DOS ATTACK DETECTION IN WIRELESS NETWORKS USING RINJINDAEL ALGORITHM

S GOMATHI[#1], *PG-STUDENT MUTHAYAMMAL ENGINEERING COLLEGE,*
gomkct@gmail.com
N ANANDH[*2] *ASSISTANT PROFESSOR, MUTHAYAMMAL ENGINEERING COLLEGE*
anandhme1983@gmail.com
SHERIN DOMINIC[#3] *PG- STUDENT MUTHAYAMMAL ENGINEERING COLLEGE,*
sherindominic@gmail.com

[#]DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, ANNA UNIVERSITY CHENNAI

MUTHAYAMMAL ENGINEERING COLLEGE, RASIPURAM=637 408, NAMAKKAL DT., TAMIL NADU, INDIA.

[*]DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, ANNA UNIVERSITY CHENNAI

MUTHAYAMMAL ENGINEERING COLLEGE, RASIPURAM=637 408, NAMAKKAL DT., TAMIL NADU, INDIA.

ABSTRACT

The current trend in wireless network is to share important data among the nodes in that network. There are several off-the shelf components that help in stopping this sharing of vital data through the process called jamming. Jamming is simply the cause of a Denial of Service attack. A simple example of this process is when a malicious node can transmit a lot of data to a particular node in the network to stop the reception of data sent by another legitimate node in the network. There are several other types of jamming like radio signal jamming, continual transmission of interference signal, etc. while we deal with data jamming. Here we provide a system with several nodes connected through Wi-Fi and an illegitimate node sends lot of data to stop the communication of the legitimate nodes in the network. This system consists of technique to provide non-interrupted transmission between the legitimate nodes and to protect data during transmission through encryption and to provide e-mail notification about the jamming node.

KEYWORDS

Wireless Denial of Service, Jamming, Encryption, e-mail notification, security.

1. INTRODUCTION

In recent days, security has been a priority during the transmission of data in wireless network, be it through adhoc, Wi-Fi or wireless sensor network (WSN). This is because of the existence of hacking and other malicious activities that occur just like any other common day-to-day routine. Due to the progress in technology, wireless networks are coming into existence as they've become more affordable and easily accessible through the off-the-shelf components. So they are some equipment to disrupt these advancements. Since wireless networks are more accessible for the use of internet in the near past and future, it is more vulnerable to attacks than any wired network. The widely known actuality about the wireless network is its easy accessibility and sharable nature of medium. This actuality is both the pro and con when it comes to a wireless

network i.e., it is very easy for the rival to initiate an attack. This attack can be the disruption of network operations and flooding the user and kernel buffers. It is termed as Denial of service attack or jamming, depending on whether one looks at the consequence or the cause of attack. A most common example of such an attack is while browsing the internet, the page that is to be opened is not getting loaded properly and the refresh button is clicked several times than necessary. This is an example of jamming or the Denial of Service attack that is done inadvertently. This attack can also be done deliberately. For example, one can use a mobile device to send volume of SMS in hinterland. This is enough to block communication between any two wireless nodes.

In fact, it has become more like a race between the adversary to attack a network and the security experts to invent efficient methods to block the attack. The network must be capable of transmission of data between the legitimate nodes irrespective of the attack induced by the adversary. There must not be any interruption between the legitimate users. An intimation about the presence of an attacker must be given to the head of the network. It is also not ethically and morally accepted if the legitimate node/ user communicates with the attacker. At such times the node involved in such a scam must be identified and warned of any other misleading activities in the network may compromise both the network and the data.

In this paper, a real time implementation of data jamming done between two nodes in a network that must receive legitimate data from a legitimate node in the network is discussed. Bearing in mind the issues and the responses required in present day necessities, we provide a system where there can be an uninterrupted data flow between the legitimate nodes. Rinjindael encryption algorithm is provided to ensure the secure transmission of data between legitimate users. Also Simple Mail Transfer Protocol (SMTP) is used to send an e-mail notification about the presence of the jammer and also about the legitimate node's compromise of network.

Our paper is organized as follows: In section II, we discuss the related theory about the jamming and various techniques. Section III comprises of the system design and proposed system. Section IV describes about the two algorithms for encryption and e-mail transmission. Section V will conclude the paper.

2. RELATED THEORY

Denial of service attack is basically done in order to block a node from receiving legitimate data or to block the node completely from another legitimate node. This blocking can be done either with the data sent continually or by sending radio signals or by any other means of transmission signal jamming. We have several authors who have discussed about the various jamming techniques and their detection and/ or prevention techniques.

In [1], the authors, Pelechrinis K, Iliofotou M and Krishnamurthy S V, University of California have surveyed the various types of denial of service attacks and the performance issues due to the DoS attack in each network. They have provided several intrusion detection techniques in their survey and have mentioned that there must be system implementation to avoid real world adversaries. In all of the jamming techniques and the detection algorithms, throughput is 0 which effectively reduces the performance of the network.

In [2], the authors have detailed about the selective jamming where the adversary chooses the data to jam preferentially a high priority data when it concerns security and privacy. They do so by performing packet classification at the physical layer. The authors have evaluated the effects of packet hiding by measuring the effective throughput of the TCP connection in the following scenarios:

1. No packet hiding (N.H.).
2. MAC-layer encryption with a static key (M.E.).
3. SHCS (C.S.).
4. Time-lock CPHS (T.P.).
5. Hash-based CPHS (H.P.).
6. Linear AONT-HS (L.T.).
7. AONT-HS based on the package transform (P.T.).

In [3], data forwarding without any delay in the defending jamming in a wireless sensor network is proposed. This proposal consists of sensor nodes as clusters for a particular frequency. Here when a frequency where data forwarding occurs is jammed, the cluster of sensor

nodes in that frequency becomes inoperative and the other clusters act as backup.

[4] Discusses the technique of game theory. Game theory provides powerful tools to model and analyze such attacks. This article discusses a class of such jamming games played at the MAC layer among a set of transmitters and jammers. The equilibrium strategies resulting from these jamming games characterize the expected performance under DoS attacks and motivate robust network protocol design for secure wireless communications. A key characteristic of the distributed wireless access networks is that users do not have complete information regarding the other user's identities, the traffic dynamics, the channel characteristics, or the costs and rewards of other users.

Various forms of uncertainty can be present as illustrated in Fig. 2, including:

• **User types**: Users may not know each other's type, where type refers to whether a node is a transmitter or jammer.

• **Physical presence**: Users may not know whether or not the opponent is physically present to transmit.

• **Packet traffic**: Users may not know traffic dynamics of the opponent, that is, whether or not the opponent's queue is backlogged.

• **System parameters**: Users may not know each other's utilities (reward and cost functions).

• **Physical channel**: Users may not know physical channel characteristics, such as channel gains, channel noise, or packet capture probability.

In [5], there is a discussion about Rinjindael algorithm which was proposed by NIST. This algorithm is very similar to AES encryption algorithm except that the Rinjindael algorithm supports significantly larger key and also various bits of block length (128, 192 and 256) whereas in AES algorithm, the block length remains the same (128 bits).

3. SYSTEM DESIGN AND PROPOSED SYSTEM

In the proposed system, a wireless network where a few laptops that act as nodes are connected through a Wi-Fi network. This is shown in Fig.1. This system is based on the nodes that transfer data through the network and these data must not reach the intended recipient. This is the jammer's activity. The jamming node transmits large number of data to the legitimate node thereby creating buffer overflow of the legitimate user. In this system, there is no interruption in the data transmission between the legitimate nodes. The IP address of the legitimate nodes from the sender to receiver is saved in the centralized database and the receiver obtains the legitimate IP from the database. If the IP is not recognizable, then that system contains an illegitimate node (in other words a jammer causing Denial of service Attack) and the data sent from the jamming node, the time and the receiver node of this jamming attack is sent to the head of the network through e-mail using the SMTP protocol.

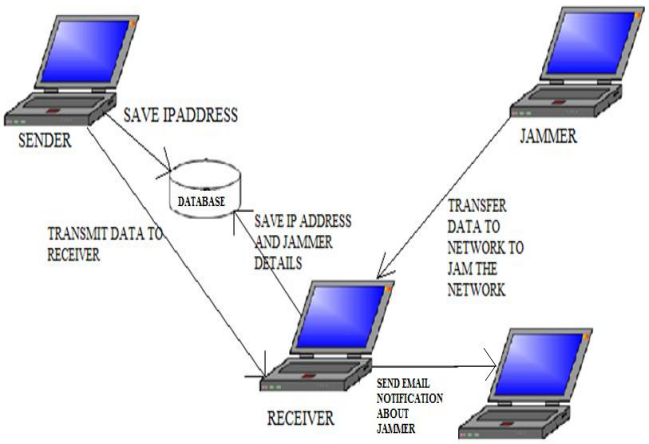

Figure 1: SYSTEM DESIGN

Also for secure data transmission between the sending and receiving node, we provide Rinjindael encryption. This ensures that even if the jamming node gets access to the data, it will be very difficult to do a decryption process without the encryption key. The block diagram of the above system is given in Fig.2. This block diagram helps in determining the nature of the proposed system along with its basic features. The system design shows the exact nodes in action whereas the block diagram shows the operation of the proposed system.

The email notification is sent through an SMTP protocol that is integrated through .net coding. This system provides an example for data jamming where the jamming device sends unwanted data to the receiving device in order to stop legitimate access. An email notification unknown to the receiving device is sent to the network head about the presence of some jamming device in the network. The database used is SQL server 2005 where the secure IP addresses are stored and the sender stores the sending and

receiving IP addresses. The receiving device checks the database for the IP address and when a data from an unknown IP has entered the network, then the jammer is detected and the information sent by the jamming device is stored separately without mixing it with the legitimate sender's data.

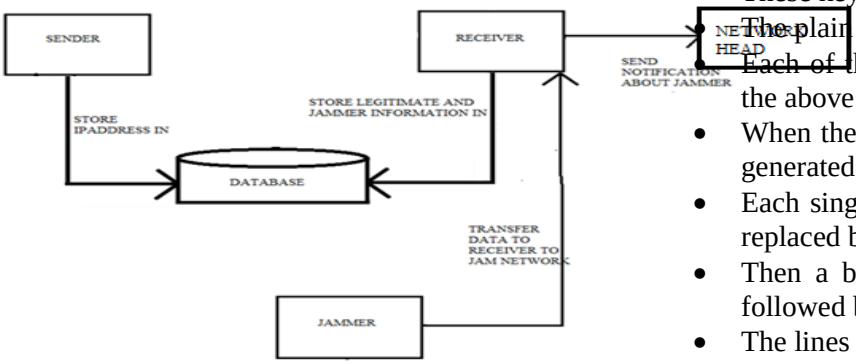

Figure 2: BLOCK DIAGRAM

In this system, there is an uninterrupted flow of data between the legitimate nodes and the jamming device cannot hinder the activities of the legitimate node. Also there might arise a concern when the jamming node sends a lot of data so that the receiving node has buffer overflow. But this concern does not arise because the data sent from the jamming device is stored separately as mentioned above that even if there is data overflow it will not affect the transmission of data through the legitimate nodes which is saved separately.

4. RINJINDAEL ALGORITHM AND SMTP

As mentioned earlier, Rinjindael encryption algorithm is used in this system to provide secure data transmission and SMTP protocol is used for email notification about the presence of an adversary node that causes the jammer.

A. Rinjindael Encryption Algorithm

The main reason behind using the Rinjindael algorithm is that it provides different block length options unlike the usual Advanced Encryption Standard (AES). This algorithm is merely an advanced version of AES algorithm with same functionality except for the block length which can vary between 128, 192 and 256 bits as required by the user. In this algorithm, the block length is kept to 128 bits and the key size is also set to 128 bits for simplicity's sake.

The number of rounds in this algorithm is 10 and in the case of 192 bit block and key size, it is 12 rounds and 256 bits, it is 14 rounds.

- In this algorithm, the single 128 bit key given by the user for data encryption is generated into 10 keys of 128 bits each.
- These keys are then placed into 4x4 arrays.
- The plain text is also placed into a 4x4 array.
- Each of this 128 bit plain text is processed in the above mentioned 10 rounds.
- When the 10th round is completed, the code is generated.
- Each single byte is substituted into S box and replaced by the reciprocal on GF (2 8).
- Then a bit-wise modulo-2 matrix is applied, followed by an XOR operation with 63.
- The lines of the matrices are sorted cyclically.
- The columns of the matrix multiplication are interchanged on GF (2 8).
- The subkeys of each round are subjected to an XOR operation.

This is the exact operation of the Rinjindael algorithm.

There is also another special reason for choosing this encryption algorithm. It is nothing but the fact that it takes 149 trillion years for a system to break a 128 bit AES key (assuming that the system could find a DES key in a second i.e., trying 255 keys in a second). Hence Rinjindael algorithm, which could use 128, 192 and 256 key and block size, would be more secure and there will not be any compromise of the data through encryption.

B. SMTP Protocol

SMTP is a mail transfer protocol used to transfer mail to different emails. It is a TCP/IP protocol that sends mail with the help of IP address and Email ids given. The mail server is set to a definite browser. In this case, it is www.gmail.com and the SMTP uses only the gmail accounts to send and receive mails. An object for the MailMessage() class is created and a subject, to address, from address and the body of the mail is added to the mail through the object. Another object for the SMTPClient() class is initialized and the host, port and the credentials are set and the mail is sent through this object.

The port id of SMTP protocol is usually 25. But for SMTP submission the port

number is 587 and it also used to initialize the SMTP protocol. The protocol for new submissions is same as the protocol for SMTP except for the port number.

The SMTP credentials is a class function that is used to get or set the username and password that helps in authenticating the sender. The Network credential() initializes a new object with the username and password that is specified in the function.

Also an IsBodyHtml() function is used to set or get values based on whether the body is in HTML format or not. To initiate the function under which the SMTP protocol is defined, the function should be called in the code in the appropriate place in order to send the e-mail messages. This e-mail message proves to be another indication for the presence of jamming device apart from the detection obtained while the receiver checks for legitimate IP address.

We can also detect the response of the receiving node in the network that helps the jamming device to compromise the network as well as data. This is also sent via an e-mail message to the network head's mail address with the IP address and the data file's name. This helps in cornering the culprit inside the network and throws the adversary who comes from outside the network and tries to infiltrate the network full of legitimate user.

```
public void sendmail(string body)
{

string eml = "networkhead@gmail.com";
MailMessage mail = new MailMessage();
mail.To.Add(eml);
mail.From = new
MailAddress("cms.automaticmail@gmail.com");
mail.Subject = "Mail Notification";
string Body = body.ToString();
mail.Body = Body;
mail.IsBodyHtml = true;
SMTPClient SMTP = new SMTPClient();
SMTP.Host = "SMTP.gmail.com";
SMTP.Port = 587;
SMTP.UseDefaultCredentials = false;
SMTP.Credentials = new
Svstem.Net.NetworkCredential("cms.automaticmail@
```

Code snippet of SMTP protocol

Above mentioned is the code snippet used to define a mail sent to an email address indicating the presence of jamming node along with the to and from address, subject and the mail body that is passed to this function sendmail().

5. CONCLUSION

This paper provides a jamming technique that is not widely used and is usually not implemented as a real time implementation. The algorithms used ensure that data is transferred in a secure manner and the presence of jammer is detected by two ways. The Rinjindael encryption algorithm takes care of security and privacy of data even if the data is compromised to the jamming node.

Since the files from a jamming device and legitimate user are saved separately in their respective folders, no confusion will arise between the data and the files and it does not get mixed up with each other.

The SMTP protocol that is used to send mail notification about the jamming node is also a useful technique to detect the presence of the jammer. It is also brought to the reader's notice that the mail sending algorithm is implemented without the knowledge of the receiver or jammer in order to provide a head start to the security personnel.

6. REFERENCES

[1] Konstantinos Pelechrinis, Marios Iliofotou and Srikanth V. Krishnamurthy(2011), "Denial of Service Attacks in Wireless Networks:The Case of Jammers" Communications Surveys & Tutorials, IEEE, vol 13: issue:2, nos 245- 257.

[2] Proano, A.; Lazos, L.;(2011) "Packet-Hiding Methods for Preventing Selective Jamming Attacks" Dependable and Secure Computing, IEEE, vol. 9 issue 1. Nos 101- 114.

[3] Ghosal, A.; Halder, S.; Mobashir, M.; Saraogi, R.K.; DasBit, S.;(feb- 28th to march 3rd 2011)" A jamming defending data-forwarding scheme for delay sensitive applications in WSN" Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference, nos 1- 5.

[4] Sagduyu, Y.E.; Berry, R.A.; Ephremides, A.;(aug 2011)" Jamming games in wireless networks with incomplete information", Communications Magazine, IEEE, vol 49, issue 8, nos 112- 118.