International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 19 (2018) pp. 14313-14322

Anomalous Attacker Evidence and Detection System in WSN

***B. Srinivasa Rao** [1] and **P. Premchand** [2]

[1] *Department of Computer Science and Engineering, Gokaraju Rangaraju Institute of Engineering and Technology (Autonomous), Bachupally, Hyderabad-50090, Telangana, India.*
Affiliated to Jawaharlal Nehru Technological University Hyderabad, Hyderabad-500072 India.
[2] *Department of Computer Science Engineering, University College of Engineering, Osmania University, Hyderabad-500007, India*
*Emial id: * bsrgriet2015@gmail.com, [2]p.premchand@uce0u.edu*

Abstract

Due to the features like distributed structure, open wireless network system etc. the Wireless Sensor Networks (WSN) are pruned to security attacks at various levels. These attacks may have significant influence on the efficiency of WSN. During the anomalous attacks, attackers manage to get unauthorized accesses to the network and harm the network system and services to make them ineffective. A counter mechanism is essential to overcome the influence of the attacks and sustain the efficiency of the network. In that process it is required to find the evidence for the activities of the attacker in the network. In the present research work, an attempt has been made to develop and implement a mechanism or scheme to find the evidence for the existence of an attacker in the network and to provide security measure to the WSN system by filtering the attacker to prevent the attacks. This is achieved by designing and implementing an Anomalous Attacker Evidence and Detection System (AAEDS) as a simple network security measure in wireless sensor networks systems. The proposed AAEDS is designed for homogeneous and heterogeneous WSN models considering single and multiple-sensing detection schemes. The present security measure and its simulation results have been presented and discussed. The results reveal that the present AAEDS works as per expectations for both the types WSNs and can be a proto-type for further extensions.

Keywords: Information security, Network Security, Attack, Attacker, Intrusion Detection, intruders, WSN, Heterogeneous

INTRODUCTION

Now-a-days, it has become essential for every organization to have its own security policy as per its requirements based upon its adopted technology like Communication Network, Parallel Computing System, Distributed Computing System, Cloud System, Adhoc Network, Mobile Network, Wireless Sensor Network etc. This security policy may be intended to protect organization through pro-active policy stance [1]. From the literature it is well understood that Computer Security is concerned with the loss or harm to the hardware, software or information of an organization. It also includes denial, disruption and misdirection of the services and facilities provided by the computer system [2-6]. The Computer Security may be considered as combination of System Security, Network Security and Data or Information Security. Data security or Information Security deals with security issues, policies and services of data under communication. Data Security provides security services for threats concerned with data confidentiality, authentication, integrity, non-repudiation, access control and availability [7-10]. As Information Systems are designed in multilayered structures, the above security issues have their influence at different layers of the systems and affect the performance of the Systems [11]. In this context, the security issue like confidentiality is becoming a challenge task in the environment of new technologies such as cloud computing, wireless communication systems etc. [12]. One aspect of the confidentiality of an Information System is unauthorized access to the network by a third party to steal important information or causing damage to the efficiency of the Information System [7-10]. An unauthorized access to the computer networking system is known as attack/hack/intrusion and is one of the most serious threats to the Computer Security. Hence, it is essential to design a security measure to detect the attacker to assess the vulnerability of the system or to protect the system from misuse [7]. An Attacker Evidence system (AES) is software and/or hardware based security scheme to detect the attempts of an attacker intended to misuse the systems such as network or the Internet [13].

A wireless sensor networks (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions [14]. The WSN have many applications such as military, civil, healthcare, home automation, traffic control etc. It normally constitutes a wireless adhoc network associating with a multi-hop routing algorithm [15]. A WSN is an adhoc distributed system consisting of several wirelessly connected sensor nodes and can be deployed to collect information about surrounding environment [16]. WSNs are highly vulnerable to security attacks at various levels due to various factors like distributed nature, multi-hops, open wireless medium etc.[16-18]. Hence an effective security measure is to be designed to overcome the attacks like intrusion or hacking in WSN. An Attacker Evidence system (AES) can be designed and implemented to detect and prevent from security attacks [19]. Survey reveals that earlier, several researchers have designed and implemented Intrusion Detection Systems for WSN in different scenarios such as Anomaly-based IDS, Signature-based IDS, and Cross layer IDS etc. [13, 17, and 18]. The probability of creating more

false alarms is a problem with Anomaly-based IDSs, even though they are lightweight in nature. Overheads like updating and inserting new signatures and suitability to larger WSN are the disadvantages with Signature-based IDSs. As the WSNs have resource limitation, the Cross layer IDSs are usually not suitable [13, 17 and 18]. Based upon the capability the WSNs can be classified as homogeneous and heterogeneous. Large sensing range, more power and broad casting power management information are the significant features of Heterogeneous WSNs in comparison with homogeneous WSNs [13 and 14]. The two important conditions for ensuring detection probability in WSNs are the network connectivity and broad cast reach ability in a secured manner [14, 18 and 20]. A few have considered the case of IDS for heterogeneous WSN security in comparison with homogeneous one with a simple simulation method. A comparative study may be considered for both homogeneous and heterogeneous WSNs in terms of intrusion/hacker detection. Hence this is the motivation for the present work to design and implement an Attacker Evidence system (AES) for homogeneous and heterogeneous WSNs by using a simple simulation method. This simple method may be a proto-type but would be useful to extend further. To the best of our knowledge, our effort is the first to address this issue both in homogeneous and heterogeneous WSNs for a simple simulation using Attacker Evidence system (AES).

EARLIER INTRUSION DETECTION SYSTEMS (IDS) AND WSN

Various attacker/intrusion/ hacker detection systems have been designed and implemented in different scenario and detailed information is available in vast literature [13-29]. It is already understood that An Intrusion Detection system (IDS) is software and/or hardware based security scheme to detect the attempts of an intruder intended to misuse the systems such as network or the Internet [13]. From [14], the IDS comprise of mainly three components namely sensors, console and central engine. The security events of the WSN are produced by sensors. The WSN events and their related alerts are monitored by console. The centrals records events and set rules for generation of alerts. The intrusion detection is possible in two ways: intrusion detection by a single sensor or multiple sensors collective cooperation. As the former is ineffective in some cases, multiple sensor detection can be considered for intrusion detection. The data flow in homogeneous and heterogeneous wireless sensors is as shown in fig.1. S and D indicate Source and Detector and R1, R2, and R3 are receiving nodes in WSN. The directions indicate the flow of data through the networks. The intruder may be denoted by a cloud symbol.

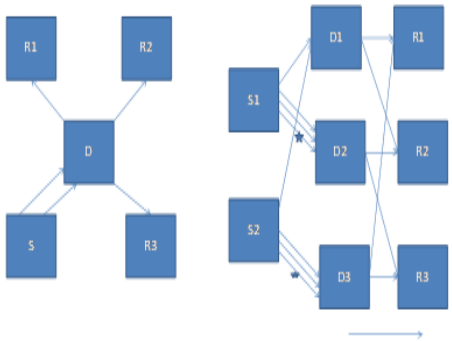


Figure.1. Homogeneous and Heterogeneous WSNs

ANOMALOUS ATTACKER EVIDENCE AND DETECTION SYSTEM(AAEDS)

With reference to [14], the presently proposed simple Anomalous Attacker Evidence and detection System (AAEDS) can be designed in five modules: 1.WSN construction, 2. Generation of Packets. 3. Identifying authorized and unauthorized port. 4. Inter-Domain Packet Filter construction and 5.Valid packet reception. In the first module WSN is designed such a way that each node is connected to the neighboring nodes and each port number is authorized by all nodes. In the second module a browser is designed to convert selected data into a fixed size of packet. These packets are sent from source to detector. In the third module in order to find authorized and unauthorized port a detection mechanism is designed. This module checks whether the path is authorized or unauthorized using the port number and if path is authorized the packet is send to valid destination. Otherwise the packet will be deleted. In the fourth module the Inter-Domain Packet Filter is designed. The Packet Filter filters the packets received from other than the designated port number and authorized packets will be send to destination. Finally, the valid packet reception module receives all the valid Packets. Thus only valid packets reach the destination from the source node [30]. The design logic for the Attacker Evidence System (AES) is shown in Fig. 2. The system design comprises of mainly data input and output mechanisms. 1. Input Design: (i) Source file browsing (ii) Conversion of selected data into fixed size packets. (iii) Write program to hack the packet (iv) Selection of port number to send the packet (v) Sending packet from source to detector. 2. Output Design: (i) Filtering and discarding of packet from unauthorized port (ii) Sending authorized packets to destination. The functional flow of data, data input, intruder detection, packet filtering, and reception packets are shown in data flow diagram (fig.2).

At first the user will input the data from a file and sends this packet to the detector and the detector filters the received packets. In case the packet is authorized it will be sent to a valid receiver. If the packet is an unauthorized one, then it will be discarded into the sink. Thus the design plan is

implemented in four modules: Network construction module, Detector module, Packet filter module and Receive packet module. The corresponding software design plan is shown in fig.3 and fig.4. The Network Construct module is a network, with attributes Construct and with responsibilities container.add(c); The Detector module comprises the attributes analyzing and responsibilities void server() ; The packet filter contains attributes Testing and responsibilites r1.server; Finally the sink module contains attributes Receive packets and responsibilites get.packet().

(a)User Requirement Specification: The main user requirements are User Characteristics, Functional Requirements, and Non Functional Requirements.

The user requirements are briefly outlined below:

1. User Characteristics: A user interface is used to search the data and services. An operational user interface can be used to add new data as and when required. Provision for operations like update/delete the data. No access rights for the user to access the system.

2. Functional Requirements: (i) Frame a packet and send the packet over the network. (ii) Write the instruction program to hack the packet over inappropriate, incorrect, anomalous attackers. (iii) This should be for both homogeneous and heterogeneous WSN models.

3. Non-Functional Requirements: (i) Usability: A procedure is designed to establish connection between a sender and a receiver with no third party intervention. (ii) Reliability: The java platform makes the system more reliable. (iii) Performance: The system performance depends on the high level languages and the advanced network technologies.

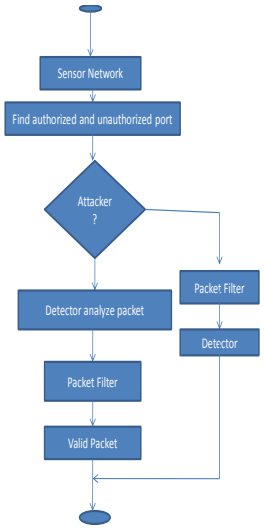


Figure 2. Data flow diagram for Attacker Evidence System (AES)

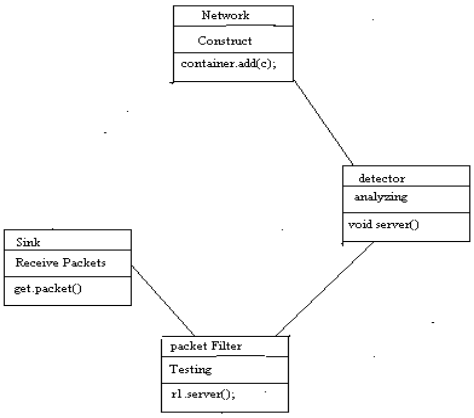


Figure 3. Software Design plan for AES

(iv)Supportability: A cross platform supported system is to be designed. (v) Implementation: The system is implemented in java network programming environment with Windows xp professional platform.

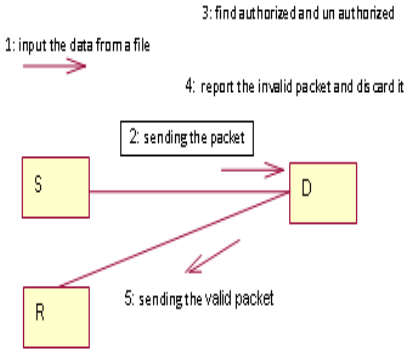


Figure 4. Mechanism for receiving valid packets

(b)System Requirements: The system requirements for the AES are: Hardware: Pentium IV 2.6 GHz Processor, 512 MB DD RAM, 20 GB Hard Disk, LG 52X CD Drive, Standard Keyboard, Mouse, Internet/Networking. Software: Java, JFrameBuilder and Windows Xp.

AES Implementation

The architecture of a WSN node is as shown in fig.5. According to the networking principles each node contains the data of authorized ports of all other nodes in the network. Each node can verify whether a packet is from an authorized port or not by running a suitable algorithm and accordingly takes the decision for next action. All the operations, respective screen display operations and screen displays involved in the simulation at source, detector and receiver

level are presented in Table-I. Predefined authorized and unauthorized ports data has been stored in files and the files have been browsed to select the ports for communicating packets through the WSN. The present AES has been simulated in the environment of Java, JFrame Builder and Windows XP operation system using the specified hardware and software. The simulated results that have been obtained by implementing the operations as per the Table-1 have been reported in Table-2. Also important screen shots have been presented for better understanding of the simulated results and the process of AES in Fig. 6.

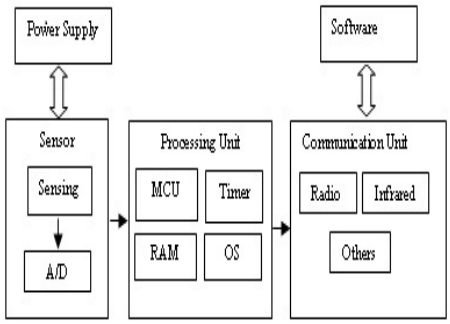


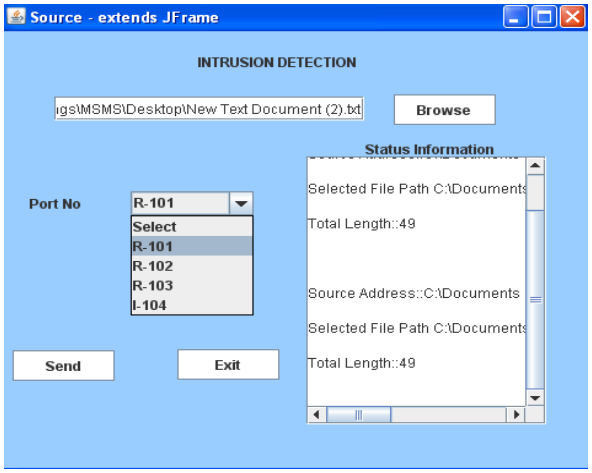
Figure 5. Architecture of a WSN node

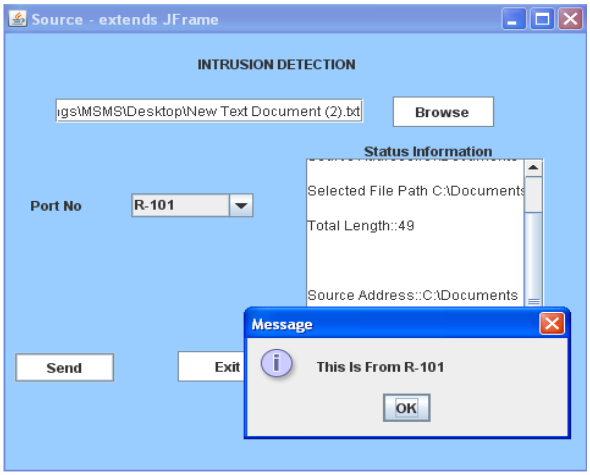
Table-1. Operations and Result displays on Computer during the simulations

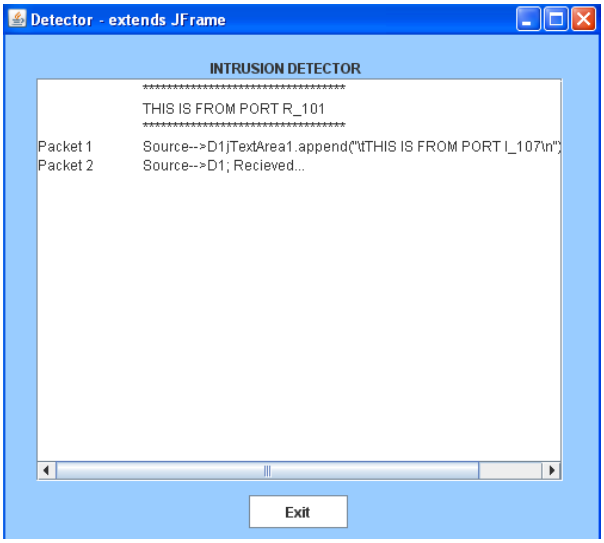
Source		Detector		Receiver	
Operations	Screen Display operation	Operations	Screen Displays operation	Operations	Screen Displays
1.Double click on source batch file 2. Click on browse button to select the file 3. Select the port number 4.Click the send button 5.Click on the OK button	1.Displays selected file information 2.Displays the selected port information 3. After clicking the send button, displays an alert window. 4.After clicking the OK button the packet is sent to the Detector	1. The detector checks the validity of port of the received packet. 2. If the packet is from an authorized port, detector sends it to a valid receiver. Else, it discords the packet and reports the intrusion.	1. Displays that the port is a valid port in case of a valid port. 2. In case of invalid port, displays that arrived port is an intruder port. 3. Also displays that which detector has detected.	1. It receives the packet from the Detector, if the packet is from an authorized port. 2. It has to display on the screen that from which port the packet has been received.	1. Displays on the screen that from which port the packet has been received.

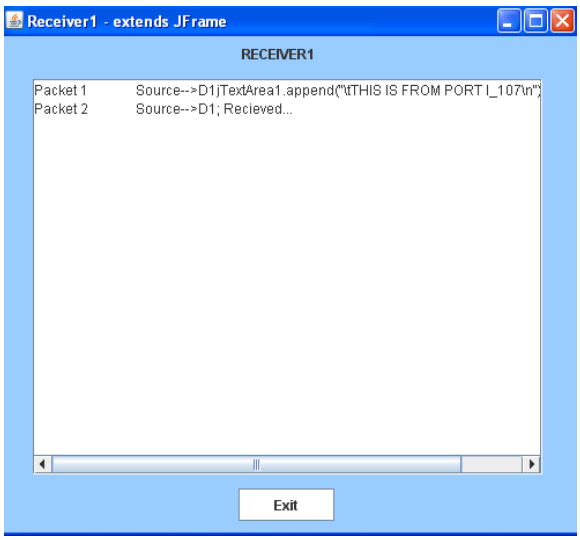
Table-2. Simulated Results of Attacker Evidence Scheme

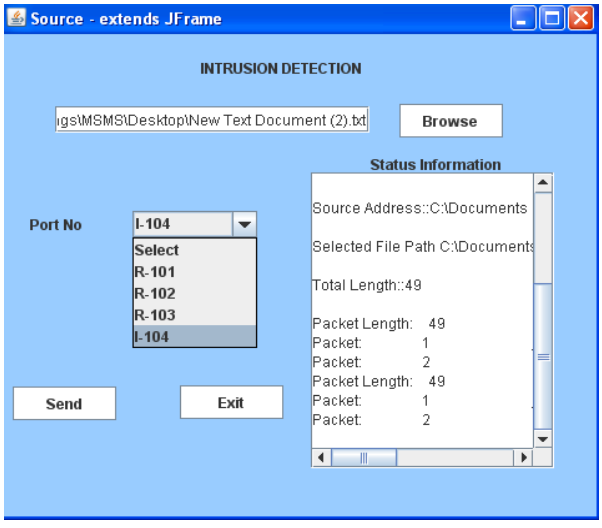
Source	Selected Port	Port Authorized/ Unauthorized	Detector	Hacking Detection	Packet Receiver/Sink	Packet Status
Homogeneous Network						
S	R-101	Authorized	D	NO	R1	Received
S	I-104	Unauthorized	D	YES	-	deleted
Heterogeneous Network						
S1	R-101	Authorized	D1	NO	R1	Received
S1	I-102	Unauthorized	D1	YES	-	deleted
S1	I-105	Unauthorized	D2	YES	-	deleted
S2	R-106	Authorized	D3	NO	R3	Received
S2	I-109	Unauthorized	D3	YES	-	deleted

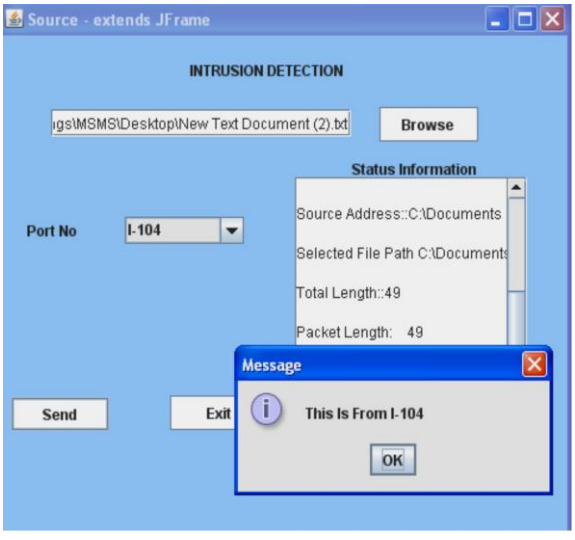

Source - extends JFrame
INTRUSION DETECTION
igs\MSMS\Desktop\New Text Document (2).txt
Browse
Status Information
Port No
R-101
Select
R-101
R-102
R-103
I-104
Selected File Path C:\Documents
Total Length::49
Source Address::C:\Documents
Selected File Path C:\Documents
Total Length::49
Send
Exit

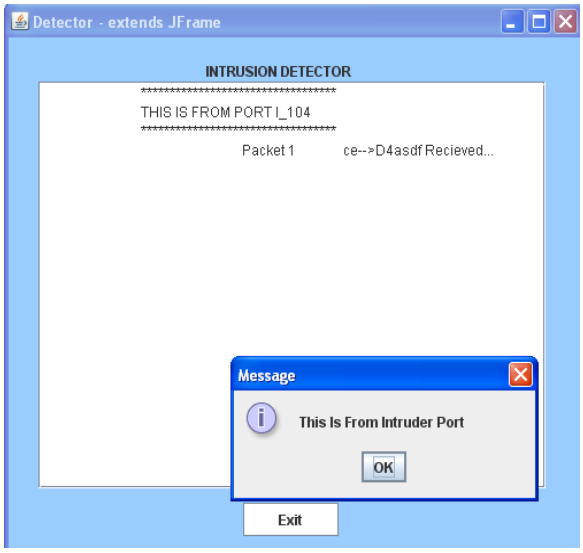

Source - extends JFrame
INTRUSION DETECTION
igs\MSMS\Desktop\New Text Document (2).txt
Browse
Status Information
Port No
R-101
Selected File Path C:\Documents
Total Length::49
Source Address::C:\Documents
Message
This Is From R-101
OK
Send
Exit

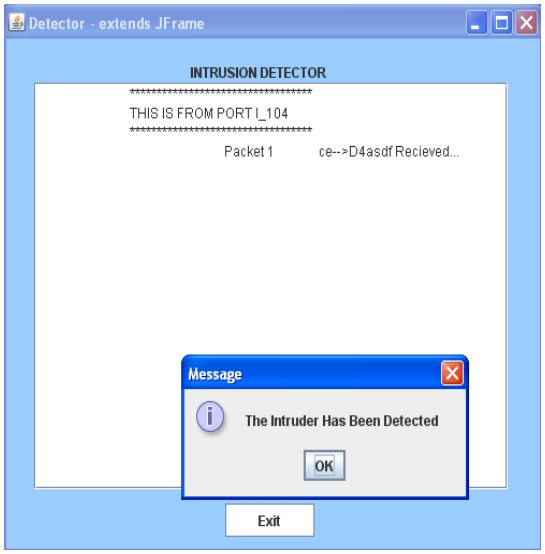

Detector - extends JFrame
INTRUSION DETECTOR
THIS IS FROM PORT R_101
Packet 1
Source-->D1jTextArea1.append("\tTHIS IS FROM PORT I_107\n")
Packet 2
Source-->D1; Recieved...
Exit

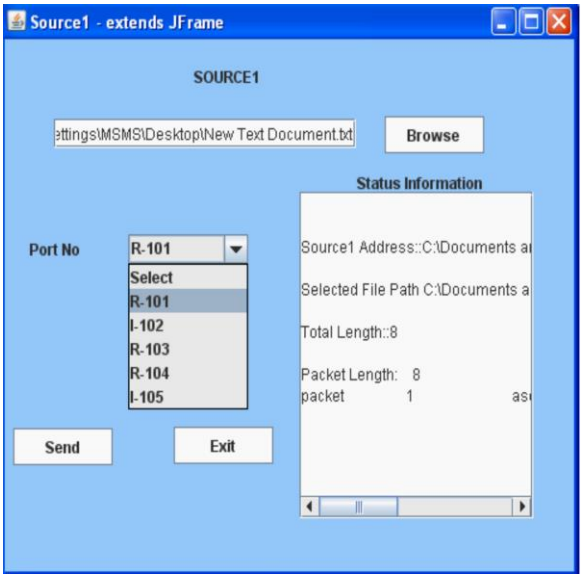

Receiver1 - extends JFrame
RECEIVER1
Packet 1
Source-->D1jTextArea1.append("\tTHIS IS FROM PORT I_107\n")
Packet 2
Source-->D1; Recieved...
Exit

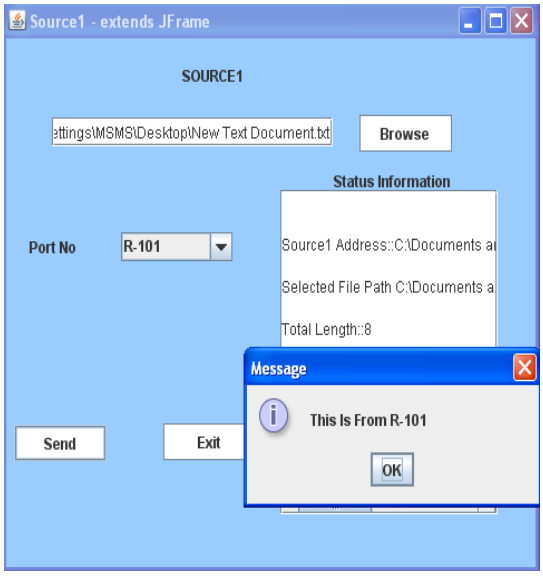

Source - extends JFrame
INTRUSION DETECTION
igs\MSMS\Desktop\New Text Document (2).txt
Browse
Status Information
Port No
I-104
Select
R-101
R-102
R-103
I-104
Source Address::C:\Documents
Selected File Path C:\Documents
Total Length::49
Packet Length: 49
Packet: 1
Packet: 2
Packet Length: 49
Packet: 1
Packet: 2
Send
Exit

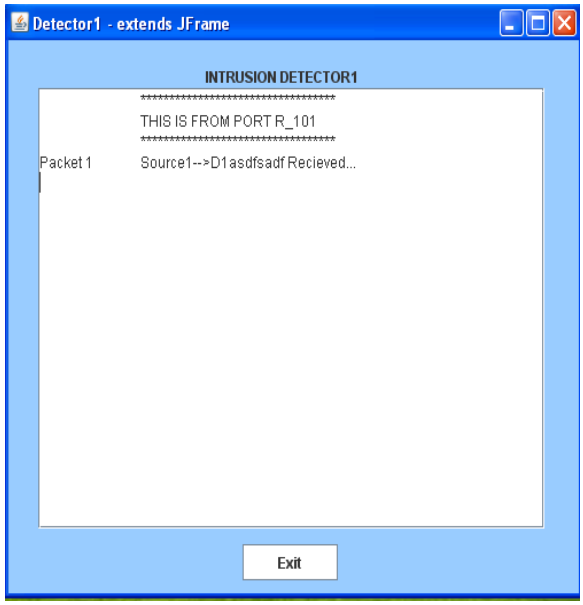

Source - extends JFrame
INTRUSION DETECTION
igs\MSMS\Desktop\New Text Document (2).txt
Browse
Status Information
Port No
I-104
Source Address::C:\Documents
Selected File Path C:\Documents
Total Length::49
Packet Length: 49
Message
This Is From I-104
OK
Send
Exit

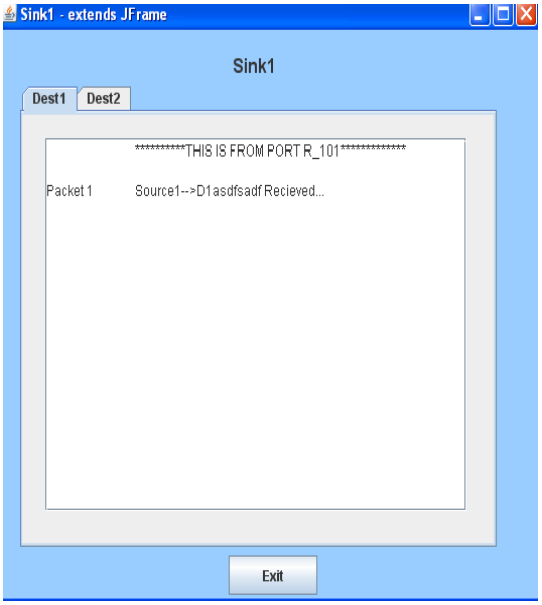

Detector - extends JFrame
INTRUSION DETECTOR
THIS IS FROM PORT I_104
Packet 1 ce-->D4asdf Recieved...
Message
This Is From Intruder Port
OK
Exit

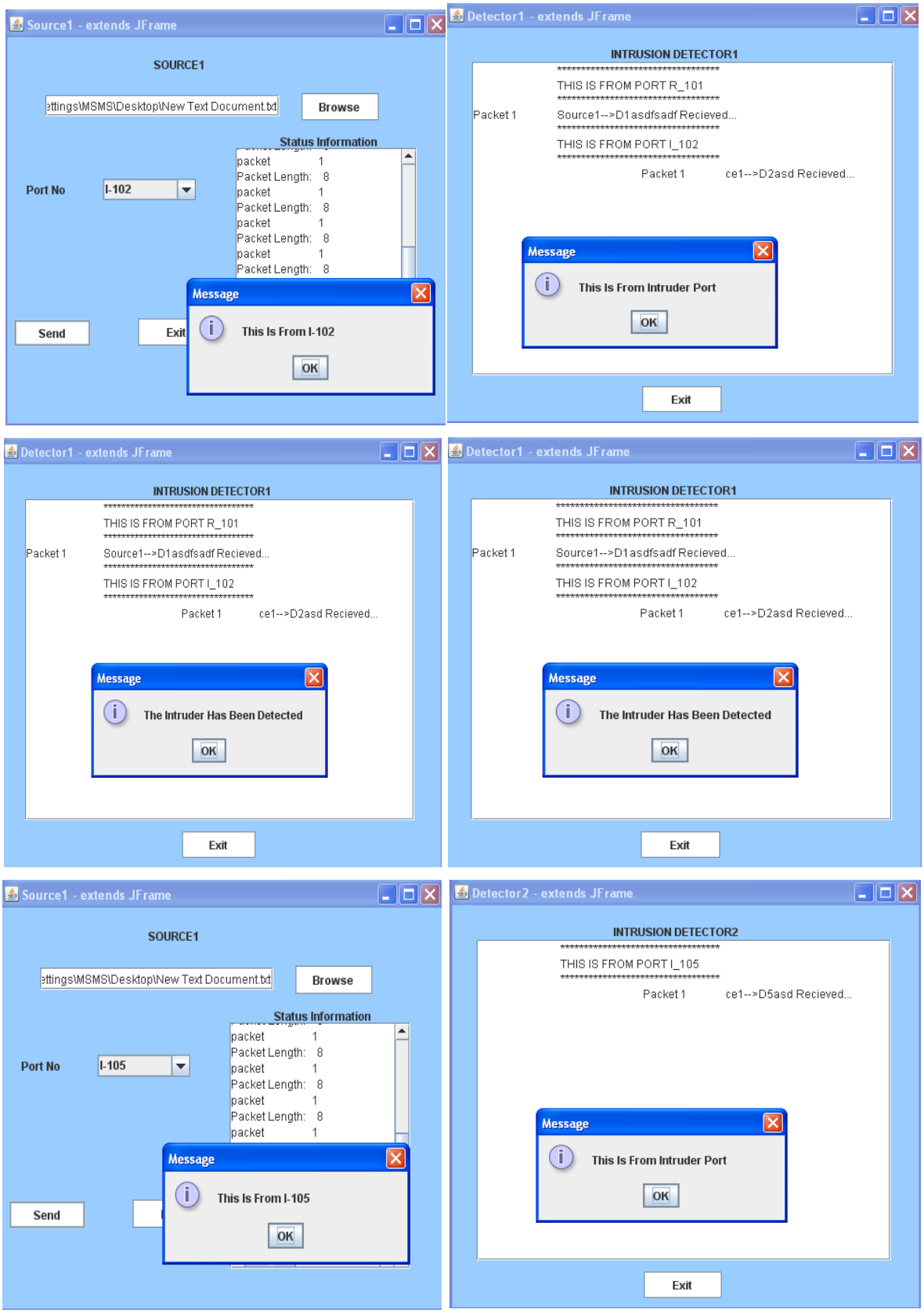

Detector - extends JFrame
INTRUSION DETECTOR
THIS IS FROM PORT I_104
Packet 1 ce-->D4asdf Recieved...
Message
The Intruder Has Been Detected
OK
Exit

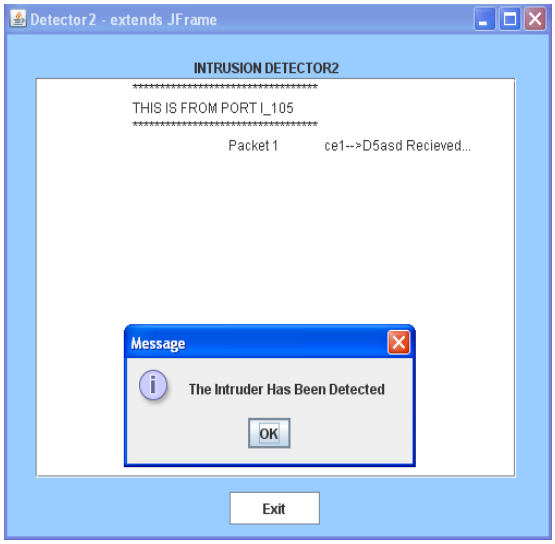

Source1 - extends JFrame
SOURCE1
ettings\MSMS\Desktop\New Text Document.txt
Browse
Status Information
Port No
R-101
Select
R-101
I-102
R-103
R-104
I-105
Source1 Address::C:\Documents a
Selected File Path C:\Documents a
Total Length::8
Packet Length: 8
packet 1
Send
Exit

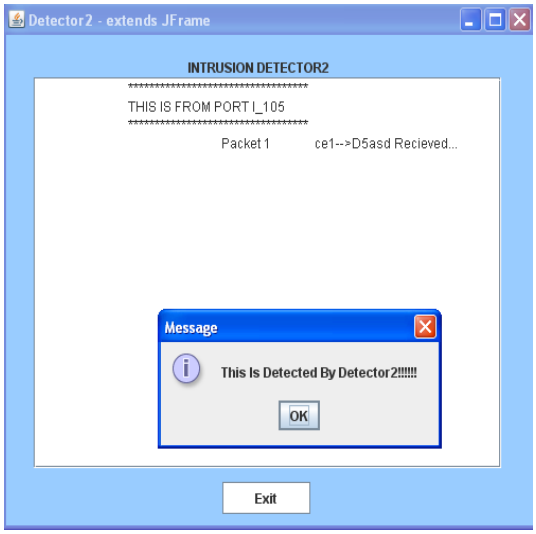

Source1 - extends JFrame
SOURCE1
ettings\MSMS\Desktop\New Text Document.txt
Browse
Status Information
Port No
R-101
Source1 Address::C:\Documents a
Selected File Path C:\Documents a
Total Length::8
Message
This Is From R-101
OK
Send
Exit

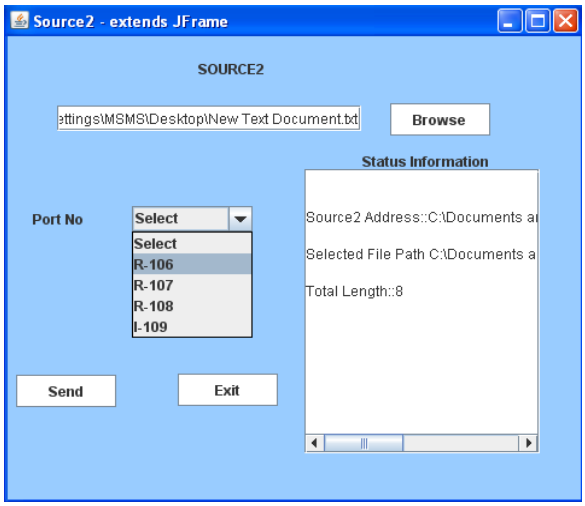

Detector1 - extends JFrame
INTRUSION DETECTOR1
THIS IS FROM PORT R_101
Packet 1 Source1-->D1asdfsadf Recieved...
Exit

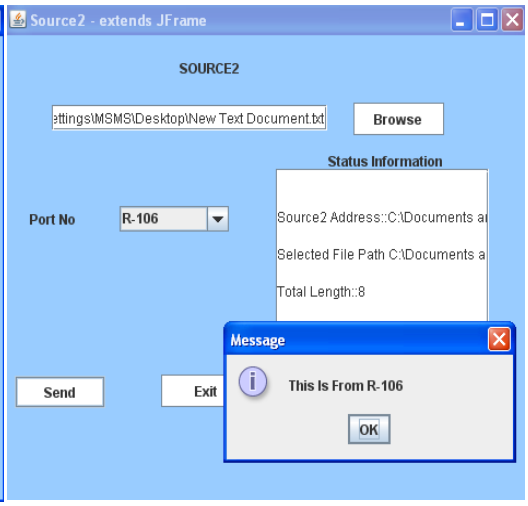

Sink1 - extends JFrame
Sink1
Dest1
Dest2
**********THIS IS FROM PORT R_101**********
Packet 1 Source1-->D1asdfsadf Recieved...
Exit

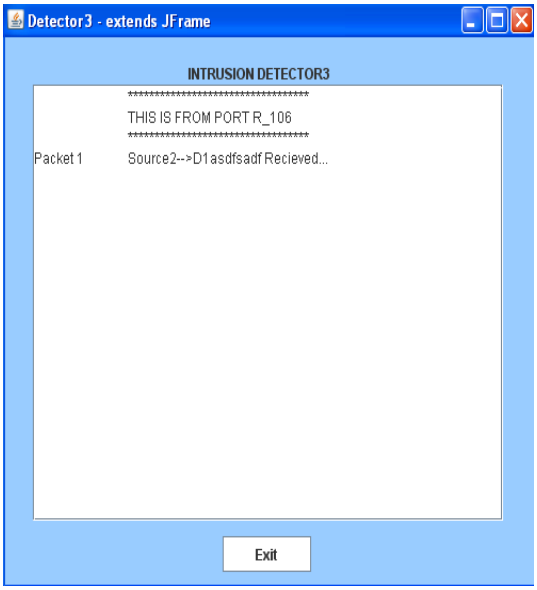

Source1 - extends JFrame
SOURCE1
ettings\MSMS\Desktop\New Text Document.txt
Browse
Status Information
Port No
I-102
packet 1
Packet Length: 8
Send
Exit
Message
This Is From I-102
OK
Detector1 - extends JFrame
INTRUSION DETECTOR1
THIS IS FROM PORT R_101
Packet 1 Source1-->D1asdfsadf Recieved...
THIS IS FROM PORT I_102
Packet 1 ce1-->D2asd Recieved...
Message
This Is From Intruder Port
OK
Exit
Detector1 - extends JFrame
INTRUSION DETECTOR1
THIS IS FROM PORT R_101
Packet 1 Source1-->D1asdfsadf Recieved...
THIS IS FROM PORT I_102
Packet 1 ce1-->D2asd Recieved...
Message
The Intruder Has Been Detected
OK
Exit
Detector1 - extends JFrame
INTRUSION DETECTOR1
THIS IS FROM PORT R_101
Packet 1 Source1-->D1asdfsadf Recieved...
THIS IS FROM PORT I_102
Packet 1 ce1-->D2asd Recieved...
Message
The Intruder Has Been Detected
OK
Exit
Source1 - extends JFrame
SOURCE1
ettings\MSMS\Desktop\New Text Document.txt
Browse
Status Information
Port No
I-105
packet 1
Packet Length: 8
Send
Message
This Is From I-105
OK
Detector2 - extends JFrame
INTRUSION DETECTOR2
THIS IS FROM PORT I_105
Packet 1 ce1-->D5asd Recieved...
Message
This Is From Intruder Port
OK
Exit

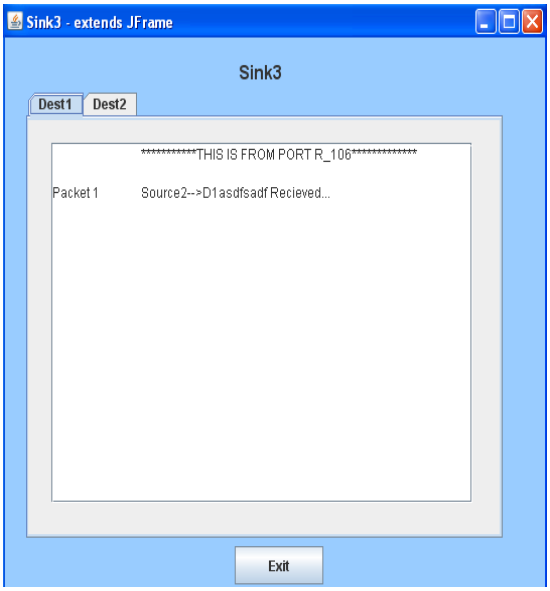

Detector2 - extends JFrame
INTRUSION DETECTOR2
THIS IS FROM PORT I_105
Packet 1 ce1-->D5asd Recieved...
Message
The Intruder Has Been Detected
OK
Exit


Detector2 - extends JFrame
INTRUSION DETECTOR2
THIS IS FROM PORT I_105
Packet 1 ce1-->D5asd Recieved...
Message
This Is Detected By Detector2!!!!!!
OK
Exit


Source2 - extends JFrame
SOURCE2
ettings\MSMS\Desktop\New Text Document.txt
Browse
Status Information
Port No
Select
Select
R-106
R-107
R-108
I-109
Source2 Address::C:\Documents a
Selected File Path C:\Documents a
Total Length::8
Send
Exit


Source2 - extends JFrame
SOURCE2
ettings\MSMS\Desktop\New Text Document.txt
Browse
Status Information
Port No
R-106
Source2 Address::C:\Documents a
Selected File Path C:\Documents a
Total Length::8
Message
This Is From R-106
OK
Send
Exit


Detector3 - extends JFrame
INTRUSION DETECTOR3
THIS IS FROM PORT R_106
Packet 1 Source2-->D1asdfsadf Recieved...
Exit


Sink3 - extends JFrame
Sink3
Dest1
Dest2
**********THIS IS FROM PORT R_106**********
Packet 1 Source2-->D1asdfsadf Recieved...
Exit

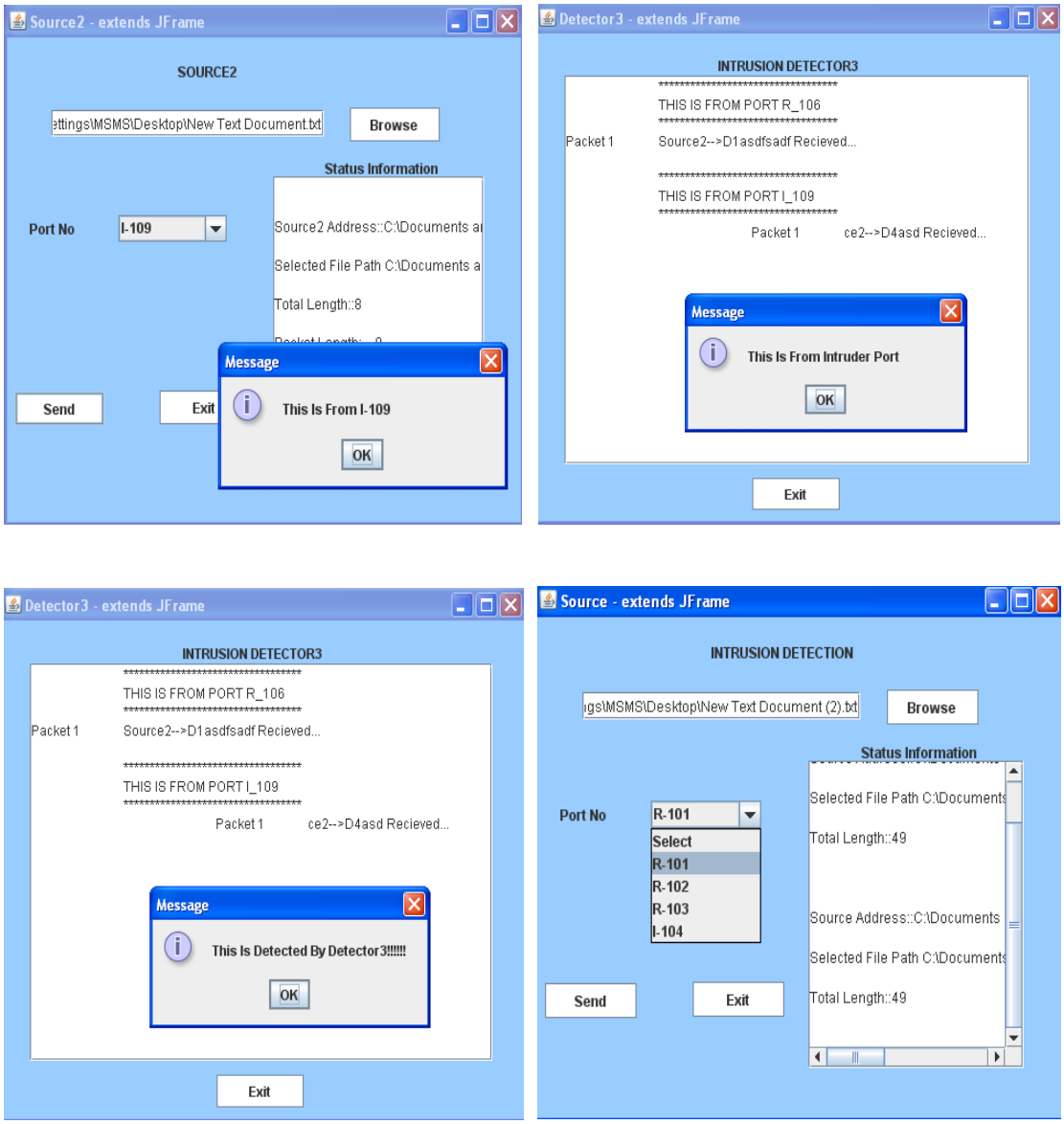


Figure 6. Simulated Results (Screen shots)

CONCLUSIONS

In the present research work we have designed and implemented an Attacker Evidence system (AAEDS) as a simple network security measure in a wireless networks system considering both a homogeneous and heterogeneous structures. Also we considered the two sensing detection models: single-sensing detection and multiple-sensing detection. The implemented security measure scheme and its simulated results have been presented and discussed. From Table-1 and Table-2, it is evident that the AAEDS is working as per the expectations. The attacker is being detected and reported properly. The screening of the packets from unauthorized ports and at the same time allowing the valid packets to the receiver are also executed as per the expectations. Thus the present AES can be useful to send information in a secured manner through the WSN. By using multiple sensors network in the present scheme we could not only detect the presence of malicious elements but also preventing the attacks by filtering and discarding them. A comparison can be done from the results for both homogeneous and heterogeneous WSNs in terms of attacker detection and it is inferred that the mechanism is more effective in later one. Thus the present Anomalous Attacker Evidence and Detection System (AAEDS) shows the existence of the attacker and also prevents the attack and in turn acts as security measure for a wireless network system which is the objective of the present research work. In scope, the present AAEDS may be a proto-type, but the simulation can be extended to study intrusion detection probability within a certain intrusion distance under various application scenarios. The model can be further improved for a larger and more realistic WSN by characterizing attacker detection probability with respect to the intrusion distance and the network parameters like node density, sensing range, transmission range etc. The model can be further enhanced for attacker/hacker /intrusion detections in internet applications and parallel computer interconnection networks.

ACKNOWLEDGEMENTS

B. Srinivasa Rao is very much thankful to Dr. L. Pratap Reddy, Professor, Department of ECE, JNTUH, Hyderabad, for his valuable suggestions. Also thankful to the Management of GRIET for their encouragement and cooperation for pursuing his Ph.D. work.

REFERENCES

[1]. Garret, C. :Importance of Security Policy, https://www.slideshare.net (2012) 11380022

[2]. https://www.uniassignment.com/essay-samples/information-technology/importance-of-information-security-in-organizations-information-technology-essay.php (2017)

[3]. New firewall can protect your phone from security threat, e-paper: http:// www.deccanchronicle.com /technology/in-other-news/060717 (2017)

[4]. http://searchitoperations.techtarget.com/definition/hardware-security (2017)

[5]. https://www.itgovernance.co.uk/shop/category/information-security 2017

[6]. https://en.wikipedia.org/wiki/Network_security

[7]. Stallings, W. :Cryptography and Network Security-Principles and Practices, ed.4, Pearson Education (2006)

[8]. Stallings, W. : Data and Computer Communications, ed.5,, PHI, (1999)

[9]. Forouzan, B. A. : Cryptography and Network Security, Special Indian Edition, TMH (2007)

[10]. Forouzan, B. A. :TCP/IP Protocol Suite, TMH (2000)

[11]. Kisielnicki, A. and Sroka, H. :Systemy informacyjne biznesu, Warszawa: Placet, S. 17 (ISBN 83-85428-94-1) (2005)

[12]. Wawak, S.: The importance of information security management in crisis prevention in the company, Proc. Of ISBAGECC-2017 http://www.academia.edu/1649676 (2017)

[13]. Alrajeh, N. A., Khan, S. and Shams, B. :A Review - Intrusion Detection Systems in Wireless Sensor Networks, Int. J. of Distributed Sensor Networks, vol. 2013, pp 1-9, (2013) http://dx.doi.org(10.1155/2013/304628)

[14]. www.vidhatha.com

[15]. research.ijcaonline.org

[16]. connection.ebscohost.com

[17]. Agrawal, D.P. and Zeng, Q. A. :Intrusion Detection in Wireless Ad-Hoc Networks in :Introduction to wireless and mobile systems, Ed.4, pp28, (2014)

[18]. Sharma, U. and Bahl, N. :A Review on Security Issues and Attacks in Wireless Sensor Networks, Int. J. Adv. Res. In Comp. Sci.(IJARCS), vol 8, 4, pp387-391(2017)

[19]. www.hindavi.com

[20]. Wireless Sensor Networks: A Networking perspective, Eds. Zheng, J. and Jamalipour, A. Jhon Wiley (2009) (and the references therein).

[21]. Butun, I, Morgera, S.D. and Ravishankar : A Survey of Intrusion Detection System in Wireless Sensor Networks, IEEE Communications Surveys & Tutorials, 16(1) (2014)

[22]. Simenthy, J.R. and Vijayan, K. :Advanced Intrusion Detection System for Wireless Sensor Networks, IJAREEIE, vol.3, 3, pp167-172(2014)

[23]. Amita, G. and Subir, H. :A Survey on Energy Efficient Intrusion Detection in Wireless Sensor Networks, JAISE, vol. 9, 2, pp239-261 (2017)

[24]. Mitche, R. and Chen, I. R. : A Survey on Intrusion Detection in Wireless Sensor Network Applications, Computer Communications, 42, pp 1-23 (2014)

[25]. Singh, J. and Thaper, V. : Intrusion Detection System in Wireless Sensor Networks, IJCSCE,vol.1, 2 (2012)

[26]. Kamaev, A., Finogeev, A. G., Finogeev, A.A. and Parygin, D .S., J.Phys. Conference series, 803,1 (2017)

[27]. Sathya, D. and Krishneswari, K. : A Novel Cross Layer Rule Based Intrusion Detection System to Detect the Attacks Coming from Different Layers in WSN", http://nopr.niscair.res.in/handle/123456789/34052 (2016)

[28]. Yarvis, M., Kushalnagar, N., Singh, H., Rangarajan, A., Liu, Y. and Singh, S. :Exploiting Heterogeneity in Sensor Networks, AK Press, ed.5, vol.8 (2007)

[29]. Wang, X., Yoo, Y., Wang, Y. and Agrawal, D.P. :Impact of Node Density and Sensing Range on Intrusion Detection in Wireless Sensor Networks, ECW Press,ed.6, vol.2 (2006)

[30]. www.ijcsit.com; 1000projects.org; www.ijetr.org; www.ukessays.com; www.jpinfo.org; www.rroij.com; etd.ohiolink.edu; forums.havenworld.co.uk; www.ijrte.org; theglobaljournals.com;