ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

Vol. 4, Issue 4, April 2016

# Time-Delayed Broadcasting for Defeating Inside Jammers

Sangeetha V[1,] Sushma N[2], Sushma S G[2], Yeshaswini H[2], Rajesh D[2]

Assistant Professor, Dept. of Computer Science and Engineering, K.S.Institute of Technology, Bangalore, India[1]

8th sem, B. E Students, Dept. of Computer Science and Engineering, K.S.Institute of Technology, Bangalore, India[2]

**ABSTRACT:** Jammers in the wireless network jams the user signals adding more interference signals. Due to that user unable to grasp their own signal from the jammed network. The problem is how to recover the jamming signals to receive the emergency broadcasting message. This is called jamming-resistant broadcast communications under an internal threat model. So implement a novel Time-delayed broadcast scheme (TDBS), which implements the broadcast operation as a sequence of unicast transmissions scattered in frequency and time. TDBS does not rely on commonly shared secrets, or the existence of jamming-immune control channels for coordinating broadcasts. Instead, each node follows a unique pseudo-noise (PN) frequency hopping sequence. TDBS differs from conventional FHSS designs in that two communicating nodes do not follow the same FH sequence, but are assigned exclusive ones. Unlike the typical broadcast in which all receivers tune to the same channel, TDBS propagates broadcast messages as a sequence of unicast transmissions, spread both in frequency and time. To ensure resilience to inside jammers, the locations of these unicast transmissions, defined by a frequency band/slot pair, are only partially known to any subset of receivers. Assuming that the jammer can only interfere with a limited number of frequency bands, a subset of the unicast transmissions are intrusion-free, thus propagating broadcast messages.

**KEYWORDS**: TDBS, Jammers, unicast, broadcast ,Pseudo-noise sequence,FHSS.

## I. Introduction

Wireless networks make use of mutual transmission medium; therefore, they are open to several malicious attacks. An intruder with a radio transceiver intercepts a transmission, injects spurious packets, and blocks or jams the legitimate transmission[1]. Jammers interrupt the wireless communication by generating high-power noise across the entire bandwidth in the vicinity of the transmitting and receiving nodes. Since jamming attacks drastically degrade the performance of wireless networks, some efficient mechanisms are required to detect their presence and to avoid them. Constant, deceptive, reactive, quick, and random jammers are few jamming techniques used in wireless medium. All of them can partially or fully jam the link at unstable level of detection probabilities.

Jammer prevents the successful communication involving source and destination. Jammer node is a node which restricts the signal transmission among two nodes[2]. There are two types of jammer nodes. They are internal jammer nodes and external jammer nodes. Internal jammer nodes are distinct as the node that is present in the cluster has a chance to become jammer in future. External jammer nodes are distinct as the nodes that are outside the clusters.There are four types of jammer. They are: Constant jammer, Deceptive jammer, Random jammer and Reactive jammer. Constant Jammer is the emission of arbitrary bits which keeps the channel busy and lastly the packets will be collided. Deceptive Jammer is a dangerous kind of attack through which the attacker does not demonstrate their presence. It misleads WSN's operator to provide fake data. Random jammer switches among constant jammer and deceptive jammer. Jammer sleeps for ts random time and jams for tj random time. By changing $t_s$ and $t_j$we can achieve power saving and effectiveness. Reactive jammer listens for the channel activity and collides the packet finally. Apart from this type of jamming there are also additional jammers like Spot jammer, Barrage jammer, Sweep jammer.

Security challenges are rising day by day as the adversary are finding new ways to detect the confidential transmissions hence there is aimmense need to think differently over the situation. Since the traditional ways of defending the attack is not satisfying the need of security, hence a new approach towards this problem is required[3]. Jamming resembles to

denial-of-service attack and thus prevents genuine users to send its data as the jammers purposefully emits radio frequency signals to alter wireless transmissions. the most harder to detect is the reactive jammer since compared to others which are active in character i.e. they attempt to block the channel without having any prior information of the traffic sample on the channel while the reactive jammer reside quiet when the channel is inactive, but starts transmitting a radio signal as quickly as it senses some movement on the channel. Thus reactive jammers are harder to detect and needs more capable identification and protecting system.There are different techniques for sensing the jammed areas which has been conceded out and studied against the jamming attacks.
The jammer can't change over a bit '1' to a bit '0'; it was shown that a jammer cannot erase packets from the wireless channel. Popper et al.projected a method called Uncoordinated DSSS (UDSSS), in which broadcast transmissions are spread according to a PN code, arbitrarily selected from a public codebook. Receivers decode transmitted messages by exhaustively applying every PN code in the public codebook.The Time-Delayed Broadcast Scheme (TDBS) as an urgent situation mechanism for temporarily restoring broadcast communications awaiting inside jammers are actually removed from the network. TDBS differs from traditional FHSS designs in that two communicating nodes do not pursue the same FH sequence, but are assigned unique ones. Unlike the distinctive broadcast in which all receivers adjust to the same channel, TDBS propagates broadcast messages as a series of unicast transmissions, widen both in frequency and instance. To ensure resilience to inside jammers, the locations of these unicast transmissions, describe by a frequency band/slot pair, are only moderately known to any subset of receivers. pretentious that the jammer can only interfere with a limited number of frequency bands, a subset of the unicast transmissions are interference-free, thus propagating broadcast messages

## II. RELATED WORK

M. J. Abdel Rahman et al.[4]have proposed communications in a dynamic spectrum access (DSA) network requires communicating nodes to "rendezvous" before transmitting their data packets. Frequency hopping (FH) provides an effective method for rendezvousing without relying on a predestined control channel. FH rendezvous protocols have mainly targeted pairwise rendezvous, using fixed (non-adaptive) FH sequences and presumptuousa uniform spectrum environment, i.e., all nodes perceive the same variety opportunities. In this paper, we address these limitations by developing three multicast rendezvous algorithms: AMQFH, CMQFH, and nested-CMQFH. The three algorithms are intended for asynchronous spectrum-heterogeneous DSA networks. They provide different tradeoffs between speed and toughness to node compromise. We use the uniform k-arbiter and the Chinese remainder theorem (CRT) quorum systems to design our multicast rendezvous algorithms. We also design two "optimal" channel ordering mechanisms for direct sensing and assignment, one for AMQFH and the other for CMQFH and nested-CMQFH. Finally, we develop a practical out-of-band sensing based dynamic FH (DFH) algorithm for online adaptation of the FH sequences used in the proposed assignation algorithms. Extensive simulations are used to evaluate our algorithms.

ParamvirBahl et al. [5]have proposed Capacity improvement as one of the principal challenges in wireless networking. We present a link-layer protocol called Slotted Seeded Channel Hopping, or SSCH, that increase the capacity of an IEEE 802.11 network by utilizing frequency variety. SSCH can be implemented in software over an IEEE 802.11-compliant wireless card. Each node using SSCH switches diagonally channels in such a manner that nodes desiring to communicate overlap, while disjoint communications mostly do not overlap, and hence do not hold up with each other. To achieve this, SSCH uses a novel scheme for distributed assignation and synchronization. Simulation results show that SSCH drastically increases network capacity in several multi-hop and single-hop wireless networking scenario.

L. C. Baird et al. [6] have proposed omnidirectional and radio frequency (RF) communication, which is considered, haschallenge to jamming by the use of a secret key that is shared by the sender and receiver. There are no known methods for achieving jam conflict without that shared key. Unfortunately, wireless communication is now reaching a scale and a level of magnitude where such secret-key systems are becoming impractical. For example, the national side of the Global Positioning System (GPS) cannot use a shared secret, since that secret would have to be given to all 6.5 billion impending users, and so would no longer be secret. So civilian GPS cannot currently be confined from jamming. But the FAA has stated that the civilian airline industry will transition to using GPS for all navigational aids, even during landings. A terrorist with a simple jamming system could wreak havoc at a major airport. No existing system can solve this problem, and the problem itself has not even been widely discussed. The problem of keyless jam resistance is important. There is a great need for a system that can broadcast messages without any prior secret shared between the dispatcher and recipient. We propose the first system for keyless jam resistance: the BBC algorithm. We describe the programming, decoding, and broadcast algorithms. We then analyze it for expected resistance to jamming and error rates. We show that BBC can achieve the same level of jam resistance as traditional spread spectrum systems, at just under half the bit rate, and with no shared secret. Furthermore, a hybrid system can achieve the same average bit rate as traditional systems.

K. Bian et al.[7] have proposed how to establish a control channel for medium access control with a challenging problem in multi-channel and dynamic spectrum access (DSA) networks. In the design of multi-channel MAC protocols, the use of channel (or frequency) hopping techniques (a.k.a. parallel rendezvous) have been proposed to avoid the bottleneck of a single control channel. In DSA networks, the dynamic and opportunistic use of the available spectrum requires that the radios are able to "appointment"— i.e., find each other to establish a link. The use of a dedicated global control channel simplifies the rendezvous process but may not be feasible in many opportunistic spectrum sharing scenarios due to the dynamically changing accessibility of all the channels, including the control channel. To address this trouble, researchers have proposed the use of channel hopping protocols for enabling rendezvous in DSA networks. This paper presents a logical approach, based on quorum systems, for designing and analyzing channel hopping protocols for the purpose of control channel concern. The proposed approach, called Quorum-based Channel Hopping (QCH) system, can be used for implementing assignation protocols in DSA networks that are robust against link breakage caused by the manifestation of incumbent user signals. We describe two most favorable QCH systems under the assumption of global clock synchronization: the first system is most favorable in the sense that it minimizes the time-to-rendezvous between any two channel hopping sequences; the second system is most favorable in the sense that it guarantees the even distribution of the assignation points in terms of both time and channel, thus solving the rendezvous convergence problem. We also offer an asynchronous QCH system that does not require global clock synchronization. Our analytical and simulation consequencesdemonstrate that the channel hopping schemes designed using our framework outperform existing schemes under various network conditions.

A. Chan et al. [8] have addressed the problem of countering jamming of broadcast control channels in wireless communication systems. Targeting control travel on a system, e.g., BCCH channel in GSM, leads to smart attacks that can be four orders of extent more efficient than blind jamming. We propose several schemes based on coding theory and its applications that can counter both outside and interior attackers (traitors). We introduce a T-(traitor) resilient scheme that requires less than $(T\log_T N)^2$ control information transmissions and guarantees delivery of control information against any coalition of T traitors. The proposed scheme also allows the recognition of persistently jamming traitors.

## III. PROPOSED SYSTEM

### A. *Description:*

- TDBS broadcast series of unicasts distributed in frequency and time. The locations of these unicasts, defined by a frequency band/slot pair are only partially known to each node.
- All nodes are divided into pairs scheduledto communicate over arbitrarily selected frequencybands.
- The pairs and assigned frequency bands changeon a per-slot basis, thus realizing a FH method.
- TDBS differs from conventional FH designs in that:
- Nodes do notfollow a common FH sequence, but hop according tounique hopping patterns and,
- These patterns are coordinatedto reduce the broadcast delay.
- All nodes are divided into pairs scheduledto communicate over randomly selected frequencybands.
- The pairs and assigned frequency bands changeon a per-slot basis, thus realizing a FH system.

### B. *Description of the Proposed Algorithm:*

Aim of the proposed algorithm is to maximize the network life by minimizing the total transmission energy using energy efficient routes to transmit the packet. The proposed algorithm is consists of three main steps.

Step 1: Splitting Algorithm:

- Analyse the number of edges in the network.
- Based on 1-factorisation method, assign the frequency for the node with the slot 'i' is zero initially.
- While increase the slot, rotate the node pair in clockwise direction and assign the frequency.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Step 2: Sequential unicast Algorithm:
Consider the number of node group and assign the frequency limit K=n+1. Here permutation is used for getting the limited frequency randomly. Minimum number of frequencies is used for channel allocation by min() method.

Step 3: Assisted Broadcast Algorithm:
This algorithm makes the efficient use of reusable frequency signals similar to SU mode. Slots are mainly helpful for randomly changing the channel frequency.

## IV. PSEUDO CODE

**Sequential unicast Algorithm**

```
    Step 1: Construct a 1-factorization $F_{2n}$ of $K_{2n}$; where $F_{2n}$ = {$F_0$, $F_1$... $F_{2n-2}$}.
    Step 2: For all $F_i$€ $F_{2n}$; repeat Steps 3–5.
    Step 3: Randomly select permutation $\pi$ € $P_K$ with replacement.
    Step 4: Assign frequency bands in $\pi$ to the first min {n, K} unassigned pairs in $F_i$.
    Step 5: Repeat Steps 3 and 4 until all pairs in $F_i$ are assigned a frequency band.
    Step 6: Repeat Steps 1–5.
```

**Assisted Broadcast Algorithm**

```
    Step 1: Obtain an arbitrary 1-factor $F_0$ of $K_{2n}$. Set i = 0.
    Step 2: Randomly select a permutation $\pi$ € $P_K$.
    Step 3: Assign frequency bands in $\pi$ to the first min {n, K} unassigned pairs in $F_i$.
    Step 4: Repeat Steps 2 and 3 until all pairs in $F_i$ are assigned a frequency band.
    Step 5: Construct 1-factor $F_{i+1}$ according to the splitting algorithm. Set i = i + 1.
    Step 6: Repeat Steps 2-5.
```

## V. RESULTS

The proposed TDBS is a scheme for jamming-resistant broadcast communications in the presence of inside jammers. In TDBS, broadcast is realized as a series of unicast transmissions distributed in frequency and time.To ensure the successful deployment of pervasive wireless networks, it is crucial to localize jammers, since the locations of jammers allow a better physical arrangement of wireless devices that cause unintentional radio interference, or enable a wide range of defense strategies for combating malicious jamming attackers. It mainly focus on one common type of jammer - constant jammers. Constant jammers continually emit radio signals, regardless of whether the channel is idle or not. Such jammers can be unintentional radio interferers that are always active or malicious jammers that keep disturbing network communication.
The graph shows the jamming probability when the number of nodes k=20.The jamming probability varies slightly when compared to theoritical value during the simulation.

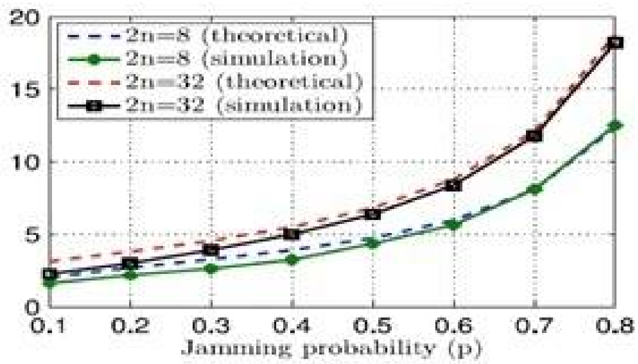

Fig 1:Function of the jamming probability p when K=20

DOI: 10.15680/IJIRCCE.2016. 0404127

## VI. CONCLUSION

The broadcast operation is a series of unicast transmissions distributed in frequency and time. TDBS does not rely on commonly mutual secrets, or the existence of jamming-immune control channels for coordinating broadcasts TDBS, broadcast is realized as a series of unicast transmissions distributed in frequency and time. This is the efficient way of overcoming jammer in the wireless network.Further developed mechanisms for updating the FH sequences assigned to nodes, when the broadcast group is dynamic. We mapped the problem of minimizing the number of FH sequence changes required for node addition, to the problem of discovering rainbow paths in proper edge-colored complete graphs. We analytically evaluated the security properties of TDBS under both an external and an internal threat model and showed that TDBS maintains broadcast communications even when multiple nodes are compromised.

## ACKNOWLEDGMENT

We would like to thank VGST for carrying out the research project in Research Centre,Department of Computer Science and Engineering, K.S.Institute of Technology, Bangalore. We would also extend our gratitude to Mrs Rekha B Venkatapur, Professor and Head, Department of Computer Science and Engineering, K.S.Institute of Technology, Bangalore.

## REFERENCES

1. Nadeem Sufyan,Nazar Abbass Saqib, and Muhammad Zia,“ Detection of jamming attacks in 802.11b wireless networks”, EURASIP Journal on Wireless Communications and Networking, vol.2013:208,15 August 2013.
2. J. Thangapoo Nancy, K. P. VijayaKumar, and P. Ganesh Kumar, “Detection of jammer in Wireless Sensor Network”,International Conference on Communications and Signal Processing (ICCSP), 10.1109/ICCSP.2014.6950086, pp. 1435-1439, 2014.
3. A. A. Bodkhe, and A. R. Raut, “Identifying Jammers in Wireless Sensor Network with an Approach to Defend Reactive Jammer,” Communication Systems and Network Technologies (CSNT),10.1109/CSNT.2014.26 , pp. 89-92, 2014.
4. M. J. Abdel Rahman, H. Rahbariand M. Krunz, “Adaptive frequency hopping algorithms for multicast rendezvous in DSA networks” Dynamic Spectrum Access Networks (DYSPAN), WA, 2012, pp. 517-528, 2012.
5. ParamvirBahl, Ranveer Chandra, John Dunagan,“Slotted seeded channel hopping for capacity improvement”, IEEE 802.11 on adhoc wireless network.
6. L. C. Baird, W. L. Bahn, M. D. Collins, M. C. Carlisle, and S. C. Butler, “Keyless Jam Resistance” Information Assurance and Security Workshop,10.1109/IAW.2007.381926,pp. *143-150, 2007.*
7. K.Bian, J. M. Park, and R. Chen, “Control Channel Establishment in Cognitive Radio Networks using Channel Hopping” in IEEE Journal on Selected Areas in Communications,10.1109/JSAC.2011.110403, vol. 29, no. 4, pp. 689-703, April 2011.
8. A. Chan, X. Liu, G. Noubir, and B. Thapa, “Broadcast Control Channel Jamming: Resilience and Identification of Traitors”, 2007 IEEE International Symposium on Information Theory,10.1109/ISIT.2007.4557594, pp. 2496-2500, 2007.

## BIOGRAPHY

**Sangeetha.V**is working as Assistant Professor at Department of Computer Science and Engineering, K.S.Institute of Technology, Bangalore, Karnataka. India. Received **B.E** degree in Computer Science and Engineering from Acharya Institute of Technology, Bangalore, VTU, Karnataka, India in 2004. Received **M.Tech** degree in Computer Science and Engineering from R.V.College of Engineering, Bangalore, VTU, Karnataka, India in 2011.Currently pursuing the part time **Ph.D** in Computer Science & Engineering from VTU, Karnataka, India. Her research interest includesMobile Adhoc Networks, Network Security, WirelessNetworkS.

**SushmaN,Sushma S G,Yeshaswini H and Rajesh D** are Project Team members of Final year Academic Project, Pursuing BE 8th semester, Department of Computer Science and Engineering,K.S.Institute of Technology, Bangalore, India.