Jamming Detection and Mitigation with Power Efficient Management in Wireless Broadcast Networks

Uday Kumar G

Abstract

Wireless broadcast Networks are frequently affected by Jamming attacks every day. Jamming attack is caused by the attackers in which adversaries attempt to overpower transmitted signals by injecting a high level of noise, thereby lowering the signal-to-noise ratio (SNR). The effective countermeasure to the jamming attack is increasing the bandwidth of the spectrum of the communication system and using spread spectrum as part of the modulation technique. Spread spectrum as part of modulation can be a highly effective technique against jamming in point-to-point wireless communication systems. In which single transmitter transmits to a single receiver. In this paper some previous jamming detection and mitigation techniques and their issues are discussed and an efficient jamming mitigation technique is proposed with Power Eficient Management (PEM).

1. Introduction

Broadcasting is one of the fundamental tasks in network communication. One node of the network, called the source, has to transmit a message to all other nodes. Remote nodes are informed via intermediate nodes, along directed paths in the network. One of the basic performance measures of a broadcasting scheme is the total time, i.e., the number of rounds it uses to perform the task. Broadcasting in networks whose nodes have complete knowledge of the topology is equivalent to centralized broadcasting in which all transmissions are scheduled in advance by a central monitor .This networks constitute one class of basic and important wireless networks, where a source node simultaneously transmits a number of information flows (messages) to different destinations were the distribution of audio and video content to a dispersed audience via any audio visual medium. Receiving parties may include the public or a relatively large subset.

Nowadays wireless communications are often suspect able to the jamming attack. Jamming attack is one of many exploits caused by the attackers used to compromise the wireless environment. The shared nature of the wireless medium, combined with the commodity nature of wireless technologies and an increasingly sophisticated user-base, allows wireless networks to be easily monitored and broadcast on. Adversaries may easily observe communications between wireless devices, and just as easily launch simple denial of service attacks against wireless networks in which the attacker injects a high level of noise into the system. By injecting noise into the channels, a jammer effectively reduces the signal to noise and interference ratio (SNIR), thereby reducing the probability of successful message reception. However, in the wireless domain, the adversary is empowered to launch more fundamentally severe types of denial of service that block the wireless medium and prevents other wireless devices from even communicating.

In order to avoid the Jamming attack in broadcast networks many effective countermeasures have been proposed. One of the effective counter measure against jamming is spread spectrum where a transmitter redundantly encodes information using a code, allowing a receiver to reject signals that do not come from the transmitter. The previous counter measures that have been proposed work with good efficiency. But the problem here is power efficiency. My proposal provides security against Jamming attack With Power Efficient Management (PEM) in wireless communications.

In this paper Section 2 presents an overview about some of the issues of jamming attacks, Section 3 discusses some of the previous jamming detection and mitigation techniques, Section 4 proposes an efficient

Power Management Spread Spectrum Technique, and Section 5 summarizes the proposed system.

2. PROBLEM DOMAIN

Wireless networks are vulnerable to many attacks such as Radio interference, Deniel-of-Service[1]. These attacks affect the transmission by jamming of packets of users. Hence detecting and mitigating these jamming attacks are essential. An effective detection protocol[3] which employs signal strength measurements and location information as the consistency check. But this is not applicable to random jammers. To resist jamming, the anti-jamming methods coördinated Frequency Hopping[4], and Uncoördinated Frequency Hopping[5] were used. These techniques enable key establishment protocol with or without sharing of a secret code proper to the communication [6]. But they have lower communication throughput, deserve higher storage and processing costs. The binary tree and tree merging schemes with spread spectrum scale to number of receiver without increasing the code used. Still there remains a problem of power management since both the legitimate and attacker node use same amount of power to modulate a signal.

3. JAMMING DETECTION AND MITIGATION TECHNIQUES.

Wireless networks are highly affected by jammers or attackers. Hence effective counter measures are essential to detect jamming and mitigate its effect. The following are some the previous jamming detection methods.

A.Jamming detection with consistency checks

The detection schemes build upon packet delivery ratio measurements which incorporate signal strength readings or location information to serve as the basis for consistency checking in detecting the presence of jamming.

Packet Sent Ratio (PSR): The ratio of packets that are successfully sent out by a legitimate traffic source compared to the number of packets it intends to send out.

Packet Delivery Ratio (PDR): The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender.

1. Signal Strength Consistency check: The detector is built using PDR .In order to reduce false detections due to legitimate causes of link degradation, the signal strength is used as a consistency check. The normal state is, there is no interference or software faults, a high signal strength corresponds to a high PDR. If the signal strength is low the PDR will be also low. On the other hand, a low PDR does not necessarily imply a low signal strength. The combination of PDR and Signal strength measurement improves jamming detection.

Case 1: If PDR is 0 and Signal strength is low then the scenario may be, non-jammed: neighbor failure, neighbor absence, neighbors being blocked, etc.

Case 2: If PDR is 0 and Signal strength is high then the scenario may be, node jammed.

Case 3: PDR is 0 and Signal strength is low then the scenario may be, non-jammed: neighbor being faraway.

Case 4: If PDR is 0 and Signal strength is high then the scenario may be, node jammed.

2. Location Consistency check:

In this protocol, every node advertises its current location and let each node to keep track of both the PDR and the location of its neighbors. Due to node mobility, it is essential that the location advertisements occur with sufficient frequency to be able to reliably confine the migration of neighbors from regions of high PDR near that node to regions of lower PDR further from it. If a jammer suddenly comes into the network near the node then the location information that it has will correspond to the location of the neighbors importance to the start of the interference.

Disadvantage: It is efficient only in detecting constant and deceptive jammers not with random and reactive jammers.

B.Jamming Detection using Uncoördinated frequency Hopping

This Uncoördinated Frequency Hopping (UFH) scheme that breaks this dependency between anti-jamming spread-spectrum communication and key establishment and allows a key establishment in the existence of a communication jammer as shown in fig 1.

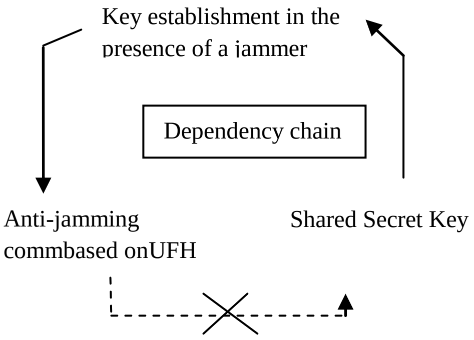

Key establishment in the presence of a jammer
Dependency chain
Anti-jamming commbased onUFH
Shared Secret Key

Fig 1:Breaking dependency using UFH

Uncoördinated Frequency Hopping enables the jamming-resistant communication and key establishment protocol between two nodes in the presence of a jammer without a pre-shared code. Each message is divided into multiple parts and then sent on random hopping frequencies chosen from a fixed frequency band. On random hopping frequencies chosen from a fixed frequency band, with sufficient transmission attempts, the sender and receiver will send and listen on the same channels in a number of time slot. The probability to jam a transmitted fragment with randomized coördinated frequency hopping is equal to the jamming probability in coördinated frequency hopping, In UFH the message is fragmented, transmitted and reassembled by the receiver using message transfer protocol. UFH key establishment is divided into two stages. Our UFH key establishment is divided into two stages. In stage 1, the nodes execute a key establishment protocol and agree on a shared secret key K using UFH; various key establishment protocols can be used in this step. Then, in stage 2, each node transforms K into a hopping sequence and, subsequently, the nodes communicate using coördinated frequency hopping. Key establishment is needed for the authentication of all exchanged messages in order to avoid the insertion of bogus messages.

Disadvantage: This achieves lower communication throughput and gains higher storage and processing costs.

C Jamming detection and mitigation using Tree-Remerging Scheme

The dynamic Tree-Remerging scheme used here t achieves higher power efficiency and scales to number of receivers without increasing the number of codes. For each transmission at most $2j + 1$ codes are used, where j is the number of jammers. The system cannot escape from jamming attacks without using at least $j+1$ codes. When there are no jammers, a transmitter can transmit on a single code. Transmissions on this code can be decoded by any legitimate receiver. The transmitter wants to transmit on a set of codes such that any user can decode

using exactly one code in the set called disjoint cover. Once jamming is detected in any codes that code should not be used by the transmitter in future. All user will lose, at most a finite number of messages due to jamming. That lose is limited using this scheme. And it allows a transmitter to split and reform a tree to reduce the number of codes in the disjoint cover. Using this Remerging, jamming will be detected at most $j[\log_2 n]$ times. The Remerging tree will be balanced using binary tree which is represented as completed binary tree that is all leaf are of same depth as shown in fig 2.

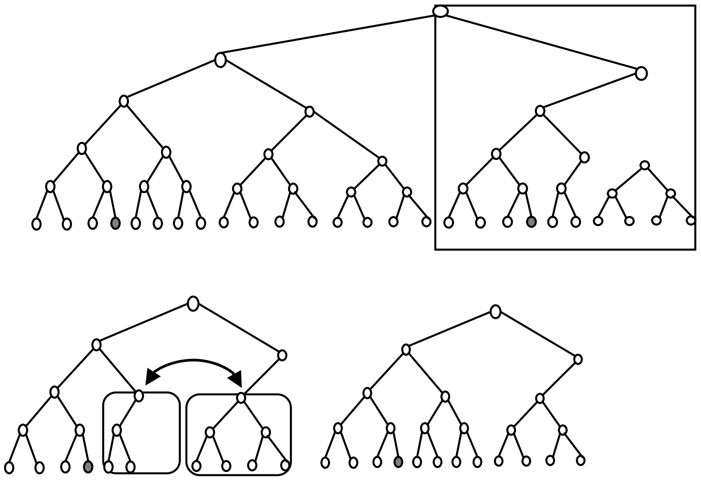
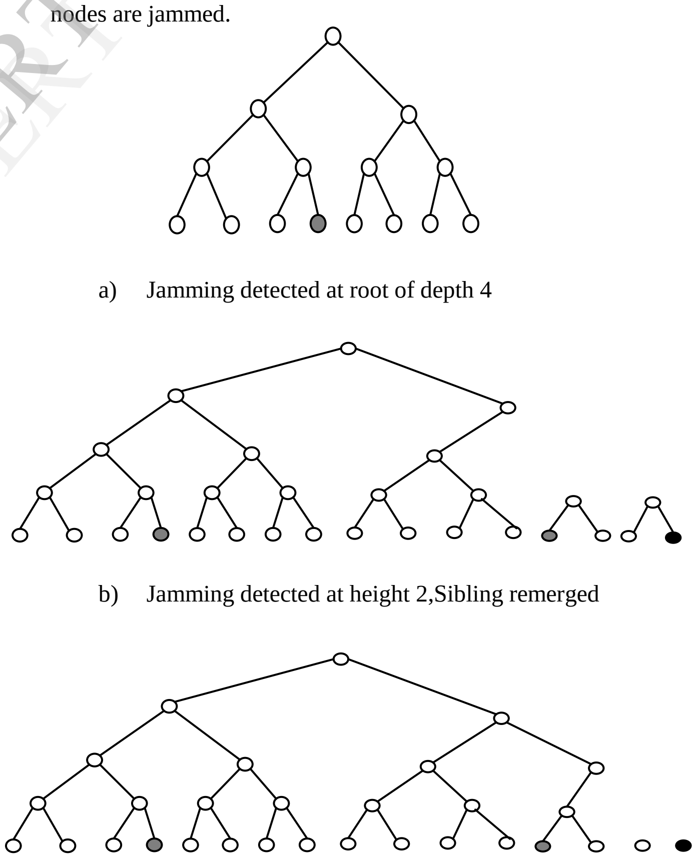


Fig 2: Code tree is merged with the main tree.

Tree Remerging: When jamming is detected in any code of the tree the Remerging is taken place by splitting the jammed nodes this reduces cost. The below fig 3 illustrates an example of Remerging when a node is jammed. The darkened nodes are jammed.



a) Jamming detected at root of depth 4

b) Jamming detected at height 2,Sibling remerged

c) Jamming detected at height 1, Sibling remerged.

Fig 3: Remerging of trees

If the scheme gives availability and termination then it must use at least j+1 codes. Emptying J periodically will reduce the false alarm to achieve power efficiency.

Disadvantage: Loss of signals when there is no jamming will raise the prospect of false alarm.

D.Jamming detection and mitigation using code tree

This paper describes the Code Tree system in which the transmitter has more information than any proper subset of receivers. Each receiver cooperates with the transmitter to detect any jamming that affects that receiver. It shows that any system uses spreading code, and no other physical factors, needs at least j+1 codes to mitigate jamming, j is the number of jammers. The fast-frequency-hopping code division multiple access (FFHCDMA) and the direct-sequence code division multiple access are the two spread-spectrum techniques used.

In a FFH-CDMA system, the entire spectrum of the communication system is divided into a number of frequency bands, and time is divided into time slots, the duration of which is much shorter than the time it takes to send 1 bit of information. Each user is assigned a frequency-hopping pattern that serves as spreading code.

In a DS-CDMA system, each bit is mapped to either 1 or 1, in which each user is assigned a pseudorandom code of length ή. To send a 1 bit, the transmitter transmits the pseudorandom code, and to send a 1 bit, the transmitter transmits the additive inverse of the code. To decode a bit, the receiver takes the inner product of the code and the signal it received; if the inner product is positive, then a -1 bit was sent, and if the inner product is negative, then a -1 bit was sent.

The spreading code used here is the secret key between sender and receiver. To avoid jamming the secret key should not be shared and so it needs to be asymmetric. This system uses the Code tree which makes some changes in the binary code tree [8].

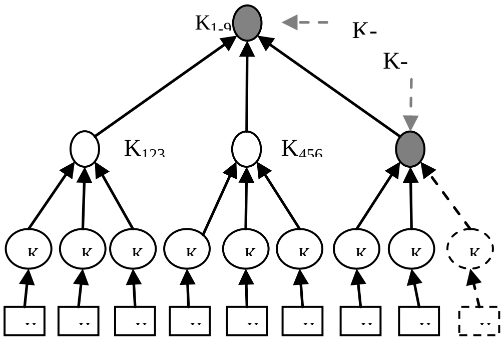


Fig 4: Multicast key graph, joined a new user (u_9)

All keys along the path from the joining point to the root node need to be changed when any new user is joined to prevent the joining user from accessing past communications. After generating new keys for these nodes, server has to securely distribute them to the other existing users as well as the joining user. For example, as shown in Fig. 5.

Each transmitter builds a balanced binary tree of randomly generated spreading codes. The transmitter associates each genuine receiver with a unique leaf in this binary tree and gives this receiver the spreading codes corresponding to that leaf and all ancestors of that leaf in the tree. Once jamming has been detected on some spreading codes the transmitter should avoid using such spreading codes in the future. When the transmitter sends a packet it uses the spreading code from the safe cover in which no jamming code has been detected so the genuine receivers can decode the packet. To detect jamming activities, the transmitter additionally transmits on a *test* spreading code that is randomly chosen from the descendants of the cover. This code allows the senders and receivers to cooperatively detect jamming on any spreading code in the cover that is an ancestor of the test spreading code. This ancestor code is called the *detectable* spreading code.

If there is no jamming detected the receiver will get one or two messages, one is from the encoded safe cover and another is from the test code. If the receiver receives the second message without the first then the detected code is suspected to be jammed. The receiver detecting jammer should report to the sender using lea node. Then the transmitter removes that code from the cover and adds its children. Jamming reports are accepted only from the host to avoid false alarms.

Tree remerging scheme allows a transmitter to split and reform a code tree to reduce the number of codes in the cover. The perception of the tree Remerging scheme is, if a code is detected to be jammed, and one of its children is also detected to be jammed. If two codes are considered to be safe they can be reassigned as a new single code. This will reduce the size of the minimal safe cover. This algorithm proves that it needs at most j+1 spreading code is needed.

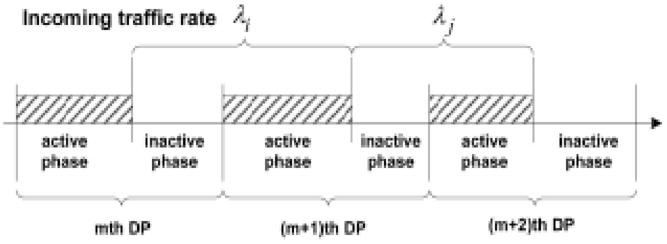
Disadvantge: When the number of jammers increases due to high interference false alarm causes the system to increase the number of size of the cover.

4.PROPOSED SYSTEM

The previous approaches are very affective in Detecting the Jamming attack in Wireless Broadcast Networking's. But the disadvantages mentioned above for detecting the Jamming attack is not having Power Efficient. Considering this problem I am proposing an approach called Power Efficient Management (PEM). This approach will be implemented with the help of Morkov Chain Mode (MCM).

In Markov Chain Model (MCM) Although each PS protocol differs in the lengths of delivery periods and in their ways to deal with multiple multicast streams, they all can be characterized by a general frame-Work. In this framework, the delivery procedure of a single frame is treated as an atomic operation, lasting for a fixed period of as we stated in assumption A2. All PS B/M data are delivered periodically in each DP. A delivery period may be a DTIM period in 802.11 PSM, an integer multiple of DTIM period in 802.11v FBMS, or a periodical service period in 802.11n PSMP. At the beginning of a DP, the AP broadcasts a notification message (may be a beacon for 802.11 PSM and FBMS or a PSMP frame for PSMP) to the network.

The message contains traffic information for data delivery, such as whether there are pending B/M data at the AP. A mobile station receiving this message determines whether there are PS data for it in this DP by parsing the information element in the message. If so, the station remains awake until a received frame has explicitly indicated the end of the data delivery for the current period by a cleared More Data field or set EOSP bit in the frame header; otherwise, the station can enter into sleep state immediately until the next DP.



The discrete MMPP model of the incoming data traffic.

In addition, there are two rules that should be followed for the data delivery procedure at the AP as follows:

R1. Once a frame (called the last frame) has indicated the end of the data delivery procedure (by a cleared More Data field or a set EOSP bit) for a stream, then all subsequent frames arriving after the transmission of that frame should be temporarily buffered until the next DP. Since in practical implementation, the setting of More Data or EOSP bit for a frame occurs at the time when putting it into the back off queue, clearly these frames arriving during the delivery time of the last frame should also be counted as buffered data for the next DP.

R2. All frames arriving before the delivery of the last frame are delivered in the current DP. This is true since at the time when setting the More Data or EOSP field of the last frame, there should be no other pending frame belonging to the stream at the AP's buffer. Otherwise, the AP cannot set a "no Data" tag to the last frame. Therefore, the last frame in a DP divides the DP into two separate phases, named as inactive phase and active phase, respectively, in this paper. In the inactive phase, all incoming PS data are buffered and no data delivery occurs, while in the active phase, all PS data backlogged since last inactive phase are delivered. The exact boundary between the two phases is the epoch when setting the More Data or EOSP bit for the last frame, which occurs at the beginning of the delivery of last frame. Thus, the active phase does not count the last frame in. In case of "delivery overflow," the active phase covers the entire DP.

5.CONCLUSION

This paper provides a protocol that allows detecting the Jamming Attack in wireless broadcast communication system with the maintenance of Power Management and dynamically changing the spreading codes used by subsets of receivers. This protocol has been developed with the help of the Morkov Chain Model (MCM). This is the optimized protocol used to mitigate jamming attack considering the maintenance of Power Management in Wireless Broadcast Networks.

6.REFERENCES

[1] J. Bellardo and S. Savage. 802.11 denial-of-service attacks:
Real vulnerabilities and practical solutions. In *Proceedings of the USENIX Security Symposium*, pages 15{28, 2003.
[2] G. Noubir and G. Lin. Low-power DoS attacks in data wireless lans and countermeasures. *SIGMOBILE Mob. Comput*
Commun. Rev., 7(3):29{30, 2003.
[3] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. 6th ACM MobiHoc*, Urbana-Champaign, IL, 2005, pp. 46–57.
[4] C. H. Bennett, G. Brassard, C. Cr´epeau, and U. Maurer. Generalized privacy amplification. IEEE Transaction on Information Theory, 41(6):1915–1923, Nov. 1995.
[5] M. Strasser, S. Capkun, C. Pöpper, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *Proc.IEEE Symp. Security Privacy*, Berkley, CA, May 2008, pp. 64–78.
[6] J. T. Chiang and Y.-C. Hu, "Dynamic jamming mitigation for wireless broadcast networks," in *Proc. 27th IEEE INFOCOM*, Phoenix, AZ, Apr. 2008, pp. 1211–1219.
[7] J. T. Chiang and Y.-C. Hu, "Cross-layer jamming detection and mitigation in wireless broadcast networks," in *Proc. 13th Annu. ACM MobiCom*, Montréal, QC, Canada, 2007, pp. 346–349.
[8] C. K.Wong, M. Gouda, and S. S. Lam, "Secure group communications using key graphs," *IEEE/ACM Trans. Netw.*, vol. 8, no. 1, pp. 16–30, Feb. 2000.