ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

BLOCKING OF EAVESDROPPING ATTACK IN THE INDUSTRIAL WIRELESS SENSOR NETWORKS

G.Sivaramasubramanium[1], G.Amsaleka[2], S. Aswin Paul[2], A.Gokulavani[2], S.Keerthana[2]
Assistant Professor[1], Final Year Students[2],
Department Of ECE,
Erode Builder Educational Trust's Group of Institutions,
Kangayam, Tirupur.

Abstract:

Blocking of Eavesdropping attack from data hacking process has attracted considerable attention from the communities of privacy security and protection. In existing system, all attackers are not based upon IP monitoring system and there is no noise aided security to collapse the hacker. So it is easy to crack the data within a short duration. In the proposed system we include IP monitoring system and secret keys to hide the data. In this method Advanced Encryption Standard (AES) algorithm is used for bitwise encryption technique which will be secure for encryption. So it is very complex to hack the encrypted data. Encrypted hidden data is generated using data hiding key. So, it will be very easiest method to block the eavesdropper.

Keyword: *Eavesdropping attack, IP monitoring method, AES algorithm, Encryption technique and cryptographic key.*

1.Introduction:

Wireless network security issues continue to make current headlines attention has been drawn away from the fact that wired networks are often affected by many of the same weakness. Eavesdropping attacks are insidious, because it's very difficult to know where they are occurring. So we use IP based monitoring system to get the warning signal to block the attacker from the predefined authenticated node design. Cryptographic encryption technique is used to encrypt the plaintext and AES algorithm is used to protect the encrypted data using secret key generation and to send information to destination safely.

Wireless sensor networks (WSNs) were initially motivated by the military for battlefield surveillance [1], and now are further developed for various industrial applications such as the assembly line monitoring and manufacturing automation for the sake of improving the factory efficiency, reliability, and productivity [2], [3], which are referred to as the industrial WSNs [4]-[6]. In industrial WSNs, due to the broadcast nature of radio propagation, the wireless medium is open to be accessed by both authorized and unauthorized users, leading WSNs to be more vulnerable to the eavesdropping attack than wired sensor networks , where communicating nodes are physically connected with wire cables and a node without being connected is unable to access for illegal activities. Therefore, it is of importance to investigate the protection of industrial WSNs against the eavesdropping attack.

2.Eavesdropping Attack:

Eavesdropping is the unauthorized real time interception of a private communication, such as a phone call, instant message, video conference or fax transmission. Eavesdropping is an electronic attack where digital communications are intercepted by an individual whom they are not intended, it is the act of intercepting communications between two points. In the digital world, Eavesdropping takes the form of sniffing for data in what is called network eavesdropping. A specialized program is used to sniff and record packets of data communications from a network and then subsequently listen to (or) read using cryptography tools for analysis and decryption.

Actual eavesdropping that is the simple act of listening to the other people talk without then knowing it, can be done using current technology such as hidden microphones and records. Hacking into devices such as IP phones is also done in order to eavesdrop on the owner of the phone by remotely activating the speaker phone function. For example, "e-mail" if the sender has not encrypted the e-mail message and has not used digital signature the attacker can exploit security loop holes on the network to launch the eavesdropping attack.

3.Advanced Encryption Standard Algorithm (AES):

Advanced version of data encryption and it is a symmetric key encryption algorithm. To overcome the disadvantage of DES algorithm we move to AES. AES cipher has block length of 128 bit. Key size is independently specified to 128,192, or 256 bits.AES parameters N_b = number of columns in the state, N_k= number of 32 bit words in the key $N_{r=}$ Number of rounds.AES methods convert to state array, transformation, key expansion.

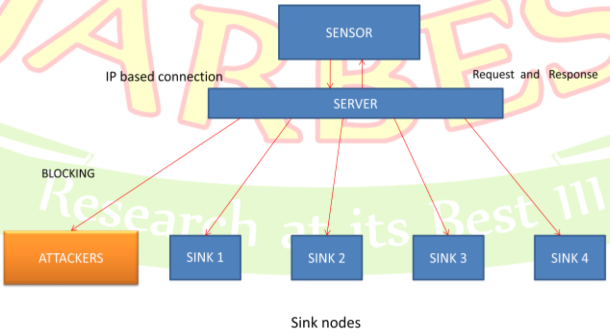
Encryption technique: Encryption is a great defense against eavesdropping. By only using applications and systems which use strong encryption, you can make an attacker's life far more difficult. But it isn't a panacea, for a couple of reasons. First, we continue to see a dual pronged attack against encrypted data. Faster PC's reduce the time of an attacker needs to crack a password , cracking technologies, such as rainbow tables can reveal password in seconds.

4.Cryptographic Key:

The term Cryptography means "secret writing". An encryption algorithm transforms the plain text into cipher text, a decryption algorithm transforms cipher text into plain text. Sender sends the information in the form of plain text it is encrypted as the cipher text and decrypted as a original message called plain text to the receiver. Cipher is used to different categories of algorithms in cryptography.

Cryptography is divided into two groups: Symmetric key and Asymmetric key. Symmetric key is a secret key and asymmetric key is a public key. In symmetric key cryptography the same key is used by the sender and receiver. In asymmetric key different key is used by the sender and receiver.

5.Block Diagram:



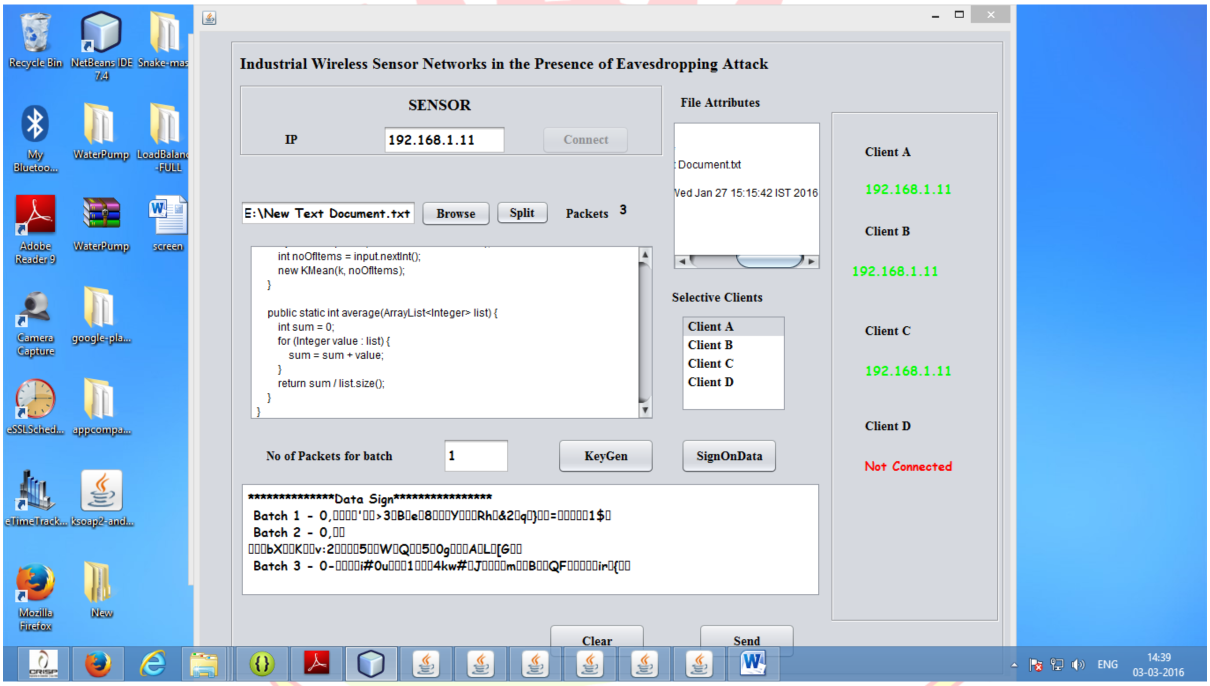
6.Software requirements:

Operating System	: Windows
Simulator Tool	: Net Beans 7.2.1
Language	: Java
Development Kit	: JDK1.7
Platform	: Independent

7.Simulation output :

In this project, we are using a NetBeans IDE 7.2.1 software for designing a layouts. The designing of layouts includes labels, text fields, text areas, buttons and panels.The layouts for Sensor node, Monitoring node, Sink nodes and Hacker node were designed and coded by "JAVA" language.

SENSOR NODE



IP 192.168.1.11

E:\New Text Document.txt Packets 3

: Document.txt
Ved Jan 27 15:15:42 IST 2016

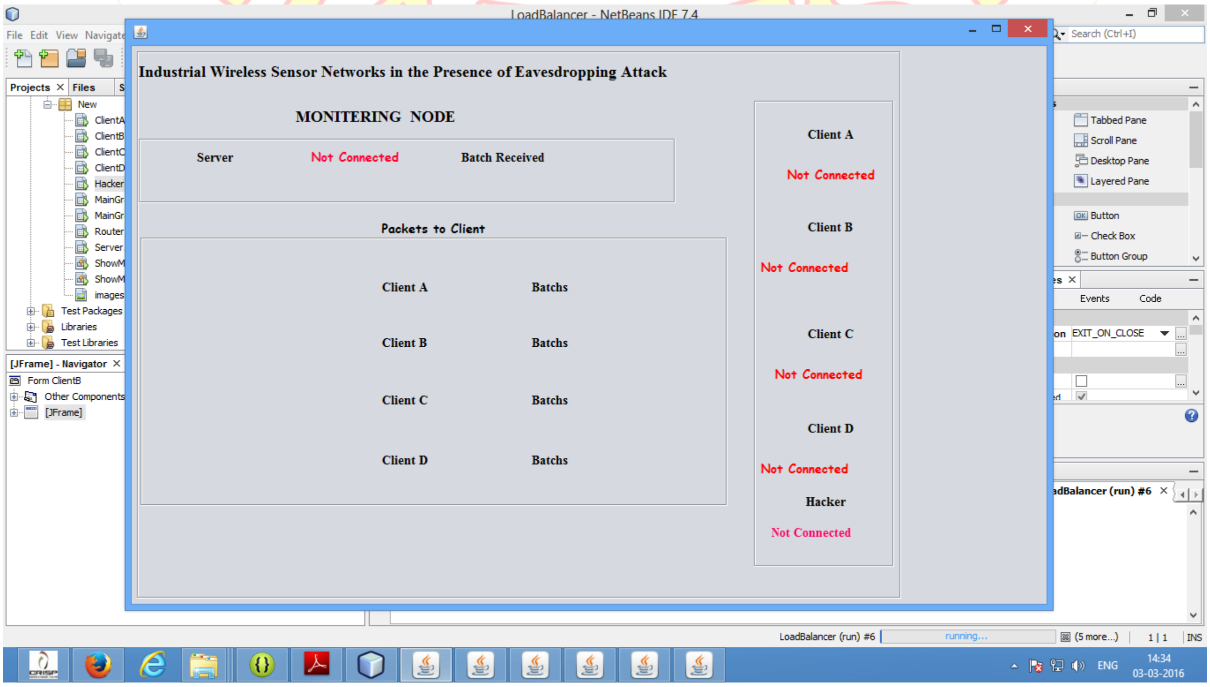
```
        int noOfItems = input.nextInt();
        new KMean(k, noOfItems);
    }

    public static int average(ArrayList<Integer> list) {
        int sum = 0;
        for (Integer value : list) {
            sum = sum + value;
        }
        return sum / list.size();
    }
}
```

No of Packets for batch 1

```
**************Data Sign****************
 Batch 1 - 0,□□□□'□□>3□B□e□8□□□Y□□□Rh□&2□q□}□□=□□□□□1$□
 Batch 2 - 0,□□
□□□bX□□K□□v:2□□□□5□□W□Q□□5□0g□□□A□L□[G□□
 Batch 3 - 0-□□□□i#0u□□□1□□□4kw#□J□□□□m□□B□□QF□□□□□ir□{□□
```

Client A 192.168.1.11
Client B 192.168.1.11
Client C 192.168.1.11
Client D Not Connected

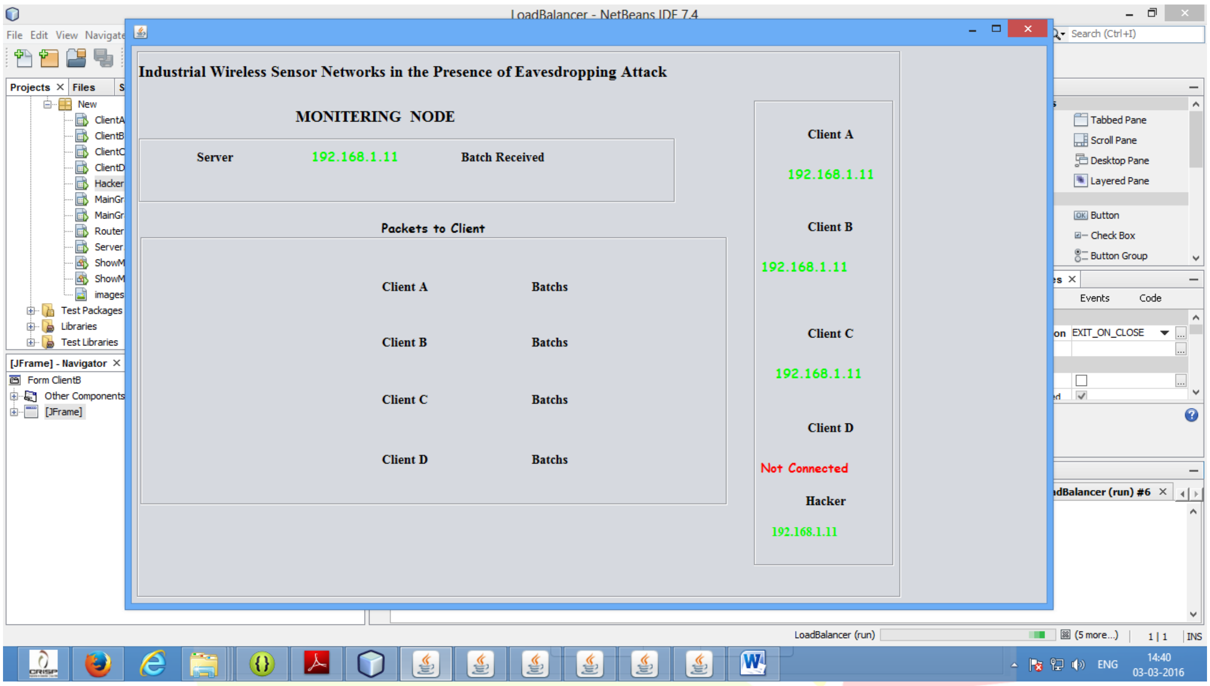
MONITOR NODE:



Server Not Connected

Client A Not Connected
Client B Not Connected
Client C Not Connected
Client D Not Connected
Hacker Not Connected

CONNECTED DETAILS:



Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack

MONITERING NODE

Server 192.168.1.11 Batch Received

Packets to Client

Client A	Batchs
Client B	Batchs
Client C	Batchs
Client D	Batchs

Client A
192.168.1.11

Client B
192.168.1.11

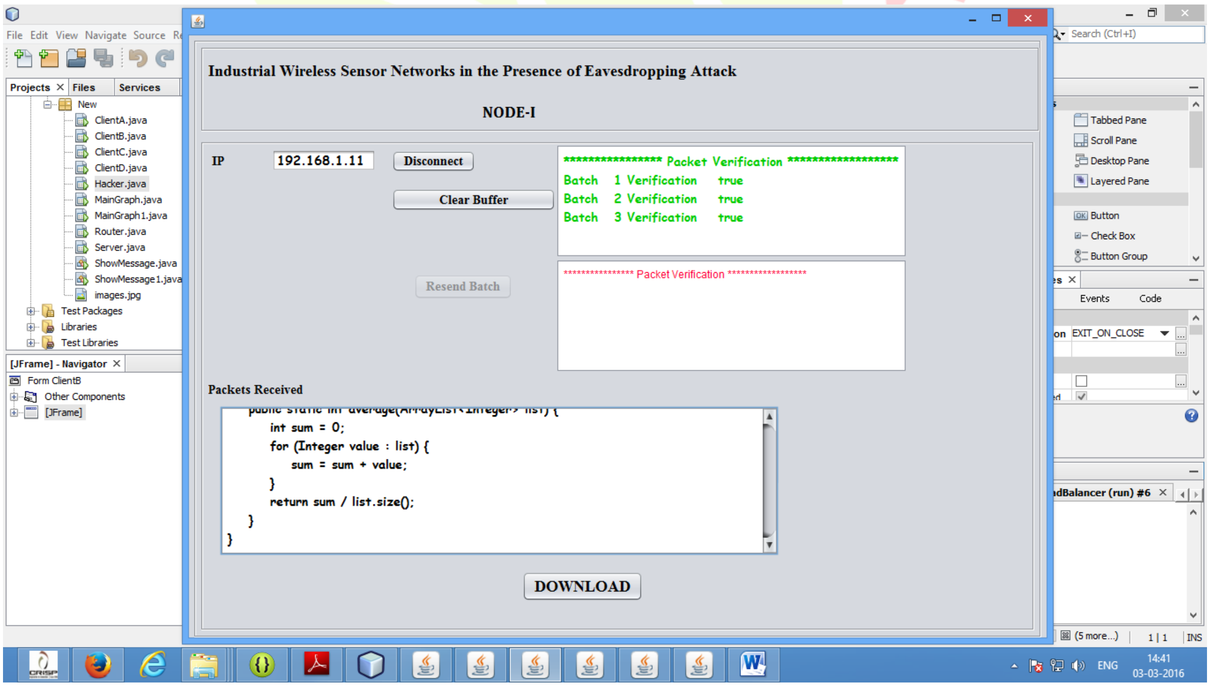
Client C
192.168.1.11

Client D
Not Connected

Hacker
192.168.1.11

NODE 1:

RECEIVE THE PACKET



Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack

NODE-I

IP 192.168.1.11 Disconnect

Clear Buffer

Resend Batch

```
***************** Packet Verification *******************
Batch   1 Verification    true
Batch   2 Verification    true
Batch   3 Verification    true
```

```
*************** Packet Verification *****************
```

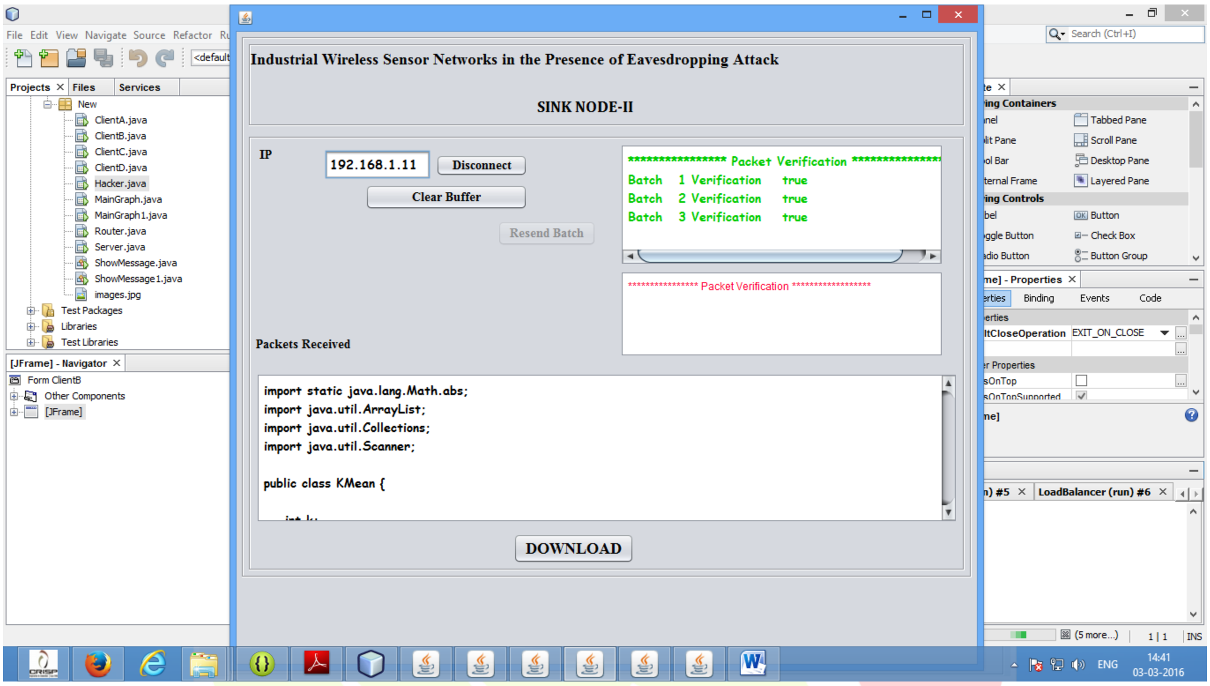
Packets Received

```
    public static int average(ArrayList<Integer> list) {
        int sum = 0;
        for (Integer value : list) {
            sum = sum + value;
        }
        return sum / list.size();
    }
}
```

DOWNLOAD

NODE2:

RECEIVE THE PACKET



Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack

SINK NODE-II

IP 192.168.1.11

```
**************** Packet Verification ****************
Batch  1 Verification   true
Batch  2 Verification   true
Batch  3 Verification   true
```

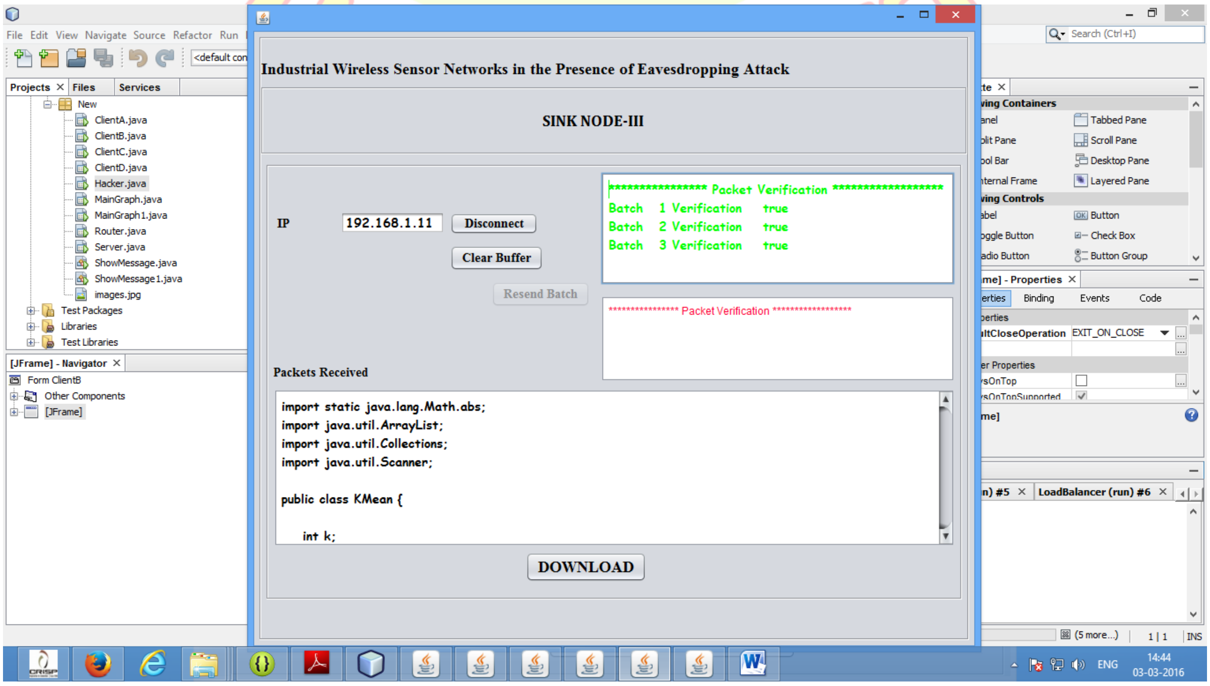
```
*************** Packet Verification ******************
```

Packets Received

```
import static java.lang.Math.abs;
import java.util.ArrayList;
import java.util.Collections;
import java.util.Scanner;

public class KMean {
```

NODE 3:

RECEIVE THE PACKET



Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack

SINK NODE-III

IP 192.168.1.11

```
**************** Packet Verification ******************
Batch  1 Verification   true
Batch  2 Verification   true
Batch  3 Verification   true
```

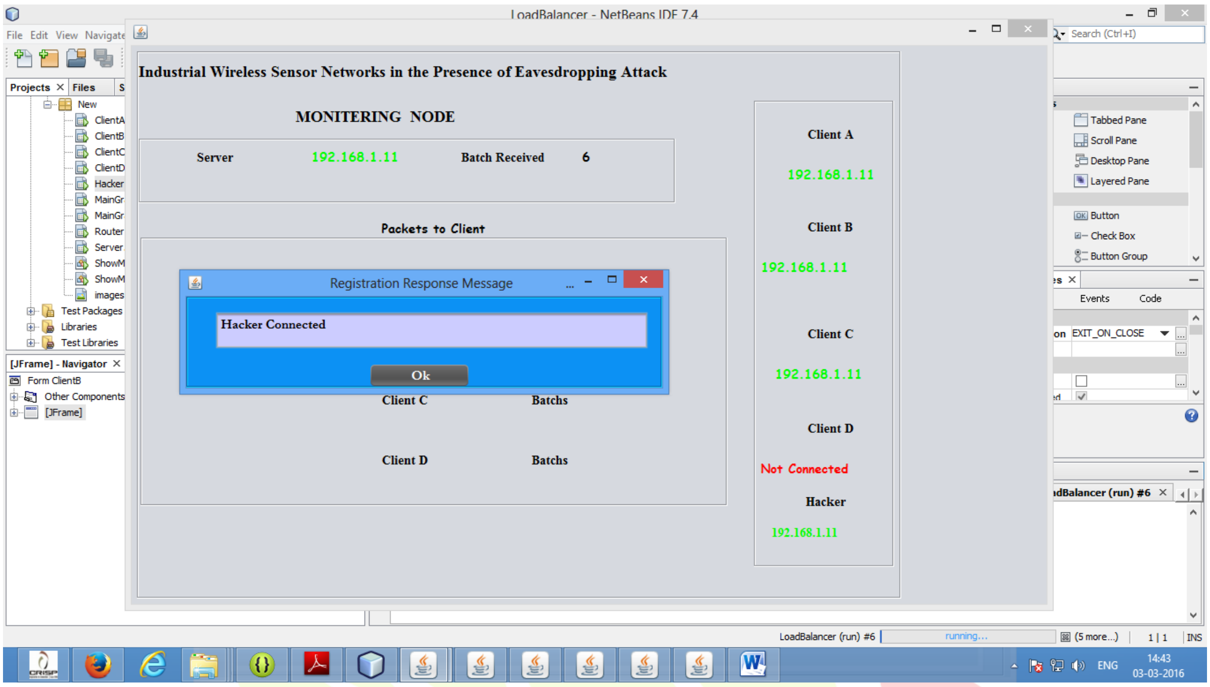
```
*************** Packet Verification ******************
```

Packets Received

```
import static java.lang.Math.abs;
import java.util.ArrayList;
import java.util.Collections;
import java.util.Scanner;

public class KMean {

    int k;
```

8.EXPECTED OUTPUT:

HACKER INFORMATION VIEW MONITER NODE



Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack

MONITERING NODE

Server 192.168.1.11 Batch Received 6

Packets to Client

Registration Response Message

Hacker Connected

Ok

Client C Batchs

Client D Batchs

Client A 192.168.1.11

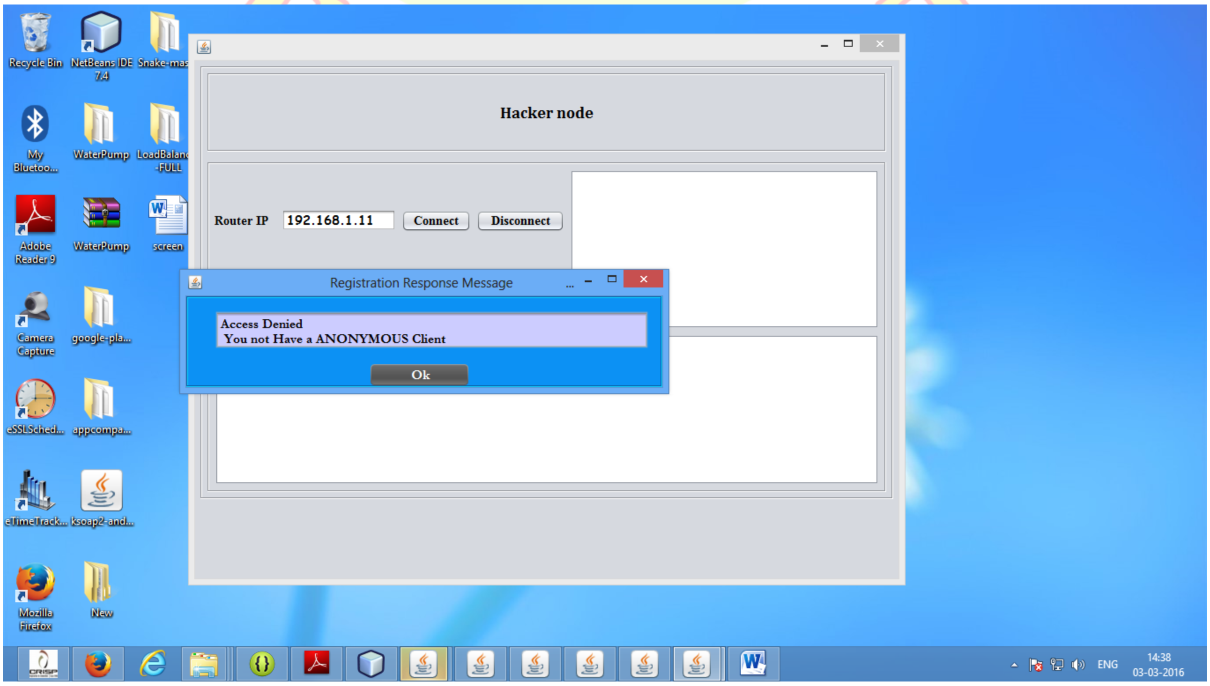
Client B 192.168.1.11

Client C 192.168.1.11

Client D Not Connected

Hacker 192.168.1.11

HACKER NODE BLOCK



Hacker node

Router IP 192.168.1.11 Connect Disconnect

Registration Response Message

Access Denied
You not Have a ANONYMOUS Client

Ok

9.CONCLUSION:

In this paper, we propose an AES (Advanced Encryption Standard) algorithm for text encryption and decryption of wireless transmissions from sensor to the sink nodes. AES algorithm is more secure to transfer files from sensor to sink nodes. And also IP monitoring is provided to block the Eavesdropping attack. IP provides the end to end communications between nodes. By IP monitoring we can identify what are all the nodes are connected to the server and how much amount of packets are have been receiving to the sink nodes from sensor. We can easily block the attacker by IP monitoring.

10.REFERENCE:

[1]. C. E. Shannon, “Communication theory of secrecy systems,” Bell System Technical Journal, 1949.

[2]. W. Shen, T. Zhang, F. Barac, and M. Gidlund, “PriorityMAC: A priorityenhanced MAC protocol for critical traffic in industrial wireless sensor and actuator networks,” IEEE Trans. Industrial Informatics, Feb. 2014.

[3]. J.-C. Wang, C.-H. Lin, E. Siahaan, B.-W. Chen, and H.-L. Chuang, “Mixed sound event verification on wireless sensor network for home automation,” IEEE Trans. Industrial Informatics, vol. 10, no. 1, pp. 803-812, Feb. 2014.

[4]. T. M. Chiwewe and G. P. Hancke, “A distributed topology control technique for low interference and energy efficiency in wireless sensor networks,” IEEE Trans. Industrial Informatics, vol. 8, no. 1, pp. 11-19, Feb. 2012.

[5]. P. T. A. Quang and D.-S. Kim, “Enhancing real-time delivery of gradient routing for industrial wireless sensor networks, ” IEEE Trans. Industrial Informatics, Feb. 2012.

[6]. M. Cheminod, L. Durante, and A. Valenzano, “Review of security issues in industrial networks,” IEEE Trans. Industrial Informatics, vol. 9, no. 1, pp. 277-293, Feb. 2013.

[7]. “Amit Kumar Mishra”, “Text and Image Encryption Decryption Using Advanced Encryption Standard ”, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 3,May -June 2014.