

PIGGYBACKING METHOD COMBINED WITH SHCS TECHNIQUE FOR SPOT JAMMING ATTACKS IN WIRELESS NETWORKS

N.Kavitha

*Research Scholar, Department of Computer Science,
Vivekanandha College of Arts and Sciences for Women,
Tiruchengode-637205,India*

A.ArunJoseph

*Assistant Professor, Department of Computer Science,
KSR College of Arts and Sciences,
Tiruchengode,Namakkal-637215,India*

ABSTRACT

Wireless networks provide wide range of services which is never so easy by any other medium, its mode of working tends it to have many security breaches. Wireless networks are built upon a shared medium that makes it easy for adversaries to launch jamming-style attacks. In this work, we address the problem of spot jamming attacks in wireless networks. In these attacks, the adversary is active only for a short period of time, spotly targeting messages of high importance. It is an attempt of making the users not possible to use network resources. The fact that no single measurement is sufficient for reliably classifying the presence of a jammer is an important observation, and necessitates the development of enhanced detection schemes that can remove ambiguity when detecting jammer. To address this need we propose the Strong Hiding Commitment Scheme (SHCS) with Piggybacking Technique that localize the jammer presence in physical-layer attributes. We develop schemes that prevent real-time packet classification by combining cryptographic primitives.

Key Term: *Spot Jamming Attacks, Denial of Service, SHCS, TCP, Wireless Network.*

1.Introduction

Wireless networks are meant for transferring information of any kind between two or more points that are not physically connected. Wireless networks are vulnerable to various kinds of attacks because of its shared medium. Wireless networks are very less security due to the open nature of wireless medium. In wireless medium anyone can be eavesdrops the messages from the information channel. Here the jammer interrupts the communication between the two legitimate users. The wireless jamming attack aims at preventing wireless nodes from accessing the shared wireless medium or from successful reception. Jammers keep the medium busy or cause high radio interference at the receiver.

Jamming can be as simple as sending out a strong noise signal in order to prevent packets in the victim network from being received. This method of jamming is not the subject of this paper. Jamming gain is the increase in efficiency from exploiting features of the victim network relative to continuous jamming.

More precisely, it is the amount of energy (or power as appropriate) used to achieve a desired effect relative to the amount of energy used to achieve the same effect with continuous jamming. This gain translates directly into reduced energy requirements for the attacker. At the link level, corrupting a single bit in a packet will cause the packet to fail its checksum and be discarded. For a 10,000 bit packet (1250 bytes) it implies that jamming gains as high as 40dB are possible. Further, typical wireless packet networks are lightly loaded so that jamming only when packets are present has further jamming gains.

Targeted jamming refers to jamming only specific victim nodes, links, or flows. The attacker may be interested in only certain parts of the victim network, and attacking only these parts can lead to further jamming gains. With reduced probability of detection, the victim network may not realize that jamming countermeasures are necessary. Targeting some TCP-DATA packets will cause the TCP window to collapse and poor connection performance that a user might attribute to network congestion or a low quality wireless connection. Further, if ICMP packets are not blocked the victim users will have

contradictory views of the network state. If jamming is discovered, lower probability of detection jamming will be harder to detect, localize, and suppress.

Jamming is not a transmit-only activity. It requires an ability to detect and identify victim network activity, which we denote as *sensing*. At the physical layer a sensor needs to identify the presence of packets. Since the network is encrypted, only the start time and size of the packet can be measured. At higher layers a sensor needs to classify packets using protocol information. The broadcast nature of wireless networks makes them more susceptible to attacks.

2. Connected Work

In modern era the accommodations provided by the 802.11 based mostly wireless access network crystal rectifier to its readying in numerous sectors likedefence, shopper and industrial sector. Openness of wireless network makes it prone tonumerousstyles of attacks. Out of variedstyles of attacks, Denial-of-service (DoS) attack is one amongthe foremostdifficult threat thatstop legitimate users from accessing the network. it'sideal in some wayslike intentional interference or ECM. ECM is one amongseveral exploits accustomed compromise the wireless setting. It works by denying service to approved users as legitimate traffic is crowded by the overwhelming frequencies of illegitimate traffic. If ANassaulterreallyneeded to compromise your LAN and wireless security, the foremost effective approach would be to send random unauthenticated packets to each wireless station within the network. to attenuate the impact of AN unintentional disruption, it'svitalto spot its presence. ECM makes itself well-known at the physical layer of the network, additionalunremarkablyreferred to as the raincoat (Media Access Control) layer [2]. The inflated noise floor ends up in a faltered noise to signal quantitative relation, which is able to be indicated at the shopper. It even be measurable from the access purposewherever network management options should able to effectively report noise floor levels that exceed a planned threshold. From there the access points should be dynamically reconfigured to transmit channel in reaction to the disruption as known by changes at the physical layer.

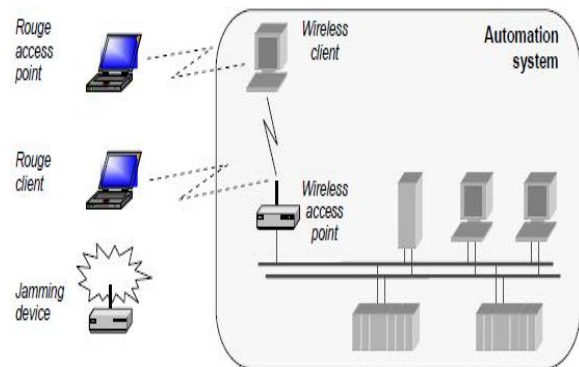


Figure :1 spot jamming and Random access purpose
2.1 DETECTION OF JAMMING

The network employs a monitoring mechanism for detecting potential malicious activity by a jammer. The monitoring mechanism consists of the following:

- (i) determination of a subset of nodes M that will act as network monitors
- (ii) employment of a detection algorithm at each monitor node.

The assignment of the role of monitor to a node can be affected by energy limitations and detection performance specifications. In this work, we fix M and formulate optimization problems for one or more monitor nodes. We now fix attention to detection at one monitor node. First, we define the quantity to be observed at each monitor node. In our case, the readily available metric is probability of collision that a monitor node experiences, namely the percentage of packets that are erroneously received.

2.2 JAMMING TYPE

Jammer is an entity who is purposefully trying to interfere with transmission and reception of message across the wireless channel. Recently, several jamming strategies have been introduced. Later, jammers were categorized into four models. They are

❖ Constant jammer

In this model, jammer continuously emits RF signals and it transmits random bits of data to channel. It does not follow any MAC layer etiquette. Being constant to the transfer it does not wait for channel to become an idle.

❖ Reactive jammer

In this model, jammer will stay quite when the channel is idle. As soon as it senses activity on channel, it starts transmitting signal. In order to sense the channel jammer is ON and should not consume energy.

To mitigate jamming attacks many hiding schemes were used. These are

- Strong hiding commitment scheme
- Cryptographic puzzle base scheme
- All-or-nothing transmission
- ❖ *Deceptive jammer*

In this model, jammer constantly injects series packets to the channels without any gap between subsequent transmissions. It also broadcasts fabricated messages and reply old ones. Jammer will pass rambles out to the network and just check the preamble and remain silent.

- ❖ *Random jammer*

In this model, jammer alternates between period of continuous jamming and inactivity. After jamming for t_1 units of time, it stops emitting radio signals and enter into sleep mode. The jammer after sleeping for t_2 units of time wakes up and resumes jamming. Both time t_1 and t_2 is either random or fixed.

3. Basic Statistics For Detection Of Jamming

The evaluation of the proposed scheme in terms of end-to-end delay and throughput is described. Simulations have been conducted using OPNET Modeler 16.0 [9]. We compare the proposed scheme with jammed area mapping scheme [4]. In order to implement proposed robust rate adaptation scheme, we modify IEEE 802.11 DCF (Distributed Coordination Function) scheme in OPNET Modeller.

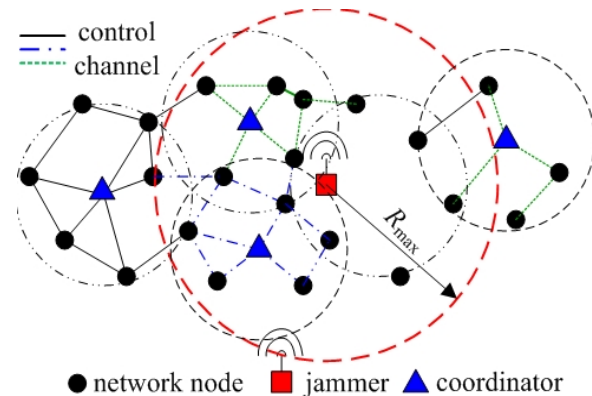


Figure : 2. Detection of the Collision and control channel

3.1 PIGGYBACKING

Piggybacking is well known and extensively used for real - world applications. For large packets such as I, the source produces a further compressed packet by discarding the less- important bits and attaches this small and redundant packet to data packet $i+1$. In this proposed work we propose two new methodologies to send data between the server and numerous clients in the secure manner. First the data encryption technique is handled by the RSA Algorithm. Secondly the encrypted text is transfer over the network. When the decryption is done on the clients there the piggybacking operation takes place. For packet hiding technique the A Strong Hiding Commitment Scheme (SHCS) is implemented.

- ❖ *Piggybacking Technique*

We proposed a novel method using piggybacking technique of packet loss during large volume of packets sent to more number of clients. At the decryption end, the data in huge volume will be loss due to congestions. But by piggybacking the packets along with the header and sequence ID and the host name the data will be send directly to the selected host.

Hence, the data will be buffered and after that process the data will be sending to all the clients that are alive on the network. Thus the piggybacking techniques the data will be directly send to the client network, after the acknowledgement is received. The TCP protocol is responsible for the processing.

- ❖ *Congestion Control and Packet Classification*

One of the major problems in the wireless communication is the congestion control and avoidance problem. We addressed the problem of discerning congestion attacks in the wireless networks. We considered an internal adversary model which is responsible for the congestion. In the adversary model, in that which the congestion is taken place as a part and hence easily identified and prevented. The Adversary model proposed here is responsible for the packet classification in the in real time applications. Once the packet is classified, the adversary is responsible to choose the technique for jamming avoidance.

3.2 JAMMING ATTACK METRICS

A variety of metrics can be used to compare various jamming attacks. Clearly, the following metrics are all relevant:

1. Energy efficient
2. Low probability of detection
3. Stealthy
4. Strong DoS, complete if so desired
5. Maintain behaviour consistent with or close to the protocol standard
6. Authenticated or unauthenticated users
7. Strength against error correction algorithm
8. Strength against physical layer techniques such as FHSS, DSSS, CDMA.

These are most important will depend greatly on the application addressed. Energy efficiency may be the most important metric for jammers of sensor networks that are expected to last a long time. Strong DoS may be the key component if even a few successful messages will compromise your situation such as behind enemy lines. Low probability of detection is crucial if you need to maintain a modestly long-term presence in a hostile area.

3.3 A STRONG HIDING COMMITMENT SCHEME (SHCS)

In this paper, we propose a strong hiding commitment scheme that is based on the symmetric cryptography method. Main impetus is to satisfy the strong hiding property while keeping the computation and the communication overhead to a minimum. The proposed SHCS requires the joint consideration of the MAC and PHY layers. To reduce the overhead the de-commitment value or the decryption key value is done in the same packet in which the encryption is taken place.

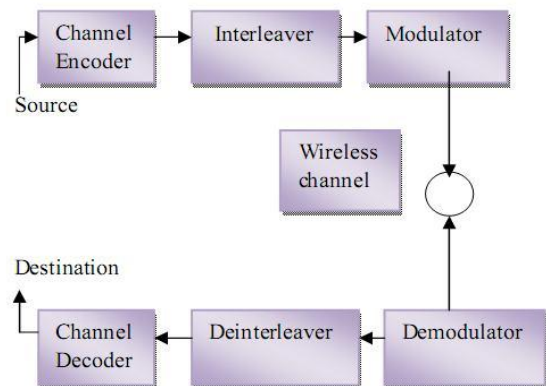


Figure : 3. A general communication system diagram.

Main impetus is to satisfy the strong hiding property while keeping the computation and the communication overhead to a minimum. The proposed SHCS requires the joint consideration of the MAC and PHY layers. To reduce the overhead the de-commitment value or the decryption key value is done in the same packet in which the encryption is taken place.

A new sub layer is found between the existing two layers, which is responsible for the packet formatting and data hiding. It will form as a frame structure. The purpose of this is to randomize the input to the encryption algorithm.

❖ Encryption of Data

The data is encrypted by using the RSA Algorithm. It is the public key algorithm that uses the huge prime numbers in their factoring and their multiples as the code or key to encode the data given. Since the key size is large the intruders cannot be easily able to hack the data. Through this RSA (Rivest, Shamir, Adleman) algorithm the data will be more secure.

Cryptography is the process of transforming information (plain text/Image) into unintelligible form (Cipher text/ Cipher Image). The technology of encryption is called cryptology. For encryption the RSA algorithm is used to encrypt and decrypt the text, because it is considered as a better solution for data encryption. In cryptography, RSA is an algorithm for public key cryptography. The RSA algorithm involves

the use of two Keys a public key, which may be known by anybody, and can be used to encrypt Messages a private key, known only by the recipient, and used to decrypt messages.

4. Conclusion

In this paper, we propose a new technique for the security of the data by piggyback the data with thesequence ID and with the host name. Along with the piggybacking we also maintain the strong hiding scheme that provides the packet from loss and stored in the buffer. The congestion control is maintained in this paper by following the sequential number ID of the packets. In the wireless network, the confidentiality of the data is more important aspect and is maintained in this paper by piggybacking the packets without loss.The RSA algorithm is used for the encryption and the decryption purpose. The encrypted data will then piggybacked by which the data is hidid and then moved to the destinations. Through this the congestion on the network can be controlled.

5. References

- [1] Timothy X Brown Jesse E. James.*Jamming and Sensing of Encrypted Wireless Ad Hoc Networks*.AmitaSethi University.
- [2] Mr.PushphasChaturvediMr.KunalGupta.*Detection and Prevention of various types of Jamming Attacks in Wireless Networks*. Dept. Of Computer Science, Amity University.
- [3] NehaThakur.*Introduction to Jamming Attacks and Prevention Techniques using Honeypots in Wireless Networks*. Dept. of Software Engineering ,SRMUniversity,Chennai, India.
- [4] KwangsungJu and Kwangsue Chung *Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks*. Department of Communications Engineering sKwangwoon University, Seoul, Korea.
- [5] S. Periyanyagi and V. Sumathy.*A Swarm Based Defense Technique for Jamming Attacks in Wireless Sensor Networks*.
- [6] Alejandro Proaño and LoukasLazos .*Packet-Hiding Methods for Preventing Selective Jamming Attacks*. Dept. of Electrical and Computer Engineering, University of Arizona, Tucson, AZ, USA.
- [7] T. X. Brown, J. E. James, and A.Sethi. *Jamming and sensing of encrypted wireless ad hoc networks*. In Proceedings of MobiHoc, pages 120–130, 2006.
- [8] M. Cagalj, S. Capkun, and J.-P. Hubaux.*Wormhole-based antijamming techniques in sensor networks*. IEEE Transactions on Mobile Computing, 6(1):100–114, 2007.
- [9] A. Chan, X. Liu, G. Noubir, and B. Thapa. *Control channel jamming: Resilience and identification of raitors*. In Proceedings of ISIT, 2007.
- [10] T. Dempsey, G. Sahin, Y. Morton, and C. Hopper.*Intelligent sensing and classification in ad hoc networks: a case study*. Aerospace and Electronic Systems Magazine, IEEE, 24(8):23–30, August 2009.
- [11] Y.Desmedt.*Broadcast anti-jamming systems*. *Computer Networks*. 35(2-3):223–236, February 2001.
- [12] K. Gaj and P. Chodowiec.*FPGA and ASIC implementations of AES*. Cryptographic Engineering, pages 235–294, 2009.