ISSN:0975-9646

Intrusion Detection in Wireless Sensor Network Using Random Sensors by Implementing DES Algorithm

B.Joshua, G.Veena, K.Sandhya Rani, M.Anupama

Department of Computer Science Engineering,
Lendi Institute of Engineering and Technology, Vizianagaram, India.

Abstract: Intrusion detection in Wireless Sensor Network (WSN) is of practical interest in many applications such as detecting an intruder in a battlefield. The intrusion detection is defined as a mechanism for a WSN to detect the existence of inappropriate, incorrect, or anomalous moving attackers. In this paper, we consider this issue according to heterogeneous WSN models. Furthermore, we consider detecting an intruder in terms of sensing range of random sensors. Here we are preventing unauthorised access of data by providing symmetric key algorithm.

Index Terms:
Sensing range, intrusion detection, heterogeneity, wireless sensor network.

INTRODUCTION:

A Wireless Sensor Network (WSN) is a collection of spatially deployed wireless sensors by which to monitor various changes of environmental conditions (e.g., forest fire, air pollutant concentration, and object moving) in a collaborative manner without relying on any underlying infrastructure support .Recently, a number of research efforts have been made to develop sensor hardware and network architectures in order to effectively deploy WSNs for a variety of applications. Due to a wide diversity of WSN application requirements, however, a general-purpose WSN design cannot fulfill the needs of all applications. Many network parameters such as sensing range, transmission range, and node density have to be carefully considered at the network design stage, according to specific applications. To achieve this, it is critical to capture the impacts of network parameters on network performance with respect to application specifications. Intrusion detection (i.e., object tracking) in a WSN can be regarded as a monitoring system for detecting the intruder that is invading the network domain.

In a WSN, there are two ways to detect an object (i.e., an intruder): single-sensing detection and multiple-sensing detection. In the single-sensing detection, the intruder can be successfully detected by a single sensor. On the contrary, in the multiple-sensing detection, the intruder can only be detected by multiple collaborating sensors .In some applications, the sensed information provided by a single sensor might be inadequate for recognizing the intruder. It is because individual sensors can only sense a portion of the intruder. For example, the location of an intruder can only be determined from at least three sensors’ sensing. We define the sensor capability in terms of the sensing range and the transmission range. In a heterogeneous WSN some sensors have a larger sensing range and more power to achieve a longer transmission range. In this paper, we show that the heterogeneous WSN increases the detection probability for a given intrusion detection distance. This motivates us to analyze the network connectivity in this paper. Furthermore, in a heterogeneous WSN, high capability sensors usually undertake more important tasks (i.e., broadcasting power management information or synchronization information to all the sensors in the network),it is also desirable to define and examine the broadcast reach ability from high-capability sensors. The network connectivity and broadcast reachability are important conditions to ensure the detection probability in WSNs. They are formally defined and analyzed in this paper. To the best of our knowledge, our effect is the first to address this issue in a heterogeneous WSN .

Purpose:

The main purpose of the project is to detect the unauthorised user entry in the system while exchanging the data between two authorised users. The project focuses on involving only few random sensors in detecting the intruder while improving the energy effiency. The data is received securely by the authorised receiver using symmetric key.

Logical Organisation

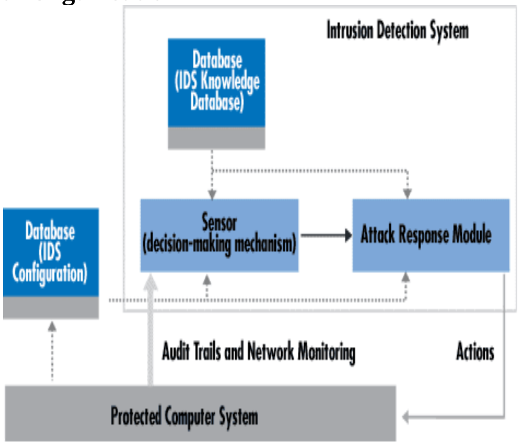

Intrusion Detection System
Database (IDS Knowledge Database)
Database (IDS Configuration)
Sensor (decision-making mechanism)
Attack Response Module
Audit Trails and Network Monitoring
Actions
Protected Computer System

Figure 1

In the above fig1. The sensor is involved in detecting the intruder by verifying the IDS knowledge database. If intruder is detected, the attack response module will give an alert information of the intruder. This information is displayed. The information of the intruder is stored in the database.

Problem Definition:

Single-sensing detection, the intruder can be successfully detected by a single sensor. Previous work was according to homogeneous single sensor in wireless sensor network. It is because individual sensors can only sense a portion of the intruder.

Means of solution:

Intrusion detection in heterogeneous WSNs by characterizing intrusion detection with respect to the network parameters. We are detecting the intruder using multiple sensor heterogeneous wireless sensor networks. Here multiple sensors are involved in detecting multiple intruders .Even though the intruder attacks the system, the data is sent securely to the receiver end by using symmetric key algorithm. **Symmetric-key algorithms** are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text as in fig.2. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption.

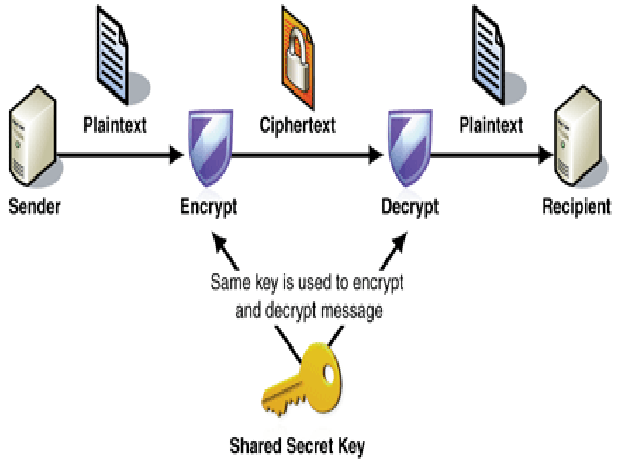


Figure 2

Here we are using DES(Data Encryption Standard) symmetric encryption algorithm for securely sending the data. DES is the archetypal block cipher — an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits, and it is always quoted as such.

The key is nominally stored or transmitted as 8 bytes, each with odd parity. One bit in each 8-bit byte of the KEY may be utilized for error detection in key generation, distribution, and storage. Bits 8, 16,..., 64 are for use in ensuring that each byte is of odd parity.

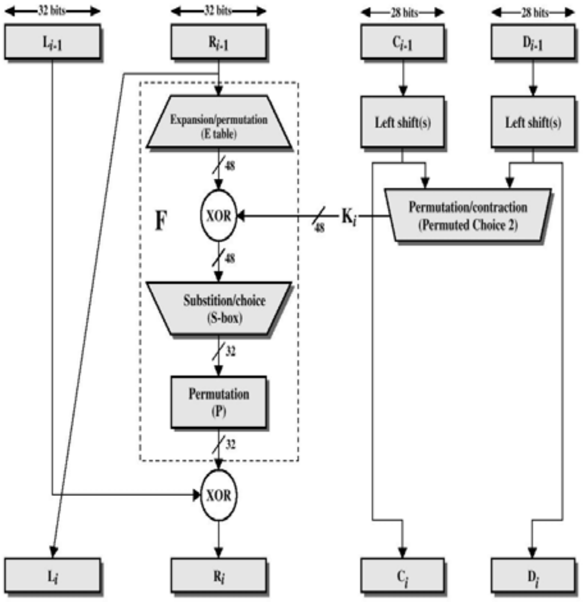


Figure 3

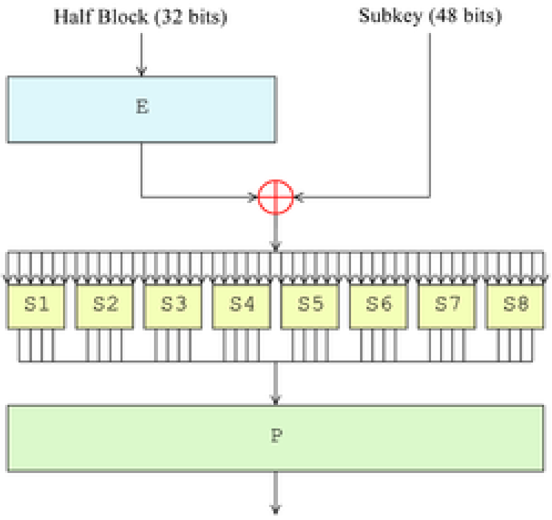
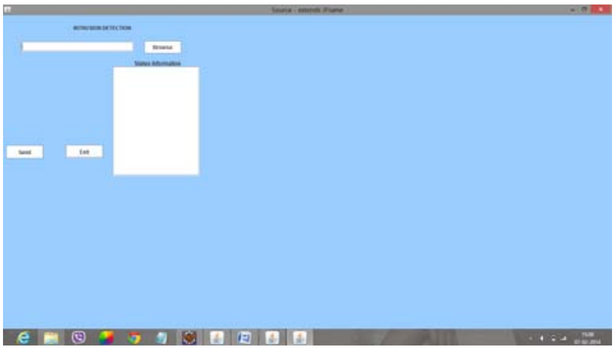
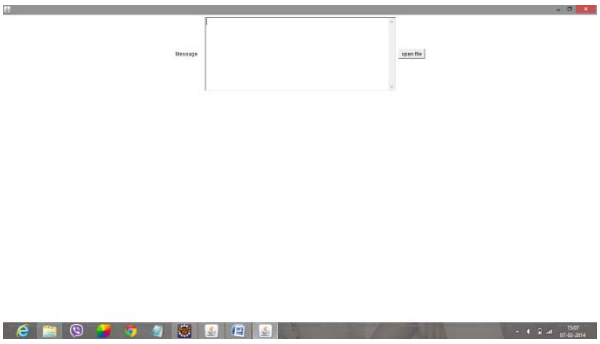


Figure 3

Here the user selects the data to be sent, while sending if any intruder appears the random sensor that was generated detects the intruder. We are using the DES symmetric encryption algorithm in order to avoid the unauthorised access of the data in the sender side.

RESULT:





CONCLUSION:

System should be secure against unauthorized access to any data. The system is prevented from any loss of data by the detection of intruder. Multiple intruders can be detected at a time by random sensors.

REFERENCES:

[1] D. Bri, M. Garcia, J. Lloret, and P. Dini, “Real deployments of wireless sensor networks, in Proceedings of the 3rd International Conference on Sensor Technologies and Applications (SENSORCOMM ’09), pp. 415–423, Athens, Greece, June 2009.

[2] A. Radhika, D. Kavitha, and D. Haritha, “Mobile agent based routing in MANETS—attacks & defences,” Network Protocols and Algorithms, vol. 3, no. 4, pp. 108–121, 2011.

[3] K. SahadevaiahandP. V.G.D. PrasadReddy, “Impactof security attacks on a new security protocol for mobile ad hoc networks,” Network Protocols andAlgorithms, vol. 3, no.4,pp. 122–14,2011.

[4] N. Alrajeh, S. Khan, andB. Shams, “Intrusion detection systems in wireless sensor networks: a review,” International Journal of Distributed Sensor Networks, vol. 2013, Article ID167575, 7pages, 2013.

[5] M. S. Sisodia and V. Raghuwanshi, “Anomaly base network intrusion detection by using random decision tree and random projection a fast network intrusion detection technique,” Network Protocols and Algorithms, vol. 3, no. 4, pp. 93–107, 2011.

[6] N. A. Alrajeh, S. Khan, J. Lloret, and J. Loo, “Artificial neural network based detection of energy exhaustion attacks in wireless sensor networks capable of energy harvesting,” Ad Hoc & SensorWireless Networks, vol. 2013, pp. 1–25, 2013.