International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017), e-ISSN: 2455-2585
Volume 5, Issue 02, February-2019

SINGLE AND MULTIPLE SENSING DETECTION MODELS FOR INTRUSION DETECTION IN WIRELESS SENSOR NETWORK

V. A. Rajgure[1], M. S. Ali[2]

[1]*Department of Computer Science and Engineering, Prof Ram Meghe College of Engineering and Management, Badnera, Amravati,*
[2]*Department of Computer Science and Engineering, Prof Ram Meghe College of Engineering and Management, Badnera, Amravati,*

Abstract— This paper presents various existing techniques for network security and heterogeneous systems. The proposed methodology for intrusion detection in heterogeneous wireless sensor network is described in this paper. The details of development of the proposed single and multiple sensing detection models with their evaluations in heterogeneous systems are presented here.

Keywords— Single sensing detection model, intrusion detection, multiple sensing detection model, wireless sensor network, homogeneous systems, heterogeneous systems

I. INTRODUCTION

In homogeneous systems or networks, all the devices or nodes are identical in terms of hardware intricacy and other hardware parameters. In homogeneous systems or networks, the same platform is utilized and every device or node in the network shares the identical functionality where as in heterogeneous systems or networks all the devices and nodes treated in a different way. In the actual world, the homogeneous systems, nodes, or sensors are uncommon and less practical because most of the applications (such as sensing applications) may require heterogeneous environment in terms of their data transfer, communication, and sensing capabilities in order to improve system and network reliability and increase system or network life span. Also, even if the systems or nodes are prepared with the same hardware, they may not for all time have the identical data transfer, communication and sensing components. In fact, at the industrialized stage, there is no assurance that two devices using the identical platform have accurately the similar physical properties. This taxonomy focuses on heterogeneity at the designing phase, when devices are intended to have non identical functionalities to meet the particular requirements of desired applications. In the heterogeneous systems, the average power and energy utilization for transferring data from the source devices to the sink in heterogeneous environment will be much smaller than the power and energy utilized in homogeneous systems.

There are diverse intrusion detection techniques based on two fundamental methodologies namely distributed method and hierarchical method. A protocol is proposed in [Misra et. al, 2010] that satisfy the unique necessities of WSNs, which is small complexity and energy efficiency. The protocol has two distinctive properties: self-learning and distributed in nature. Simple Learning Automata based Intrusion Detection (S-LAID) functions in a distributed behavior with every node functioning autonomously without any information about the adjacent nodes. If a node is compromised it will not influence other working nodes because the network is in distributed arrangement. This representation is based on the concept of stochastic learning automata on packet sampling method, which benefits the proposed work to accomplish the objective of energy aware intrusion detection system.

It has been tried to resolve the problems of wireless sensor network, by using multi-agent and semantic approaches [Mao, 2010]. Thus, a semantic based intrusion detection outline is proposed. In this IDS security ontology is created depending on the features of WSN to symbolize the formal semantics for intrusion detection. The ontology is used to enhance the process of intrusion detection. This approach utilizes distributed environment of the network and has a layered architecture of the proposed framework. There are a lot of algorithms proposed by the author and these algorithms have attempted to resolve the problem in decentralized and cooperative methodologies. In this method, every chosen rule of security ontology is mapped to sensing data gathered from regular sensor nodes to detect anomaly. The proposed intrusion detection system is a hierarchical design based system for wireless ad-hoc networks.

The noteworthy confront of wireless ad-hoc sensor networks is to preserve the security of the network, and this confront has been addressed in [Mamun and Kabir, 2010]. The proposed hierarchical design based intrusion detection system satisfies the demands and limitations of WSN. The intrusion detection system utilizes policy dependent detection mechanism. This framework follows core defence approach where cluster-head is the centre point to protect intruder and concentrates on preserving the power of sensor nodes by distributing the conscientiousness of intrusion detection to three layer nodes.

One more IDS method based on hierarchical wireless sensor networks is proposed in [Chen et. al, 2010]. This approach utilizes routing tables and isolation tables to identify the intrusions and to approximate the usage of IDS. The proposed approach isolates malicious nodes by neglecting consumption of unnecessary energy by IDS (ITIDS). The IDS makes use of four different nodes, which are BS, Primary Cluster Head, numerous Secondary Cluster Heads and the remaining sensor nodes MNs. The ITIDS is based on cluster networks and can detect serious attacks.

As there are intrinsic disadvantages of static IDS a dynamic model of intrusion detection system (DIDS) is proposed in [Huo and Wang, 2008]. This is a hierarchical framework of IDS based on clustered network to combat the low energy problem of sensor networks. It can utilize distributed defence which has the benefit of detecting multiple intruders, although, with an increased rate of energy consumption with increase in cluster size.

A Hybrid Intrusion Detection System (HIDS) has been proposed in [Yan et. al, 2009] cluster based WSN (CWSN). As the sensor network is cluster dependent, the nodes in the network may acquire different capabilities, and hence, the network is called as heterogeneous wireless sensor network. As the cluster heads and sensor nodes have diverse capabilities and responsibilities, there should be a hybrid IDS to detect intruders. The cluster head identifies the intruders that endeavor to decrease the energy utilization as well as decrease the quantity of information in the whole network. Also the proposed IDS prove to be beneficial in prolonging the networks life span.

A protocol that detects and isolates the compromised nodes is proposed by [Crosby et. al, 2011]. In accumulation to reputation based trust framework, the allocation-aware trust-based protocol is proposed that not simply detects the compromised nodes but also can isolate the node. The wireless sensor network is established in clusters by means of secure cluster formation algorithms. The trust and reputation values are calculated by means of a method where the neighboring nodes monitor every other. A straightforward location verification algorithm is also proposed. This algorithm has been constructed by using the signal strength information. The simulation results demonstrated that the protocol efficiently detects and isolates the compromised nodes even when the nodes are colluding.

The model of ontology is used for collecting and organizing the attributes of attacks. But there is an association between ontology concept and lightweight intrusion detection system (IDS). The author explores how the intrusion detection system about ontology and lightweight IDS are connected. Ranger based IDS (RIDS) has been proposed in [Hsieh et. al, 2011]. It combines the ranger method to decrease energy consumption and the isolation tables to evade detecting anomaly constantly. This lightweight IDS model relates ontology conception mechanism about anomaly detection. In this technique, rough set theory (RST) is used for pre-processing of packets and anomaly models will be trained by support vector machine.

A detection system is proposed in [Atakli et. al, 2008], which is deployed on a hierarchical WSN architecture. The author states that, it is complicated to discover a compromised node and to avoid the situation were the victim can be misled by the counterfeit information given by the adversary through a compromised node. The proposed scheme is based on the weighted-trust assessment. The hierarchical architecture of WSN has three types of nodes which makes it a three layered architecture: Access Points (AP) layer, Forwarding Nodes (FN) Layer and the Sensor Nodes (SN) layer. The most important hypothesis made in this scheme is that the base stations are trusted and preponderance of the sensor nodes are working appropriately.

A security administration model is proposed in [Peng et. al, 2009] for self organizing wireless sensor networks based on intrusion detection. It can avoid majority of attacks. Then an analysis of each layer of networks in security model is presented and the security administration measures in the data link layer and network layer are elaborated in detail mainly. Such a structure is built, based on the existing encryption and authentication protocols.

Administration platform and security framework for WSN is developed by [Lee et. al, 2008]. The proposed framework has advantages as observe secure association and intrusion detection. It also provides the background of WSN, its security problems and requirements. An intruder detection algorithm has been developed by [Wang and Wang, 2008] for static wireless sensor networks. The proposed IDS is of small complexity. The intrusion detection model comprises characteristics that discover the average frequency of execution of order. A distributed algorithm in which the sensor gathers the information from the neighboring nodes to analyses the anomalies if any from the neighbors. The intrusion identification algorithm on detecting anomalies packets received from its neighbors basic alarms to report the anomaly. In this research work the security strategies are proposed and designed for wireless sensor networks, hence following sections describes homogeneous and heterogeneous wireless sensor networks.

II. Models for Security in Heterogeneous Wireless Sensor Networks

In this research work intrusion detection in heterogeneous wireless sensor networks is performed by proposed single sensing detection and multiple sensing detection models using the network parameters. These models filter the packets and deliver only authorized packet to sink node. The power of sensor nodes is conserved by utilizing awake and sleep techniques. Using the proposed multiple sensing detection model intruders can be detected anywhere in the multiple sensor heterogeneous wireless sensor networks. The proposed models try to improve response scheduling, priority responses and control on response enhancement mechanism. The proposed models provide greater level of security, fault tolerance and robustness for different wireless sensor network architecture. User interfaces are developed using proposed models which allow dynamic reconfiguration of systems and visualizes the activities of these systems. The simulated networks detailed information of different system activities is centralized for analysis.

The high capacity nodes in terms of sensing coverage and transmission range are selected by using the proposed node selection algorithm.

Proposed Node Selection Algorithm

Si K- set of type-k sensors in the wireless sensor network

```
S W- set of all wireless sensors
N(a) A - set of neighbors of node a
Repeat
For i=1 to M
Select ‘a’ node with min A in set K
If $A \neq Ø$
Select ‘a’
KA= {d/the distance between ‘a’ and A < ($r_k$/2)}
If KA > 1
W=W - (KA U ‘a’)
Else
W= W – ‘a’
Until W is null
```

The proposed algorithm pick a certain set of nodes that cover the whole area based on category of node, its sensing and transmission range.

Proposed Single Sensing Detection Model

In proposed single sensing detection model an intruder is identified when it comes in the sensing range of a sensor. When the intruder comes in the area all the way through the boundary and the boundary is enclosed by the sensors, then the intruder will be sensed as soon as it comes in the wireless sensor network area. Or else it has to shift a definite distance L before sensed by any of the sensors. When the intruder begins from a point of the network border, given an intrusion distance L > 0, the analogous intrusion identification volume V is approximately a quadrilateral volume.

The probability P(L) that an intruder can be instantly identified as soon as it comes in a heterogeneous wireless sensor network can be defined by,

$$P(L=0)=1-\prod_{i=1}^{N}e^{-ni}$$

Where, ni is the number of type-i nodes activated in the area $\pi r_K^2/2$

Suppose λ is the maximum distance permissible for intrusion occurrence in a given application, the probability P(L) that the intruder can be identified within λ in the given heterogeneous wireless sensor network can be derived as:

$$P(L<\lambda)=1-\prod_{i=1}^{N}e^{-ni}$$

Where, ni is the number of type-i nodes activated in the area $A=2\lambda r_K+(1/2)r_K^2$.

Proposed Multiple Sensing Detection Model

In the multiple sensing detection model an intruder has to be detected by at least s sensors for intrusion identification in a wireless sensor network. The number of needed sensors depends on particular applications. For example, at least three sensors used for information sensing are needed to identify the location of the intruder. In the multiple sensing detection model, multiple sensors have to discover an intruder at the same time. Consider Ps (L = 0) be the probability that an intruder is detected instantly as soon as it comes in a wireless sensor network multiple sensing detection model. This probability can be defined as:

$$Ps(L=0)=1-\prod_{i=1}^{N}\sum_{j=0}^{s-1}P(j,A_i)$$

Where, A_i is the area covered by type-I sensor node and it is assumed that n_i number of type-I sensors are activated in the area A_i. It gives the probability of detecting the intruder with less than s sensor nodes.

III. Evaluation of the Proposed Models

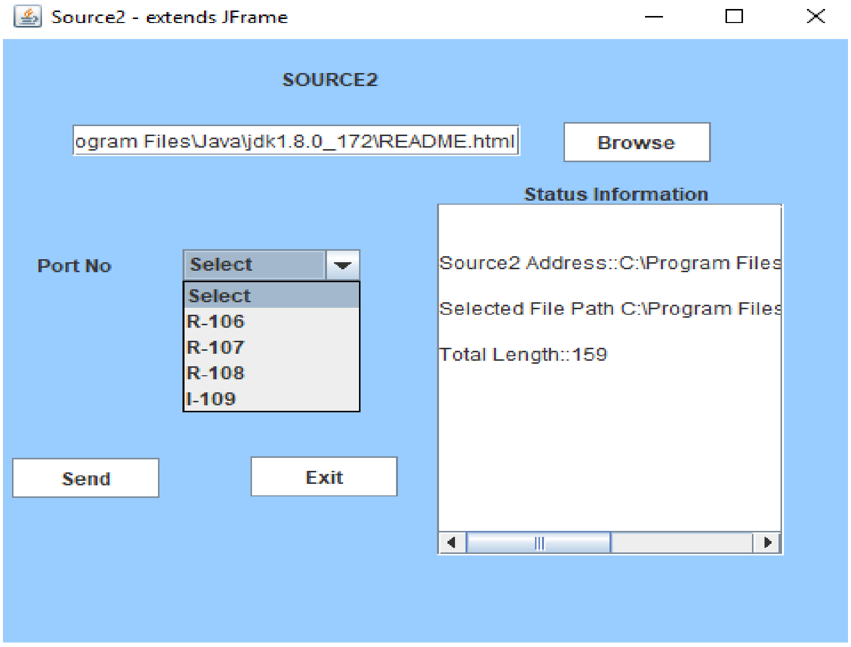
In the proposed methodology a wireless sensor network is constructed. A sensor network normally constitutes a wireless ad-hoc network, meaning that each sensor supports a multi-hop routing algorithm. Several nodes may forward data packets to the base station. In the existing single-sensing detection, the intruder can be successfully detected by a single sensor. Existing work considers homogeneous single sensor in wireless sensor network. Therefore individual sensors can only sense a portion of the intruder. The sensed information provided by a single sensor might be inadequate for recognizing the intruder. So that there is no guarantee for information transferred has been sent securely.

In the proposed methodology intrusion detection in heterogeneous networks is performed by characterizing intrusion detection with respect to the network parameters. In the proposed methodology two detection models are developed: single-sensing and multiple-sensing. Using the developed models the intruder can be detected in both single sensor and multiple sensor heterogeneous wireless sensor networks. Using the developed strategies the network is sensed which results in finding the actual nodes in the wireless sensor network. The intruder nodes are separated out which corresponds to secured transmission of information.

For demonstrating proposed models various modules are developed. Sensor Network Construction Module: In this module, the network is connected. Each node is connected with the neighboring node and it is independently deployed in network area. It also deploys each authorized port number in a node. Packet Creation Module: In this module, the source file is selected. The data available in selected file is converted into fixed size of packets. These packets are used for transmission from source to detector. Authorized and Unauthorized Port Identification Module: The intrusion detection is defined as a mechanism for a network to detect the existence of inappropriate, incorrect, or anomalous moving attackers. In this module the path is checked whether authorized or unauthorized. If path is authorized the packet is send to valid destination. Otherwise the packet will be deleted. Using the deployed authorized port numbers only we are going to find the path is authorized or unauthorized. Inter-Domain Packet Filters Module: If the packet is received from other than the authorized port number it will be filtered and discarded. This filter only removes the unauthorized packets and authorized packets send to destination. Valid Packet Reception Module: In this module, after filtering the invalid packets all the valid packets are delivered to the intended destination. Screenshot 1 shows the developed interface for sending data securely in wireless sensor networks.

The proposed methodology analyzes the intrusion detection problem by characterizing intrusion detection probability with respect to the intrusion distance and the network parameters (i.e., node density, sensing range, and transmission range). The analytical model for intrusion detection allows us to analytically formulate intrusion detection probability within a certain intrusion distance under various application scenarios. The proposed models can be extended for intrusion detections in internet applications and parallel computer interconnection networks.

Screenshot 2 shows the data transmitted by a normal wireless sensor node through port R-101. It also shows the data to be transmitted, length of data, and source address. The transmitted data from source 1 R-101 is received securely by the wireless sink node 1 as shown in screenshot 3.



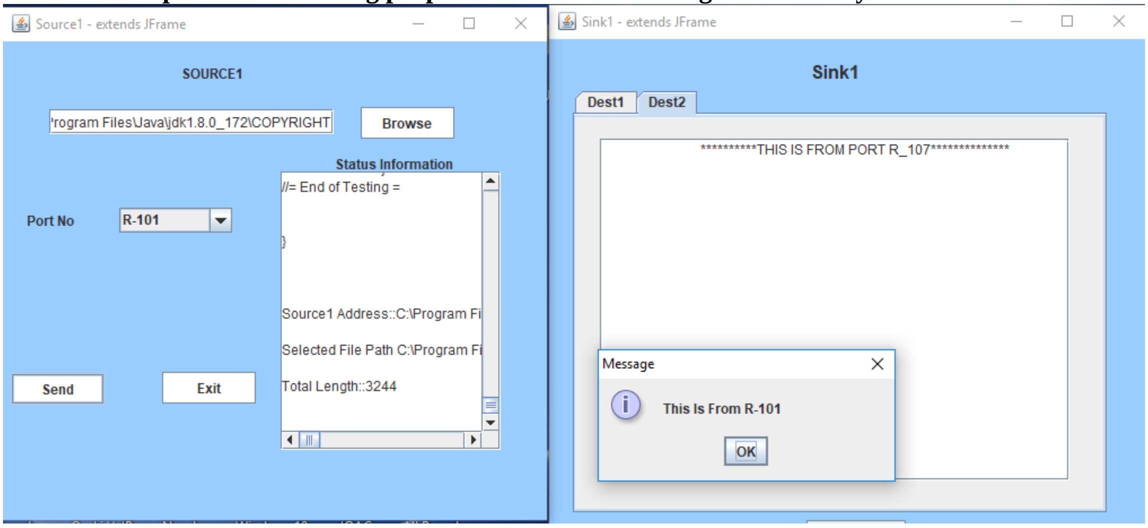
ogram Files\Java\jdk1.8.0_172\README.html

Source2 Address::C:\Program Files

Selected File Path C:\Program Files

Total Length::159

Screenshot 1: Developed interface using proposed models for sending data securely in wireless sensor networks.



'rogram Files\Java\jdk1.8.0_172\COPYRIGHT

Port No: R-101

//= End of Testing =

}

Source1 Address::C:\Program Fi

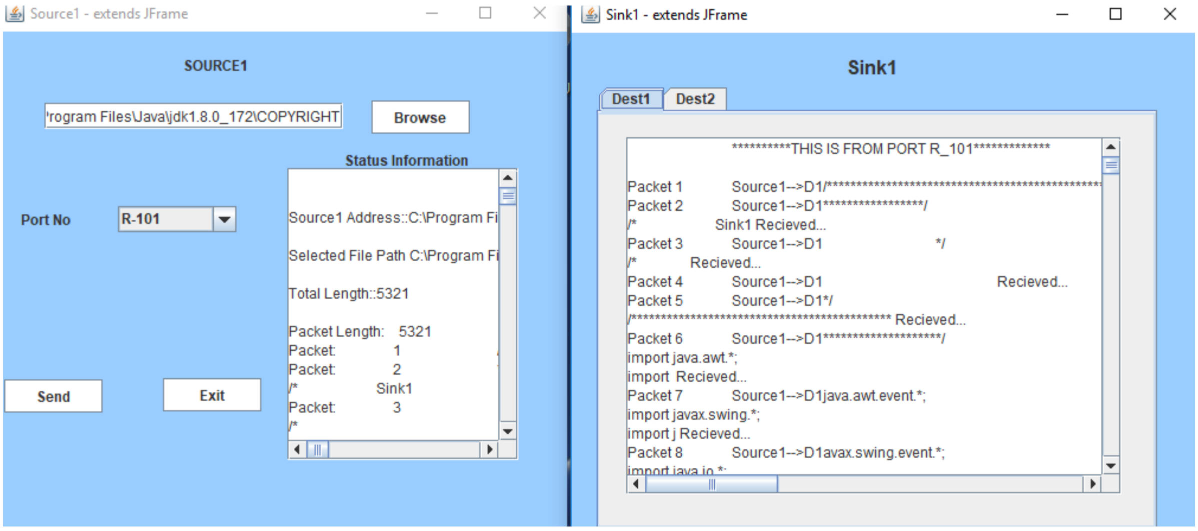
Selected File Path C:\Program Fi

Total Length::3244

**********THIS IS FROM PORT R_107**************

This Is From R-101

Screenshot 2: Data transmitted from normal source node in wireless sensor network through port R-101.



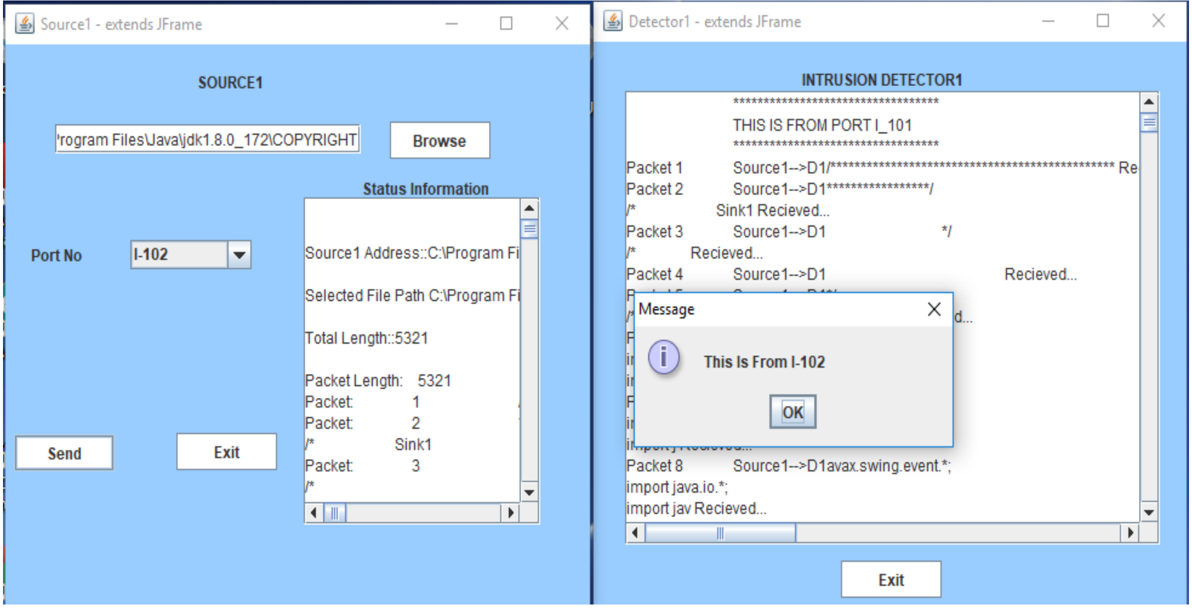
'rogram Files\Java\jdk1.8.0_172\COPYRIGHT

Port No: R-101

```
Source1 Address::C:\Program Fi

Selected File Path C:\Program Fi

Total Length::5321

Packet Length:   5321
Packet:          1
Packet:          2
/*               Sink1
Packet:          3
/*
```

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

Packet 1      Source1-->D1/***********************************************
Packet 2      Source1-->D1****************/
/*          Sink1 Recieved...
Packet 3      Source1-->D1                    */
/*      Recieved...
Packet 4      Source1-->D1                                    Recieved...
Packet 5      Source1-->D1*/
/******************************************* Recieved...
Packet 6      Source1-->D1*******************/
import java.awt.*;
import  Recieved...
Packet 7      Source1-->D1java.awt.event.*;
import javax.swing.*;
import j Recieved...
Packet 8      Source1-->D1avax.swing.event.*;
import java.io.*;
```

Screenshot 3: Data received securely on wireless sensor sink node 1.



'rogram Files\Java\jdk1.8.0_172\COPYRIGHT

Port No: I-102

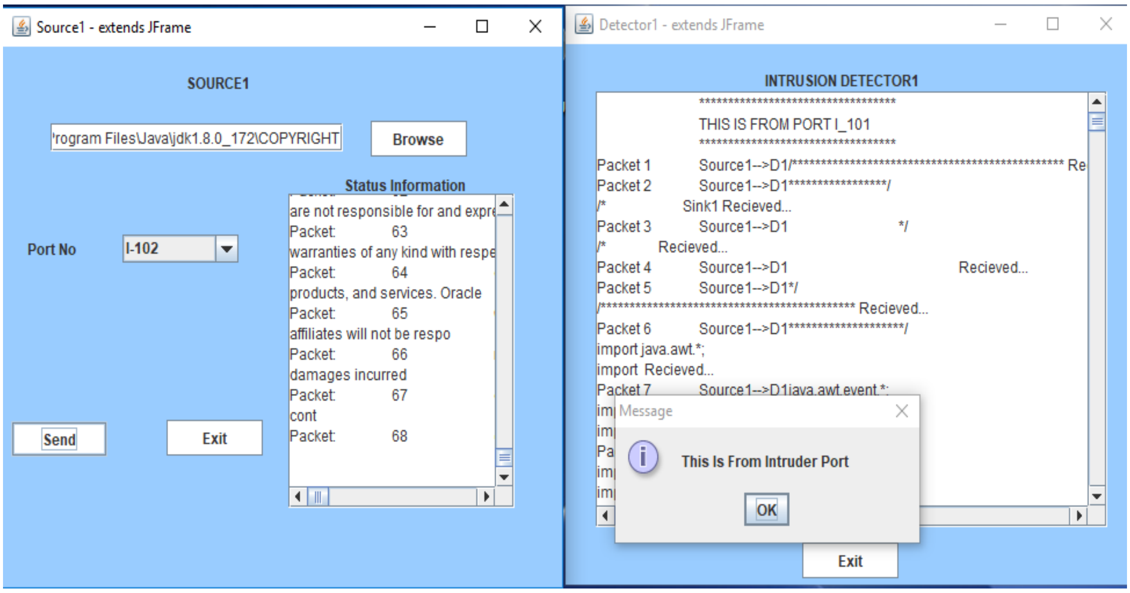
```
Source1 Address::C:\Program Fi

Selected File Path C:\Program Fi

Total Length::5321

Packet Length:   5321
Packet:          1
Packet:          2
/*               Sink1
Packet:          3
/*
```

```
              **********************************
              THIS IS FROM PORT I_101
              **********************************
Packet 1      Source1-->D1/*********************************************** Re
Packet 2      Source1-->D1****************/
/*          Sink1 Recieved...
Packet 3      Source1-->D1                    */
/*      Recieved...
Packet 4      Source1-->D1                                    Recieved...
Packet 8      Source1-->D1avax.swing.event.*;
import java.io.*;
import jav Recieved...
```

This Is From I-102

Screenshot 4: An intruder node I-102 is trying to enter in wireless sensor network.

As shown in screenshot 4 an intruder node I-102 is trying to enter in the created wireless sensor network by sending data. The proposed models immediately identify the intrusion by indicating the port from which intrusion is occurring as shown in screenshot 5. The notification of the occurred intrusion is immediately sent to the administrator as shown in screenshot 6.



'rogram Files\Java\jdk1.8.0_172\COPYRIGHT

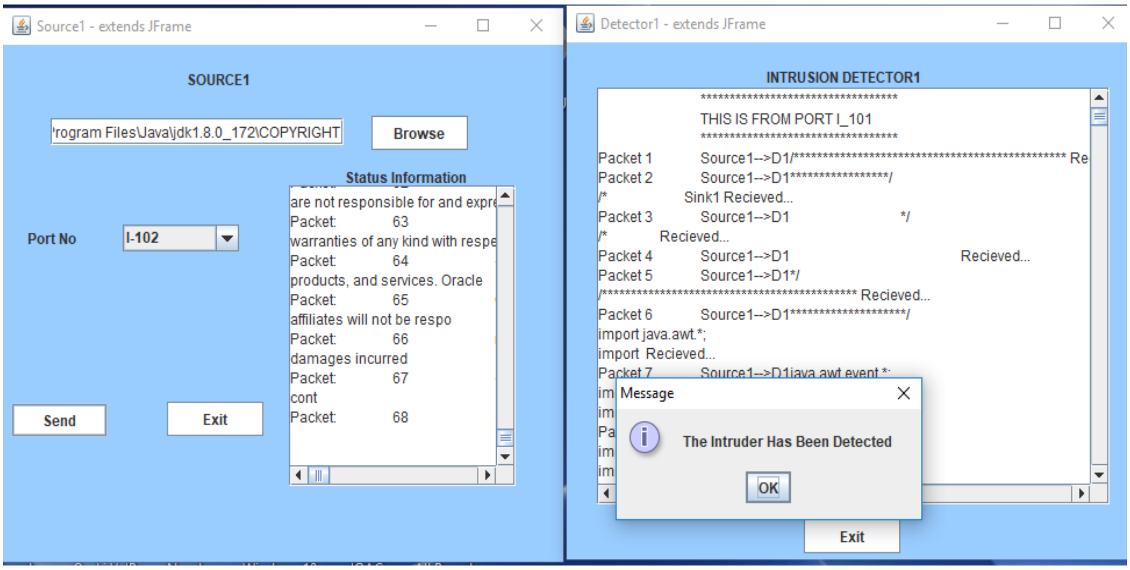
Port No: I-102

```
are not responsible for and expre
Packet:          63
warranties of any kind with respe
Packet:          64
products, and services. Oracle
Packet:          65
affiliates will not be respo
Packet:          66
damages incurred
Packet:          67
cont
Packet:          68
```

```
              **********************************
              THIS IS FROM PORT I_101
              **********************************
Packet 1      Source1-->D1/*********************************************** Re
Packet 2      Source1-->D1****************/
/*          Sink1 Recieved...
Packet 3      Source1-->D1                    */
/*      Recieved...
Packet 4      Source1-->D1                                    Recieved...
Packet 5      Source1-->D1*/
/******************************************* Recieved...
Packet 6      Source1-->D1*******************/
import java.awt.*;
import  Recieved...
Packet 7      Source1-->D1java.awt.event.*;
```

This Is From Intruder Port

Screenshot 5: An intruder is immediately detected by sensing detection models.



'rogram Files\Java\jdk1.8.0_172\COPYRIGHT

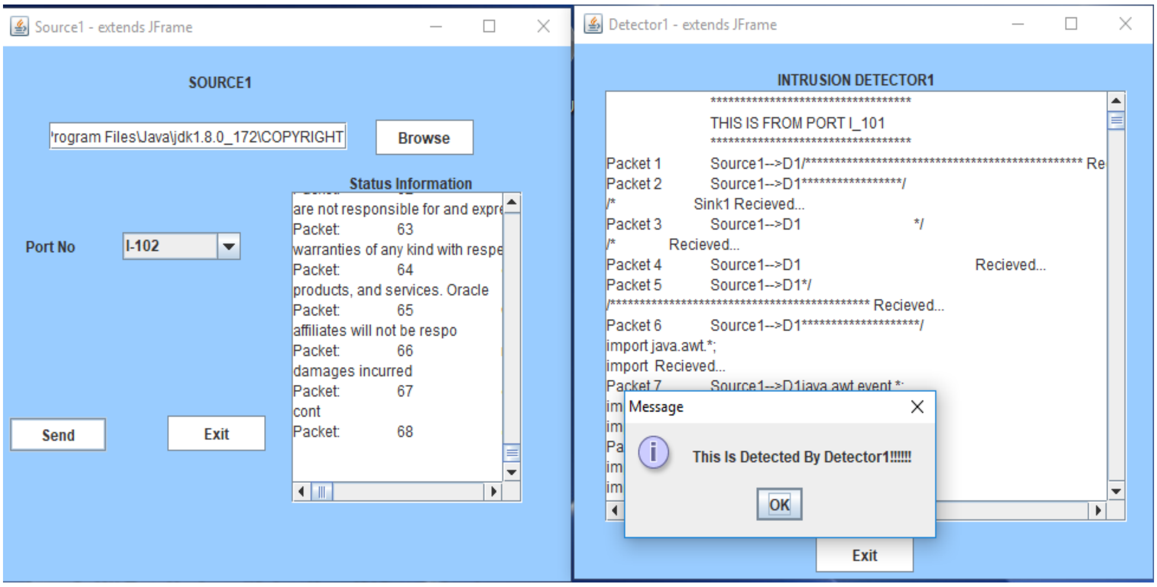
```
are not responsible for and expre
Packet:      63
warranties of any kind with respe
Packet:      64
products, and services. Oracle
Packet:      65
affiliates will not be respo
Packet:      66
damages incurred
Packet:      67
cont
Packet:      68
```

```
                 **********************************
                 THIS IS FROM PORT I_101
                 **********************************
Packet 1         Source1-->D1/********************************************** Re
Packet 2         Source1-->D1*****************/
/*            Sink1 Recieved...
Packet 3         Source1-->D1                  */
/*      Recieved...
Packet 4         Source1-->D1                                  Recieved...
Packet 5         Source1-->D1*/
/******************************************** Recieved...
Packet 6         Source1-->D1*******************/
import java.awt.*;
import  Recieved...
Packet 7         Source1-->D1java.awt.event.*;
```

The Intruder Has Been Detected

Screenshot 6: An administrator is notified regarding the occurred intrusion.

In multiple-sensing detection model, as there are many sensor nodes sensing the intrusion the developed system shows the information of sensor node detected the intrusion. As shown in screenshot 3.7 the intrusion is detected by the sensor node named as Detector 1. Administrator can view the log recorded by the Detector 1 for fetching detailed information of the intrusion as shown in screenshot 8.



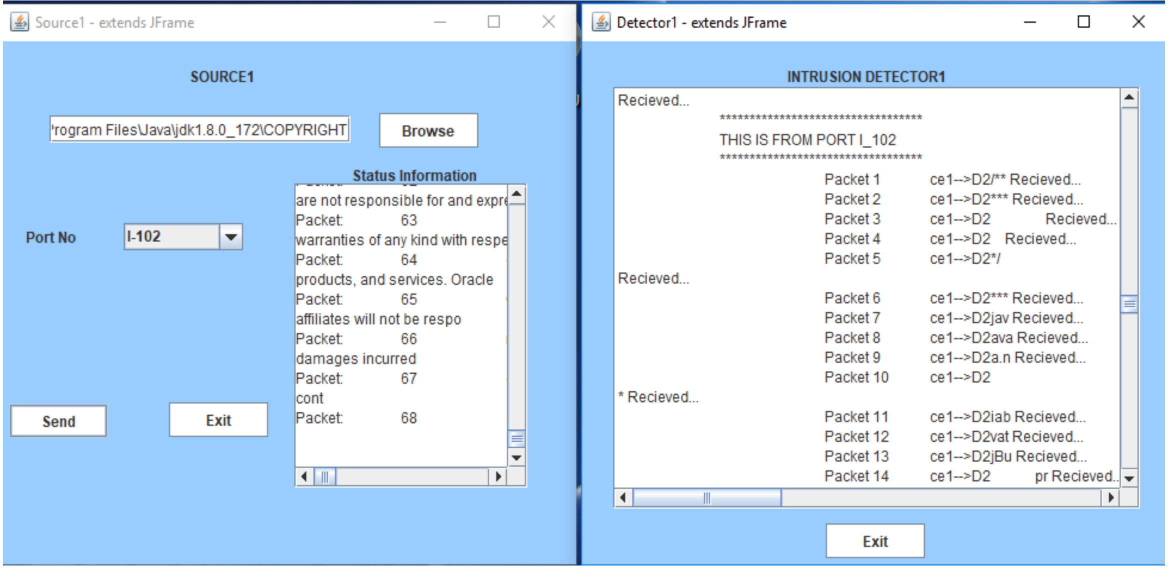
'rogram Files\Java\jdk1.8.0_172\COPYRIGHT

```
are not responsible for and expre
Packet:      63
warranties of any kind with respe
Packet:      64
products, and services. Oracle
Packet:      65
affiliates will not be respo
Packet:      66
damages incurred
Packet:      67
cont
Packet:      68
```

```
                 **********************************
                 THIS IS FROM PORT I_101
                 **********************************
Packet 1         Source1-->D1/********************************************** Re
Packet 2         Source1-->D1*****************/
/*            Sink1 Recieved...
Packet 3         Source1-->D1                  */
/*      Recieved...
Packet 4         Source1-->D1                                  Recieved...
Packet 5         Source1-->D1*/
/******************************************** Recieved...
Packet 6         Source1-->D1*******************/
import java.awt.*;
import  Recieved...
Packet 7         Source1-->D1java.awt.event.*;
```

This Is Detected By Detector1!!!!!

Screenshot 7: An administrator is notified regarding the wireless sensor detected the intrusion.



'rogram Files\Java\jdk1.8.0_172\COPYRIGHT

```
are not responsible for and expre
Packet:      63
warranties of any kind with respe
Packet:      64
products, and services. Oracle
Packet:      65
affiliates will not be respo
Packet:      66
damages incurred
Packet:      67
cont
Packet:      68
```

```
Recieved...
                 **********************************
                 THIS IS FROM PORT I_102
                 **********************************
                               Packet 1      ce1-->D2/** Recieved...
                               Packet 2      ce1-->D2*** Recieved...
                               Packet 3      ce1-->D2        Recieved...
                               Packet 4      ce1-->D2   Recieved...
                               Packet 5      ce1-->D2*/
Recieved...
                               Packet 6      ce1-->D2*** Recieved...
                               Packet 7      ce1-->D2jav Recieved...
                               Packet 8      ce1-->D2ava Recieved...
                               Packet 9      ce1-->D2a.n Recieved...
                               Packet 10     ce1-->D2
* Recieved...
                               Packet 11     ce1-->D2iab Recieved...
                               Packet 12     ce1-->D2vat Recieved...
                               Packet 13     ce1-->D2jBu Recieved...
                               Packet 14     ce1-->D2         pr Recieved...
```

Screenshot 8: An administrator visualizing detailed information of detected intrusion at Detector 1.

IV. CONCLUSIONS

In this paper initially the intrusion detection issues in both homogeneous and heterogeneous wireless sensor networks are analyzed by characterizing intrusion detection probability with respect to the intrusion distance and the network parameters such as number of nodes, sensing range, and transmission range. On the basis of this analysis two detection models are proposed, designed and developed namely single-sensing detection and multiple sensing detection models. This paper provides insights in designing homogeneous and heterogeneous wireless sensor networks and assists in choosing critical network parameters to meet the wireless network application requirements.

This paper presents proposed energy efficient intrusion detection mechanisms resulting in life span enhancements of wireless sensor nodes. Wireless sensor networks are vulnerable to several attacks because of their deployment in an open and unprotected environment. This paper presents the key security vulnerabilities in heterogeneous WSN and also presents different intrusion detection approaches by using various algorithms. Furthermore, the paper describes numerous existing techniques to discover how they have implemented intrusion detection system.

The utilized algorithms and the development details of the proposed models are presented in this paper. The proposed models for intrusion detection allows analytical formulation of intrusion detection probability within a certain intrusion distance under a variety of application situations. The evaluation results carried out using the developed interfaces shows the accuracy of the proposed intrusion detection models.

REFERENCES

[1] [Misra et. al, 2010] S. Misra, P. Venkata Krishna and Kiran Isaac Abraham, “Energy Efficient Learning Solution for Intrusion Detection in Wireless Sensor Networks”, COMSNETS'10 proceedings of the 2nd international conference on Communication systems and Networks, 2010.

[2] [Mao, 2010] Yuxin Mao, “A Semantic-based Intrusion Detection Framework for Wireless Sensor Network”, Networked Computing (INC), 6th International Conference, Gyeongju, Korea, 2010.

[3] [Mamun and Kabir, 2010] M. S. I. Mamun, A.F.M. Sultanul Kabir, “Hierarchical Design Based Intrusion Detection System for Wireless Ad Hoc Sensor Network”, International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3 July 2010.

[4] [Chen et. al, 2010] Rung-Ching Chen, Chia-Fen Hsieh and Yung-Fa Huang, “An Isolation Intrusion Detection System for Hierarchical Wireless Sensor Network”, Journal of Networks, Vol. 5, Number 3 March 2010.

[5] [Huo and Wang, 2008] G. Huo and Xiaodong Wang, “DIDS: A Dynamic Model of Intrusion Detection System in Wireless Sensor Networks”, IEEE, International Conference on Information and Automation, Zhangjiajie, China, June 20 –23, 2008.

[6] [Yan et. al, 2009] K. Q. Yan, S.C. Wang and C.W. Liu, “A Hybrid Intrusion Detection System of Cluster-based Wireless Sensor Networks”, Proceedings of the International MultiConference of Engineers and Computer Scientists 2009 , Vol IIMECS 2009 ,Hong Kong, March 18 - 20, 2009.

[7] [Crosby et. al, 2011] Garth V. Crosby, Lance Hester, and Niki Pissinou, “Location-aware, Trust-based Detection and Isolation of Compromised Nodes in Wireless Sensor Networks”, International Journal of Network Security, Vol.12, No.2, PP.107- 117 March 2011.

[8] [Hsieh et. al, 2011] Chia-Fen Hsieh, Yung-Fa Huang and Rung-Ching Chen, “A Light-Weight Ranger Intrusion Detection System on Wireless Sensor Networks”, published in IEEE Genetic and Evolutionary Computing (ICGEC), 2011.

[9] [Atakli et. al, 2008] Idris M. Atakli , Hongbing Hu, Yu Chen, Wei-Shinn Ku, Zhou Su “Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation”, The Symposium on Simulation of Systems Security (SSSS’08), Ottawa, Canada, April 14 –17, 2008.

[10] [Peng et. al, 2009] Xi Peng, Wuhan Zheng Wu, Debao Xiao, Yang Yu,"Study on Security Management Architecture for Sensor Network Based on Intrusion Detection "' IEEE, Volume: 2, 25-26 April 2009.

[11] [Lee et. al, 2008] Byunggil Lee, Seungjo Bae and Dong Won Han, “Design of network management platform and security framework for WSN”, IEEE International conference on signal image technology and internet based system, 2008.

[12] [Wang and Wang, 2008] Qi Wang, Shu Wang, “Applying an Intrusion detection algorithm to wireless sensor networks”, Second international workshop on Knowledge Discovery and Data Mining, 2009.