BROADCASTING THE MESSAGE OVER THE NETWORK USING DIFFERENT FREQUENCY AND TIMING TECHNIQUE TO BYPASS THE JAMMERS

Pooja.S[1], Pooja.K.B[2]

Department of Computer Science and Engineering, Global Academy of Technology (GAT), Rajarajeshwari Nagar, Bangalore, India,
poojasuresh0709@gmail.com
Department of Computer Science and Engineering, Global Academy of Technology (GAT), Rajarajeshwari Nagar, Bangalore, India
pooja.kb04@gmail.com

Abstract

The author addresses the problem of Jammers present in wireless network by jamming the user signals by adding more interference signals. This paper gives the solution to recover the jamming signals to receive the emergency broadcasting message. This paper implements a novel time-delayed broadcast scheme (TDBS). The transmissions are unicast and are broadcasted in a series in consideration with time and frequency. TDBS neither reckons on the secrets that are shared nor on the controlling channels of the jammer system for coordinating the broadcasts. Instead there is presence of Pseudo Noise (PN) frequency hopping system which is unique and followed by every single node. TDBS is divergent from the designs of Frequency Hopping Spread Spectrum (FHSS) and these nodes do not follow the same Frequency Hopping (FH) sequence, instead they are deputized with unique ones. Contradicting to every other typical broadcast where all the receivers have similar channels, TDBS have the transmissions that are unicast and present in series to broadcast the messages using time and frequency. For the flexibility of the jammers present inside, the unicast transmissions location that is defined by the frequency band are partially known to the subset of receivers. By making an assumption that the jammers can thwart with very few number of frequency bands, the subset of transmissions are thwart-free and thus proliferating the broadcasted messages.

Keywords: *Jamming, Broadcast Communications, Denial-of-Service, Wireless Networks, Graph Factorization, Security.*

---***---

I. INTRODUCTION

Wireless networks are used to connect the network nodes using wireless data connections thus they are open to many malignant and harmful attacks. The transmission process will be blocked or jammed by the intruder by injecting fraudulent packets. These fraudulent packets can also be called as jammers. Jammers are illegal and their use in the wireless networks can result in huge fines. Jamming works by not allowing the authorized users as legitimate traffic is jammed using staggered frequencies. Due to this Jammers attack, the efficiency of the wireless communication drastically decreases. Thus different methods are need to be found to detect the presence of the jammers or the jamming device, to avoid them in the transmission process[1-2].

Jammers prevent the communication between the two nodes by not allowing the signal transmission to take place between them. The two nodes are referred to as source node and the destination node. The jammer nodes to reject the signal transmission can be present within the cluster of nodes. Such type of jammer nodes are called as internal jammers. The nodes which are detected outside the cluster are known as external nodes. There are several jamming strategies that have been introduced recently. There are mainly four types of jamming models [5]. They are constant jammers, reactive jammers, eavesdropper jammers and random jammers.

Constant jammers are the one which sends the jamming signals in a transmission process at constant intervals. When there is any communication present in the channel then reactive jammers send jamming signals at constant duration. The eavesdropper jammer does the work of listening and records the wireless traffic in channels. Random jammers send the jamming signals at any randomly chosen interval. The four models are as shown in the below (figure.1).

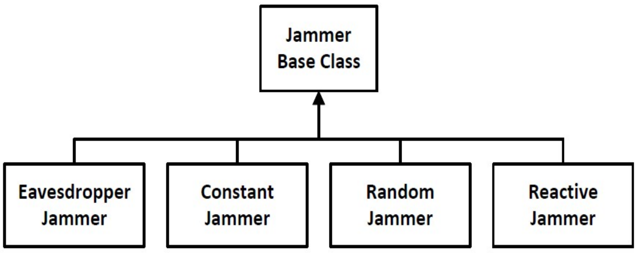


Fig.1 Types of jammers

Since there is increase in the security challenges everyday and there are new ways detected for the confidential transmissions, there is an immense need to think over the situation [3]. Since the traditional approaches do not work, new approaches towards this problem are required. Jamming resembles the denial of service attack by emitting the radio frequency signals to alter the wireless transmissions and thus prevents its users from sending its data through wireless networks.

The reactive jammers are the hardest to detect if present, as they do not react unless there is sound detected in the communication channel. If there is no noise present in the channel then the reactive jammers stay inactive while the other jammers sends the jamming signals without having any prior information of the traffic sample on the channel. There are different techniques for sensing the jammed signals. Popper et al. introduced a technique called Uncoordinated DSSS (UDSSS). In this technique a pseudo noise (PN) code is used to broadcast the messages by applying every PN code. Thus Time Delayed Broadcasting Scheme (TDBS) is a mechanism for restoring the broadcast messages temporarily.

TDBS differs from the traditional Frequency Hopping Spread Spectrum [FHSS] designs and do not undergo the same Frequency Hopping [FH] sequence. TDBS broadcasts the messages as a series of unicast transmissions using both frequency and time that are generated using 1-factorization method. The location of these unicast transmissions are known only to the subset of the receivers, aware that the jammer can interference with only limited number of frequency bands, the subset of frequency bands are free from the interference and thus broadcast the messages[15-19].

This paper is organized as follows. Section 2 gives a Brief overview of the related work. Section 3 describes the proposed system and its implementation. Section 4 shows the result and conclusion is given in Section 5.

II. RELATED WORK

Uncoordinated direct sequence spread spectrum (UDSSS) is a spread spectrum communication scheme where the sender and the receiver communicate using secret spreading codes that they choose randomly and independently from a public set of channels. The receiver is unaware of the codes used by the sender to transmit the messages prior to their communication. By using UDSSS type of broadcast, the escalations of transmissions are done in consonance with the PN code, tabbed randomly from the public codebook. By exhaustively applying each and every PN code in the public codebook, the receivers decode the transmitted messages. With ample computational power an advanced adversary can jam a UDSSS system if it can recover before the end of an ongoing transmission by selecting the PN code from the public codebook. RDDSSS delays the exposure of the secret PN code and is resilient to the reactive jammers. Thus the prevention of jammer from acquiring the PN code before the message will be completely received is done by delaying the seed disclosure.

To vanquish the presence of jammers in the communication network the most traditional way employed is frequency hopping technique. It can either be proactive or reactive. Considering the reactive case, the presence of jammers is perceived by the nodes in the network and hence it transits to a different channel and remits a beacon message on the new channel, ensuring its presence. The neighbors of non-jammed network will recognize the absence of the nodes and as a result will change their bands of operation to verify with the other channels whether the nodes have sent beacons promulgating the presence of it on a different channel. If the beacons are not detected on any of the channels then they assume that the nodes just moved away. In defiance of, if the beacon is apperceived then they will edify the other nodes in to switch the channels to the other new ones. [3]

Direct sequence spread spectrum (DSSS) is a technology used for the transmissions done in the local area wireless network. In the above technology, merging of a data signal with a high data rate bit sequence is done, which results in the division of the user data based on the spreading ratio. The frequency channel which will be present across the spectrums will be associated with small pieces of information that is present in DSSS. This technology also consists of the chipping code. This code is a redundant bit pattern cohered with each bit transmitted. The signal's resistance towards the interference increases due to the chipping code. Even if there are many hurdles during the transmissions and the data is lost or blemished, the original data can be recovered due to the redundancy of transmission. The radio frequency carrier and a pseudo-noise (PN) digital signal plays vital role in the entire process. The sizable benediction of using the above technology are sharing signal channels among multiple users, relative timing between transmitter and receivers, resistance to jamming and less background noise. [3].

Disadvantages of the typical broadcast are where all receivers tune to the same channel, then only message can be received. The problem can be occurred while unicast-transmissions are distributed in time and frequency and can be viewed as a problem of link scheduling under node-exclusive interference model. Jammers are able to receive the broadcasting information spoiling the overall networking resources. It is an unauthorized process as there is no guarantee to deliver data.

III. PROPOSED DESIGN

Based on the distribution of time and frequency, a series of unicasts transmissions are broadcasted by TDBS scheme. These unicasts locations are only partially known to each node and they are defined by frequency band. The nodes communicate over the randomly selected frequency bands and these nodes will be present in pairs. The frequency assigned to these pair of nodes change according to per-slot basis, hence attaining the FH method. According to TDBS scheme the nodes follow a unique hopping pattern and these coordinated patterns lessen the delay of broadcast and hence they do not sequence a common FH sequence. [11-15]

3.1 Proposed System Architecture

The procedure of interpreting the modules, data for a system, architecture and components to satisfy the given requirements is called as system design. Development of the product is done using the application of the system theory. The principles of system engineering, system analysis and system architecture overlaps with each other. [7-9]. Designing includes act of information marketing along with the creation of the product to be manufactured.

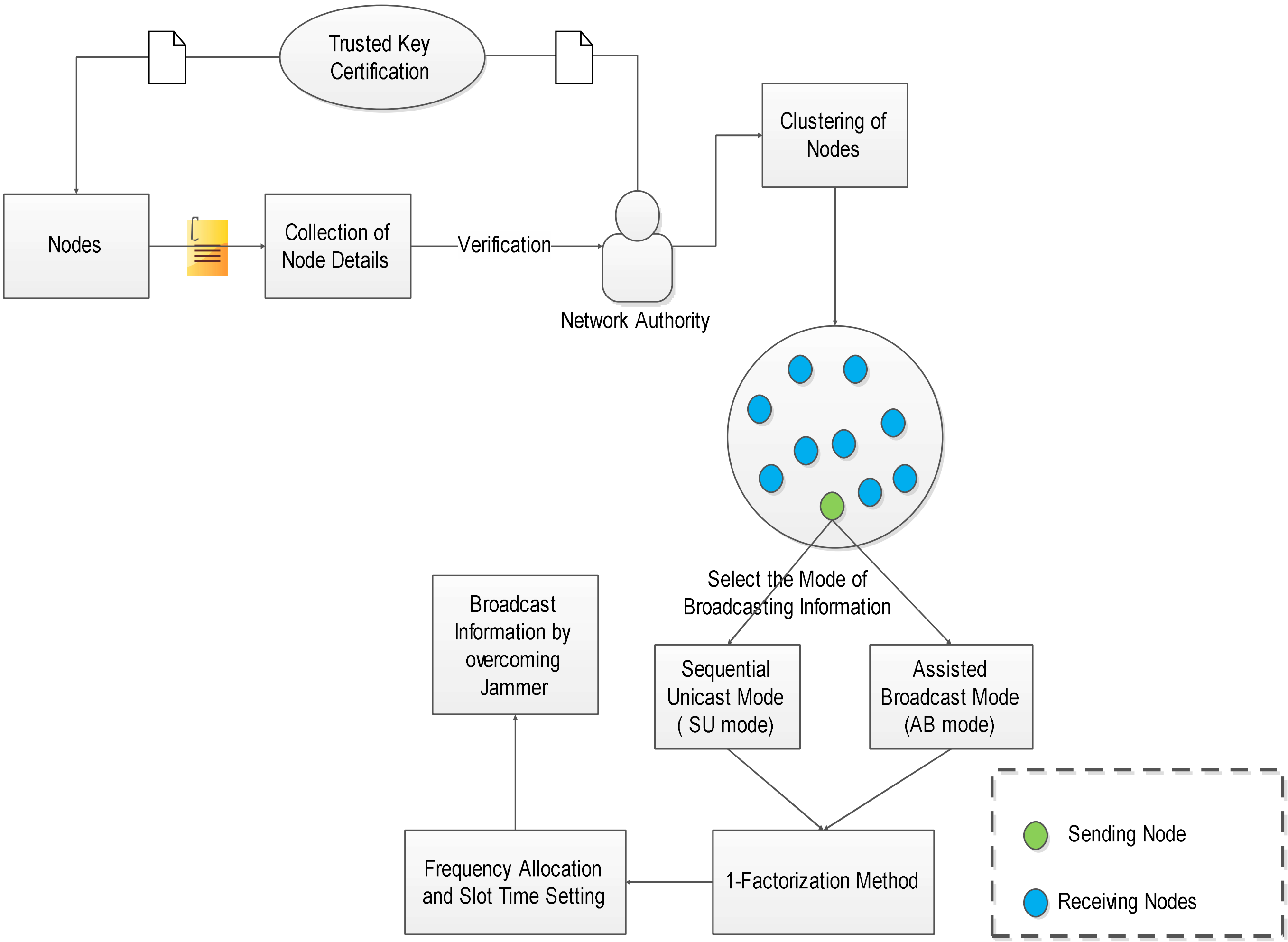

Trusted Key Certification
Nodes
Collection of Node Details
Verification
Network Authority
Clustering of Nodes
Select the Mode of Broadcasting Information
Broadcast Information by overcoming Jammer
Sequential Unicast Mode (SU mode)
Assisted Broadcast Mode (AB mode)
Sending Node
Receiving Nodes
Frequency Allocation and Slot Time Setting
1-Factorization Method

Fig.2 Proposed system architecture

In this proposed System architecture (Figure.2) assuming TCA to be the trustworthy of the wireless communication network, each node will be registered to the network authority along with its details. TCA verifies the node detail with the network authority after the verification process is done it sends the trusted key certificate to the nodes. Once the clustering of the nodes are done the frequency for each nodes are generated and the nodes with similar frequency are paired using the 1-Factorization method. We can broadcast the messages by overcoming jammers using two types of methods:

1) Sequential Unicast Method 2) Assisted Unicast Method.

3.2 System Modules

3.2.1 Trusted Central Authority certification for the node

Each node has to register their details to the central network authority in the wireless network communication by considering central network authority (Figure.3) as trustworthy in the whole data transmission process. In order to the registered node information, trusted central authority verifies the details provided by each node. After validation all details, this authority generates the authentication certification with unique node id by saving all node details in server database.

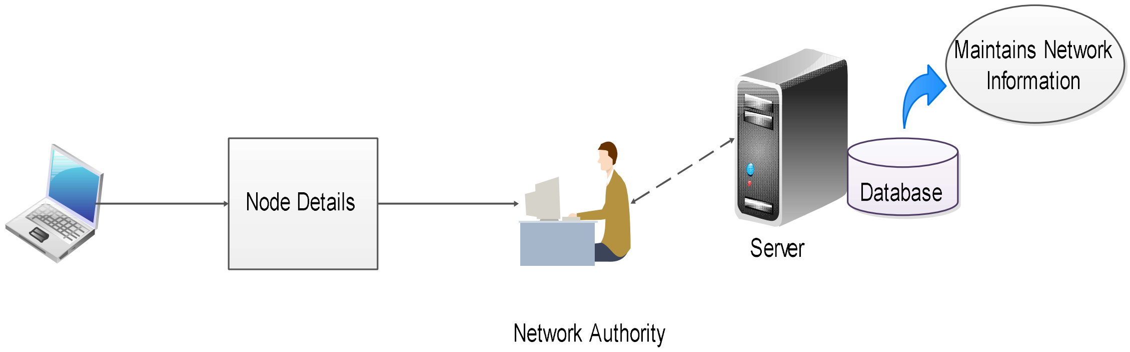


Fig.3 Trusted Central Authority

3.2.2 Mapping to1- Factorization Method for nodes

In mapping to 1-Factorization method (Figure.4) first, count the number of edges in the networking nodes and let it be €. Generally number of edges are €= 2n-1 where 2n represent the total number of nodes in network. In a schedule constructed according to F_{2n}, every node rendezvous with all remaining (2n - 1) nodes. Using Splitting Algorithm, assign the frequency for time slot *i*.

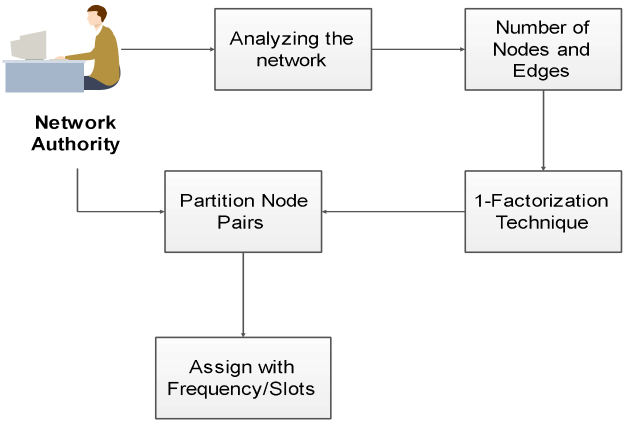

Network Authority
Analyzing the network
Number of Nodes and Edges
1-Factorization Technique
Partition Node Pairs
Assign with Frequency/Slots

Fig 4. Mapping to 1- Factorization

3.2.3 Sequential Unicast Mode for Single Hop broadcast

Sequential unicast mode (Figure.5) represents the broadcasted data with different frequency signals based on the distance between receiver and particular sender. Using TDBS-SU - Sequential Unicast Mode algorithm, broadcasts the data to all the receivers by the single sender only, in which random permutation is used to select current receivers within their vicinity.

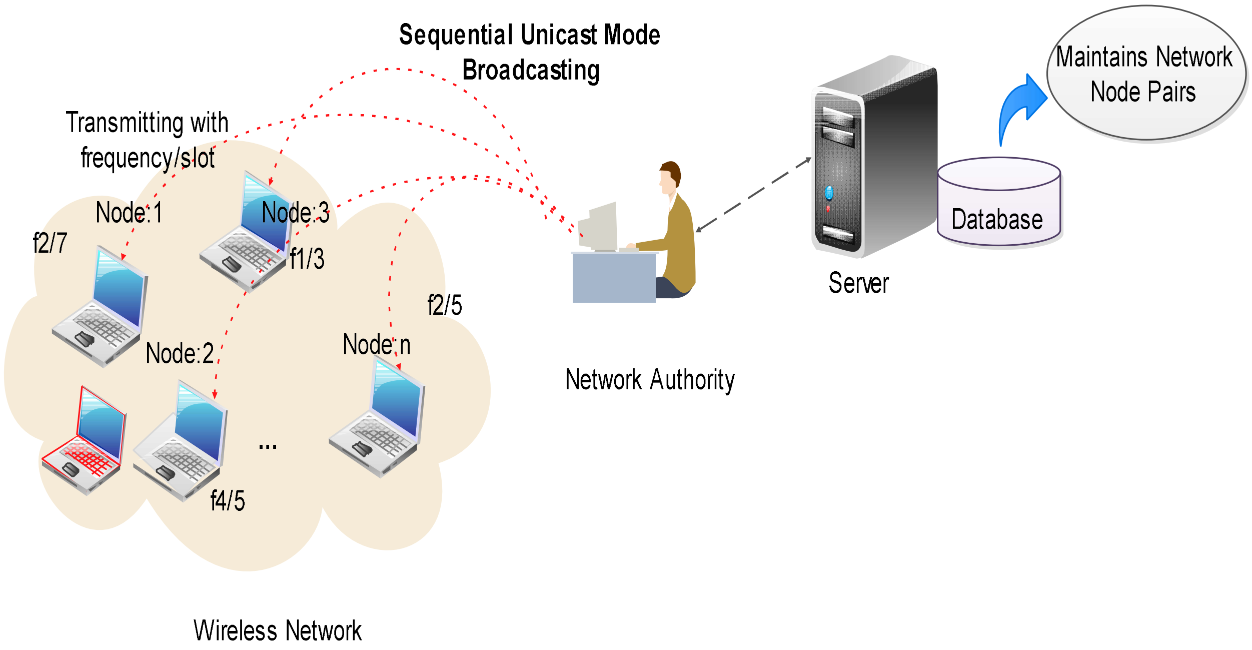

Sequential Unicast Mode Broadcasting
Transmitting with frequency/slot
Node:1
Node:3
f2/7
f1/3
f2/5
Node:2
Node:n
...
f4/5
Maintains Network Node Pairs
Database
Server
Network Authority
Wireless Network

Fig.5 Sequential Unicast Mode for Single Hop broadcast

3.2.4 Assisted Broadcast Mode for Single Hop broadcast:

In this mode sender send their data to their direct neighbors with the certain frequency. After accepting the data, receiver needs to send them to their neighbors. This method of transmission solves problem of various frequency signals and reusability of signals with particular is possible is shown in bellow (Figure.6).

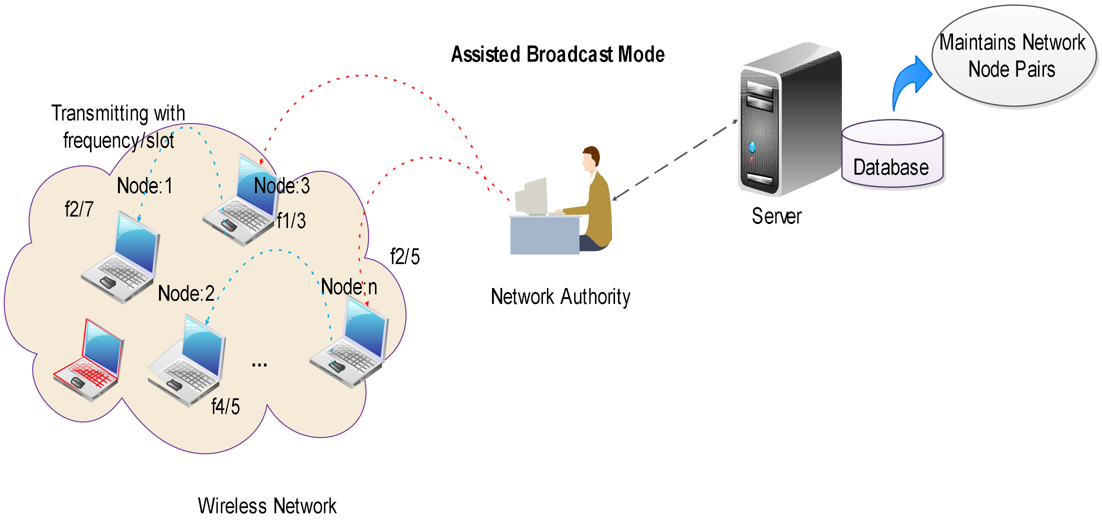


Fig.6 Assisted Broadcast Mode for Single Hop broadcast

3.3 Data Flow Diagram for Time Delayed Broadcasting Scheme

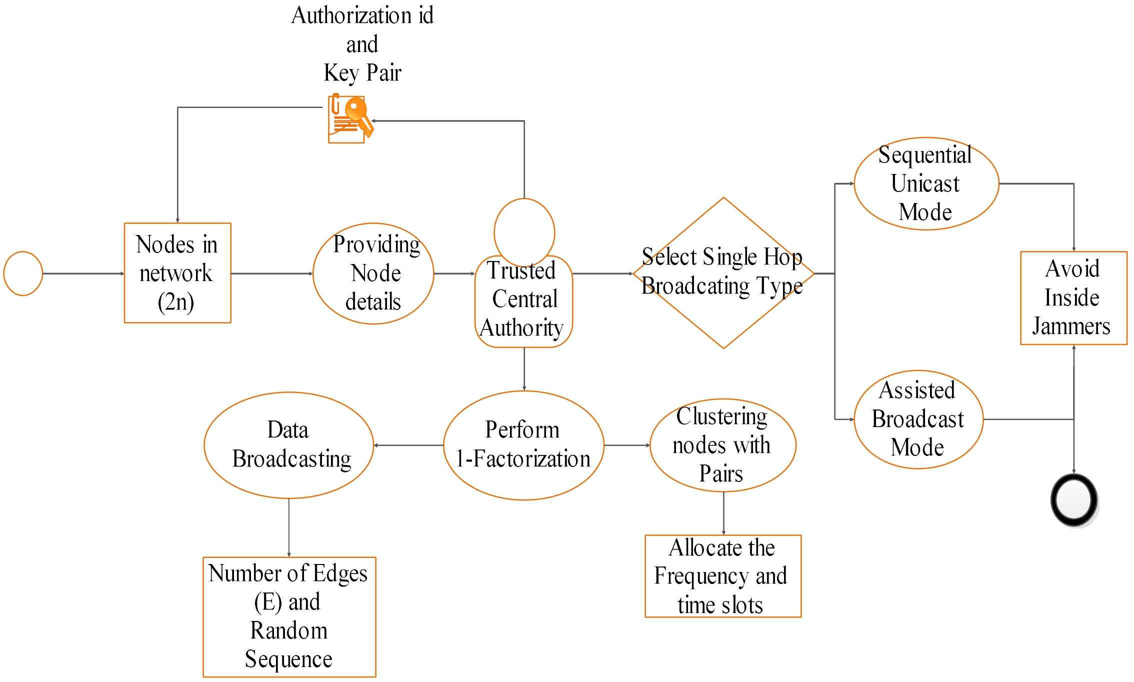

Authorization id and Key Pair
Nodes in network (2n)
Providing Node details
Trusted Central Authority
Select Single Hop Broadcasting Type
Sequential Unicast Mode
Assisted Broadcast Mode
Avoid Inside Jammers
Data Broadcasting
Perform 1-Factorization
Clustering nodes with Pairs
Allocate the Frequency and time slots
Number of Edges (E) and Random Sequence

Fig.7 Data Flow Diagram for time Delayed Broadcasting Scheme

The explanation of the above Fig.7 is as follows: Firstly each nodes in the network (number of nodes in the network are given by 2N and number of edges are given by E=2N-1) are registered with their node details in the Trusted Central Authority (TCA).Once the TCA receives the node details it verifies and validates with their own node details and generates its own unique node id for all the nodes. After generation of the unique node id for all the nodes, the message has to be broadcasted to the receivers using the two modes Sequential Unicast Mode and Assisted Broadcast Mode by avoiding the inside jammers. The TCA analyses and performs the 1-Factorization Method by pairing the nodes(in the network)with the same frequency. Once the frequency is generated for all the nodes in the network, the clustering of the nodes is done that is., allocate the frequency and time slots for the nodes in the cluster. The data is broadcasted to the receivers within their vicinity by using the random sequence permutation.

3.4 Case Diagram for Time Delayed Broadcasting Scheme

An actor is represents a user or another system that will interact with the system modeled as shown in the figure below (Figure.8).

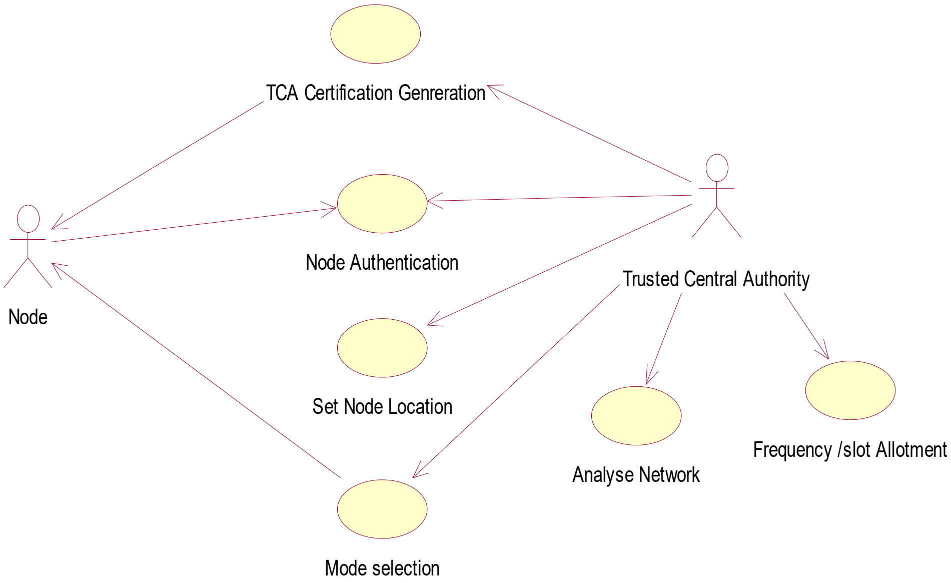

TCA Certification Genreration
Node Authentication
Node
Trusted Central Authority
Set Node Location
Analyse Network
Frequency /slot Allotment
Mode selection

Fig.8 Use case diagram Time delayed Broadcast Scheme

As shown in the above use case diagram the actions take place between the Trusted Central Authority (TCA) and the nodes.

Primarily TCA sends TCA certification to the nodes followed by node authentication, setting the node location and mode selection is done. Later the whole system performs the required action.

3.5 Sequence Diagram For Time Delayed Broadcasting Scheme

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that depicts (Figure.9) how processes operate with each other and in which sequential order.

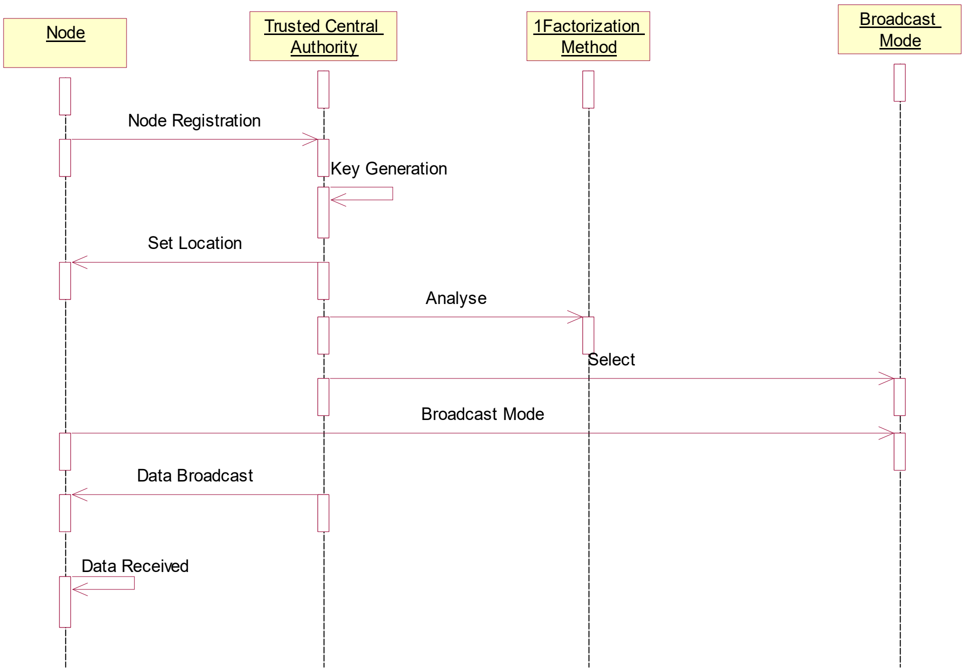


Fig.9 Sequence diagram for Time delayed Broadcast Scheme

The node registrations are done in the Trusted Central Authority (TCA), where the TCA generates a unique Private and Public Key for node details. After the Key Generation, the TCA sets the location for the nodes(taken as Local Host).TCA analyze the Nodes in the network and pairs the nodes with the same frequency using the 1-Factorization Method, to broadcast the message to the Receivers.TCA can broadcast the message using two methods: Sequential Unicast Method, Assisted Broadcast Method. The broadcasted data is received by the receiver nodes in the network.

3.6 Time Delayed Broadcasting Scheme

The static structure (Figure 10) which analyzes the systems structure displaying its related attributes classes and the relations between the classes are said to be Unified Modeling Language (UML). UML can also be said to be a class diagram. [20-25]

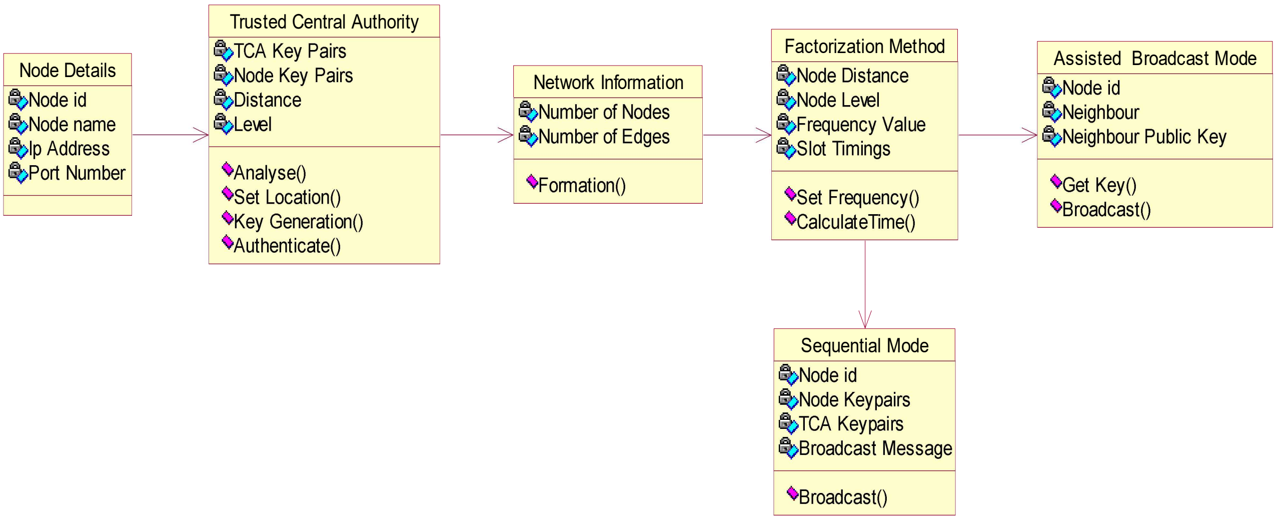


Fig.10 Class Diagram for Time Delayed Broadcasting Scheme

In the figure shown above the node details is represented as a class in which the node, node address, node number represents the attributes present. The node detail class is connected to the Trusted Central Authority (TCA) class and this represents the relationship between two classes. Similarly the other classes such as network authority class, factorization class, sequential unicast class and assisted broadcast classes are interconnected with the related classes along with their respective attributes.

3.6 System Implementation Algorithm

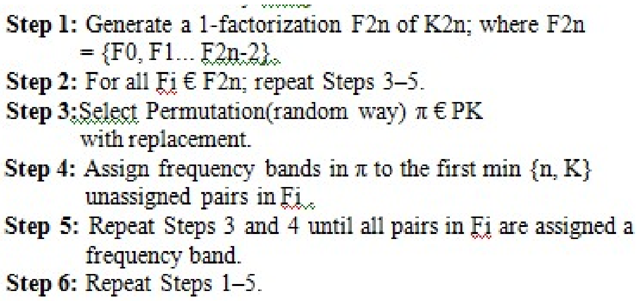
The main desideratum of the given algorithm is to attenuate the total energy transmitted with the help of efficient energy routes and also to exalt the network life. The contemplated algorithm consists of mainly three steps:

Splitting Algorithm:

- Analyze 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

Sequential unicast Algorithm:

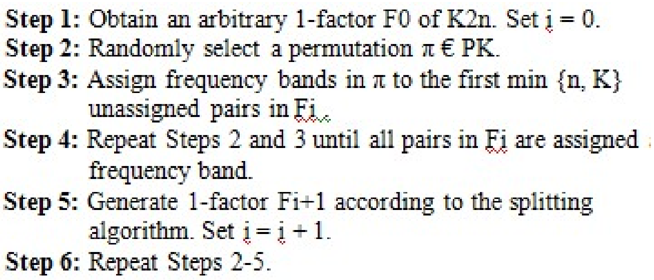
Consider the number of node group and assign the frequency limit K=n+1. Here permutation is used for getting the limited frequency randomly. Minimum number of frequencies is used for channel allocation by min () method.



Step 1: Generate a 1-factorization F2n of K2n; where F2n = {F0, F1... F2n-2}.
Step 2: For all Fi € F2n; repeat Steps 3–5.
Step 3: Select Permutation(random way) π € PK with replacement.
Step 4: Assign frequency bands in π to the first min {n, K} unassigned pairs in Fi.
Step 5: Repeat Steps 3 and 4 until all pairs in Fi are assigned a frequency band.
Step 6: Repeat Steps 1–5.

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.



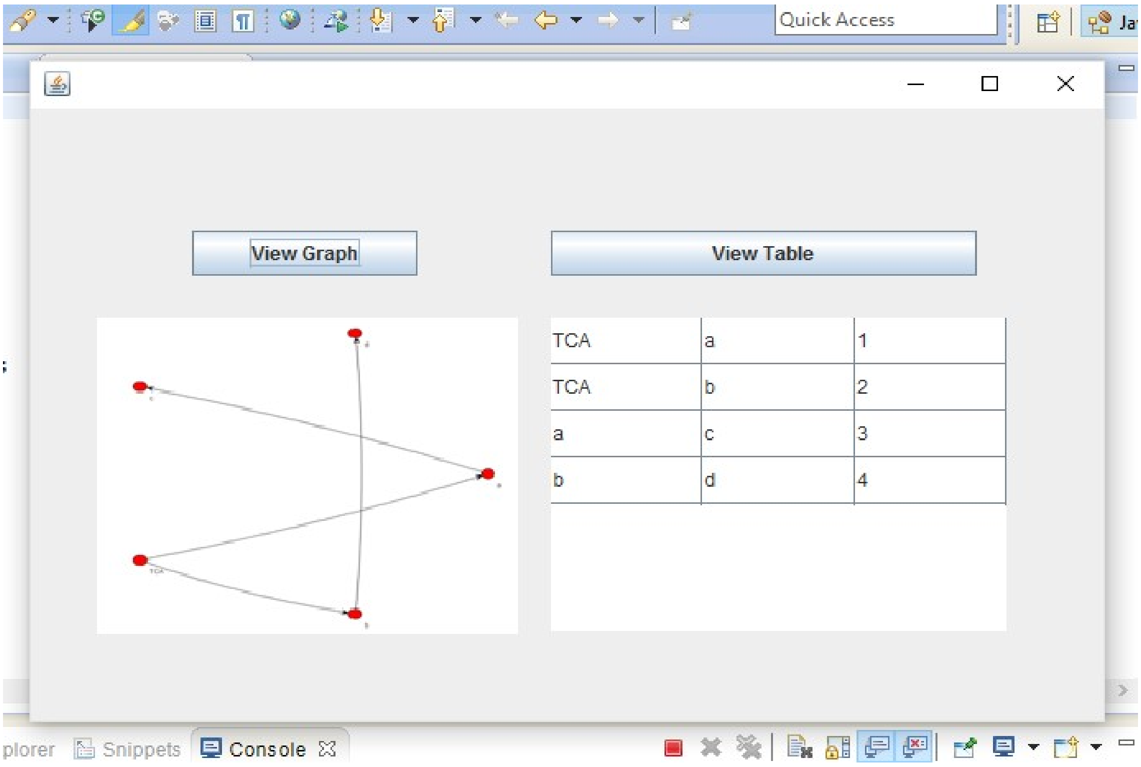
Step 1: Obtain an arbitrary 1-factor F0 of K2n. Set i = 0.
Step 2: Randomly select a permutation π € PK.
Step 3: Assign frequency bands in π to the first min {n, K} unassigned pairs in Fi.
Step 4: Repeat Steps 2 and 3 until all pairs in Fi are assigned frequency band.
Step 5: Generate 1-factor Fi+1 according to the splitting algorithm. Set i = i + 1.
Step 6: Repeat Steps 2-5.

IV. RESULT

The presence of inside jammers in the series of unicast transmissions or broadcast communications, it leads to the proposal of Time Delayed Broadcast Scheme (TDBS). These series of transmissions are broadcasted along with time and frequency. It is necessary coalesce the jammers to make sure that the ubiquitous wireless networks are successfully deployed. Unpremeditated radio interference or a wide range of defense strategies for combating dangerous jamming attackers will be caused due to the better physical arrangement of the wireless devices, which is done with the help of locations of jammers. Constant jammers are those which are mainly aimed by the malicious attackers. Regardless of the channel being idle or not constant jammers unceasingly emit radio signals. This radio interferes are active and keep agitating the network communication.

Table.1 Test Cases Execution Result Table

MODULE	GIVEN INPUT	EXPECTED OUTPUT	ACTUAL OUTPUT	RESULT
Sender	Filename & IP of receiver	Location key	Location key generated	OK
Sender	Location key	Location key should be forwarded to neighbors	Location key successfully forwarded	OK
sender	Decryption key	Decrypted file contents	File contents successfully decrypted	OK
Receiver	Location key of sender	File matching with location key to be sent	File found and sent	OK
Receiver	Encryption key	Message to be encrypted	File contents encrypted successfully	OK



TCA	a	1
TCA	b	2
a	c	3
b	d	4

Fig.11 Simulation Result using Eclipse.

V. CONCLUSIONS

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

VI. 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. Abdel Rahman, H. Rahbari, and M. Krunz, “Adaptive frequency hopping algorithms for multicast rendezvous in DSA networks,” in Proc. IEEE DYSPAN Symp., 2012, pp. 517–528.

[5] D. Adamy, EW 101: A First Course in Electronic Warfare. Norwood, MA, USA: Artech House, 2001.

[6] L. D. Andersen, “Hamilton circuits with many colours in properly edge-coloured complete graphs,” Math. Scandinavica, vol. 64, pp. 5–14, 1989.

[7] K. Appel and W. Haken, “Every planar map is four colorable: Part I,” Illinois J. Math., vol. 21, no. 3, pp. 491–567, 1977.

[8] P. Bahl, R. Chandra, and J. Dunagan, “SSCH: slotted seeded channel hopping for capacity improvement in IEEE 802.11 ad-hoc wireless networks,” in Proc. MOBICOM Conf., 2004, pp. 216–230.

[9] L. C. Baird, W. L. Bahn, M. D. Collins, M. C. Carlisle, and S. C. Butler, “Keyless jam resistance,” in Proc. IEEE Workshop Inf. Assurance United States Military Acad., 2007.

[10] K. Bian, J. Park, and R. Chen, “A quorum-based framework for establishing control channels in dynamic spectrum access networks,” in Proc. MOBICOM Conf., 2009, pp. 25–36.

[11] A. Chan, X. Liu, G. Noubir, and B. Thapa, “Broadcast control channel jamming: Resilience and identification of traitors,” in Proc. ISIT Conf., 2007, pp. 2496–2500.

[12] P. Chaporkar, K. Kar, X. Luo, and S. Sarkar, “Throughput and fairness guarantees through maximal scheduling in wireless networks,” IEEE Trans. Inf. Theory, vol. 54, no. 2, pp. 572–594, Feb. 2008.

[13] J. T. Chiang and Y.-C. Hu, “Dynamic jamming mitigation for wireless broadcast networks,” in Proc. INFOCOM Conf., 2008, pp. 1211–1219.

[14] J. H. Dinitz and D. R. Stinson, “A hill-climbing algorithm for the construction of one-factorizations and room squares,” SIAM J. Algebraic Discrete Meth., vol. 8, no. 3, pp. 430–438, 1987. [12] S. Ganeriwal, C. P€opper, S. Capkun, and M. B. Srivastava, , “Secure time synchronization in sensor networks,” ACM Trans. Inf. Syst. Security, vol. 11, no. 4, p. 23, 2008.

[15] S. Gollakota and D. Katabi, “Zigzag decoding: Combating hidden terminals in wireless networks,” in Proc. ACM SIGCOMM Conf., 2008, pp. 159–170.

[16] A. Gupta, X. Lin, and R. Srikant, “Low-complexity distributed scheduling algorithms for wireless networks,” IEEE/ACM Trans. Netw., vol. 17, no. 6, pp. 1846–1859, Dec. 2009.

[17] A. Gyarfas and M. Mhalla, “Rainbow and orthogonal paths in factorizations of kn,” J. Combinatorial Des., vol. 18, no. 3, pp. 167–176, 2010.

[18] L. Lazos, S. Liu, and M. Krunz, “Mitigating control-channel jamming attacks in multi-channel ad hoc networks,” in Proc. 2nd ACM WiSec Conf., 2009, pp. 169–180.364 IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 12, NO. 3, MAY/JUNE 2015

[19] A. Liu, P. Ning, H. Dai, Y. Liu, and C. Wang, “Defending DSSSbased broadcast communication against insider jammers via delayed seed-disclosure,” in Proc. Annu. Comput. Secur. Appl. Conf., 2010, pp. 367–376.

[20] S. Liu, L. Lazos, and M. Krunz, “Thwarting inside jamming attacks on wireless broadcast communications,” in Proc. 4th ACM WiSec Conf., 2011, pp. 29–40.

[21] Y. Liu, P. Ning, H. Dai, and A. Liu, “Randomized differential DSSS: Jamming-resistant wireless broadcast communication,” in Proc. INFOCOM Conf., 2010, pp. 1–9.

[22] E. Mendelsohn and A. Rosa, “One-factorizations of the complete graph-a survey,” J. Graph Theory, vol. 9, no. 1, pp. 43–65, 1985.

[23] G. Noubir and G. Lin, “Low-power DoS attacks in data wireless LANs and countermeasures,” Mobile Comput. Commun. Rev., vol. 7, no. 3, pp. 29–30, 2003.

[24] B. O’hara and A. Petrick, IEEE 802.11 Handbook: A Designer’s Companion, IEEE Standards Assoc., 2005.

[25] M. D. Plummer, “Graph factors and factorization: 1985–2003: A survey,” Discrete Math., vol. 307, no. 7, pp. 791–821, 2007.