IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Aspects of Network Security Based on Graph Theory

Mr.Vallabh Shinde, Mr. Karim Mulani

Assistant professor, Assistant professor
NMIET,Pune,India, SIT-Lonavla,India

Abstract: Graph theory is a very important component of many computing applications, including networking and security. As a result, it is also a challenging topic to understand and apply. The purpose of this paper is to review some of the key applications of graph theory in network security. The first segment of our discussion covers algorithmic aspects, followed by a discussion of network coding and its relationship to routing.

INTRODUCTION

Mobile communication networks are growing rapidly, requiring new solutions. Mobile devices suffer from reduced bandwidth and constantly changing network topologies. This creates a need for network algorithms with:

1. least possible communication traffic
2. High speed execution.

By using graph theory to create local algorithms (algorithms with few communication rounds), the two problems can be solved. The "four-color" theorem and network coding are highlighted in this study's exploration of graph theory's uses in cellular networks as they pertain to wireless mobile networks.

RELATED WORK

Chung and Lu [1] conducted in-depth research on graph theory and how it relates to a variety of real-world applications, including security. As an illustration, they looked into power-law models and its connection to network topologies. They also established upper and lower bounds for numerous significant computational issues. Ahmat's research [6] concentrated more on graph theory-related optimisation problems and their security implications. He discussed some fundamental graph theory ideas that are used to depict many kinds of networks. Then he went into detail about how networks are modelled to look into issues with network protocols. He concluded by describing a few of the techniques used to create graphs that represent real-world networks. In terms of tackling problems with graph optimisation complexity in networking and security, this work is regarded as one of the most thorough. Earlier this year, Shirinivas et al. [12] gave a general review of graph theory's usefulness in a variety of domains, but it largely concentrates on computer science applications that make use of the theory.

A groundbreaking study on Ethernet topology discovery, which is important for network security, was described by Breitbart et al. [2]. For locating physical topology in heterogeneous (i.e., multi-vendor) IP networks, they

presented new techniques. Their techniques don't alter the operating system software running on hosts or elements; instead, they rely on the widely accepted standard SNMP MIB information. Additionally, they integrated their algorithms into a topology discovery tool that had been tried out on Lucent's own test network. The methods created in this research only function when all of the MIB information is available.

The identical issue was addressed by Gobjuka and Breitbart [3] when the data from MIBs was insufficient. They specifically looked at the issue of determining the layer-2 network architecture. For locating physical topology in heterogeneous (i.e., multi-vendor) IP networks, they presented new techniques. Their techniques don't alter the operating system software running on hosts or elements; instead, they rely on the widely accepted standard SNMP MIB information. Additionally, they integrated their algorithms into a topology discovery tool that had been tried out on Lucent's own test network. The methods created in this research only function when all of the MIB information is available.

The identical issue was addressed by Gobjuka and Breitbart [3] when the data from MIBs was insufficient. They specifically looked on the issue of locating the layer-2 network architecture of sizable, heterogeneous multisubnet Ethernet networks that may have network nodes that aren't cooperating. They demonstrated how locating a layer-2. For locating physical topology in heterogeneous (i.e., multi-vendor) IP networks, they presented new techniques. Their techniques don't alter the operating system software running on hosts or elements; instead, they rely on the widely accepted standard SNMP MIB information. Additionally, they integrated their algorithms into a topology discovery tool that had been tried out on Lucent's own test network. The methods created in this research only function when all of the MIB information is available.

The identical issue was addressed by Gobjuka and Breitbart [3] when the data from MIBs was insufficient. They specifically looked on the issue of locating the layer-2 network architecture of sizable, heterogeneous multisubnet Ethernet networks that may have network nodes that aren't cooperating. They demonstrated how locating a layer-2 There are several researchers who explored graph theory and its practical aspects to Mobile Ad Hoc Networks MANET) too. Saleh Ali K. Al Omari and Putra Sumari [4] presented an exhaustive survey about the Mobile Ad Hoc Network (MANET) and They made a comparison between the different papers, most of its conclusions pointed to a phenomenon, not a routing protocol can adapt to all environments, whether it is Table-Driven, On-Demand or a mixture of two kinds, are limited by the network characteristics. Oliveira et al. [13] proposed a solution for securing heterogeneous hierarchical WSNs with an arbitrary number of levels. Our solution relies exclusively on symmetric key schemes, is highly distributed, and takes into account node interaction patterns that are specific to clustered WSNs.

From privacy prospective, S. Sumathy and B.Upendra Kumarb[7] proposed a key exchange and encryption mechanism that aims to use the MAC address as an additional parameter as the message specific key [to encrypt] and forward data among the nodes. In the model they proposed, the nodes are organized in spanning tree fashion, as they avoid forming cycles and exchange of key occurs only with authenticated neighbors in ad hoc networks, where nodes join or leave the network dynamically.

Donnet and Friedman [10] discussed past and current mechanisms for discovering the internet topology at various levels: the IP interface, the router, the AS, and the PoP level. In addition to discovery techniques, they provided insights into some of the wellknown properties of the internet topology. Maarten van Steen [8] focused on the commonly-used measures, namely, those concerning vertex connectivity, small- world property, correlations in connectivity pattern, and centrality. Unless otherwise specified, the complex networkmeasures are of an undirected unweighted linguistic network N

= (V, E) with n vertices and m edges as the model of a particular language sub-system.

Breitbart *et al.* [11] described a method for minimizing network monitoring overhead based on Shortest Path Tree (SPT) protocol. They describe two different variations of the problem: the A-Problem and the E-Problem, and show that there is a significant difference between them. They also proved that finding optimal solutions is NP-hard for both variations, and propose a theoretically best possible heuristic for the A- Problem and three different heuristics for the E-Problem.

Patrick P. C. Lee *el al.* [14] proposed a distributed secure multipath solution to route data across multiple paths so that intruders require much more resources to mount successful attacks. They include a distributed routing decisions, bandwidth-constraint adaptation, and lexicographic protection, and proved their convergence to the respective optimal solutions. In his book [15], Remco van der Hofstad studied random graphs as models for real-world networks. He concluded that, these networks turn out to have rather different properties than classical random graph models, for example in the number of connections the elements in the network make. As a result, a wealth of new models was invented so as to capture these properties.

GRAPH THEORY MODELS IN SECURITY

Graph theory

A graph is a straightforward geometric design composed of vertices and lines. The lines, which each connect a pair of vertices, can be directed arcs or undirected edges. Among other things, planning wireless communication networks has found use for graph theory as applied to mapping.

THE FOUR-COLOR GRAPH THEOREM

According to the well-known "four-color theorem," any map, like the one of the adjacent (touching) French provinces below, can be colored using no more than four different shades so that no two provinces on either side of a common boundary are the same color. Mathematicians have used computers to demonstrate that this holds true for all maps, regardless of the boarder or surface shape.

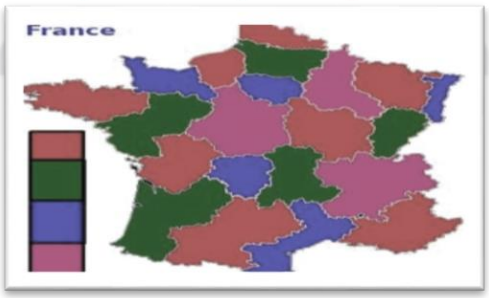

Fig 1 Provinces of France

APPLYING OF THE FOUR-COLOR THEOREM IN WIRELESS ACELL TOWER PLACEMENT PLAN.

If you take a look at the cell tower placement map above, where each broadcast channel from a cell tower is represented by a color and there are only four possible channel colors, the challenge of figuring out where to strategically place broadcast towers for the most coverage is comparable to the four-color map problem.

The two challenges are:

1. Elimination of the no-coverage spots (marked red inthe diagram above)
2. Allocation of a different channel in the spots where channel overlap occurs (marked in blue). In analogy, *colors* must be different, so that cell phone signals are*handed off* to a different channel.

Each cell region therefore uses one control tower with aspecific channel and the region or control tower adjacent to it

will employ a different tower and channel. It is simple to understand how a node coloring algorithm, which is a very well-liked technique currently being used by mobile service providers, can be used to effectively plan towers and channels in a mobile network by using 4 channels.

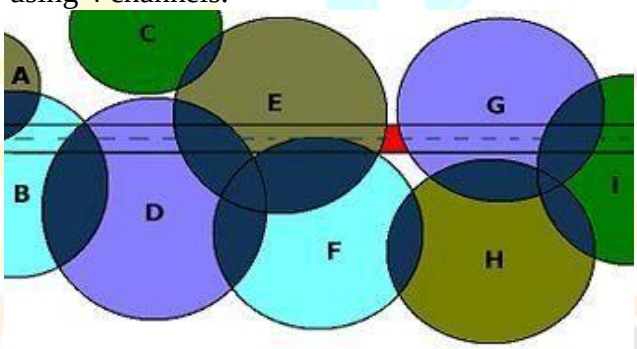

fig)2

NODE COLORING THEOREM

Borders wander, as seen in the map below, making it challenging to analyze a map. Using node coloring makes the problem easier to solve than using a complex map with numerous wandering boundaries. Two nodes cannot be the same color if they are connected by a line. Wireless service providers use node coloring to simplify an incredibly complex network map..

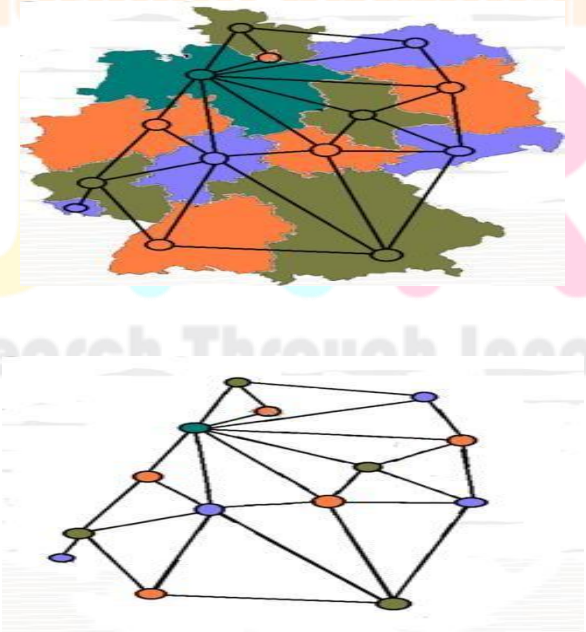

Fig3(b). The simplified network version of the map derived bynode coloring

NETWORK CODING

In mobile communication networks, network coding is another technique where graph theory is used. Nodes in a conventional network can only forward or replicate incoming packets. However, nodes can algebraically combine received packets to produce new packets by means of network coding.

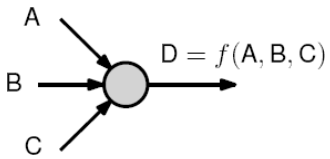

Fig4. Node replication of forward incoming packets

Network coding opens up new possibilities in the fields ofnetworking. Such would include:

Wireless multi-hop networks:

- Wireless mesh networks
- Wireless sensor networks
- Mobile ad-hoc networks
- Cellular relay networks

Peer-to-peer file distribution

- Peer-to-peer streaming
- Distributed storage

APPLICATION OF NETWORK CODING IN A CONTENTDISTRIBUTION SCENARIO

For this application, the following assumptions are made

1. The network is a multicast system where all destinations wish to receive similar information fromthe source.
2. That all Links have a unit capacity of a single packetper time slot
3. That the links be directed such that traffic can onlyflow in one direction.

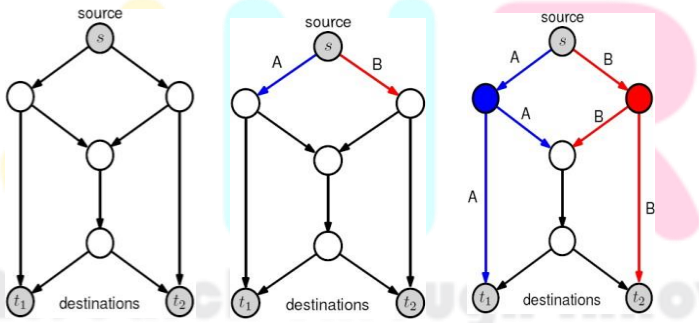

Fig5 Content distribution scenario

1ST TIME SLOT

Following the first time slot:

Destination t1 will have received information traffic A whereas Destination t2 will have received both traffic A and traffic B as shown below.

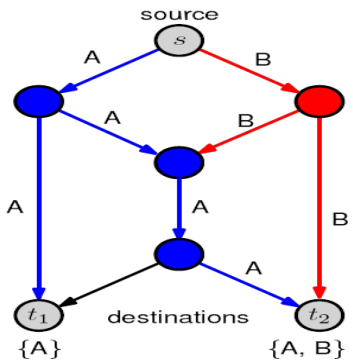

Fig6 First time slot

2nd slot

In the second time slot:

Both Destination t1 and t2 will have received traffic A andtraffic B and C as shown below

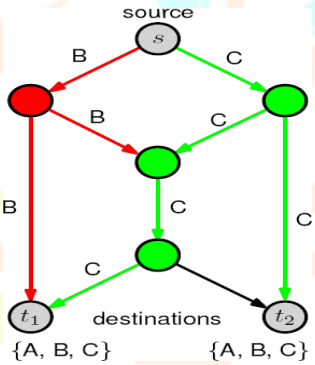

Fig 7 Second time slot

Finally, when Destination t1 receives A and A(EX-OR)B, it will be able to compute B by B=A (EX-OR){ A(EX-OR)B}

Likewise, when Destination t2 receives B and A (EX-OR) B, it will be able to compute A by:

A= {A (EX-OR) B} (EX-OR) B as shown below

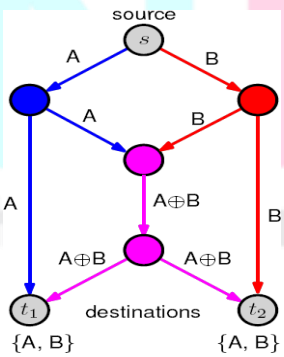

Fig 8 EX-OR Computation

NETWORK CODING APPLICATION IN OPPORTUNISTICROUTING

Opportunistic routing is a technique that makes use of multiple paths in a network to obtain diversity. Network coding can be applied in such a case (fig 9) to coordinate transmissions in order to avoid duplicate packets

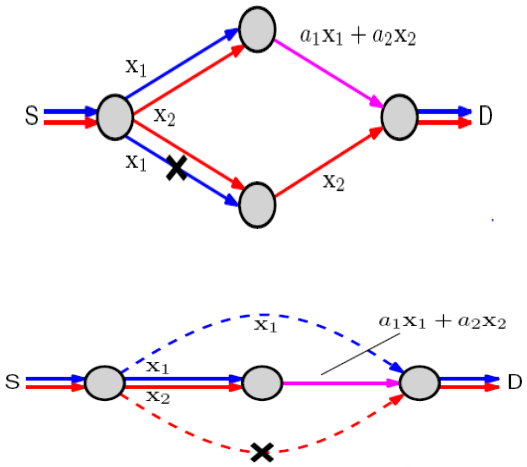

Fig 10 shows how network coding simply helps us determinehow many packets should be sent by each node

NETWORK CODING APPLICATION IN A PHYSICAL LAYERNETWORK

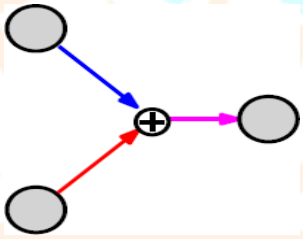

Fig.11

Network coding can be used with a physical layer network to enable networks benefit from interference rather than avoid it. Assuming the wireless channel performs network coding over the air. Fig 12 below shows how traditional network coding would perform, while Fig 13 shows physical layer network coding.

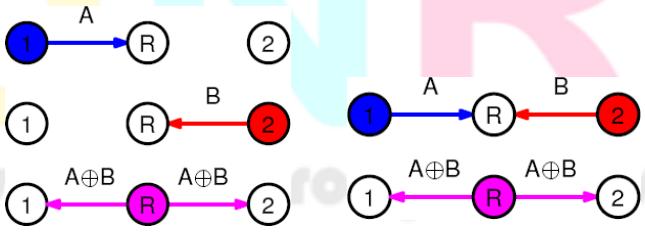

Fig 12 Traditional N *Fig 13 Fig 12 Physical layer NC*

Here, the challenge is inferring w1 (EX-OR) w2 from theobserved signal

y = h1x1 + h2x2 + z Special case: h1 = h2 = 1

Physical-layer Network coding Scheme with BPSK ModulationThis one requires phase synchronization and power control

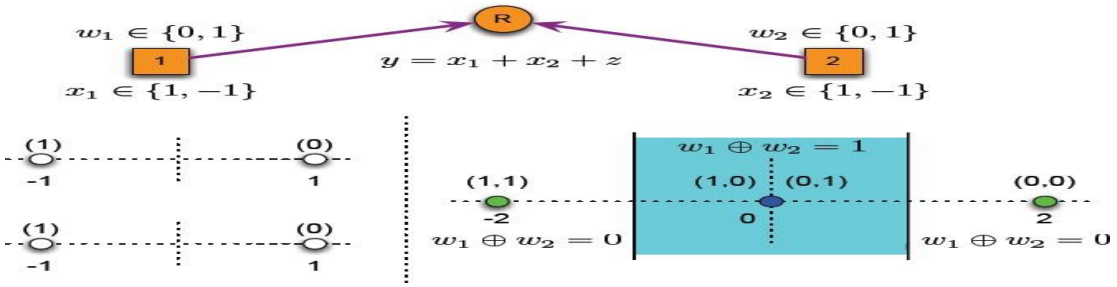

Fig 14 Physical layer network coding with BPSK Modulation

Physical-layer Network coding Scheme with QPSK Modulation

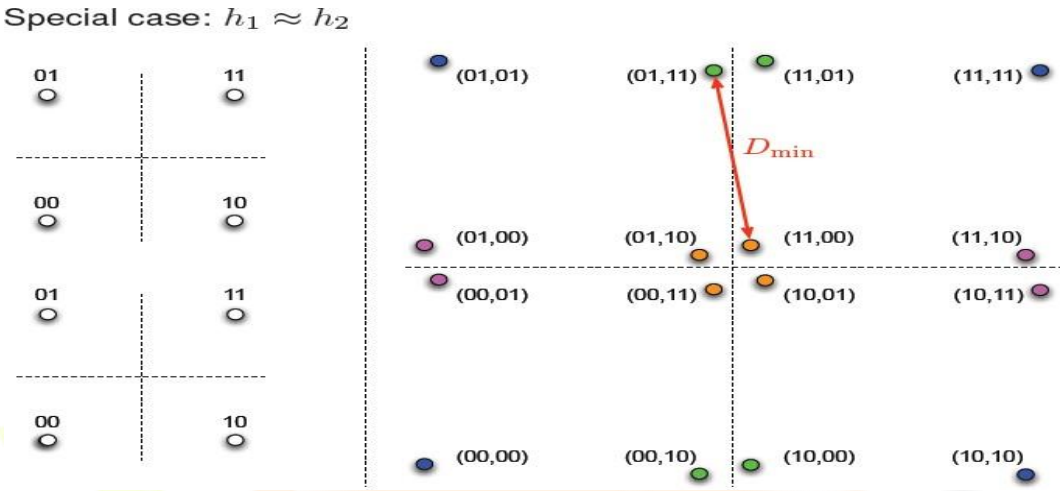

Fig 16 (a) Physical *layer network coding with QPSK Modulation*

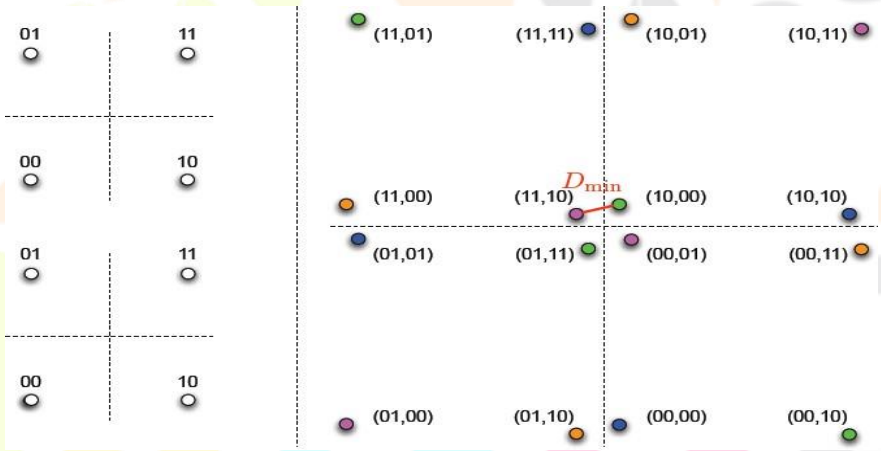

Fig 16 (b) Physical layer network coding with QPSK Modulation

CONCLUSION

Graph theory can help provide significant throughput gains for network coding and the four-color theorem, as demonstrated by the examples discussed.:

• Multihop wireless networks

content distribution scenariosother benefits are:

- Savings in time, resources, and energy streamlined operation.

References

[1] F.R.K. Chung and L. Lu. Complex Graphs and Networks, volume 107 of CBMS Regional Conference Series in Mathematics. American Mathematical Society, 2006.

[2] Y. Breitbart, M. Garofalakis, C. Martin, R. Rastogi, S. Seshadri and A. Silberschatz. " Topology Discovery in Heterogeneous IP Networks" In Proceedings of IEEE INFOCOM, 2000.

[3] H. Gobjuka and Y. Breitbart. Ethernet topology discovery for networks with incomplete information. In IEEE/ACM Transactions in Networking, pages 18:1220–1233, 2010.

[4] Saleh Ali K. Al Omari and Putra Sumari, " An overview of Mobile Ad Hoc Networks for the existing protocols and applications", International Journal on applications of graph theory in wireless ad hoc networks and sensor networks, vol. 2, no. 1, March 2010.

[5] K. Ahmat, Ethernet Topology Discovery: A Survey," CoRR, vol. abs/0907.3095, 2009.

[6] K. Ahmat, Graph Theory and Optimization Problems for Very Large Networks. City University of New York, United States, 2009

[7] S. Sumathy et. al. ,"Secure key exchange and encryption mechanism for group communication in wireless ad hoc networks", Journal on Applications of graph theory in wireless ad hoc networks and sensor networks, Vol 2,No 1,March 2010.

[8] van Steen M. Graph Theory and Complex Networks: An Introduction. Maarten van Steen; 2010.

[9] F.R.K. Chung and L. Lu. Complex Graphs and Networks, volume 107 of CBMS Regional Conference Series in Mathematics. American Mathematical Society, 2006.

[10] B. Donnet, T. Friedman, Internet topology discovery: A survey, Communications Surveys & Tutorials, IEEE 9 (2007) 56–69.

[11] Y. Breitbart, F. Dragan, and H. Gobjuka, "Effective network monitoring," in International Conference on Computer Communications and Networks (ICCCN), 2004.

[12] S. G. Shirinivas, S. Vetrivel, and N. M. Elango, "Applications of graph theory in computer science—an overview," International Journal of Engineering Science and Technology, vol. 2, no. 9, pp. 4610–4621, 2010.

Oliveira, L.B., Wong, H.C., Dahab, R., Loureiro, A.A.F.: On the design of secure protocols for hierarchical sensor networks. International Journal of Security and Networks (IJSN) 2(3/4) (2007) 216–227 Special Issue on ryptography in Networks