VOL. 10, NO. 8, MAY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

# DEFENDING AGAINST SECURITY BREACHES OF BYZANTINE ATTACKS IN MANETS

R. Sivakami and G. M. Kadhar Nawaz
Department of Master of Computer Applications, Sona College of Technology, Salem, India
E-Mail: shiv_sounder@yahoo.co.in

**ABSTRACT**

MANETs are widely used in military operations than their usage in commercial applications. Unmanned Army Systems, autonomous ground vehicles, automated battlefields and robots are the latest technologies of warfare and vigilance systems. The significance of MANETs in defense operations is inseparable. This increased use of MANETs in army leads to the need for improved ways of secured communications and robustness of the network. One of the major potential threats to military MANETS is Byzantine attacks. Byzantine attack is a kind of insider attack who knows very well about the functioning of established MANETs. This work gives a solution to eradicate Byzantine attacks from the MANET in an efficient manner with reduced complexity. There are different ways of attacking the system as an insider. This paper presents the different ways of attacking the system as insider and solution for prevail over the attackers. The security breaches of the attacks are studied carefully and to protect and recover the system from the malicious nodes through spatial connectors and Kirchhoff matrix along with strong cryptographic techniques is presented.

**Keywords:** byzantine attacks, MANETs, army, insider attack, security, robust, security breaches, kirchhoff matrix, spatial connectors.

## 1. INTRODUCTION

In wired networks, there are nodes such as routers, modems and firewalls specially committed for performing essential network functions. Wired networks are connected through wired medium such as coaxial cables or fiber optic cables. Wired medium ensure the smooth functioning and security of networks. Wireless networks are of two major categories- infrastructure based and ad hoc networks. The nodes can communicate only through the access points in infrastructure based wireless networks and the access points protect the network from invalid access. Access points have full control over the medium access. Whereas in ad hoc networks, there is no central point of control and nodes have to depend upon each for establishing the network. The wireless medium of propagation and the absence of centralized control make the ad hoc very weak in security concerns.

Mobile Ad Hoc Networks are wireless network of mobile nodes without any basic infrastructure. An instantaneous network is established between the mobile nodes to share the resources. Though the MANETS are now widely applicable in commercial applications, their prominent usage is in military fields and rescue operations of natural or manmade calamities. MANETS are prone to more attacks than the wired networks because of the wireless medium and no fixed infrastructure to monitor the network and mobility of the nodes. Among the various attacks on MANET, Byzantine attacks are strongest attacks. Various solutions have been provided to this problem and an in depth study on these solutions is carried out in this work. The comparison is made by categorizing the solutions into two major divisions based on how they overcome this type of attacks. One set of solutions are known as replication protocols and the other one is cryptographic protocols.

Byzantine attacks are the attacks made by the insiders who are well aware of the system behavior. The intention behind the attacks is not only to block the normal functioning of the system but also to corrupt the system. Handling such attacks helps in retaining the reliability and security of the system. Single node failure or attack is knows as black hole attack and colluding node attacks is known as worm hole attack. This attack got its name from the historical event of fall of Roman Empire by the attack of Byzantine.

### A. Historical event -origin of byzantine attack

The Byzantine attack was a popular attack in the invasion of Rome by Barbarians. The name Byzantine is derived after the ancient Greek city Byzantium on the Bosporus strait established by a person Byzas. Byzantium was a famous trading Centre of Greece, a link between Black Sea and Mediterranean Sea. The powerful Byzantine Empire arose with Byzantium as its capital. One of the main causes for the fall of the Roman Empire was the Barbarians knowledge of the Roma Military Tactics. Barbarians had a detailed knowledge of Roman style of warfare and the military strategies by serving in the Roman Army. With this military knowledge gained by working under Roman Army, they turned against the Roman Empire and led to the fall of Rome. These types of attacks are still carried out not only in battle fields but also at organization level to suppress the normal functioning.

**Figure-1.** Historical Byzantine Attacks in fall of Roman Empire.

### B. Byzantine attacks related to computer world

The Byzantine attackers are related to the authorized insiders and indulge in numerous malfunctions to block the system from normal functioning. This type of attack is not only faced in networks but also in retaining the reliability of a single system when some of its components fail down. It is a major problem to be solved in distributed system where the resources are distributed across many nodes and if one or many of them deviate from their regular work and they compromise with each other and indulge in malicious activities. Overcoming these Byzantine attacks increases the reliability in distributed systems and networks. There is a boom for distributed system in this decade. Instead having centralized power and control in a single system like super computer, it is better to distribute among multiple nodes. Researchers defeat these attackers in two ways: By replicating the resources and enriching the safety measures. First one is categorized as State Machine Replication protocols and the later is identified under the domain cryptographic security protocols.

### C. MANETS in Military

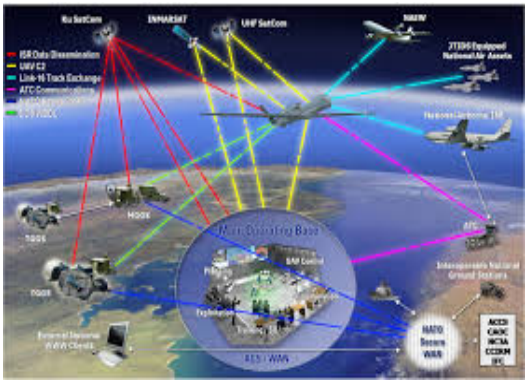

**Figure-2.** Unmanned Army system in Military.

As shown in Figure-2, the increased use of unmanned aerial and ground vehicles in military leads to the considerable use of MANETS in military. They are used not only in the battlefield but also in vigilance systems to secure the country. Unmanned ground vehicles and robots are used to check the landmines and communicate this to the others in the military network. An insecure ad-hoc network causes the entire network to become vulnerable to security breaches. Lot of research have been carried out and still going on in protecting the network from intruders. Nodes are reckless in military networks and lead to frequent path loss. This nature of network is prone to lot of attacks. The very dangerous attack is the Byzantine attacks. It becomes a highly powerful attack when more than one inside attackers joins together and performing brutal activities against the benign ones. This kind of Byzantine attacks was implemented by Nazi Germany during the Second World War Blitzkrieg in [2] illustrates the third generation where "attack relied on infiltration to bypass and collapse the enemy's combat forces rather than seeking to close with and destroy them". This paper presents a work carried out to defeat the Byzantine attacks and retains a high level of reliability and security of the MANET.

## 2. BYZANTINE ATTACKS

A set of malicious nodes collude with each other and carries out attacks such as creating routing loops, routing packets on non-optimal paths, dropping packets selectively as said in [10]. The network would seem to be operating normally in the viewpoint of nodes, though it may actually be exhibiting Byzantine behaviour [8], [9]. It is difficult to provide security due to the collaborative nature of the attack and are internal adversaries. Based on the number of nodes involved in attacking the network and the way they attack, the Byzantine attacks are classified into Black hole attack, Flood Rushing Attack, Worm Hole Attack and Network Overlay Attack as given in [9].

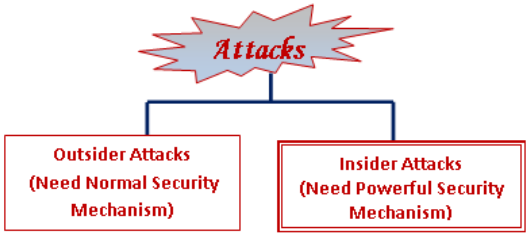


**Figure-3.** Broad categories of active attacks.

Attacks on MANETS are categorized into passive and active attacks as in [9]. Passive attacks do not harm the system. They simply monitor and overhear the communication and try to trace out the traffic pattern and the actual message being transferred. Identification this passive attacker is very difficult but they can be blocked from retrieving useful information about the system through enriched encryption mechanisms. Active attacks should be handled efficiently to secure the system. They drop or modify the data being transmitted or block the system from usual functioning. Active attackers are classified into two major divisions as outsiders and insiders as given in Figure-3 for any system. In networking, further they are divided into sub domains based on the layers they attack and method of attacking the system. Byzantine attack comes under the branch of insider's attacks. These sorts of adversaries are tough to find out and block. Byzantine Fault Tolerant algorithms [24] are broadly categorized into two classes - one that gives solution by replicating the hardware or the service and the other using cryptographic methods. The very first solution to Byzantine General Army problem was by Lamport, Shostak and Marshall [1], later it was enhanced by Schneider *et al*. [18] in 1990 and Reiter in 1995 [16]. Castro and Liskov *et al* addressed it as Seminal Practical Byzantine Fault Tolerance widely known as PBFT [14]. Abd -El-Malek *et al* [20] improvise the performance of State machine replication through Query /Update Protocol. Cowlind *et al* came out with powerful HQ - Hybrid Quorum Replication.

Very few crypto graphical solutions were there for Byzantines attacks and there is protocol available to address all kinds of Byzantine attacks. Hass and Papadimitratos et al resolves only single node Byzantines in Secure Routing Protocol –SRP [3] and not worm hole and network overlay Byzantines. Single node attacks are resolved by multipath message transmission and an end to end security association between source and destination. The paths are rated based on their past behavior. ARIADNE protocol by Hu, Perrig and Johnson [11] is immune to wormhole attack.Hu and Perrig et al were able to identify these attacks using packet leashes. But all these protocols won't work when such a case depicted in Fig.4 arises. The source is disconnected from the destination by the Byzantines. This work gives a solution in those situations too.

## 3. SECURITY BREACHES OF BYZANTINE ATTACKS

Normal cryptographic systems and simple replications are not enough to suppress these malicious nodes since they collaborate with each other and the medium of propagation is shared and insecure, the system is not robust and the intruders are internals. Single node Byzantine attacks in the network layer of the ad hoc networks are of two kinds known as black hole attacks and flood rushing attacks. Multiple node Byzantine attacks are wormhole Byzantine Attacks and Network Overlay Byzantine Attacks.

### A. Black hole Byzantines

One of the well known attacks is black hole attack. A black hole is a region in space which absorbs everything surrounding it and the objects that comes close to that region. Black hole [23] in general is a boundary in space through which matter and light can only pass inward towards the mass of the black hole. Nothing, not even light, can escape from inside the event horizon. Like this black hole, the compromised intruder drops all the transmissions that pass through it and the node does not forward anything out of it or else it will take part only in route discovery and not in data transmission. There is only one way of transmission towards the intruder and got the name Black hole attack. Hence all the routes having this adversary on their path to destination are affected.

If the black hole is node 6 or 13 as in Figure-4, then there is no way for the data transferring between source and destination. The network will be disconnected if node 13 exhibits Byzantine Black Hole attack. In such a case, the system has to identify the faulty node and check the connectivity of the network when the node is removed from the network. The connectivity has to be preserved even after the omission of the malicious node. There should be at least one path between the source and destination for communication to take place.

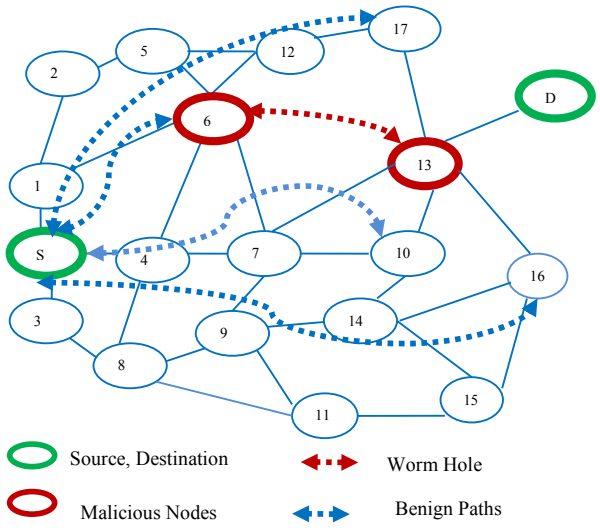


**Figure-4.** Worm hole attacks of Ad Hoc networks.

### B. Flood rushing and fake routing Byzantine

Almost all the routing protocols in Ad Hoc network establish route between the end nodes by flooding route request packets in the network. The nodes which did not receive the request packet so far will include its identification in the RREQ packet and flood it again in the network. This process repeats till the RREQ reaches the destination. The Byzantines create fake routes or flood the false RREQ packets and rushes the false route request packets in the network prior to the loyal RREQ packets. The requests sent by the loyal nodes are discarded since it arrives later than the false floods created by malicious nodes. Through the creation of bogus floods, the adversaries guide the source into wrong routes. For example in the scenario depicted in Fig.4, if node 6 floods fake packets to nodes 12 and 7 before the arrival of genuine RREQ, then the original RREQ are dropped out by nodes 7 and 12 by considering them as duplicate floods.

### C. Security threats of colluding Byzantines

**1) Byzantine wormholes:** The adversaries can send a route request and discover a route across the ad hoc network, then tunnel packets through the non-adversarial nodes to execute the attack. The adversaries can use the low cost appearance of the wormhole links in order to increase the probability of being selected as part of the route, and then attempt to disrupt the network by dropping all of the data packets. The Byzantine wormhole attack is an extremely powerful attack that is carried out even if only two nodes have been compromised.

Wormhole is an imaginary route between two nodes in terms of distance and time. The wormhole creates two deceptive points of traffic control to attack and analyze the network. The wormhole end nodes falsely propagate a one hop distance between them to other nodes.

In Figure-4, the nodes 6 and 13 can join together and form a wormhole tunnel between them.

**2) Byzantine network overlays:** Network overlay attacks is the one where the compromised nodes are scattered across the network and perform actions leads to degrade the performance of the system. The distributed denial service attack also comes under this category.

## 4. SECURING COMMUNICATION FROM BYZANTINE ATTACKS

### A. Spatial movers and connectors in retaining connectivity

The network becomes partitioned when the Byzantines are the critical points of the network. To handle such situation demonstrated in Figure-4, the nodes in the system are classified into loyal nodes and adversaries. Every node in the network is updated with the current topology and node status. Each node has a classifier table for the other nodes in the network. The network nodes are rated down or up based on its behavior in CTS, route establishment and data forwarding phases. Information is gathered from MAC, network and transport layers. Details of the neighboring nodes of the top rated and suspected nodes are stored in the status table. The number of toppers and the suspected nodes varies considering the size of the network and the purpose for which the network has been established.

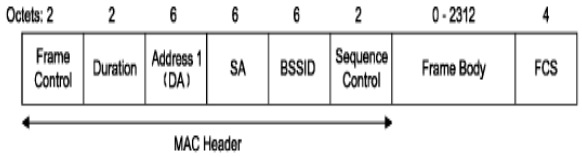


**Figure-5.** Connector beacon frames.

After the identification of Byzantines by intrusion detection system, the source nodes checks whether the network remains connected if the adversaries are removed from the system. This is done with the help of Kirchhoff matrix. If the Byzantines isolates the destination from the system as in Figure-4, then the source picks up the top rated nodes that are at one hop distance from the adversaries. It elects them as connectors and sends beacon frames intimating the distance to be covered for the connectivity of the network. This spatial movement is made only when the network is partitioned. The connector beacon frames body contains the minimal and maximal distance the nodes can move.

**Table-1.** Status table of any loyal node.

| S. No. | Node | Rate | Willingness to act as connectors | List of neighbors | Time stamp |
|---|---|---|---|---|---|
| 1 | N2 | High | Yes | N1,N5,N6 | --:-- |
| .. | .. | .. | .. | .. | .. |
| 18 | N13 | Low | Yes | N7,N17,N16,ND | --:-- |
| .. | .. | .. | .. | .. | .. |

### B. Kirchhoff or Laplacian discrete matrix in determining network connectivity

Kirchhoff matrix is also known as discrete Laplacian or information matrix [25]. If the network is represented by a graph G, then the discrete Laplacian matrix L(G) of can be obtained from the adjacency matrix –A(G), degree matrix-D(G) by applying (1).

The degree matrix D (G) is

$$D(G) = \begin{pmatrix} d(n1) & 0 & \dots & 0 \\ 0 & d(n2) & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & d(nn) \end{pmatrix}$$

If there are n nodes in the network, then L(G) is an nxn positive semi diagonal matrix with positive diagonal elements and zero or negative non diagonal elements. L(G) can also be computed from the incidence matrix Q(G) by (2).

Q(G) is the vertex - edge incidence matrix. If there are n vertices and m edges then the order of Q is nxm.

$$Q(G) = \begin{pmatrix} q_{11} & q_{12} & \dots & q_{1m} \\ q_{21} & q_{22} & \dots & q_{2m} \\ \dots & \dots & \dots & \dots \\ q_{n1} & q_{n2} & \dots & q_{nm} \end{pmatrix} \quad \text{where } q_{ij} = \begin{cases} 1 \text{ if edge } j \text{ originates at vertex } i \\ -1 \text{ if edge } j \text{ terminates at vertex } i \\ 0 \text{ if edge } j \text{ and vertex } i \text{ are not incident.} \end{cases}$$

The Eigen values of the matrix are sorted in ascending order and the list is $\lambda_1 < \lambda_2 < \lambda_3 < \lambda 4 < \dots < \lambda_n$. If the network is connected then the following two conditions are satisfied as given in [26].

- $\lambda_1 = 0$ and $\lambda_i > 0 \ \forall\ i >= 2$.
- Rank of the Kirchhoff matrix is n-1for an n nodal graph.

The connectivity of the network is checked by removing the vertex row and column from the matrix and computing the Eigen values. If the removal of the vertex from the matrix disconnects the network then it is known as the critical point. The connectors are called when the Byzantines are the critical points of the system.

### C. Secure data communication

Once the reachablity of the destination is verified and route establishment is finished up, the data is transmitted in three folded secured mechanism. The three main phases of securing data transmission against Byzantine attacks is given in Figure-6.

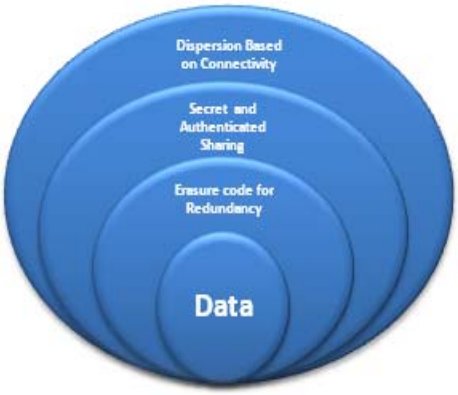


**Figure-6.** Securing data communication.

Redundant Data: To retrieve the data from normal loss a minimal redundancy is added before transmission. On the receiver side, the original data sent can be retrieved with the allowable loss in it. If no data is lost then the added redundancy is erased on the receiver side. The optimal erasure code of Rabin's scheme is used for adding minimal redundancy to the data.

**Secret and authenticated sharing:** The members of the network have unique identifier and that is the secret key of them. The public key of each node is known to every other node of the network. The source disseminate the data by encrypting it with the public key of destination and sign the data with its private key using digital signature , integrity is also maintained with the help of SHA-256 hashing algorithm.

**Dispersion based on connectivity:** The final phase is message dispersion. The encrypted, authenticated data added with redundancy and message digest is dispersed in multiple paths using Rabin cryptosystem [5]. The paths are selected from the Kirchhoff matrix to reveal the current topology and loyalty of the nodes.

## 5. RESULTS AND CONCLUSIONS

The proposed work is implemented in Java. This work supports the continuous data communication even when the Byzantines are the critical points of the network.This improves the robustness of the network. One of the major applications of MANETs is in the combat force and the main motive of the network is the nodes should be reachable at any cost and the system must support robustness.This is met by the proposed work. This system enriches the robustness and improves the data comminication since no other existing system provides solution when the Byzantines are the critical points and corners a node or part of the system to disconnect it from the network.

## REFERENCES

[1] Lamport, L.; Shostak, R.; Pease, M,"The Byzantine Generals Problem", ACM Transactions on Programming Languages and Systems, Vol. 4, Issue 3 p. 382, 1982.

[2] Marcin Szczodrak, Dr. Jinwoo Kim, "4G and MANET, Wireless Network for Future Battlefield", Proceedings of the International Conference on Security Management, 2007, pp: 282-290.

[3] Papadimitratos P. and Haas Z.J. 2006. Secure data communication in mobile ad hoc networks"IEEE journal on Selected Areas in Communications, vol: 24, Issue: 2, pp: 343- 356.

[4] R. Sivakami, Dr. G. M. Kadhar Nawaz, "Secured Communication for MANETS in Military", International Conference on Computer, Communication and Electrical Technology - ICCCET2011. vol. no., pp. 146-151, 18th, 19th March 2011, published in IEEE Xplore.

[5] M. O. Rabin. 1989. "Efficient dispersal of information for security, load balancing and fault tolerance," J. ACM, vol. 36, no. 2, pp. 335-348.

[6] A.Perrig, Y-C Hu and D.B. Johnson, "Wormhole Protection in Wireless Ad Hoc Networks", Technical Report TR01-384, Department of Computer Science, Rice University.

[7] Y.-C. Hu, A. Perrig, D.B. Johnson, "Packet Leashes: A defense against wormhole attacks in wireless ad hoc networks", Infocom 2003.

[8] James Cowling, Daniel Myers, Barbara Liskov, Rodrigo Rodrigue, and Liuba Shrira, "HQ Replication: A Hybrid Quorum Protocol for Byzantine Fault Tolerance",

[9] C.Siva Ram Murthy and B.S Manoj. 2004. Ad Hoc Wireless Networks- Architecutres and Protocols", Pearson Education.

[10] L.Lamport, R.Shostak, M.Pease, "The Byzantine Generals Problem", ACM Tran.Program. Languages, Vol. 4, no. 3, pp. 382-401, July 1982.

[11] Y. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks", in Proc. 8th ACM MobiCom, Atlanta, GA, Sep. 2002, pp. 12-23

[12] Wen-Chao Yang, Che-Yen Wen, "The Novel Data Dispersal and Verification Framework for Keeping Digital Evidence", Forensic Science Journal, 2004, Vol.3, pp. 33-44.

[13] M. H. Shirdareh-Haghighi, Z. Sepasdar and A. Nikseresht, "On the Kirchhoff Index of Graphs and Some Graph Operations", 2010 Mathematical Subject Classification: 05C12, 05C50.

[14] Reed. I. S. and G. Solomon, "Polynomial codes over certain finite field," Siam Journal on Applied Mathematics, vol. 8, no. 2, pp. 300-304, 1960.

[15] M.Castro and Barbara Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery", ACM Transactions on Computer Systems. 20(4): 398-461, 2002.

[16] James Cowling, Daniel Myers, Barbara Liskov, Rodrigo Rodrigues, and Liuba Shrira, "HQ Replication: A Hybrid Quorum Protocol for Byzantine Fault Tolerance " in Proceedings of 7th Sysmposium of Operating systems design and implementation, USENIX Association Berkley, CA, USA, November 2006, pages:177-190.

[17] Malki. D, and Reiter M., "Byzantine Quorum Systems", Journal of Distributed Computing 11, 4 (1998), 203-213.

[18] R. Kotla, L. Alvisi, M. Dahlin, A. Clement, E. Wong, "Zyzzyva: Speculative Byzantine Fault Tolerance", ACM Transactions on Computer Systems, v. 27 n. 4, December 2009.

[19] Schneider, F. B., "Implementing fault tolerant services using the state machine approach: A tutorial", ACM Computing Surveys, 22(4): 299-319, 1990.

[20] M. Abd-El-Malek, G. R. Ganger, G. R. Goodson, M. K. Reiter, and J. J. Wylie, "The Read/Conditional-Write and Query/Update protocols", Technical report CMU -PDL-05-107. Parallel Data Laboratory, Carnegie Mellon University, Pittsburgh, PA, September 2005.

[21] S. J. Lin and W. H. Chung, "An Efficient (n, k) Information Dispersal Algorithm for High Code Rate System over Fermat Fields," IEEE Communications Letters, vol. 16, no. 12, pp. 2036-2039, 2012.

[22] Frost and Sullivan, "Advances in Radio Communications and Wireless Networking Fuel Innovations in MANETs", MANETs in Military Communications - Strategic Insights and the Road Ahead, March 2010.

[23] Wheeler, J. Craig. 2007. Cosmic Catastrophes (2nd Edition) Cambridge University Press.ISBN 0-521-85714-7.

[24] R. Sivakami, Dr. G. M. Kadhar Nawaz, "Adaptive IDA to Protect Message Transmission against Byzantine Attacks ", International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.5 March 2015, pp. 4084-4088.

[25] C.W.Wu. Algebraic connectivity of Directed Graphs, Linear and Multilinear Algebra. 53(3): 202-223, 2005.

[26] Joseph D.Fehribachl, "Matrices and Their Kirchhoff Graphs", WPI Mathematicl Sciences. MA 01609-2247.