isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6 Issue: 3 Apr,2017,ISSN_NO: 2321-3337

Energy and Memory Efficient Clone Detection in Wireless Sensor Networks

[1]Vladymir.F ,[2]J.Sivanesa Selvan,[3]Mr.Prabhu.D
[1]*(Information Technology, Loyola Institute of Technology, Chennai)*
(Email: vladymir_f@yahoo.in)
[2]*(Information Technology, Loyola Institute of Technology, Chennai)*
(Emial: sivanesh433.rock@gmail.com)
[3]*Asst.Professor(Information Technology, Loyola Institute of Technology,*
Chennai)

.

ABSTRACT - *Intrusion detection plays an important role in the area of security in WSN. Detection of any type of intruder is essential in case of WSN. WSN consumes a lot of energy to detect an intruder. Therefore we derive an algorithm for energy efficient external and internal intrusion detection. We also analyse the probability of detecting the intruder for heterogeneous WSN. This paper considers single sensing and multi sensing intruder detection models. It is found that our experimental results validate the theoretical results.*

Keywords : WSN, MANET SPINS,LEAPS

1.INTRODUCTION

WSN is common in different types of application scenarios. It includes a set of sensor nodes deployed over a geographical area to monitor a variety of phenomenons. However, challenges and difficulties still exist. The sensor nodes own limited power, processing and sensing ability. The sensor nodes are prone to failure because of lack of power, physical damage etc. Since the information generated by a single node is usually incomplete or inaccurate, and the applications need collaborative communication and computation among multiple sensors multiple sensing models can be used. A Heterogeneous WSN is more complex as compared to homogeneous WSN and which consists of a number of sensor nodes of different types deployed in a particular area and which are collectively working together to achieve a particular aim. The aim may be any of the physical or environmental condition. For e.g. the wireless sensor network is mainly used in military applications such as in borders for finding out the infiltrations. It is also used in industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation and traffic control. WSN become increasingly useful in variety critical applications, such as environmental monitoring, smart offices, battlefield surveil- lance and transportation traffic monitoring. The sensor nodes are tiny and limited in power. Sensor types vary according to the application of WSN. Whatever be the application, the resources such as power, memory and band width are limited. Moreover, most of the sensor nodes are throw away in nature. Therefore it is vital to consider energy efficiency so as to maximize the life time of the WSN. Great efforts have been devoted to minimizing the energy consumption and extending the lifetime of the network. One common way is to put some sensor nodes in sleep mode to save energy and wake them up under some strategies. Work towards maximizing the life time of WSN has been studied in many research works. Some of them lead to the need of heterogeneous WSN deployment. Lee et al. analyse heterogeneous deployments both mathematically and through simulations in different deployment environments and network operation models. Hu et al. investigate some fundamental questions for hybrid deployment of sensor network, and propose a cost model and integer linear programming problem formulation for minimizing energy usage and maximizing lifetime in a hybrid sensor network. Their studies show that network lifetime can be increased dramatically with the addition of extra micro-servers, and the locations of micro-servers can affect the lifetime of network significantly. Intrusion detection plays an important role in the area of computer security, in particular network security, so an attempt to apply the idea in WSNs makes a lot of sense. However, there are currently only a few studies in this area. Da Silva et al. and Onat and Miri propose similar IDS systems, where certain monitor nodes in the network are responsible for monitoring their neighbours, looking for intruders. They listen to messages in their radio range and store in a buffer specific message fields that might be useful to an IDS system running within a sensor node. For this purpose, a number of sensors, N, are deployed in an area of interest, A, to monitor the environmental changes by using optical, mechanical, acoustic, thermal, RF and magnetic sensing modalities . In this way, possible intruder approaching or travelling inside the deployment field can be detected by the WSN if it enters into the sensing range(s) of one or multiple sensor.

2, SYSTEM ANALYSIS

2.1 Existing System

In single-sensing detection, at a time only one intruder detected by the WSN.

Our Previous work was according to homogeneous and heterogeneous single sensor in wireless sensor network

. **Disadvantage:**

The sensed information provided by a single sensor might be inadequate for recognizing the intruder.

So that there is no guarantee for our information has been sent securely.

Data will not routed if primary

2.2 Proposed System

In Heterogeneous wireless sensor ,Intruder detected anywhere in the network.

We are detecting the intruder in multiple sensor heterogeneous wireless sensor networks.

Advantage:

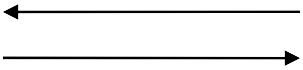
If primary detector fails another detector detect the intruder.

By finding the intruders we can send our information in a secured manner

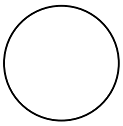
3. IMPLEMENTATION

3.1 A graphical tool used to describe and analyze the moment of data through a system manual or automated including the process, stores of data, and delays in the system. Data Flow Diagrams are the central tool and the basis from which other components are developed. The transformation of data from input to output, through processes, may be described logically and independently of the physical components associated with the system. The DFD is also know as a data flow graph or a bubble chart. DFDs are the model of the proposed system. They clearly should show the requirements on which the new system should be built. Later during design activity this is taken as the basis for drawing the system's structure charts. The Basic Notation used to create a DFD's are as follows:

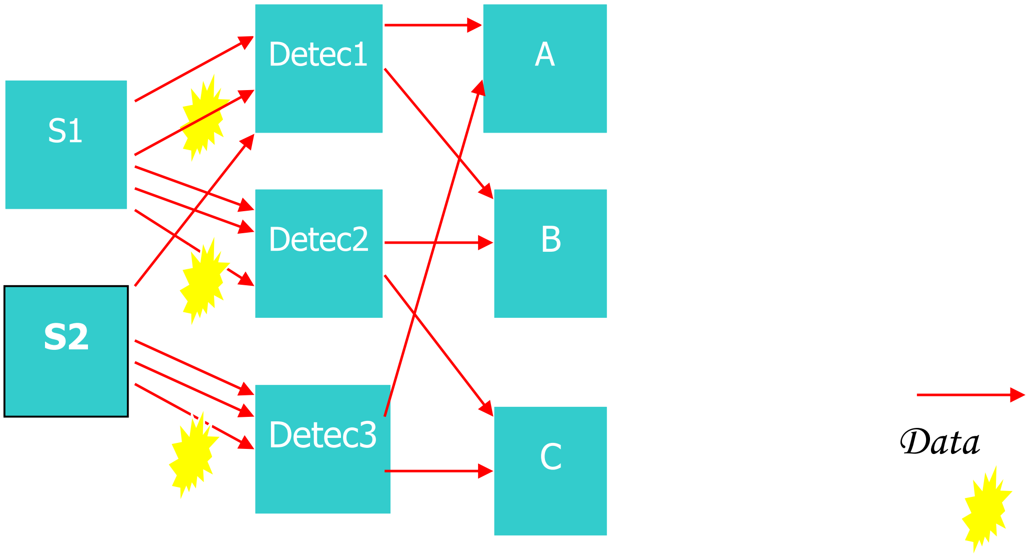
1. Dataflow: Data move in a specific direction from an origin to a destination.



2. Process: People, procedures, or devices that use or produce (Transform) Data. The physical component is not identified.



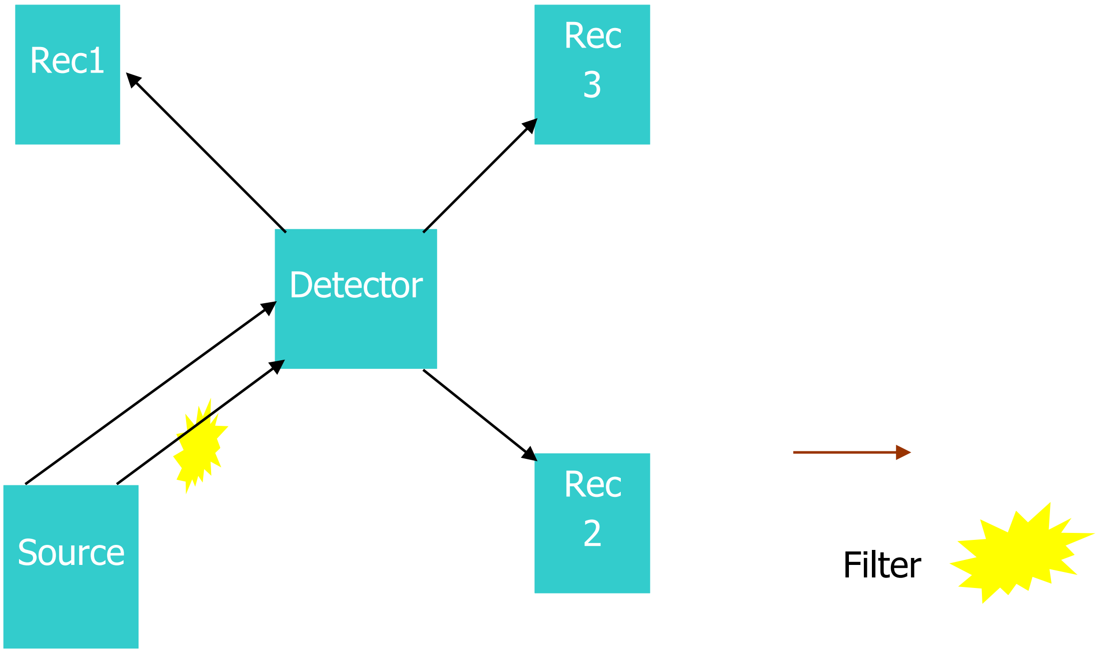
3. Source: External sources or destination of data, which may be People, programs, organizations or other entities.



- Sending packet from source S to D

- In tr u

Homogeneous



TESTING

TESTING OBJECTIVES

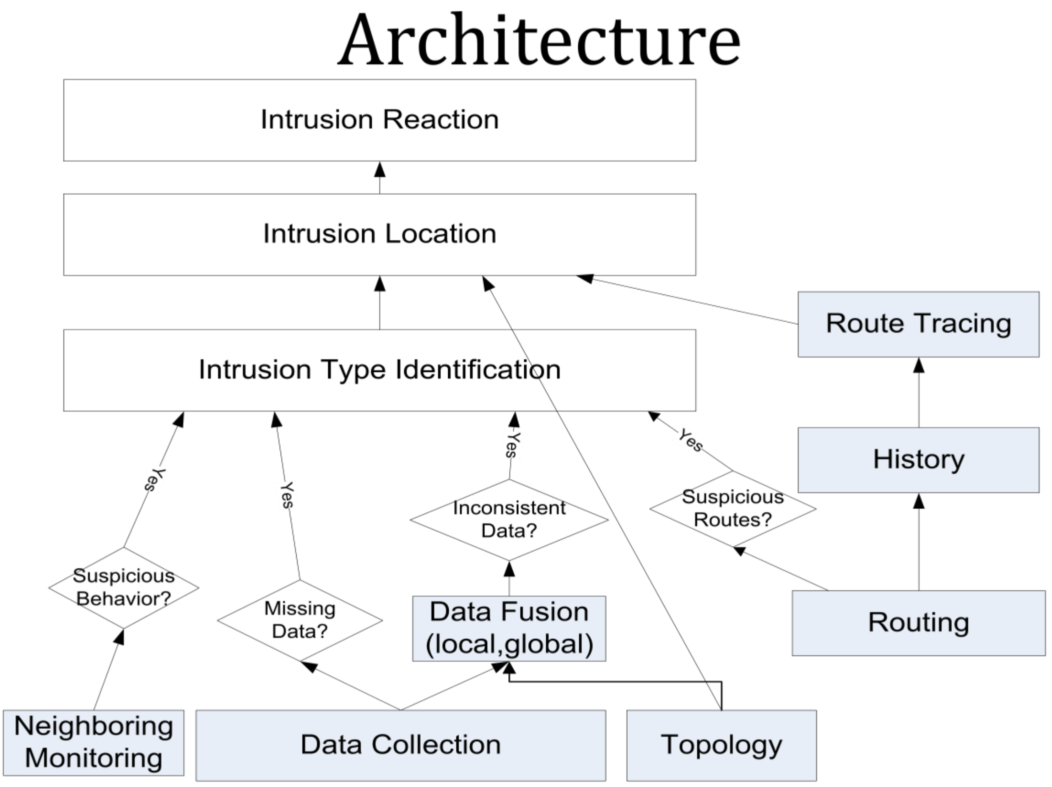
Performance Tests are utilized in order to determine the widely defined performance of the software system such as an execution time associated with various parts of the code, response time(in case of embedded systems),and device utilization. The intent of this type of testing is to identify weak points of a software system and quantifying its shortcomings, leading to further improvements.

Stress Tests are designed to break a software module. This type of testing determines the strengths and limitations of the software.

Structure Tests are aimed at exercising the internal logic of a software system.

Testing In Small-Testing In The Large. The underlying criterion concerns which part of the system is subject to testing. If we are concerned with individual modules, procedures, and functions, this lead to testing in the small. Testing in the large is primarily devoted to integration testing when the system is developed out of some already constructed modules.

Black Box-White(Glass)Box Testing. As the name suggests, the criterion leading to this type of discrimination specifies whether the internal(logical)structure of the system is available for testing purposes. if so,we are concerned with white box testing. If the internal structure is not available or exercised when developing the test suite, we confine ourselves to black box testing. Depending which way was selected, the points of view on testing are also radically different. In black box testing we are interested to test what the system is supposed to do. The testing is worked out from input data perspective; subsequently we see if the outputs (actions) of the software match the expected values. Functional, stress, and performance tests fall under this general category. In white box testing, testing concentrates on what the system does.essentially, using detailed knowledge of code, one creates a battery of tests in such a way that they exercise all components of the code (say, statements, branches, paths).structural testing sub schemes whiteboxtesting



2.CONCULSION AND FUTUREWORK:

This paper speaks about the minimization of external intrusion detection in an energy efficient way and probability of intrusion detection in a heterogeneous WSN deployed in a two dimensional space. This probability gives an insight in to the required number of sensors in a given deployment, their sensing and transmission range to efficiently detect an intruder in a given WSN. We have developed an analytical model for intrusion detection and applied the same into single-sensing detection and multiplesensing detection scenarios for heterogeneous WSNs. The correctness of the analytical model is proved by simulation.

REFERENCES

I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, “A Survey on Sensor Networks”, IEEECommunication Magazine, vol. 40, no. 8, pp. 102-14, Aug. 2002.

[2] Lee, J.J., Krishnamachari, B., Kuo, C.C.J.: Impact of Heterogeneous Deployment on Lifetime Sensing Coverage in Sensor Networks (IEEE SECON). (2004)

[3] Hu, W., Chou, C.T., Jha, S., and Bulusu, N.: Deploying Long- Lived and Cost-effective Hybrid Sensor Networks. Elsevier Ad- Hoc Networks, Vol. 4, Issue 6. (2006) 749-767.

[4] 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.*

[5] I. Onat and A. Miri, “An intrusion detection system for wireless sensor networks,” in *Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, vol. 3, Montreal, Canada, August 2005, pp. 253–259.

[6] A. Perrig, et al., “SPINS: Security Protocols for Sensor Networks”, *Wireless Networks*, 8(5):521- 534, Sep. 2002.

[7] 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. 2003.

[8] 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.

[9] Y. Wang, X. Wang, B. Xie, D. Wang, and D. P. Agrawal, “Intrusion detection in homogeneous and heterogeneous wireless sensor networks,” *IEEE Transactions on Mobile Computing*, vol. 7, no. 6, pp. 698–711, 2008.

[10] O. Dousse, C. Tavoularis, and P. Thiran, “Delay of intrusion detection in wireless sensor networks,” in *Proceedings of the Seventh ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2006.