Multiple Sensing Intrusion Detection System in Wireless Sensor Networks

R.Brintha
Research Scholar
Department of Computer Science
Pondicherry University,Karaikal

S.Bhuvaneswari
Head
Department of Computer Science
Pondicherry University,Karaikal

ABSTRACT

Availing security in a wireless sensor network requires more than user authentication with passwords or digital certificates and confidentiality in data transmission. The openness of wireless sensor network model makes it vulnerable and prone to sophisticated intrusion attacks like Denial of Service (DDOS) and side channel attacks. To handle large scale network access traffic and administrative control of data and application in wireless sensor network, a Multiple Sensing Intrusion Detection model has been proposed. Our proposed Multiple Sensing Intrusion Detection model handles large flow of data packets, analyze them and generate reports efficiently by finding the probability of network being attacked by an intruder. The intrusion distance, the minimum coverage of an area where the intruder can be sensed is found and multiple (sensing) detectors are situated there to detect the intruder once it enters or establishes its effect in the network.

Keywords

Wireless Sensor Networks, Multiple Sensing, Heterogeneous/Homogeneous, Intrusion Detection System, attacks, packet filtration, packet generation

1. INTRODUCTION

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors combined together to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. The concept of wireless sensor network is initially motivated by military applications in battlefield surveillance. Now, it has established its However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control.

A sensor network normally constitutes a wireless ad-hoc network that follows a routing algorithm which is used to forward the packets in the network to reach the destination. A numerous kind of network architecture is deployed to work on various applications. But there is a vast requirement to be satisfied in order to fulfill the needs of the 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.

2. LITERATURE SURVEY

Wireless Sensor Networks (WSNs) offer an excellent opportunity to monitor environments, and have a lot of interesting applications in warfare. The problem is that security mechanisms used for wired networks do not transfer directly to sensor networks. Some of this is due to the fact that there is not a person controlling each of the nodes, and even more importantly, energy is a scarce resource. Batteries have a short lifetime and cannot be replaced on deployed sensor nodes. Some of the studies have been undergone in WSNs versus wire-line networks, reviewing some of the approaches to intrusion detection as well as offering a new game theoretic-approach. It have been seen that WSNs have special vulnerabilities that do not exist in wire-line networks and it cannot therefore, simply transfer all our protocols for wire-line networks to WSNs. Protocols must be designed with low computational power and low energy requirements in mind. A study in attacks made in wireless sensor networks have seen some of the protocols that are used, as well as some ways to determine where to check packets, including a new game theoretic approach in which we saw that by allowing the attack to have some utility, and are able to increase ours through energy saving for sufficiently large, resource constrained networks.

3. PROPOSED WORK

Availing security in a wireless sensor network requires more than user authentication with passwords or digital certificates and confidentiality in data transmission. The openness of wireless sensor network model makes it vulnerable and prone to sophisticated intrusion attacks like Denial of Service (DDOS) and side channel attacks. To handle large scale network access traffic and administrative control of data and application in wireless sensor network, a Multiple Sensing Intrusion Detection model has been proposed. Our proposed Multiple Sensing Intrusion Detection model handles large flow of data packets, analyze them and generate reports efficiently by finding the probability of network being attacked by an intruder. The intrusion distance, the minimum coverage of an area where the intruder can be sensed, is found and multiple (sensing) detectors is situated there to detect the intruder once it enters or establishes its effect in the network.

3.1 PROPOSED ALGORITHM

An algorithm is proposed to generate the packets for the data that is to be transmitted in the Wireless Sensor Network. The data is divided into n no of packets in fixed size for further transmission. After creating the packets, a valid path is assigned for routing in the network

Algorithm Generate Packet (data or file D)

```
[$P_1$,$P_2$........ $P_n$]  ←  D
  For each packet
    Assign path to packet and route packet
  End For

End Algorithm
```

An algorithm is proposed to construct an Intrusion Detection System to detect the attackers survival. An efficient model is being delivered so that an intruder can be detected once it enters into the sensor area. And the packet is marked as invalid and discarded from further transmission.

Algorithm IDS

```
 On receiving packet in node(Detector)
    If packet is authorized
       Mark as valid and transmit to destination
    Else
       Mark as invalid and discard.
       Report to the admin
    End if

End Algorithm
```

4. IMPLEMENTATION

The Multiple Sensing Intrusion Detection model includes a network model and a detection model which specifies the WSN environment and the detection of intruder. The sensors are deployed in such a way that, the amalgamation of all the sensing ranges covers the whole area; the intruder/hacker can be detected instantly when the attacker enters the area of coverage. The system finds the probability of the intrusion distance within which the intruder should be detected. 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, the intrusion detection model is constructed in heterogeneous WSN models with multiple sensing intrusion detection system.

WSN in a two-dimensional (2D) plane with N sensors, denoted by a set N is considered. These sensors are uniformly and independently deployed in a square area. Such a random deployment results in a 2D Poisson point distribution of sensors. All sensors are static once the WSN has been deployed Heterogeneous WSNs. In a heterogeneous WSN, high capability sensors usually undertake more important tasks it is also desirable to define and examine the broadcast from high-capability sensors. In a heterogeneous WSN, a node is said to be covered by a sensor if it is located in the sensing range of any sensor(s). In our network model, the intruder does not know the sensing coverage map of the WSN. The distance is of central interest to a WSN used for intrusion detection. The network connectivity and broadcast are important conditions to ensure the detection probability in WSNs. They are formally defined and analyzed in this project.

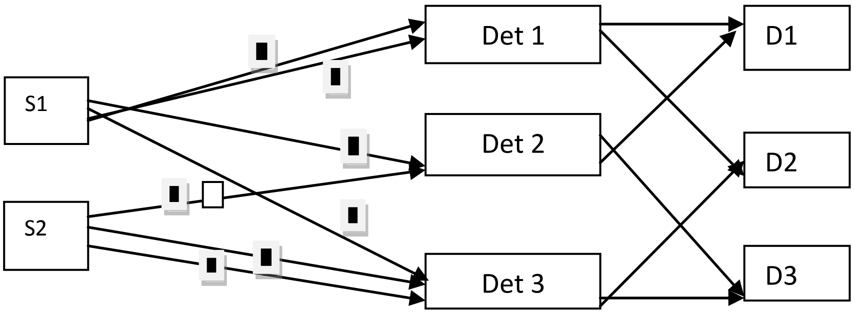


Fig 1: Data Flow from Source to Destination

→	Data flow
S	Source
D	Destination
Det	Detector
■	Data instance
□	Data filter

5. MODULES

1 **Designing Sensor Network**
2 **Packet Generation**
3 **Detecting Intruder**
4 **Packet Filtration**
5 **Arrival of the valid packet**

5.1 Designing Sensor Network

The reference architecture is being constructed for the Wireless Sensor Network. The nodes are interconnected in such a way that the node is connected to the neighboring node and it is independently deployed. While deploying, each node is provided with the authorized port number.

5.2 Packet Generation

The file or the data that is to be sent is converted into packets with fixed size. The packets produced would be sent from the source to the destination by routing through the intermediate nodes.

5.3 Detecting Intruder

The Multiple Sensing Intrusion Detection system is a computational model for a WSN to find the survival of an intruder who is an attacker producing invalid/inappropriate requests, data leakage, etc., in a vulnerable zone. The legitimate users can be found by checking the port no., and the packets having unauthorized port no are detected. The authorized packets are sent to the valid destination.

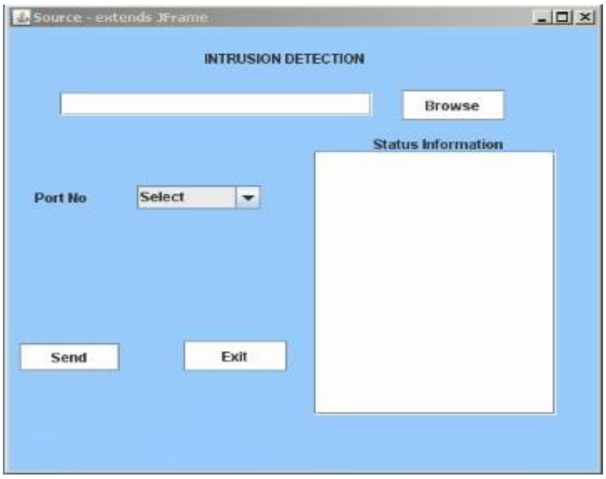
5.4 Packet Filtration

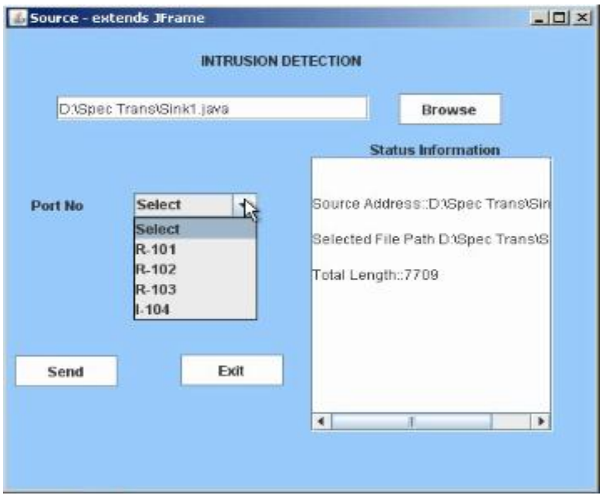
The packets received from the unauthorized port no are filtered and discarded. The authorized packets received from the legitimate users will be moved further in the authorized path.

5.5 Arrival of the Packet

The valid packets are moved further in the authorized path to reach the destination.

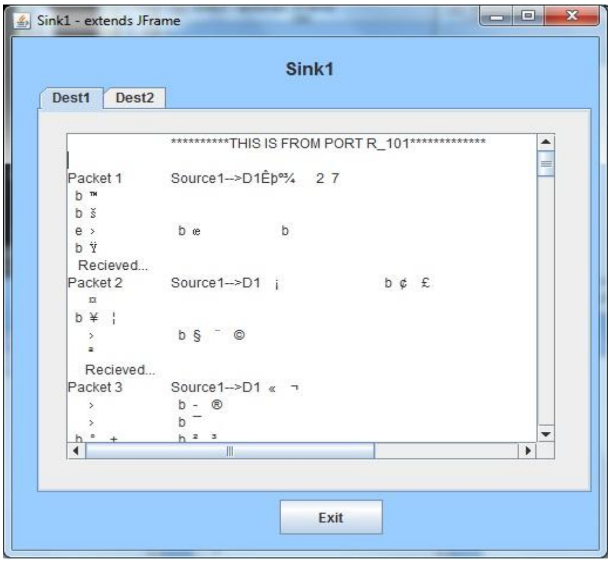
6. SNAPSHOTS





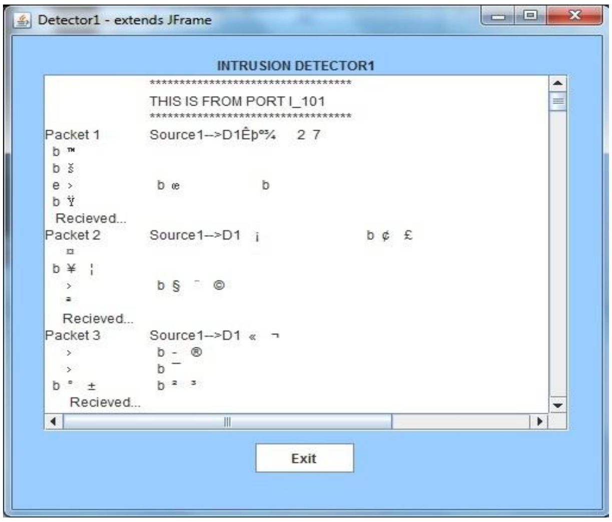
D:\Spec Trans\Sink1.java

```
Source Address::D:\Spec Trans\Sin
Selected File Path D:\Spec Trans\S
Total Length::7709
```



```
                **********THIS IS FROM PORT R_101*************

Packet 1        Source1-->D1Êþº¾   2 7
 b ™
 b š
 e ›             b œ          b
 b Ÿ
  Recieved...
Packet 2        Source1-->D1  ¡               b ¢  £
   ¤
 b ¥  ¦
   ›             b §  ¨  ©
   ª
   Recieved...
Packet 3        Source1-->D1 «  ¬
   ›             b   ®
   ›             b ¯
 b °  ±          b ²  ³
```



```
                ***********************************
                THIS IS FROM PORT I_101
                ***********************************
Packet 1        Source1-->D1Êþº¾   2 7
 b ™
 b š
 e ›             b œ          b
 b Ÿ
  Recieved...
Packet 2        Source1-->D1  ¡               b ¢  £
   ¤
 b ¥  ¦
   ›             b §  ¨  ©
   ª
   Recieved...
Packet 3        Source1-->D1 «  ¬
   ›             b   ®
   ›             b ¯
 b °  ±          b ²  ³
    Recieved...
```

7. CONCLUSION

This paper works on both the homogeneous and heterogeneous Wireless Sensor Networks to provide security against the intruders. The intruders may flood invalid requests to make the network busy, so that the legitimate users would be starved without the resources or their sensitive data would be leaked. Multiple-sensing intrusion detection system is constructed to find the probability of an intruder to compromise the nodes and make the network vulnerable. These models are formulated to find the probability of intrusion distance in WSN under different paradigms in a heterogeneous environment. The architecture of homogeneous and heterogeneous WSNs is constructed and the prompt parameters for detecting the intrusion distance are found. The observed results are examined and it is verified with the correctness of the proposed system.

8. REFERENCES

[1] R. Hemenway, R. Grzybowski, C. Minkenberg, and R. Luijten, “Optical-packet-switched interconnect for supercomputer applications,”*OSA J. Opt. Netw.*, vol. 3, no. 12, pp. 900–913, Dec. 2004.

[2] C. Minkenberg, F. Abel, P. Müller, R. Krishnamurthy, M. Gusat, P.Dill, I. Iliadis, R. Luijten, B. R. Hemenway, R. Grzybowski, and E.Schiattarella, “Designing a crossbar scheduler for HPC applications,”*IEEE Micro*, vol. 26, no. 3, pp. 58–71, May/Jun. 2006.

[3] E. Oki, R. Rojas-Cessa, and H. Chao, “A pipeline-based approach formaximal-sized matching scheduling in input-buffered switches,” *IEEE Commun. Lett.*, vol. 5, no. 6, pp. 263–265, Jun. 2001.

[4] C. Minkenberg, I. Iliadis, and F. Abel, “Low-latency pipelined crossbar arbitration,” in *Proc. IEEE GLOBECOM*, Dallas, TX, vol. 2, pp. 1174–1179, *2004.*

[5] C. Minkenberg, R. Luijten, F. Abel, W. Denzel, and M. Gusat, “Current issues in packet switch design,” *ACM Comput. Commun. Rev.*, vol. 33, no. 1, pp. 119–124, Jan. 2003.

[6] C. Minkenberg, F. Abel, P. Müller, R. Krishnamurthy, and M. Gusat,“Control path implementation of a low-latency optical HPC switch,” in*Proc. Hot Interconnects 13*, Stanford, CA, pp. 29–35,Aug. 2005.

[7] C.-S. Chang, D.-S. Lee, and Y.-S. Jou, “Load-balanced Birkhoff-von Neumann switches, part I: One-stage buffering,” *Elsevier Comput.Commun.*, vol. 25, pp. 611–622, 2002.

[8] A. Tanenbaum, *Computer Networks*, 3rd ed. Englewood Cliffs, NJ: Prentice Hall, 1996.

[9] R. Krishnamurthy and P. Müller, “An input queuing implementation for low-latency speculative optical switches,” in *Proc. X Int. Conf.Parallel Processing Techniques and Applications (PDPTA’07)*, Las Vegas, NV, vol. 1, pp. 161–167, , Jun. 2007.

[10] H. Takagi, *Queueing Analysis, Volume 3: Discrete-Time Systems*. Amsterdam: North-Holland, 1993.