ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Sensor Network Deployment and Critical Parameter Selection for Intrusion Detection System

Manjula.N[1], Sumathi.P[2]

PG Student, CSE, KSR Institute for Engineering and Technology, Tiruchengode, Tamilnadu, India[1]

AP, CSE, KSR Institute for Engineering and Technology, Tiruchengode, Tamilnadu, India[2]

ABSTRACT: Intrusion detection is applied to detect malicious or unexpected attackers in Wireless Sensor Network (WSN). The intruder can be an enemy in a battlefield, or a malicious moving object in the area of interest. Same detection probability is used in the uniform distribution model WSN. Gaussian-distributed WSNs can provide differentiated detection capabilities at different locations. Different degrees of probability are used in Gaussian distribution model WSN. Detection probability is estimated with respect to the application requirements and the network parameters. Single-sensing detection and multiple-sensing detection scenarios are the two types of sensing scenarios and used in intrusion detection system. Relaxed intrusion detection and immediate intrusion detection models are used in the single sensing scenarios. In the immediate intrusion detection model the intruders are detected before any movement in the WSN. In the relaxed intrusion detection model the intruders are detected after some movements in the WSN.

I. INTRODUCTION

1.1 AREA OF INTEREST

1.1.1 Wireless Sensor Networks

Microcontroller performs tasks, processes data and controls the functionality of other components in the sensor node. Other alternatives that can be used as a controller are: General purpose desktop microprocessor, Digital signal processors, Field Programmable Gate Array and Application-specific integrated circuit. Microcontrollers are most suitable choice for sensor node. Microcontrollers are the best choices for embedded systems. Because of their flexibility to connect to other devices, programmable, power consumption is less, as these devices can go to sleep state and part of controller can be active. In general purpose microprocessor the power consumption is more than the microcontroller. Therefore it is not a suitable choice for sensor node.

Digital Signal Processors are appropriate for broadband wireless communication. But in Wireless Sensor Networks, the wireless communication should be modest i.e., simpler, easier to process modulation and signal processing tasks of actual sensing of data is less complicated. Therefore the advantage of DSP's is not that much of importance to wireless sensor node.

1.1.2 Transceiver

Sensor nodes make use of ISM band which gives free radio, huge spectrum allocation and global availability. The various choices of wireless transmission media are Radio frequency, Optical communication and Infrared. Laser requires less energy, but needs line of sight for communication and also sensitive to atmospheric conditions. Infrared like laser, needs no antenna but is limited in its broadcasting capacity. Radio Frequency (RF) based communication is the most relevant that fits to most of the WSN applications. WSN's use the communication frequencies between about 433 MHz and

2.4 GHz. The functionality of both transmitter and receiver are combined into a single device know as transceivers are used in sensor nodes. Transceivers lack unique identifier. The operational states are Transmit, Receive, Idle and Sleep.

1.1.2.1 External Memory

The energy perspective is the most relevant kinds of memory are on-chip memory of a microcontroller and FLASH memory - off-chip RAM is rarely if ever used. Flash memories are used due to its cost and storage capacity. Memory requirements are very much application dependent. Two categories of memory based on the purpose of storage a) User memory used for storing application related or personal data. b) Program memory used for programming the device. The memory is also contains identification data of the device.

1.1.2.2 Power Source

Power consumption in the sensor node for the sensing, communication and data processing. More energy is required for data communication in sensor node. Energy expenditure is less for sensing and data processing. The energy cost of transmitting 1 Kb a distance of 100 m is approximately the same as that for the executing 3 million instructions by 100 million instructions per second/W processor. Power is stored either in batteries or capacitors. Batteries are the main source of power supply for sensor nodes. The two types of batteries are used chargeable and non-rechargeable. The process are also classified according to electrochemical material used for electrode such as NiCd(nickel-cadmium), NiZn(nickel-zinc), Nimh (nickel metal hydride), and Lithium-Ion. Current sensors are developed to re-new the energy from solar, thermo-generator, or vibration energy.

Two major power saving policies are used Dynamic Power Management (DPM) and Dynamic Voltage Scaling (DVS). DPM takes care of shutting down parts of sensor node which are not currently used or active. DVS scheme varies the power levels depending on the non-deterministic workload.

1.1.2.3 Sensors

Sensors are hardware devices are produce measurable response to a change in a physical condition like temperature and pressure. Sensors sense or measure physical data of the area to be monitored. The continual analog signal sensed by the sensors is digitized by an analog-to-digital converter and sent to controllers for further processing. Characteristics and requirements of Sensor node should be small size, consume extremely low energy, operate in high volumetric densities, autonomous and operate unattended, and adaptive to the environment. As wireless sensor nodes are micro-electronic sensor device, can only be equipped with a limited power source of less than 0.5 Ah and 1.2 V. Sensors are classified into three categories.

1.3 Application of WSN

Although the number of implementations of wireless sensors is great, there is no exact standard defining a “mote”. The term “mote” implies a small sized platform, but no absolute separation can be done. Irrespective of the exact type of platform, already known applications can be categorized under some general headings: military applications, environmental monitoring, commercial or human centric applications and applications to robotics.

II. EXISTING SYSTEM

Due to recent technological advances in wireless communication, manufacturing of small- and low-cost sensors has become economically feasible. A large number of sensors can be deployed in an ad hoc fashion to form a Wireless

Sensor Network (WSN) for many civil and military applications. Intrusion detection has received a great deal of attention since it supports various applications such as environmental monitoring and military surveillance.

WSNs with Gaussian distributed sensors can provide differentiated node densities at different location. Different from uniformly distributed WSNs in a Gaussian distributed WSN, the closer the area is to the central deployment point T, more sensors are deployed to provide enhanced detection capability.

2.1 Drawbacks of the Existing System

Intrusion detection is applied to detect malicious or unexpected attackers in Wireless Sensor Network (WSN). The intruder can be an enemy in a battlefield, or a malicious moving object in the area of interest. Same detection probability is used in the uniform distribution modeled WSN. Gaussian-distributed WSNs can provide differentiated detection capabilities at different locations. Different degrees of probability is used in Gaussian distribution modeled WSN.

The following drawbacks are identified in the existing system.

- Deployment scheme optimization is not provided.
- Detection parameter selection is not provided.
- Detection latency is high.
- Sensing and transmission capacity are not integrated.

III. PROPOSED SYSTEM

Proposed Application Specific Packet Traffic model for sensor networks to detect intrusion more effectively in WSN Traffic load generated heavily depends on application categorized as event-driven or periodic data generation. Event-driven scenarios such as target detection and tracking generate busty traffic unable to model as either CBR or Poisson.

Define set of parameters for the application before proceeding with traffic model development Constructing accurate and analytically tractable source models for sensor network traffic Performance evaluation of WSNs is performed with realistic traffic load. Effects of system parameters such as node density and target velocity are analyzed. Intrusion detection application predetermined surveillance area (e.g., a border) is represented in the form of a square grid Possible sensor node locations are defined to be the grid corners even if deployment is random Quality of grid modeling depends heavily consistence between two nearest grid cross-points.

3.1 ADVANTAGES

Fault tolerant detection scheme are performed from the different deployment schemes. Malicious attack controlling model can de improvised in the wireless sensor network. Traffic overhead is reduced because the achievement of the scheduling process. Intrusion detection is provided for different deployment scheme notification latency is low in the intrusion detection system. Energy consumption is low in the process. Data capture accuracy is improved.

IV. CONCLUSION

The entire system is planned for the process is allocated to carry out the study and analysis for the existing system. The domain knowledge is collected and analyzed in the introductory levels. A wide literature survey is conducted to analyze the techniques and concepts that proposed earlier. The literature survey is conducted in the area of pattern based sensor deployment, target detection schemes, coverage and connectivity based sensor deployment and mobile target detection. All the merits and demerits are analyzed. The existing system and its problems are extracted from the literature survey. The design of the proposed system is prepared to solve the problems in the existing system. Module level development procedures are also finalized.

REFERENCES

1. Akyildiz, I.F and Cayirci,.E andSankarasubram,Y(2002)'A Survey on Wireless Sensor Networks,' IEEE Comm. Magazine,vol. 40, no. 8, pp. 102-114.

2. Al-Karaki,J.N and A.E. Kamal, (2004) 'Routing Techniques in Wireless Sensor Networks: A Survey,' IEEE Wireless Comm., vol. 11, no. 6, pp. 6-28.

3. Agah, A. and Asadi,M and Basu, K.and Das, S(2004)'Intrusion Detection in Sensor Networks: A Non-Cooperative Game Approach,'Proc. Third IEEE Int'l Symp. Network Computing and Applications (NCA '04), pp. 343-346.

4. Agah, A. and Basu, K. and Das, S(2004)'A Game Theory Based Approach for Security in Wireless Sensor Networks,' Proc. IEEE Int'l Conf. Performance, Computing, and Comm., pp. 259-263.

5. Arora, A. and Bapat, S. and Dutta, P. and Kulathumani, V. and Zhang, H.,(2007). 'A Line in the Sand: A Wireless Sensor Network for Target Detection, Classification, and Tracking,' Computer Networks, vol. 46, no. 5, pp. 605-634.