Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 4, April 2015, pg.886 – 892

RESEARCH ARTICLE

Detection and Prevention Jamming Attack in Wireless Communication

Ashwini Mane, Rupali Gobe, Poonam Umadikar, Namrata Gawali

Prof. M.A.Ansari

maqans@gmail.com

Department of Information Technology

JSPM's Rajarshi Shahu College of Engineering

Tathawade Pune-411033

Mailtonamrata27@gmail.com

rupaligobe2012@gmail.com

Abstract: Wireless communication uses air as a medium because of which small amount of interference remains in it. Here we have consider The adversary who is aware of all the specification of protocol which are being used in communication can perform an denial of service attack with the help of jamming the channel used in communication for exchanging the messages. Blocking the radio transmission is called as jamming. The jammer is an entity who intentionally tries to do interference with transmission and reception of messages while the communication is going on. The jammer continuously transmits the radio frequency to fill the channel used in communication so that legitimate traffic will get block. The problem of jamming is being addressed in this work. The attacker is active for short time and will only focus on targeting the data or messages with high importance .this is basically called as targeted jamming. Targeted jamming means jamming only particular part, computer or link. May be the adversary is interested in some specific portion of the victim network and attacking only these portion can proceed to further jamming.

Keyword: Targeted jamming attack, threat model, credential details of communication.

1. Introduction

Wireless networks are highly dependent on undisturbed availability of the medium used in wireless communication to connect the involved nodes. The availability will make sure that the service which is offered by one user must be available to the other user when it is expected. For example the resources must get allocated to the user whenever they are needed. As the Wireless communication uses air as a medium because of which it leads to security threats.
This communication takes place with the help of IP addresses. So the attacker who has the IP address of the user can harm the transmission, send fake messages, or jam the authorized users. Even though the Eavesdropping and sending of fake can be prevented by using various techniques but the jamming attacks are much difficult to address. The simplest example of jamming could be as follows: the attacker will continuously transmit the fake messages or multiple short jamming signals to interfere with receiving of messages.
There is an external threat model in which jamming attacks are usually considered where the attacker or jammer is not a part of network. There are various jamming strategies are available in which they transmit continuous or discrete radio signals with high power. One of them is "al-ways-on" strategy but it has multiple drawbacks. Typical anti jamming is based on various spread spectrum communication. The spread spectrum methods provide safety at bit level as they distribute bits according to the secret key which is only accessible to the authorized communicating parties. In the external threat model this technique can provide protection for wireless transmission. As wireless communication networks are specifically vulnerable to the external threat model. The Broadcast communication networks are vulnerable to internal one because all the nodes who are participating in the communication must know the secret key used to keep secure the transmission. Hence the cryptographic information can be exposed if a single receiver compromises.

So here in this paper we have shown the jamming attack under the internal threat model. We have assumed a clever attacker who knows all the confidential information and the details of protocol used in the network. The attacker will make use of his knowledge to launch jamming attack to target the messages with "high importance". For example the attacker target is sending or receiving acknowledgement in the session so that it can degrade the quality of throughput of an end to end communication.

As there are various techniques some of them are as follows. The attacker must be able to implement the "classify-then-jam" strategy before the completion of wireless transmission or reception takes place then only the attacker can launch selective jamming attack on selective nodes. The above stated strategies can be implemented either by decoding the packets once they being transmitted or by classifying the transmitted packets using various protocol semantics. In second method the jammer must be able to decode only first few bits of packet in order to recover important identifiers of packet such as packet type destination and source addresses. After the successful classification of packet the attacker must inject a sufficient amount of error bits so that the message or packet cannot be recovered at the receiver side. To implement the selective jamming attack the adversary must be aware of physical layer details as well as upper layer specific details.

2. Literature Survey

2.1 Jamming and Sensing of Encrypted Wireless Ad Hoc Networks[1].

In this paper the problem of jamming can be considered as the attacker is trying to disturb the encrypted victim ad-hoc network. so in this type of network packets with encrypted header and payload are used. Thus the attacker can not directly interrupt the communication.
Only information about packet size ,timing, sequence of packets can be used by the attacker. In order to prevent the packets from being received in ad-hoc network noise signals are transmitted continuously by the attacker. Mostly attacker concentrates on high importance messages like route request, route reply, etc.

Attacker is interested in some part of network and focus on only those parts to achieve targeted jamming. Jamming also includes identifying the victim network activities which is referred as sensing. sensing can be of two

type it may online or offline. sensor is used to identify packets in the network and also for classifying those packets using protocol conformation at the physical layer. The transport/network layer interacts with IP,TCP and UDP protocols and senses the flows and packet types which can be targeted by jamming further. Jamming service referred as jamming for specific period , jamming specific type of packets.

2.2 Mitigation of Control Channel Jamming under Node Capture Attacks [2].

Availability of service for network users in wireless networks is based on the ability of establishing and maintaining communication channels using control messages from various base stations and users. Communication channels are used to exchange control messages. An attacker with vast knowledge of the underlying communication protocol can easily mount (implement) the DOS attack by jamming such channels.

The spread spectrum techniques can be useful against such external adversary (attacker).
But, as they know the required spreading sequences can't be deterred by spread spectrum. However, with the help of different cryptographic schemes in which assignment of key takes place can be used to hide the control Channels (or messages).Use of multiple access protocols allows mobile users to share the wireless medium in the network which makes communication in mobile networks more efficient. However, to maintain the efficiency of the multiple access protocol allocation of access and resources to mobile users must be periodically updated.
For security and authentication purpose we proposed the RC6 and SPEKE algorithm.

2.3 Anti-jamming Timing Channels for Wireless Networks [8].

Wireless communication is exposed to the radio interference. Such radio interference is responsible for prevention of the communication in wireless network. Some preventive strategies have been recommended in opposition to broadband jammers. But such strategies are not that much effective and also they are expensive. An alternative for dodging or preventive strategies have been searched. Such alternatives involve the formation of a timing channel. These channels exist even in the presence of jamming. To build the timing channel failed packet reception times are used and failed packet event can be detected for the jamming. Single sender and multi-sender timing channel can be used for the construction of a low-rate overlay link-layer. To stop or halt wireless connectivity many strategies may be applied. Some network -based attacks (e.g. dissociation attacks) have been applied to disrupt wireless system. Such powerful threats can be addressed by Authentication. Certain defense (or resistive) strategies have been proposed for reconstruction network connectivity in the presence of interference.

3. Proposed System

The system will work in a set of operational functions in that firstly the user have to sign up or need to make an account in the system. The sign up window consist of personal information of the user like name, email id etc. once the sign up done successfully the user will get an acknowledgement if the user missed any of the field then he will get an error message . This falls under the part of validation. Then the user can move towards login window the user have to enter the username and password. If the user is authenticated he is being moved to next window. Here the user has to enter the name of the recipient to whom he wants to send message. 16 bit secret key will get generated by the system which is based on AES algorithm.

Fig: LOGIN

Fig: Encryption

Then the user has to browse the text file which he wants to send to the recipient. The association of the text file with the 16 bit secret key will take place this is called as encryption. After encryption the user have to move towards embedding window. In that another 16 bit secret key will get generated. The user have to browse an image file with which the output of previous form will get embed. Once user will click on embed button the embedding will get take place and will get send to the user.

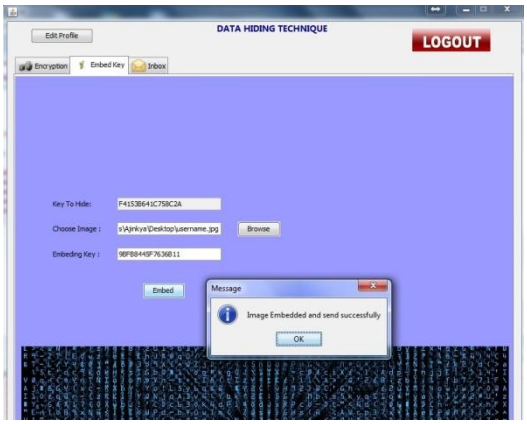

Fig: Embedding

As soon as transmission gets over the second 16 bit secret key will be send to the registered email id.

Fig: At Receiver Side

On the receiver side after successful logging the user will see the number of messages received. The user have to select the require message to download. Once he selects the message the path will get generated and in the key field user have to enter the 16 bit secret key which he has received on the email id. After that the user can download the image. If the user failed to enter correct 16 bit key then user could not download the file. For security enhancement we have included the feature to which we will called as "anti virus".

In this on the reception side after entering valid 16 bit key as soon as the user click on download button if the file contains virus then user will get a error message indicating that the image is corrupted and also provide an option to recover the file. If user wants to download the file then the system will recover the image .and then user can see the downloaded image.

Following figure shows the system Architecture: There are two images namely
Figure (A): System at transmission side.
Figure (B): System at reception side

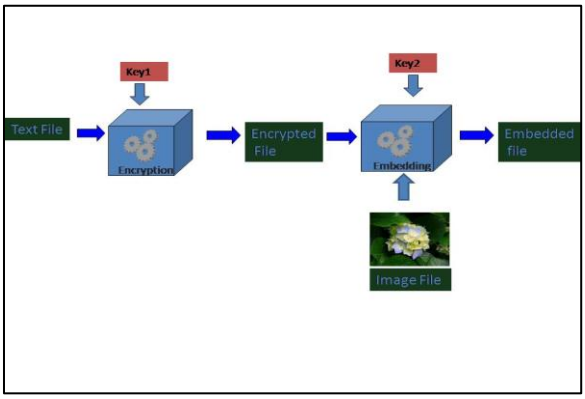

Fig (A): System at transmission side

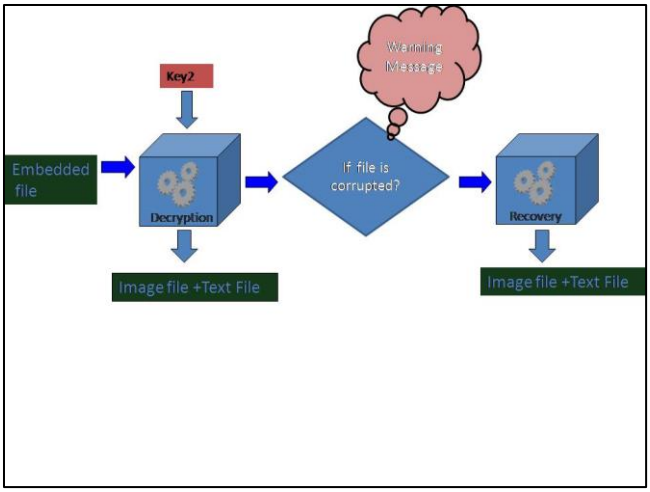

Fig (B): System at reception side

4. Algorithm Used

Advanced Encryption Standard **(AES)** is a block cipher algorithm. AES has been developed by the US. It is an extension to Data Encryption Standard. In this algorithm, same key is used for both encrypting and decrypting the data. AES uses combination of both substitution and permutation. In this algorithm a block length of 128 bits is used. Keys of different lengths 128, 192, or 256 bits are used. We have assumed that the key length is 128 bits.

In AES four steps used in each round which are Byte substitution, Shift rows, Mix columns, and Add round key. Depending on the size of key rounds can be conducted. The Encryption process consists of 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. For encryption and decryption four steps are performed in different order. 128-bit block as consisting of a 4 × 4 matrix of bytes is used. So the first column in the 4 × 4 matrix of bytes is of four bytes. Second column occupy next four bytes and so on. The 4×4 matrix of bytes is referred as the state array in AES. In each round processing takes place on input state array and output state array is generated. Four steps are explained as follows:

1) The sub Byte step: This step includes replacing of each byte in state array with a sub Byte .For doing this 8-bit substitution box is used.

2) The Shift Rows step: Shift Row operation is performed on rows of state array. In this step, bytes in each row of the state are shifted cyclically to the left. The first row is not changed. Each byte of the second row is shifted one to the left.

3) The Mix Columns step: In the step, linear transformation is used for combining the four bytes of each column of the state array. Operation is performed on four bytes of state array which affects all four output bytes.

4) The AddRoundKey step: In this step, the sub key is combined with each byte of state array. Subkey is derived from the main key for each round. By using bitwise XOR each byte of the state is combined with the corresponding byte of the sub key.

5. Conclusion

In this paper we overcome the problem of jamming attack in wireless communication. In this we have assume that the attacker knows all the credential details , network details and other protocol details which plays an important role while communication is going on. The problem of selective jamming attack is being addressed. For security enhancement we have implemented the concept of stenography. In which we hide the text file behind an image. So unless the user have authorized key he or she cannot view the file and that secret key is send to the registered email-id of the user. Another new aspect is if the user send corrupted file or virus infected file then the system will detect it and generate warning message and provide an option to recover the file.

References

[1] T.X. Brown, J.E. James, and A. Sethi, "Jamming and Sensing of Encrypted Wireless Ad Hoc Networks," Proc. ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 120-130,2006.

[2] P. Tague, M. Li, and R. Poovendran, "Mitigation of Control Channel Jamming under Node Capture Attacks," IEEE Trans. Mobile Computing, vol. 8, no. 9, pp. 1221- 1234, Sept. 2009.

[3] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Wormhole-Based Anti- Jamming Techniques in Sensor Networks," IEEE Trans. Mobile Computing, vol. 6, no. 1, pp. 100-114, Jan. 2007.

[4] A. Chan, X. Liu, G. Noubir, and B. Thapa,"Control Channel Jamming: Resilience a n d Identification of Traitors," Proc. IEEE Int'l Symp. Information Theory (ISIT), 2007.

[5] W. Xu, W. Trappe and Y. Zhang, "Anti-Jamming Timing Channels for Wireless Networks," Proc. ACM Co n f . Wireless Network Security (WiSec), pp. 203-213, 2008.

[6] R. Rivest, "All-or-Nothing Encryption and the Package Trans- form," P roc . Int'lWorkshop Fast Software Encryption, pp. 210- 218,1997.

[7] R. Rivest, A. Shamir, a n d D . Wagner, "Time Lock Pu z z l e s and Timed-Release Crypto," technical report, Massachusetts Inst. of Technology, 1996.

[8] W. Xu, W. Trappe and Y. Zhang, "Anti-Jamming Timing Channels for WirelessNetworks," Proc. ACM Co n f .WirelessNetwork Security (WiSec), pp. 203-213, 2008.

