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. 1, January 2015, pg.443 – 448

SURVEY ARTICLE

Survey on Detection and Prevention of Jamming Attack in Wireless Communication

Ashwini Mane, Rupali Gobe, Poonam Umadikar, Namrata Gawali

Department of Information Technology

JSPM's Rajarshi Shahu College of Engineering

ashwini8138@gmail.com

rupaligobe2012@gmail.com

***Abstract*: As the nature of wireless medium is open and leaves an intentional interference attack which is typically referred as jamming. This interference launches base for mounting denial of service kind of attacks on wireless network. Attacker can interrupts wireless network with the help of jamming technique. Jamming technique is also known as denial of service attack. When network gets jammed it does not provides any services. Jamming can be done at different layers by attacker. In this paper, we focus on jamming at the Transport/Network layer. To make less severe jamming attacks schemes are used like Strong Hiding Commitment Schemes (SHCS), Cryptographic Puzzles Hiding Schemes (CPHS), All- Or-Nothing Transformation Hiding Schemes (AONTSHS).**

Keywords: Selective jamming, Denial-of-Service, Wireless network, Packet classification.

1. INTRODUCTION

The main basis of wireless network is availability of wireless medium connecting the participating nodes. Because of its open nature it leads to security threats. Jamming service means jamming for specific period, for specific packets until stop jamming request made. Anyone with the transceiver can jam the network, can include suspicious messages. However jamming and Injection of messages can be prevented with the cryptographic mechanisms. Jamming attacks are under the external threat model where the jammer is not a part of the network. Jamming strategies focused on transmission of continuous or random transmission of more power interference signals. Transport/network layer makes the use of protocols like TCP, IP, UDP to sense the packet type and their flows. This can be further use by attacker to achieve the targeted jamming.

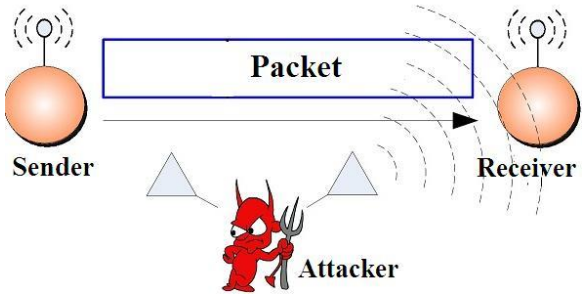


Fig 1.Jamming attack in wireless network

2. LITERATURE SURVEY

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

At various different layers jamming ad sensing can be done by attacker. This jamming and sensing technique makes the misuse of AODV and TCP protocols at transport /network layer very efficiently. With the help of this protocols attacker sense the victim packets, but as the whole packet is encrypted attacker can sense only packet size, timing and sequence. Attacker cannot read the data within packet because the whole packet is encrypted. To achieve more secure network size, timing and sequence of packets are managed efficiently. An attacker may tries to attack the victim ado network by disturbing some or all victim communication. So this kind of Denial of Service attack considered at different layers. Network Jamming can be achieved by sending strong signal which interrupts the transmission of packets through the network. Jamming means not only preventing transmission of packets being received, it also requires to detect victim network activity. It is required to sensor to recognize the presence of packets at physical layer. As network is encrypted so only packet size and start time can be measured. By doing the selfish use of AODV and TCP protocols attacker achieves advantages like it requires less energy, targeted jamming can be done and reduced probability of detected. Jamming to specific part of network, nodes can be done by attacker.

2.2 Anti-jamming Timing Channels for Wireless Networks [4]:

Wireless communication is vulnerable to radio interference. Acknowledgement of communications is prevented due to such radio interference. In opposition to broadband jammers some dodging strategies have been recommended, but they are not that much effective and also they are costly. An alternative for dodging strategies have been searched that involves the formation of a timing channel. Such channel exists even in the presence of jamming.

Failed packet reception times are used to build the timing channel. Failed packet events can be detected against the jamming. A low-rate overlay link-layer can be (is) constructed using single sender and multi-sender timing channel. There are many strategies that may be applied to halt wireless connectivity. Some network-oriented attacks such as dissociation attacks have been applied against the wireless systems (e.g. 802.11). Authentication can be used to address such powerful threats. Directly interfering with communications by jamming the communication channel is an alternative strategy to mess up wireless communications. To reconstructs network connectivity in the presence of interference, certain defense (or resistive) strategies have been proposed.

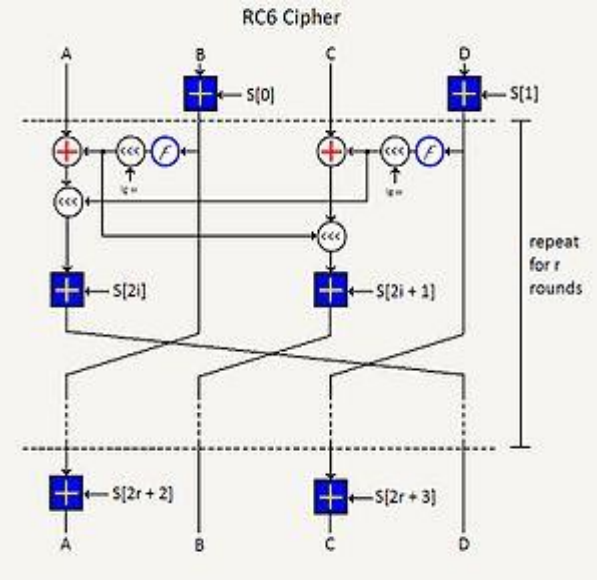
2.3 Mitigation of Control Channel Jamming under Node Capture Attacks [7]:

Availability of service in wireless networks depends on the ability for network users to establish and maintain Communication channels.
Jamming the communication channels used to exchange control messages. Spread spectrum techniques used to detect an external adversary from such control channel jamming attacks. Efficient communication in mobile networks requires the use of multiple access protocols allowing mobile users to share the wireless medium by

separating user data in any combination of time, frequency, signal space, and physical space in the network. Allocation of access and resources to mobile users must be periodically updated in order to maintain the efficiency of the multiple access protocol.

2.4 The RC6™ Block Cipher[8]:

RC6 algorithm is an extension to RC5.RC6 uses an extra multiplication operation which is not present in RC5 in order to make the rotation dependent on every bit in a word, and not just the least significant few bits. The different feature of RC6 is that it uses four working registers instead of two registers. As it uses the multiplication operation increased which results in greater security, fewer rounds and increased throughput.32-bit integer multiplication is efficiently implemented on most processors. Integer multiplication is a very effective and is used in RC6 to compute rotation amounts. To satisfy the requirements of the AES, a block cipher must be able to handle 128-bit input/output blocks. While RC5 is fast block cipher, which acts on 128-bit blocks and uses two 64-bit working registers. But the problem is that architecture and languages for AES do not support 64-bit operations in natural manner .So that RC6 Block Cipher designed to use four 32-bit registers rather than two 64-bit registers. This has one advantage that we are doing two rotations per round rather than the one round in a half-round of RC5.



3. PROPOSED SYSTEM

In this paper, we address the problem of jamming under an internal threat model. We consider an attacker who is aware of network secrets and the implementation details of network. The attacker uses his knowledge for launching selective jamming attacks in which specific messages of "high importance" are targeted. For example, a jammer can target route-request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments.

The algorithms used in this system are

- RC6
- SPEKE (key exchange algorithm).

3.1 RC6:

RC6 (Rivest Cipher 6) is a symmetric key block cipher. It is derived from RC5.It was designed by Ron Rivest, Matt Robs haw, Ray Sidney. Mainly it was designed to meet the requirements of the Advanced Encryption Standard (AES).RC6 is very similar to RC5 in structure, using data-dependent rotations, modular addition, and XOR operations. As like RC5, RC6 also makes use of data-dependent rotations.RC6 proper has a block size of

128 bits and supports key sizes of 128, 192, and 256 bits.

3.2 SPEKE:

SPEKE (Simple Password Exponential Key Exchange) is a cryptographic method for password-authenticated key agreement. It is one of the older and well- known protocol in the relatively new field of password-authenticated key exchange.

Techniques:

- **Real Time Packet Classification**
- **A Strong Hiding Commitment Scheme**
- **Cryptographic Puzzle Hiding Scheme**
- **Hiding based on All-Or-Nothing Transformations**

DESCRIPTION:

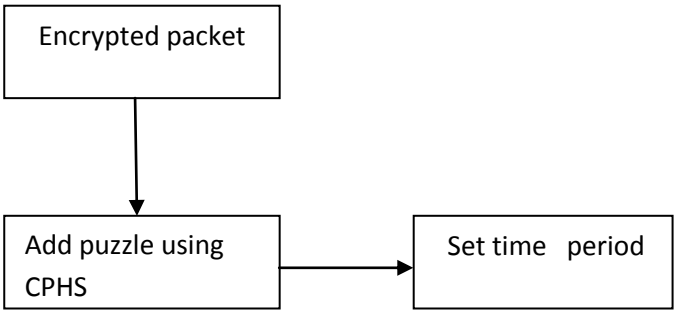
3.1Real Time Packet Classification:

In real time packet classification at the physical layer the packet p is being encoded and modulated before it is being sent to the receiver through the wireless media. When the receiver receives packet p it decodes and demodulates the signal. This communication takes place through a wireless network. During this communication there exists a jamming attacker which corrupts the contents placed in packet p. So at the receiving side the receiver will receives modified contents of packet p.

3.2 Cryptographic Puzzle Hiding Scheme:

We consider several puzzle schemes as the basis for CPHS. Cryptographic Puzzle Hiding Scheme (CPHS) is technique which is used to provide the security in non-secure channel. The time lock puzzle is designed that is fully based on the repetitive application of controlled number of modulo operations. A time-lock puzzle is a mechanism for sending messages “to the future”. The sender generates the puzzle whose solution is the message to be sent and sets the time for solving the puzzle.

Time lock puzzle will be useful if time for generating puzzle takes less time than solving it. The main aim behind such puzzle is to force the recipient of a puzzle execute a pre-defined set of estimations before he is able to extract a secret of interest. The time period required for obtaining the solution of a puzzle depends on its firmness and the computational ability of the solver. Advantage of the puzzle based scheme is that its security does not depend on the PHY layer parameters.



3.3 Strong Hiding Commitment Scheme:

We propose a strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. Our main motivation is to satisfy the strong hiding property while keeping the computation and communication overhead to a minimum. The computation overhead of SHCS is one symmetric encryption at the sender and one symmetric decryption at the receiver. Because the header information is permuted as a trailer and encrypted, all receivers in the vicinity of a sender must receive the entire packet and decrypt it, before the packet type and destination can be determined. However, in wireless protocols such as 802.11, the complete packet is received at the MAC layer before it is decided if the packet must be discarded or be further processed. If some parts of the MAC header are deemed not to be useful information to the jammer, they can remain unencrypted in the header of the packet, thus avoiding the decryption operation at the receiver.

3.4 Hiding based on All-Or-Nothing Transformations:

It is also known as an all-or-nothing protocol, which allows the data to be understood only if all of it is known. 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. AONTs can be used to increase the strength of encryption without increasing the key size. It helps to prevent several attacks.

4. Future Scope

4.1 Black-hole Attack:

In this type of attack a malicious node sends fake routing information, claiming that it has an optimal route and informs other nodes to send data packets through that route. So it does not forward data packets which are received. It drops data packets.

4.2 Gray-hole Attack:

This attack is also called as routing misbehavior attack. It concentrates on dropping of messages. It includes two phases. In the first phase include that the node informs itself as having a valid route to destination and in second phase, nodes drops intercepted packets.

4.3 Man- in- the- middle Attack:

In this attack, attacker resides in between the sender and receiver. It monitors and modifies any information being sent between sender and receiver.

4.4 Jamming:

In jamming, attacker keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. This is common type of attack in wireless network.

4.5 Wormhole Attack:

In this type of attack, at one end attacker receives packets in the network and tunnels them to another point in the network. Due to this attack routing can be disrupted when routing control message are tunneled.

5. Conclusion

In this paper, jamming attacks in wireless networks have been addressed and attacker who knows about network secrets and protocols specifications is considered. Cryptographic primitives such as strong hiding commitment schemes, cryptographic puzzles are combined and analyzed the security of our system. Along with these schemes a random key distribution has been implemented to more secure the packet transmission in the wireless networks.

References

[1] T.X. Brown, J.E. James, and A. Sethi,"Jamming and Sensing of Encrypted Wireless Ad Hoc Networks," Proc. ACMInt'l Symp. Mobile Ad Hoc Networking andComputing (MobiHoc), pp. 120-130,2006.
[2] M. Cagalj, S. Capkun, and J.-P. Hubaux,"Wormhole-Based Anti-JammingTechniquesin Sensor Networks," IEEE Trans. MobileComputing, vol. 6, no. 1, pp. 100-114, Jan.2007.

[3] A. Chan, X. Liu, G. Noubir, and B. Thapa,"Control Channel Jamming: Resilience andIdentif ication of Traitors," Proc. IEEEInt'l Symp. Information Theory (ISIT), 2007.
[4] 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.
[5] R. Rivest, "All-or-Nothing Encryption andthe Package Trans- form," P roc . Int'lWorkshop Fast Software Encryption, pp. 210-218,1997.
[6] R. Rivest, A. Shamir, a n d D.Wagner, "TimeLock Puzz les and Timed-ReleaseCrypto," technical report, MassachusettsInst. of Technology, 1996.
[7] P. Tague, M. Li, and R. Poovendran,"Mitigation of Control Channel Jammingunder Node Capture Attacks," IEEE Trans.Mobile Computing, vol. 8, no. 9, pp. 1221-1234, Sept. 2009
[8] The RC6TMBlock Cipher Ronald L. Rivest1, M.J.B. Robshaw2, R. Sidney2, and Y.L. Yin21 M.I.T. Laboratory for Computer Science, 545 Technology Square, Cambridge , MA 02139, USA rivest@theory.lcs.mit.edu2 RSA Laboratories, 2955 Campus Drive, Suite 400, San Mateo, CA 94403.

