International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137

Volume – 02, Issue – 06, June – 2017, PP – 59-63

Jamming Attacks and their Prevention in Wireless Networks

Manoj M. Chawan.

MCA Department,
DES's NMITD College, Mumbai University
Mumbai, India

Abstract: In this paper, Jamming Attacks in context of a wireless network are discussed. Wireless networks are more vulnerable to jamming attacks because of their shared wireless medium. These attacks can be easily perpetrated by an attacker by emitting radio frequency signals. they attempt to deny the user from using available network resources. Jamming attacks are dreadful Denial-of-service attacks against the wireless medium.

In this paper, Different Types of Jammers that can be used to disable the operation of wireless networks and to prevent these attacks, schemes such as Steganography, Data Hiding Schemes, DES are discussed. This paper also investigates the solutions to decrease the jamming rateas well as to reduce the effectiveness of jammer using honeypot as a contingency plan.

Keywords: Selective Jamming, DOS, Packet classification, Jammers, Steganography, All-or-Nothing Transmission, Honeypot.

I. Introduction

Transferring of information between 2 or more nodes that are physically not connected is done with the help of wireless networks. Wireless networks are vulnerable to various kinds of attacks because of its shared medium. Hence There is a need to deal with numerous security issues [1][2][4]. In the simplest form of jamming, the attacker corrupts the content or by blocks the message so that it cannot reach the intended receiver by transmitting radio signals [7]. Attackers with the right tools can easily interrupt wireless transmission, insert unwanted messages, or jam messages. Typically, jamming can be done in two forms. One is external threat model in which jammer is not part of the network. Another one is internal threat model in which jammer will be the part of the network.

Jamming is used for lowering network performance. Jamming is just one of many ways to compromise the network. an Attacker is aware of implementation details of network protocols. By using this knowledge, jammer targets the packets of high priority.An ideal jamming attacks are hard to detect, efficient, resistant to anti-jamming measures.

II. What is Jamming?

Jamming attacks are introduced by emitting radio frequency signals, such attacks are not easily preventable by regular security measures. In nutshell, jamming works by denying service to authorized users. In jamming,legal Packets are jammed by the large frequencies of illegal traffic. The issue of jamming mostly relates to older wireless LANs as they are not fully upgraded to adaptvarious new ways of interference [1].To address jamming attacks jammer should be capable of classifying packets in quick time. In order to launch jamming attacks, the feasibility of real-time packet classification is also Important. To reduce jamming attacks different techniques have been introduced such as steganography.

To reduce the effectiveness of jammer as well as to decrease the jamming rate. Honeypots techniques are also discussed.

III. Types of Jammers

Many studies have introduced jamming attacks. In a layman term jammer is an entity who is purposefully trying to interfere with transmission and reception of message across the wireless channel [7]. Jammers are categorised into four models. They are

- Constant jammer
- Reactive jammer
- Deceptive jammer
- Random jammer

A. Constant Jammer

This jammer continuously emits interference signals and it transmits random bits. It's a typical strategy of jamming. Being always-On in the transfer it won't wait for the channel to become idle. However, it has certain disadvantages, one is that continuous presence makes it easy to detect & other is, it consumes significant amount of resources

B. Deceptive Jammer

In this, jammer constantly injects series packets to the channel without any gap between subsequent transmissions [2]. It also broadcasts fabricated messages and replies old ones.

C. Random Jammer

In this, jammer switches between the period of jamming and sleep. After jamming for some time, it stops jamming and enters into sleep mode. The jammer after sleeping for some amount of time wakes up and resumes jamming. Both Timers are either random or fixed. This strategy is efficient compared to previous ones.

D. Reactive Jammer

In this, jammer will remain quiet when the channel is idle. When it senses activity on the channel, it starts transmitting signal. For the purpose of sensing the jammer whether it's ON and should not consume energy.

To reduce jamming attacks many hiding schemes can be used. These are

- Steganography
- Cryptographic puzzle base scheme
- All-or-nothing transmission

IV. Techniques For Preventing Jamming Attacks

Many prevention techniques have been proposed for tackling jamming attacks. Transmission of jamming messages can be prevented by cryptanalysis and steganography techniques.

A. Steganography

In Cryptography, It's a practice of concealing messages or information within another non-secret file, message, image, or video. it makes the sender and receiver invisible. Thus, steganography provides not only security but also anonymity.

An algorithm to hide a secret message (SM) in some cover file (CF) which could be a text or doc file. Data hiding method that hides bit patterns of the message in random locations of a file is used [7].

Algorithm for hiding SM in CF:

1. Start
2. Read host file name
3. Read secret message file name
4. Calculate NHOST= no. of blank spaces in host file
5. Calculate NSTAG= size of secret message file
6. Calculate n1= integer(NSTAG/32)
7. Calculate r1= NSTAG-n1*32
8. i) Set n= 2560 for .doc file ii) set n=0 for.txt file
9. Calculate size1=(n1+1)*256+32
10. If size1>NHOST then exit otherwise continue from step 11
11. Read 256 blank space positions from the nth position of the host file.
12. Update 'n' with the location right after last read blank space.
13. Read 32 bytes from secret messages.
14. Take 1 byte from 32-byte block and divide it into an 8-bit pattern.
15. For each bit select a random blank space location
16. If SM bit is 1, then replace this randomly selected blank space with ASCII 32.
17. Repeat steps 14 to 16 for all 32 bytes of the secret message block.
18. Repeat steps 11 to 17 for n1 times.
19. Repeat the same process for remaining r1 bytes of a secret message.
20. End [7].

B. Cryptographic Puzzle Hiding Scheme

In packet hiding scheme based on cryptographic puzzles. Puzzles force the recipient of a puzzle to execute a pre-defined set of computations before he is able to extract a secret of interest. The time required for cracking the solution of a puzzle depends on its hardness and the computational ability of the solver. It has higher computation and communication overhead [8].

C. All-Or-Nothing Transformation

The packets are pre-processed by an AONT before transmission but remain unencrypted. The jammer cannot perform packet classification until all pseudo-messages corresponding to the original packet have been received and the inverse transformation has been applied. Packet m is partitioned to a set of x input blocks m = {m1, m2, m3….}, which serve as an input to the set of pseudo-messages m = {m1, m2, m3...} is transmitted over the wireless medium. An AONT is an efficiently computable transformation on strings such that for any string x, given all of T(x), one can efficiently recover x There exists some threshold such that any polynomial time adversely that learns all but bits of T(x) obtains no information about X.

The AONT has many other applications, as well, such as enhancing the security of block ciphers and making fixedblock size encryption schemes more efficient [9].

D. Triple DES

Triple DES uses a key bundle which comprises 3 DES keys K1, K2, K3, each of which 56 bits excluding parity bits. An Encryption algorithm is: Ciphertext = EK3(DK2(EK1(plaintext))) In encryption process, the plaintext is encrypted with K1, decrypted with K2 and again encrypted with K3. Decryption algorithm is: Plaintext = DK1(EK2(DK3(cipher text))). In decryption process, cipher text is decrypted with K3, encrypted with K2, and again decrypted with K1. Each triple DES encryption encrypts one block of 64 bits of data. In each case,the middle operation is reverse of first and last [10].

V. Honeypots for Reducing Effects of Jamming

Honeypots are basically a great computer security measure which is used to fool the attacker. Honeypot tries to trap the attacker by gaining the attention of attackers. attackers think honeypot is the highly confidential part of the network and at the same time honeypot collects all the information about attackers such as attacking strategy, purpose and his techniques.

An algorithm will use honeypots to provide an efficient solution to jamming attacks.

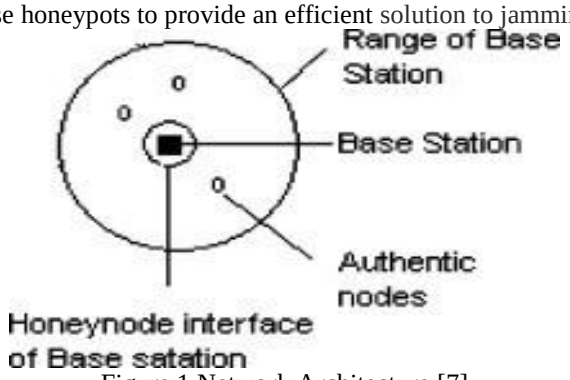

Figure 1 Network Architecture [7]

This given algorithm runs on all the nodes. When any of the nodes detects an attack, it changes its frequency of operation. However, if the honeynode detects an attack, it continues to send signals and keeps attacker busy at the same time informs the base station about the attack.

The base station then issues a frequency change command to all its associated nodes, telling them to switch to a new frequency. Later on, the honeynode switches its frequency [7].

Algorithm:

1 If (Attack detected= true) then
2 If (Node is a honeynode) then
3 Inform base station of attack
4 Continues communications to deceive jammer
5 End.
6 Change frequency of operation
7 else

8 If (node is a base station) then
9 If (honeynode has informed of attack) then
10 select frequency to jump using dynamic selection.
11 Inform associated node to switch to this frequency
12 Change frequency of operation
13 Else
14 Find the node that did not respond
15 If (any node did not respond) then
16 Broadcast frequency change command
17 Change frequency of operation
18 End [7].

VI. Universalanti-Jamming Technology

Finally, the ultimate question that needs to be addressed is, Is it possible to have a single practical anti-jamming approach which can work with all types of networks and detect all kinds of jammers? also, many researchers have introduced many jamming techniques, besides preventing intrusion attack, can we use them for any other useful purpose and if so then how?

VII. Conclusion

In this paper of jamming attacks in wireless networks, firstly the consequences of jamming attacks areacknowledged.After that, to counter them some prevention techniques for reducing jamming attacks by using steganography, Triple DES, Cryptographic Hiding Schemes are discussed. Advantages of each prevention technique listed in this study are given in following table.

Table I. Advantages of jamming prevention techniques.

Technique	Advantages
Steganography	Hides a secret data in a cover file. Hides bit pattern in random location inside file
Puzzle Hiding Scheme	The advantage of the this scheme is that its security does not rely on the physical layer parameters.
All-or-Nothing Transformation	This method solves the problem of partial key exposure: instead of storing a secret key directly.
Triple DES	3 keys with key length of 168 bits makes it difficult to break. Easy to implement. Most systems, libraries & protocols include support for it.

Still, no system can claim to be 100% safe just by implementing prevention methods. Hence, as a contingency plan to reduce the effect of jamming, honeypot technique has been used and an algorithm is used to fool jammer and decrease jamming rate just in case advisory breaks into System.

References

[1] http://www.spamlaws.com
[2] W. Xu, W. Trappe, Y. Zhang. The Feasibility of Launching and Detecting jamming attacks in Wireless Networks. In proceedings of MobiHoc, 2005.
[3] Y. Desmedt. Broadcast anti-jamming systems. Computer Networks, Feb. 2001.
[4] G. Noubir and G. Lin. " Low-Power Dos attacks in data wireless LANs and Countermeasures. SIGMOBILE mobile computing and communications, 2003.
[5] R. Ibrahim and Teoh Suk Kuan. "Steganography Algorithm to hide secret message inside an Image". Computer application and technology, February 2011.
[6] Dr. AtefJawad AL-Najjar." The decoy: Multi-level Digital multimedia steganography model." 12th WEASE international conference on communications, July 2008.

[7] Neha Thakur, ArunaSankaralingam "Introduction to Jamming Attacks and Prevention Techniques using Honeypots in Wireless Networks" in IRACST April 2013.

[8] M. Cagalj, S. Capkun, J.-P. Hubaux,"Wormhole-Based AntiJamming Techniques in Sensor Networks", IEEE Trans. Mobile Computing, Vol. 6, No. 1, pp. 100-114, Jan. 2007.

[9] R.C Merkle, secure communications over insecure channels. Communications of the ACM,21(4):2994-299,1978.

[10] https://en.wikipedia.org/

