Scientific Journal Impact Factor (SJIF) : 1.711

IJMTER

International Journal of Modern Trends in Engineering and Research

ISSN (ONLINE) : 2349 - 9745

ISSN (PRINT) : 2393 - 8161

INTRUSION DETECTION IN HETEROGENEOUS WIRELESS SENSOR NETWORKS

VINAY M S[1], SUMANTH P B[2], SUMUKH B S[3], SHASHANK DUTT C[4], C N CHINNASWAMY[5]
T H SRINIVAS[6]
[1]Dept. of ISE, The National Institute of Engineering, Mysore, India
[2] Dept. of ISE, The National Institute of Engineering, Mysore, India
[3] Dept. of ISE, The National Institute of Engineering, Mysore, India
[4] Dept. of ISE, The National Institute of Engineering, Mysore, India
[5] Associate Prof., Dept. of ISE, The National Institute of Engineering, Mysore, India
[6] Prof., Dept. of CSE, The National Institute of Engineering, Mysore, India

Abstract: This paper presents a mechanism for a Wireless Sensor Network (WSN) to detect the existence of inappropriate, incorrect or unsuspicious moving attackers. In the recent growth of wireless sensor networks deal with different functional areas, to carry out different functionalities known as catastrophe revitalization, deep search, intrusion detection and number of other functionalities in neat digital world. Efficiency of a wireless network mainly depends on energy of nodes. In many these implemented applications used for detecting intrusion in smart offices and recent network resources. Researchers have proposed various intrusion detection systems for wireless sensor networks during the last few years. In this paper, we present a survey of these mechanisms.

Keywords: Wireless Sensor Networks (WSNs), Intrusion Detection System (IDS), Node Density, N ode Heterogeneity, Sensing Range, NS-2.

I INTRODUCTION

A wireless Sensor Network (WSN) consists of spatially distributed autonomous devices called sensors, and a base station (BS) to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. Sensor nodes can be networked to gather sensory data and each sensor performs two main responsibilities, namely, (i) sensing activities, and (ii) routing the sensed data to the base station or a controller.

Wireless sensor networks are attracting great interest in a number of application do-mains concerned with monitoring and control of physical phenomena, as they enable dense and effective deployments at low cost. However, application development is still one of the main hurdles to a wide adoption of WSN technology. In current real-world WSN deployments, programming is typically carried out very close to the operating system, therefore requiring the programmer to focus on low-level system issues. This not only distracts the programmer from the application logic, but also requires a technical background rarely found among application domain experts.

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.

There are three common types of resource heterogeneity in sensor node:

i. 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.

ii. 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.

iii. 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 an area A = LxL.

The rest of the paper is organized as follows: Section II gives an insight of IDS. Section III states the problem. Section IV gives an overview on the proposed protocol. Section V gives the simulation results and analysis. Finally section VI VII gives concluding remarks and future works.

II INTRUSION DETECTION

Intrusion detection system (IDS) is a security mechanism used to detect the abnormal behavior in the network. It is thought that intrusion detection systems are “not fit" for securing WSNs. This is true to some extent because IDS approaches are usually computationally expensive. But if we consider a WSN that works for tracking the movement of the enemy, this network can provide very useful information for making a strategy to beat the enemy in that area. Moreover, there is a rapid change in technology and keeping in mind the future perspectives; the capabilities of a sensor node will increase in near future. Sensor nodes will have more memory and survival time i.e. they might be used for transmitting multimedia information as well as for underwater applications. Due to the recent advancement in sensor technology, these networks will become visible and would be used by us in our daily life. Hence, there is a requirement of a secure WSN that ensures secure transmission and reliable delivery of packets in the network. IDS based mechanisms can be very effective to detect abnormal behavior of sensor nodes whether they cause DoS attacks, act as Sybil nodes or perform any other malicious activity.

In IDS, the unit that analyzes the network and detects abnormal behavior of node(s) is called an IDS agent. IDS agent collects network data for some time 't', applies detection policy to detect abnormal activity and takes appropriate actions. Rajasegarar et al. [3] analyze several anomaly detection mechanisms in their work. Since 2005, researchers have proposed a number of IDS based security mechanisms that analyze the working of sensor node(s) and efficiently detect abnormal activities.

They mostly target routing protocol attacks to explain their proposed methodology. Their work differ from each other in two ways i.e., installation of IDS agent, and the detection policy. There are three possibilities of installing an IDS agent; purely centralized, purely distributed and hybrid. In the first approach, it is installed at sink or BS only while in the second approach, IDS agent is present in every sensor node.

III PROBLEM STATEMENT

The life span of wireless sensor network directly depends on the power. The power required to transfer a data from sensor is more compared to its internal processing. All sensors are performing the intrusion detection and passing this information to base station may cause unnecessary usage of power. It is better to activate only few sensors within a region of WSN at a time for intrusion detection. So in the case of intrusion detection, if we are able to save battery power of each sensor, then it is very easy to increase the WSN life span. In this paper, we are proposing a new technique of energy efficient Intrusion detection, which will maximize the network life time, and its probability analysis.

IV EXISTING SYSTEM

A detection based security scheme for sensor nodes have low computation and communication capacity. They have exact properties such as their stable neighborhood information that allows for detection of anomalies in networking and transceiver behaviors of the neighboring nodes has been presented. LEAP (Localized Encryption and Authentication Protocols), a key management protocol for sensor networks that is designed to support network system processing, at the same time violating the security impact of a node compromise to the immediate network neighborhood of the compromised node has been presented.

The sensors we are considering here are static sensors. The intruder is considered as a moving object. Each node has Omni antenna properties for sensing. The sink node knows each nodes location and its neighbour list. The algorithm is executed at the sink node and it sends packet to the selected nodes to activate its IDS module. Such a random deployment results in a 2D Poisson point distribution of sensors. A sensor can only sense the intruder within its sensing coverage area that is a disk with radius as centred at the sensor.

V IDS WITH LIVELINESS PROFICIENT

The LPNL algorithm is used for node selection trying to select the high capability nodes compared to other sensor nodes. High capability means that sensor node having large sensing range and transmission range. High sensing range implies the fast recognition of intruder in the high mobility network state of affairs. The proposed algorithm consider two types of nodes, in order to obtain the results of varying the parameters such as sensing radius, transmission radius, number of sensors nodes etc. This LPNL Algorithm is proved that to handle the entire intrusion detection problem without need for additional deployment of sensor nodes, select a certain set of sensor nodes that covers the complete area depends on type of node, its transmission range and sensing range.

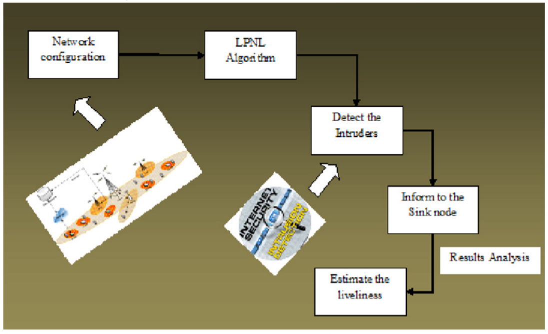

Fig. 1: System Architecture

Modules

- Network Configuration and deployment
- Liveliness Estimation
- Intrusion detection
- Performance evaluation

Network Configuration and deployment

The network model considers as wireless sensor network in a two-dimensional (2D) plane with 62 sensors. These sensors are uniformly and independently deployed in a square area$A$1 = (800*800). Such a random deployment of sensor nodes which results in a 2D Poisson point distribution of sensors. All sensors are static once the WSN has been deployed. Consider here two types WSN: homogeneous and heterogeneous. In a homogeneous WSN, each sensor has the same sensing radius of $r(s)$, and the transmission range of $rad(x)$. A sensor will sense the intruder within its sensing coverage area that is a disk with radius $r(s)$ centered at the sensor.

Liveliness Estimation

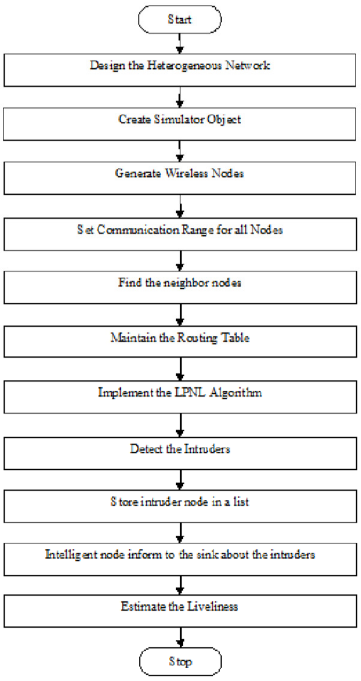
Start
Design the Heterogeneous Network
Create Simulator Object
Generate Wireless Nodes
Set Communication Range for all Nodes
Find the neighbor nodes
Maintain the Routing Table
Implement the LPNL Algorithm
Detect the Intruders
Store intruder node in a list
Intelligent node inform to the sink about the intruders
Estimate the Liveliness
Stop

Fig. 2: Flow Chart of Liveliness Estimation

The LPNL algorithm is used for node selection trying to select the high capability nodes compared to other sensor nodes. High capability means that sensor node having large sensing range and transmission range. High sensing range implies the fast recognition of intruder in the high mobility network state of affairs. This LPNL Algorithm is proved that to handle the entire intrusion detection problem without need for additional deployment of sensor nodes, select a certain set of sensor nodes that covers the complete area depends on type of node, its transmission range and sensing range.

Intrusion Detection

Intrusion Detection will detect the intruders in deployed wireless sensor networks and inform to the sink or intelligent sensor nodes dynamically as soon it is detected. There are two detection models, in terms of how many sensors are required to recognize an intruder: single sensing detection model and multiple-sensing detection model. In single-sensing detection model the intruder will be identified by using only one single sensor with their intelligent behavior. In the multiple-sensing detection model, the intruder will only be identified by using cooperative knowledge from at least m sensors (m is defined by specific application requirements).

V SIMULATION AND RESULTS

NS2 is used as a simulation platform. NS is a discrete event simulator, where the advance of time depends on the timing of events which are maintained by scheduler. NS simulator is based on two languages: C++, and an OTcl (an object oriented tool command language) interpreter used to execute users command scripts.

Table 1.Summery of the Parameters

Parameter	Value
Simulation Time	20 sec
Topology size	800 X 800 m^2
Number of nodes	62
Nodes distribution	Nodes are randomly distributed
BS position	Variable
Technique	Liveliness Estimation

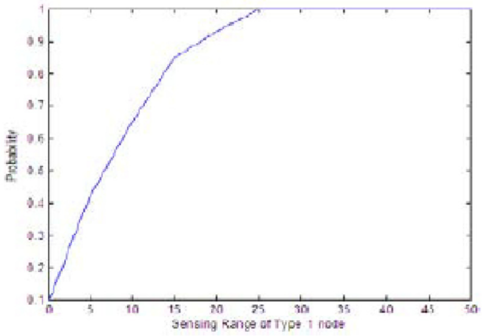

Fig. 3: Probability Analysis

VI CONCLUSION

In this work an attempt has been made to enhance the network lifetime. The process of clustering plays a very important role in utilizing the energy. So, we have attempted to change the criteria and process of clustering and cluster head rotation.

An improvement over LEACH has been proposed by incorporating energy parameter in the cluster head selection process. In this proposed protocol (TELA) the process of changing the cluster head is managed based on the energy criteria. The cluster heads will be reformed by the base station if any of the cluster heads energy goes below the preset threshold. The simulations were carried out in NS 2.34. It is observed from the simulation results that TELA achieve 32.15% better energy efficiency than LEACH protocol. The node may or may not join the old cluster again.

VII FUTURE WORK

In this work, only the procedure of changing cluster head or clusters in a network is observed.

But the energycriteria could be efficiently used in many other procedures like: (i) Network Initialization, (ii) Data Aggregation, etc. The procedure of changing the clusters/ cluster heads can also be made still efficient.

REFERENCES

[1]. Ullas. P, Brunda. J. S, Savitha. B. R, Manjunath. B. S (2012), *Energy Aware Threshold based Efficient Clustering for Wireless Sensor Networks, Bahubali College of Engineering,*

[2]. Lee, J.J., Krishnamachari, B., Kuo, C.C.J.: Impact of Heterogeneous Deployment on Lifetime Sensing Coverage in Sensor Networks (IEEE SECON). (2010).

[3]. A. P. da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," in Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks.

[4]. S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-scale Distributed Sensor Networks", Proc. Of the 10th ACM Conference on Computer and Communications Security (CCS '03), Oct. 2004.

[5]. J. Deng, R. Han, and S. Mishra, "A Performance Evaluation of Intrusion-tolerant Routing in Wireless Sensor Networks", Proc. Of the 2nd Int. IEEE Workshop on Information Processing in Sensor Networks (IPSN'03), Apr. 2003.

[6]. A. Savvides, C. Han, and M. Srivastava. Dynamic fine-grained localization in ad-hoc networks of sensors. In Proceedings of ACM MobiCom '01, pages 166-179, 2001.

[7]. *NS-2: Network Simulator (*Retrived on 02/02/2012 from (http://www.isi.edu/nsnam/ns/)

[8]. LEACH Patch for NS2 (Retrived on 08/03/2012 from *file://root/ns-allinone-2.34/notes/randomearly-detection-leach-in-ns-2-tcl.html#uds-searchresults*