A Survey on Preventing Jamming Attacks in Wireless Communication

R.Saranyadevi
SNS College of Technology
Department of CSE
Coimbatore-641035

M.Shobana
SNS College of Technology
Department of CSE
Coimbatore-641035

D.Prabakar
SNS College of Technology
Department of CSE
Coimbatore-641035

ABSTRACT

Communication in wireless network is possible with an air medium. Due to the high security threats in this system, the network may face various difficulties. One of the major threat is jamming attack which comes under Denial Of Service (DOS) attack. Jamming attack is common among many exploits that compromises the wireless environment. The work of authorized users is by denying service to as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic.In order to mitigate the impact of jamming, three techniques are being used: (a) how to thwart jamming in control channel (b) An Anti-jamming broadcast communication using Uncoordinated Spread Spectrum (USS) technique (c) Mitigating jamming impact in timing channel. We analyse these methods for reducing jamming inside a network.

KEYWORDS:

Jamming attacks, Spread spectrum, Control channel, Timing channel

1.INTRODUCTION

Wireless communication is meant for transferring information of any kind between two or more points that are not physically connected. It is a method of communication using a radio signal frequency that relies among computers and other devices. Few examples are Mobile, WI-Fi-, Bluetooth. As the data communication is done through wireless medium we may face several security threats. One of these vulnerable threats is Denial of Service. It is an attempt of making the users not possible to use the network resources. Therefore, reducing those threats in wireless networks without any data loss or modification is necessary.

As well, all the communication in a wireless medium is interrupted or disturbed through a major and familiar attack called as Jamming attack. A jammer is prevailing under this communication that interfere the physical transmission and reception. It continuously emits Radio Frequency (RF) signals that block the legitimate traffic (see FIG 1). Jamming is done by two forms. One is the External threat model in which the jammer is not a part in the network security threat .The other one is Internal threat model which sustains the jammer as a part of the network.

There are several Jamming Attack Models. They are Constant Jammer, Deceptive Jammer, Random Jammer, and Reactive Jammer.

Constant Jammer:

This model continuously emits a radio signal and it transmits random bits of data to the channel. It does not follow any MAC layer etiquette. Being constant to the transfer it does not wait for the channel to become idle.

Deceptive Jammer

This jammer constantly injects series packets into the channel. Packets will deceive Normal nodes. Jammer will pass the preambles out to the network and just check the preamble and remain silent

Random Jammer

This method alternates sleeping and jamming with intervals of time. After jamming for t_j units of time, it switch-off its radio and enters sleeping mode. The jammer after sleeping for t_s units of time wakes up and resumes jamming. Both time t_j and t_s is either random or fixed.

Reactive Jammer

This method will stay the jammer quiet when the channel is idle. Transmitting the signal as soon as it senses activity on the channel is regularly one. In order to sense the channel jammer is ON all time and it do not consume energy.

Anti jamming process involves the jammer to utilise continuous or random transmission of high-power interference signal with two steps. Initially the jammer expands the energy into jam frequency bands of interest. Next, the continuous flow of high interference levels detects the type of attack. Antijamming rely on spread spectrum(SS) communication like spatial retreats. It provides bit-level protection as according to the secret pseudonoise (PN) code. However, this method suits only for external threat model. In internal threat model the intended receivers knows the secrets to protect transmission and so the broadcasting communication is vulnerable.

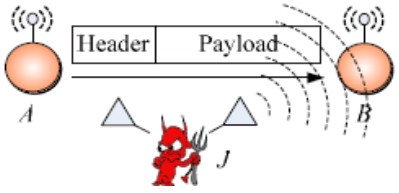

Fig 1.Jamming Attack

2.CONTROL CHANNEL JAMMING ATTACKS

Inside a wireless network the Collection of nodes organised together requires a critical network function such as a neighbor discovery, channel access and assignment, routing and time synchronization. Control channels are the functions used in a broadcast channel that are coordinated by exchanging messages.

The jammer blocks all control information within the range R_{max} by jamming a single frequency band. (Fig 2)

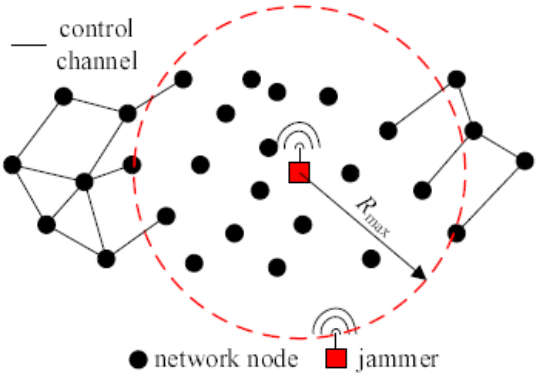

Fig 2: CONTROL CHANNEL JAMMING

A new cluster based architecture is being implemented to mitigate the impact of jamming attack by partitioning the network into set of clusters.(Fig 3) The control channels of the network are controlled by the corresponding clusters. In this method, the node of their corresponding clusters receives the control messages from their members, and the node at the boundaries of multiple clusters receives messages from the associated control channels.

Each cluster is having a clusterhead (CHs) and they are responsible for the establishment and maintenance of the control channel inside that particular cluster. It is the major activity to mitigate jamming and hence it is temporarily assigned that rotates periodically. There are several methods available for establishment of a control channel that mitigates jamming which organises a wireless network into clusters and electing their own CHs.

Our method consists of five phases,(a) hopping

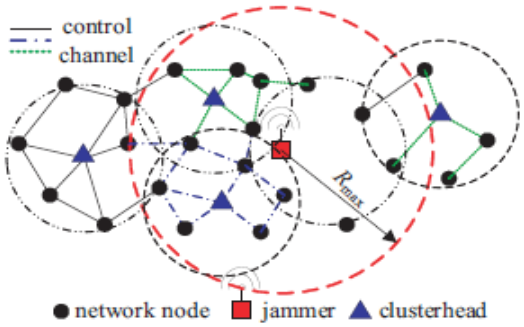

Fig 3.Cluster region with clusterhead

Sequence generation, (b) hopping sequence assignment, (c) control channel access, (d) compromised node identification. In order to adjust the hopping sequence, an intermediate step is essential for all the dynamic spectrum networks. This allocation is done as according to the current channel availability.

A. HOPPING SEQUENCE IN CONTROL CHANNEL

As said in the previous section, consider a cluster and a clusterhead of that specified range where each node is available. Inside a cluster let us assume a current control channel is jammed by an adversary. The major objective of this method is that, the hopping between channels are done by having each node in the cluster to be in a pseudo-random function. It is followed by a unique hopping sequence which is not known to the other nodes. Adversary uses a compromise node for sharing the information of the control channel without the knowledge of the sender and the receiver during hopping process. If the jammer tries to capture the hopping sequence of a declared compromise node, then the node will be identified by the implemented method. Therefore, the CH available inside the cluster updates the hopping sequences of all the nodes except the compromised node. Disadvantages of this technique is increased path length need more gateways. It also require higher battery consumption with more path breaks.

3. JAMMING IN BROADCAST COMMUNICATION

Safety and critical wireless transmissions such as emergency alerts and navigation signals represents a common way to achieve anti-jamming communication. Under this crisis a Spread Spectrum (SS) for Anti-jamming is used for reducing the threat of attackers. This method can be used both in commercial and military applications.

SS uses data-independent, random sequences for spreading out a narrow band signal in a wide bandwidth. Some of the main stages of SS are Frequency Hopping (FH) and Direct-Sequence Spread Spectrum (DSSS). This stage may share a secret prior to their prescribed communication. It enables the receiver to generate a random sequence for detecting and decoding the spread signal. Whenever a base station broadcasts a signal to multiple receivers, it shares a secret prior to the communication and the secret must be hidden from the attacker.(Fig 4) This method of jamming a network in hopping is called as Anti-jamming broadcast problem. In order to overcome this, a method is being implemented called as Uncoordinated Spread Spectrum(USS)technique.

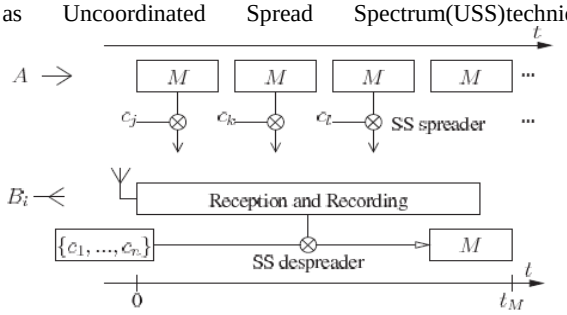

Fig 4.Principle of Uncoordinated Spread Spectrum(USS) techniques

A. Uncoordinated Frequency Hopping (Ufh)

This method opposes the system of coordinated frequency hopping which shares the secrets prior to any communication. So, UFH do not share any secret before to communication.

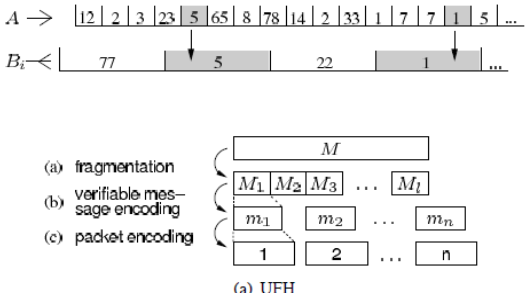

Fig 5.Stages of UFH techniques.

The sender A and receiver Bi choose the set C of available frequency. In this, data 5 and 1 are transmitted successfully. Messages are fragmented to fit on a frequency hop. During transmission, messages and packets are encoded. After reception, it is decoded and reassembled.(Fig 5)

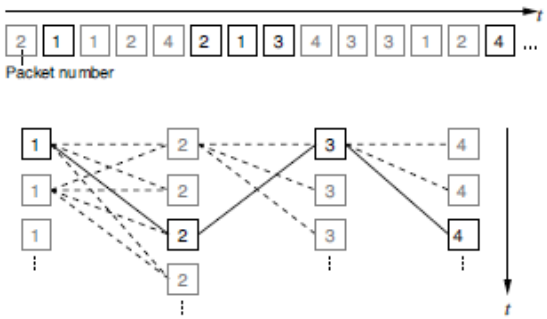

Fig 6. UFH packet reception and reassembly at Bi

It represents the UFH message reassembly in which the black packets are the original data sent successfully and gray packets were inserted by the attacker using a fragment number(and message id).(Fig 6)

4. TIMING CHANNEL COMMUNICATION

In our previous methods, jammer attacks the network and the remaining nodes only can transfer data. In this, the data must be transferred even the interrupts of a jammer or an adversary is present. The other alternate way is that , the data transmission should be over headed in some other channel not relevant to the jammer. In spite of the presence of jammer, the timing channels are built so as to suppress the activity of jammer and establish the timing channel for data communication. By detecting the failure packet events and detecting the failures, the physical and data link layers provides link for a reliable communication. Even disrupts the two layers, it is possible to create a low-rate overlay between the data link and network layer. The components required for this overlay is called as 4-Ounce Overlay.(Fig 7) This certainly replaces the functionality of the physical and link layer.

Fig 7. The 4-Ounce Overlay

Initially, the 4-Ounce Overlay creates the overlay that are detected by failed packet reception events. The further conveyance of information is done through two steps: (1) Even in presence of interference signal a node must detect a failed packet reception; (2) mapping the failed packets into the information to be delivered.

By detecting and analysing the timing of failed packet reception at the receiver it is possible to transfer data by monitoring the signal strength. It is proposed then using an inter arrival codes for building a single-sender, single receiver timing channel.

5. CONCLUSION

In this paper, the three crucial techniques for mitigating the jamming attack were discussed: (1) Cluster based architecture; (2) Spread Spectrum-Uncoordinated Frequency Hopping; (3) Timing channel. Under this survey, it is concluded that all the methods uses several terminologies for frequency hopping in the presence of an adversary and the successful conveyance of any data. In this paper, the technique used is crucially adapted for safety applications like emergency alert broadcasts or dissemination of navigation signals in adversarial settings. Here, mission-critical messages are broadcast to a huge and unknown number of receivers that rely on the availability, integrity and authenticity of the message content.

6. REFERENCES

[1] X. Zhang and L. Jacob, “Multicast Zone Routing Protocol in Mobile Ad Hoc Wireless Networks,” Proc. Local Computer Networks (LCN ’03), Oct.2003.

[2] X. Xiang and X. Wang, “An Efficient Geographic Multicast Protocol for Mobile Ad Hoc Networks,”Proc. IEEE Int’l Symp. World of Wireless,Mobile and Multimedia Networks (WoWMoM),June 2006.

[3] X. Xiang, Z. Zhou, and X. Wang, “Self-Adaptive On Demand Geographic Routing Protocols for Mobile Ad Hoc Networks,” Proc. IEEE INFOCOM, May 2007.

[4] X. Xiang, X. Wang, and Y. Yang. Supporting efficient and scalable multicasting over mobile adhoc networks, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 4, April 2011.

[5] Kaan Bur, Cem Erosy, “Ad Hoc quality of service multicast routings”, Computer communications, Vol. 29, 2005, pp. 136-148.

[6] Hui Cheng a, Jiannong Cao, Xingwei Wang, ”A fast and efficient multicast algorithm for QoS group communications in heterogeneous network”, Computer communications, Elsevier, Vol. 30, 2007 pp. 2225-2235.

[7] Khalid A. Farhan, ”Network sender multicast routing protocol”, Proceedings of seventh IEEE International conference on networking, 2008, pp.60-65.