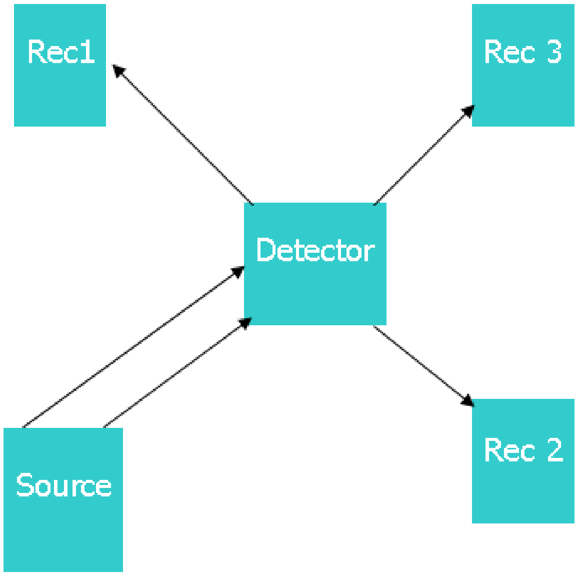


Figure: Overview of the Proposed Approach

Priyanka Deshpand [2], In is necessary in maintaining the higher throughput in the wireless sensor network that is the main requirement. Wireless senor networks are formed with a some powerful base stations and a large number of resource-constrained sensor nodes in the system. The wireless sensor network consists of 'n' number of sensors or nodes, where each and every node is connected to one or few other nodes. To provide low data rate for short coverage and long battery life, zigbee is used in wireless sensors network and ultimately zigbee nodes are used in wireless sensor network which are called as zigbee sensor nodes. On two aspects that is protocol stack and zigbee protocol wireless sensor nodes of zigbee system are basically built. In wireless sensor network sensors usually face many problems is that when data packets are transferred from one node to another node, the throughput of the wireless sensor network decreases due to packet collisions and large network traffic in wireless sensor network. To overcome this problem, various methods have been discussed to improve and maintain the throughput of wsn .

A.F.M Sultanul Kabir [3] ,Various issues and threats are considered in wireless sensor network these can be resolve by other research but security mechanism for wireless ad-hoc network can not be applied for wireless sensor network because of their architectural inequality where as all node are independent and controlled by base station in wireless sensor network, the propose of wireless sensor network is very specific such as measuring physical information like sound temperature etc. density in sensor network is higher than ad hoc network

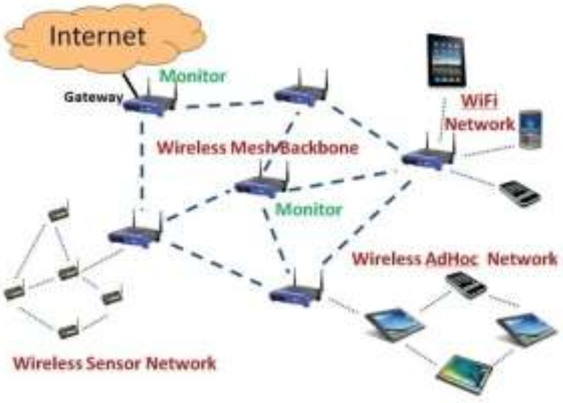
Single And Multiple Sensing detection

In the Gentry's fully homomorphic scheme, in this technique, the encryption and decryption is depends on super key and public key. As compare to different techniques. It contain the faster encryption and decryption at transmitting and receiving. It provides the secure authentication. By taking account of Heterogeneous wireless sensors, In the network Intruder detected anywhere in the programmed. We are detecting the malicious node in multiple sensor networks. Intrusion detection in heterogeneous WSNs by characterizing intrusion detection with respect to the various network characteristics

Two detection models are:

- Single-sensing detection model
- Multiple-sensing detection models

We are detecting the intruder both single sensor and multiple sensor heterogeneous wireless sensor network.



CONCLUSION

In this paper we review the We intrusion detection problem in both homogeneous and heterogeneous WSNs by characterizing intrusion detection probability with respect to the intrusion Two detection models are considered: single-sensing detection and multiple-sensing detection models. The analytical model for intrusion detection allows us to analytically formulate intrusion detection probability within a particular intrusion distance under various application scenarios. Moreover, we consider the network connectivity and the broadcast reachability in a heterogeneous WSN. Our simulation results verify the correctness of the proposed analytical model. This work provides insights in designing homogeneous and heterogeneous WSNs and helps in selecting critical network parameters so as to meet the application requirements.

REFERENCES

[1] Yun Wang, Xiaodong Wang, Bin Xie . and, Dharma P. Agrawal " Intrusion Detection in Homogeneous and.Heterogeneous Wireless Sensor Networks" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 7, NO. 6, JUNE 2008

[2] Priyanka deshpande, s Malekar, "adaptation backoff exponent mechanism in zigbee sensor network for improving throughput" .international journal of innovative research in computer and communication engineering, *vol.3 issue 3 2015*

[3] A.F.M. Sultanul Kabir, Hierarchical Design Based On Intrusion Detection System For Wireless Ad Hoc Sensor Network.*international journal on network security and its application vol.2 no.3 2010*

[4] M. V. Dijk, and A. Juels, "On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing." *IACR Cryptology ePrint Archive 2010 (2010): 305*.

[5] Data from Data Mining Based Attacks." *In High Performance Computing, Networking,*

[6] J. Zhao, R. Govindan, and D. Estrin, "Computing aggregates for monitoring sensor networks," in *Proc. 2nd Int. Workshop Sensor Netw.Protocols Appl.*, 2003, pp. 139–158.

[7] L. Huang, J. Li, M. Guizani, ―Secure and Efficient

[8] Data Transmission for Cluster-based Wireless Sensor Networks,‖ IEEE Trans. Parallel and Distri. Syst., 2012.

[9] [Modares, Hero; Salleh, Rosli; Moravejosharieh, Amirhossein;, "Overview of Security Issues in Wireless Sensor Networks," Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on , vol., no., pp.308-311, 20-22 Sept. 2011.

[10] Xiaowang Guo; Jianyong Zhu; , "Research on security issues in Wireless Sensor Networks," Electronic and Mechanical Engineering and Information Technology
(EMEIT), 2011 International Conference on , vol.2, no.,pp.636639, 12-14 Aug. 2011.

[11] HongShan Qu; Wen Liu; , "A robust key predistribution scheme for wireless sensor networks,"Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on , vol., no., pp.634-637, 27-29 May 2011.

[12] Wang Hai-Chun; Huang Tao; , "Design of Security Gateway Based on Chaotic Encryption,"Internet Technology and Applications (iTAP), 2011 International Conference on ,vol., no., pp.1-4, 16-18 Aug.2011.

[13] Burgner, D.E.; Wahsheh, L.A.; , "Security of Wireless Sensor Networks," Information Technology: New Generations (ITNG), 2011 Eighth International Conference on , vol., no., pp.315-320, 11-13 April 2011.

[14] Modares, H., Salleh, R., & Moravejosharieh, A. (2011). Overview of security issues in wirelesssensor networks. Third International Conference on Computational Intelligence, Modelling Simulation, IEEE,management module in sooawsn. International Journal of Network Security & Its Applications(IJNSA), 2(No. 4),

[15] ang, Y., Ramamurthy, B., & Xue, Y. (2008). A key management protocol for wireless sensor
networks with multiple base stations. CSE Conference and Workshop Papers. Paper 111.,
Xue, Y., Lee, H. S., Yang, M., & Kumarawadu,, P. (2007). Performance evaluation of ns-2simulator for wireless sensor networks. 0840-7789/07 ©2007 IEEE,