ISSN:0975-9646

Securing the Wireless Mesh Networks against Epidemic Attack

P. Blessing Gilba,
Student,M.E (Computer science and engineering)
St.Peter's University,Chennai, Tamil Nadu, India.

S. Siva Kumar,
Assistant Professor, Department of Computer science
St. Peter's University,Chennai, Tamil Nadu, India,

***Abstract*--- In recent years, wireless mesh networks (WMNs) have emerged as a promising platform to provide easy Internet access. However, this increasing popularity of WMNs makes them an ideal target for different attacks. One such attack is the pollution attack/ epidemic attack. Epidemic attack is a severe security problem in wireless mesh networks. Several papers in the literature bring about the idea of securing the WMN, however their role of defending the pollution attack is limited. This paper provides an environment to detect and identify the malicious node that pollutes the packets. The detection algorithm implemented is based upon the time based checksum and batch verification in the MAC Opportunistic routing and encoding (MORE). This system allows an easy way of finding the malicious neighbor node. The identified malicious node is stopped from further communication. The packets transmitting via the malicious node is dropped and the packets are retransmitted to the destination.**

***Index terms*--- Wireless mesh networks, epidemic spreading, network coding, MORE, malicious node, packet forwarding**.

I. INTRODUCTION

Wireless Mesh Network is the providing the best of its access in recent world. A wireless mesh network (WMN) is made up of several nodes organized in a mesh topology. Every node under same radio coverage can communicate with each other. Even if one node fails, the other nodes can still communicate with each other, directly or through one or more intermediate nodes. Wireless mesh networks usually produces high loss rates. Year's back, to improve the performance of wireless mesh networks opportunistic routing protocols were introduced [16], [17]. There are many types of opportunistic routing protocols like GOR Geographical Opportunistic Routing), MGOR (Multi rate Geographical Opportunistic Routing), LMTOR (Least Medium Time Opportunistic Routing), MORE (MAC Opportunistic Routing and Encoding). In Opportunistic routing protocol, any node that overhears the transmission of another node can participate in packet forwarding. Using these protocols, high end-to-end throughput was obtained even if the links are lossy All the neighbor nodes overhear the packet transmission and takes part in packet forwarding, thus collision occurs and the network capacity is reduced. To address these issues network coding enabled wireless mesh networks were introduced. Network coding is used to improve the efficiency of the mesh networks. Network coding increases the throughput. When network coding is applied it is not necessary to send each and every packets one by one, many packets of same generation can be mixed and sent through the network. This can be used to attain the maximum possible information flow in a network. Network coded mesh networks provides fewer redundant packet transmission and the network capacity is increased [1], [14]. However, network coding opens the door for pollution attacks. Any intermediate node that acts as an attacker node can intrude the malicious information into the legitimate packets transmitting via it [15]. This kind of attacker nodes should be identified immediately, if not identified the malicious packets will be sent to all the other neighbor nodes. Since all the nodes in a WMN participate in encoding and packet forwarding, polluted packets will behave like an epidemic and can be easily propagated across the entire network, thereby significantly consume the network resource and degrade the performance of legitimate flows.

This paper focuses on detecting and identifying the malicious node by using time based check sum and batch verification methods. The detection technique is implemented using MORE protocol during the packet forwarding in the wireless mesh networks. The malicious node is stopped from access and the retransmission path of the unsent packets is found and the packets are sent to the destination. This retransmission provides the secure forwarding of packets with high reliability.

This paper includes a brief explanation on wireless mesh networks and Network coding, System architecture, Detection Methodology, Experimental results, conclusion.

II. WIRELESS MESH NETWORKS

As various wireless networks evolve into the next generation to provide better services, a key technology, wireless mesh networks (WMNs), has emerged to provide easy internet access [18]. Wireless mesh networks can easily, effectively and wirelessly connect entire cities using inexpensive, existing technology. WMNs has its own advantages with lots of applications e.g., neighborhood networks, enterprise networking, broadband home networking, etc. Mesh networks are self configuring; a new node can be easily added into the mesh network without doing any type adjustments by the administrator of the network.

Mesh networks are self healing; Even if some nodes are blocked, they can find their own path automatically to transmit the datas. Under same radio coverage some nodes will be blocked some node may lose signal but the transmission will not be stopped due to these reasons.The

capacity of WMNs is affected by many factors such as network architecture, network topology, traffic pattern, network node density, number of channels used for each node, transmission power level, and node mobility [19]. A guideline to improve the capacity of ad hoc networks: A node should only communicate with nearby nodes. To implement this idea, two major schemes are suggested in [19]:

Throughput capacity can be increased by deploying relaying nodes. Nodes need to be grouped into clusters However, these schemes have limitations. In the first scheme, to increase the throughput a very large number of communication nodes are mandatory and it will increase the cost of the network. In second scheme, clustering nodes in a wireless mesh network is a difficult task. So both these schemes are not preferred.

A. Security Issues

Security for wireless networks is an important task. So every network provides the Authentication, Authorization and Accounting services. But in a wireless mesh networks due to the vulnerability of nodes authentication, authorization can not completely secure the communication systems and the packet delivery. The packets are not sent fully in a network coded system. All the packets are spitted and sent to the destination. During this type of packet delivery, there are some attacker nodes which act as the intermediate nodes. When the packet gets transmitted through these types of attacker nodes, they include all the unwanted information into the packets to make it a malicious packet. So the originality of the packet is reduced and it will produce the wrong result when it's decoded finally at the destination.

To secure the wireless mesh network from this type of attacks many papers in the literature has produced several enhancements. But all those enhancements failed to secure the network. This paper introduces the time based checksum verification. Whenever a packet is created, the time is noted from the source and the checksums are generated. If an attacker node tries to include the unwanted texts into the packets the time at which it is intruded is noted in the header of the packet. So when this packet is sent to next node, it gets detected by the checksum verification method. So now the malicious neighbor node is identified.

III. NETWORK CODING

Network coding is a concept which was proposed in the wireless mesh networks to increase the throughput. When network coding is implemented in WMNs, the message or file or information that is ready to be sent to the destination breaks up into several generations say G1, G2,…., Gn. Each generation are divided into N packets say P1, P2, P3…., Pn. The n numbers of packets in a particular generation are called its native packets. All the packets are encoded using keys generated by RSA algorithm. Network coding opens door for packet mixing. When the coded packets are getting transmitted, it has to go via a path and the nodes along that path are called the intermediate nodes. The intermediate malicious node can modify the encoded packets during packet forwarding. So, the network coding itself makes the WNMs vulnerable to pollution attack, which can make an epidemic spreading throughout the network and spoil whole of the network. This issue is addressed in this paper. Detection and identification of malicious node in a simple way is represented.

There are different types of network coding; in this paper we use linear network coding technique as it produces maximum capacity.

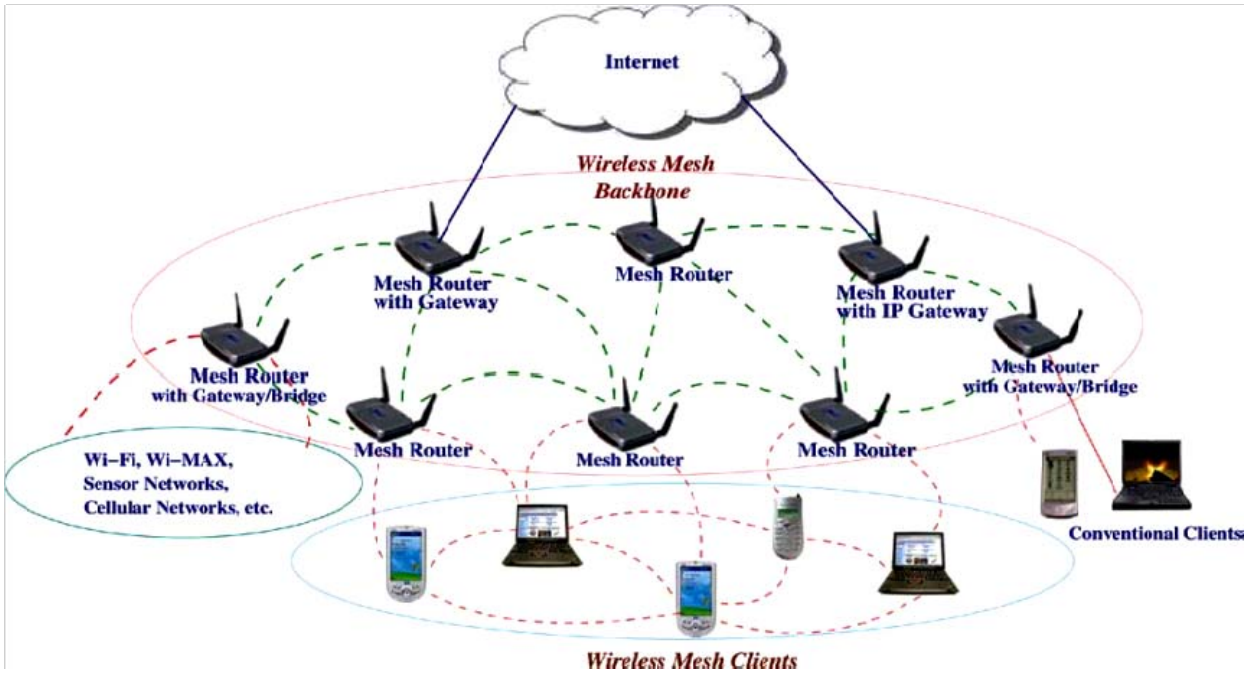

Fig. 1 Infrastructure of Wireless Mesh Networks

V. SYSTEM ARCHITECTURE

The detection algorithm proposed in this paper is based on batch verification to identify pollution attackers. In MORE, the source node sends packets in generations, and each generation contains n native packets. When the source node is permitted to transmit, it will broadcast coded packets which are the linear combination of the native packets instead of directly broadcasting the native packets.

A MORE header is attached to each coded packet which contains a list of potential forwarders. Before transmitting the packets, the source node finds the shortest path to the destination. Under the same radio coverage there will be several neighbor nodes but the source node selects only the path with shortest number of nodes. After finding the path the coded packets are transmitted through the generated path.

Whenever a node receives a packet, it checks whether the packet is in the forwarder list or not, and also checks whether the packet is innovative or not. If yes, it makes a number of transmissions wherein each transmitted packet is also a linear combination of all its received packets in the same generation. For the destination node, if it receives n independent packets, it sends an acknowledgment to inform the source to transmit next generation.

A. Network topology

Any number of nodes can be created. Each node represents the system under communication link. Each node sends "hello" message to other nodes which allows detecting it. Once a node detects "hello" message from another node (neighbor), it maintains a contact record to store information about the neighbor. Using multicast socket, all nodes are used to detect the neighbor nodes.

B. Finding Neighbors

The nodes inside same radio coverage are considered to be neighbours. Using multicast socket, all nodes are used to detect the neighbor nodes. The node without neighbours are considered to stand alone node.

C. Key Generation

The keys are generated in each node for security. Three types of keys are generated using RSA algorithm.

- Encryption key
- Decryption key
- Signatures

Encryption key: The original message is encrypted using encryption key. Encryption key is a public key.

Decryption key: The encrypted message is converted to original message by using decryption key. Decryption key is a secret key.

Signature: The receiver may need to verify that the transmitted message was originated from the sender. This type of authentication is done using the signatures. Every node has its own signature.

D. Path finding

Each node establishes the routing protocol to find the nearest node using shortest path algorithm. Multiple paths will be found for transmission. The path with minimum number of hopes will be elected for transmission. The path for retransmission is also found using the shortest path algorithm.

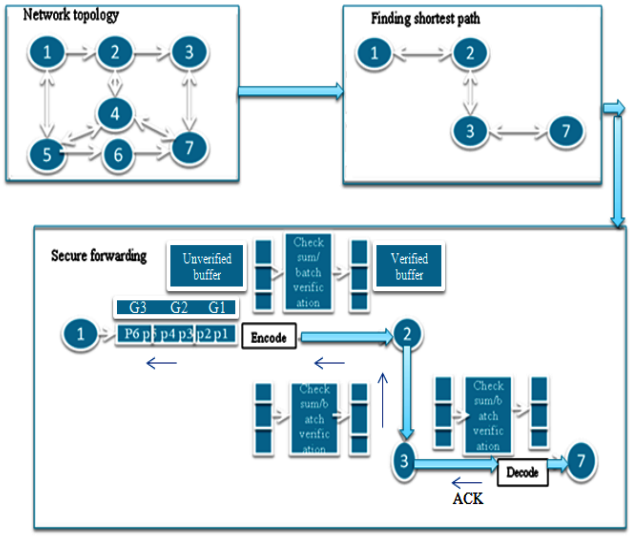

Fig. 2 secured system

E. Detection Algorithm in secured forwarding

During the forwarding phase, a MORE header is attached to each coded packet which contains a list of potential forwarders. The source node chooses all its downstream nodes which have a lower ETX distance to the destination as the potential forwarders. For a forwarder, when it receives a packet, it checks whether it is in the forwarder list or not, and also checks whether the packet is innovative or not. If yes, it makes a number of transmissions wherein each transmitted packet is also a linear combination of all its received packets in the same generation. For the destination node, if it receives n independent packets, it sends an acknowledgment to inform the source to transmit next generation.

The reason why malicious nodes may imitate legitimate nodes is to thwart the detection so as to reduce the chance of being detected. On the other hand, for any legitimate node, it strictly follows the routing protocol. Specifically, a legitimate node maintains two buffers, verified buffer and unverified buffer.

Every time when it is going to forward packets, it only encodes the packets in the verified buffer. On receiving a new packet, it buffers the packet into the unverified buffer. When a checksum packet arrives, it verifies those packets in the unverified buffer based on the time based checksum verification scheme. If the batch verification matches, then all verified packets are shifted to verified buffer, otherwise, all packets are discarded.

Note that, by dropping the packets when batch verification does not match, epidemic spreading of polluted packets is avoided so that all packets forwarded by legitimate nodes are valid.

The messages are sent along the route constructed from the source node to the source mesh router, which is protected with local session keys. Next, the source router finds out the correct destination router and routes the packet to the destination router. Every mesh router knows how to reach a specific node since each node has registered with the nearest mesh router. The destination mesh router dispatches the message to the destination node.

Fig. 3 Packet format

a) Source

The source breaks up the file into batches of *K* packets, where *K* may vary from one batch to another. These *K* uncoded packets are called native packets. When the 802.11 MAC is ready to send, the source creates a random linear combination of the *K* native packets in the current batch and broadcasts the coded packet. In MORE, data packets are always coded. A coded packet is p′j = Pi cji pi, where the cji's are random coefficients picked by the node, and the *pi*'s are native packets from the same batch. We call ~cj = (cj1, . . . , cji, . . . , cjK) the code vector of packet p′j . Thus, the code vector describes how to generate the coded packet from the native packets. The sender attaches a MORE header to each data packet. The header reports the packet's code vector (which will be used in decoding), the batch ID, the source and destination IP addresses, and the list of nodes that could participate in forwarding the packet. To compute the forwarder list, we leverage the ETX calculations. Specifically, nodes periodically ping each other and estimate the delivery probability on each link. They use these probabilities to compute the ETX distance to the destination, which is the expected number of transmissions to deliver a packet from each node to the destination. The sender includes in the forwarder list nodes that are closer (in ETX metric) to the destination than itself, ordered according to their proximity to the destination. The sender keeps transmitting coded packets from the current batch until the batch is acknowledged by the destination, at which time, the sender proceeds to the next batch.

b) Destination

Once the destination receives *K* innovative packets, it decodes the whole batch. As soon as the destination decodes the batch, it sends an acknowledgment to the source to allow it to move to the next batch. ACKs are sent using best path routing, which is possible because MORE uses standard 802.11 and co-exists with shortest path routing. ACKs are also given priority over data packets at every node.

c) Retransmission If a malicious node or the attacker node is found, it is purged from access. So that the packets in the non-verified buffer of a attacker node can not reach the destination. These packets are retransmitted via a newly found path, before the new shortest path is found for retransmission.

VI. DETECTION METHEDOLOGY

It is necessary to detect the WMNs to provide secure forwarding of datas. We focus on backbones of WMNs which use network coding enabled opportunistic routing protocol (e.g., MORE).

A. Time based Checksum and batch verification:

Every legitimate node strictly follows the routing protocol. Specifically, a legitimate node maintains two buffers, verified buffer and unverified buffer. Every time when it is going to forward packets, it only encodes the packets in the verified buffer. On receiving a new packet, it buffers the packet into the unverified buffer.

When a checksum packet arrives, it verifies those packets in the unverified buffer based on the time based checksum verification scheme. If the batch verification matches, then all verified packets are shifted to verified buffer, otherwise, all packets are discarded and the node detects a polluted packet. Note that, by dropping the packets when batch verification does not match, epidemic spreading of polluted packets is avoided so that all packets forwarded by legitimate nodes are valid.

B. Identifying malicious neighbor:

As soon as the polluted packet is detected, the next step is to identify the malicious neighbor that polluted the packet. Since the detection algorithm implements a new MORE header containing time of packet generation t, total number of generations G, generation number Gn, total number of packets in each generation P, packet number Pn, source address S, neighbor node address Na, destination address D. In each node all this information is checked by time based checksum verification.

So as soon as a polluted packet is detected the more headers help us to identify the neighbor node that polluted the packet. Thus the malicious neighbor node is identified and the node is stopped from further communication.

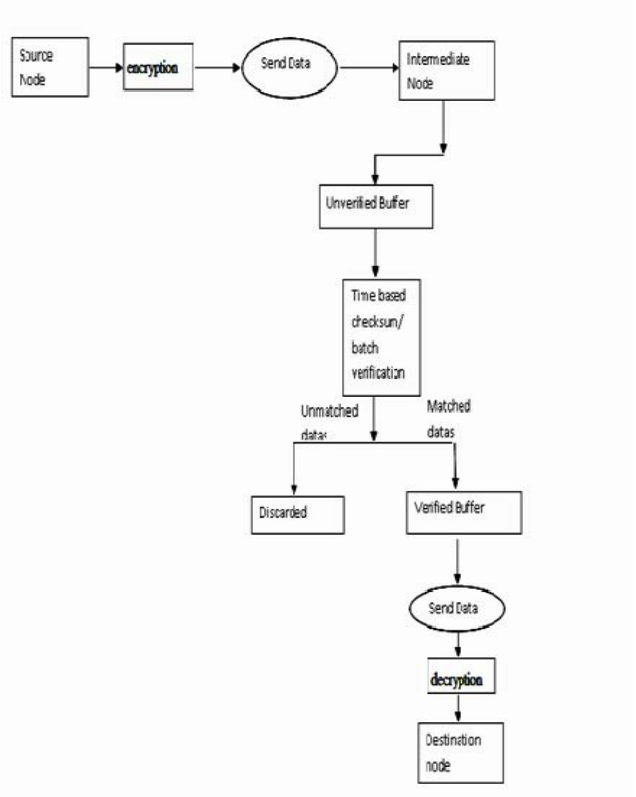

Fig.4 Architectural Diagram

VII. EXPERIMENTAL RESULT

To find out the effectiveness of the system 3 experiments with 10nodes were done. The experiments with its results are shown in the table and graph. Table 1 and 2 shows the difference between the existing and proposed systems.

TABLE I. RESULT FOR EXISTING ALGORITHM

	Malicious node	Average detection time
Exp. 1	Node 3	3.60 sec
Exp. 2	Node 3, node5	6.21 sec
Exp. 3	Node 3, node 5, node 8	10.30 sec

TABLE II. RESULT FOR PROPOSED SYSTEM

Experiment	Malicious node	Average detection time	Average Retransmission time
Exp. 1	Node 3	3.20 sec	4.10
Exp. 2	Node 3, node5	5.40 sec	5.50
Exp. 3	Node 3, node 5, node 8	9.50 sec	10.20

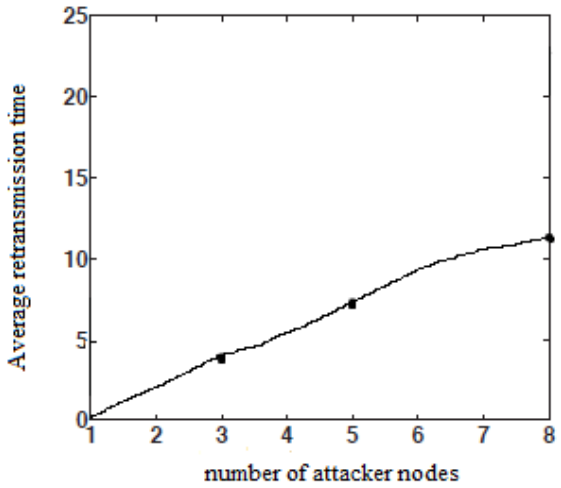

Fig. 5 Experimental result

VIII. CONCLUSION

MORE protocol is not only the best protocol in network coding enabled wireless mesh networks but also helps use to identify malicious neighbor by using time based check sum verification and batch verification. The time based check sum and batch verification methods helps to discover the malicious neighbor node without changing the existing routing algorithm. The detection algorithm used is very effective to find out the malicious node. This paper also helps to find the alternative way to send the packets / retransmission so that the packets dropped from the malicious node will reach the destination as a legitimate flow of valid packets.

REFERENCES

[1] J. Le, J. C. S. Lui, and D.-M. Chiu. On the Performance Bounds of Practical Wireless Network Coding. IEEE Transactions on Mobile Computing, 9:1134–1146, 2010.

[2] S. Chachulski, M. Jennings, S. Katti, and D. Katabi. Trading Structure for Randomness in Wireless Opportunistic Routing. In SIGCOMM'07: Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications, pages 169– 180, New York, NY, USA, 2007. ACM.

[3] J. Dong, R. Curtmola, R. Sethi, and C. Nita-Rotaru. Toward Secure Network Coding in Wireless Networks: Threats and Challenges. Secure Network Protocols, 2008.

[4] S. Katti, H. R. D. Katabi, W. Hu, and M. Medard. The Importance of Being Opportunistic: Practical Netowk Coding for Wireless Environments. In In Proceedings of 43rd International Conference on Communication, Control and Computing, 2005.

[5] S. Vyetrenko, A. Khosla, and T. Ho. On Combining Informationtheoretic and Cryptographic Approaches to Network Coding Security Against the Pollution Attack. In Asilomar'09: Proceedings of the 43rd Asilomar conference on Signals, systems and computers, pages 788–792, Piscataway, NJ, USA, 2009. IEEE Press.

[6] J. Le, J. C. S. Lui, and D.-M. Chiu. Dcar: Distributed Coding-Aware Routing in Wireless Networks. IEEE Transactions on Mobile Computing, 9:596–608, 2010.

[7] Mesh Networking Forum, Building the business case for implementation of wireless mesh networks, Mesh Networking Forum 2004, San Francisco, CA, October 2004.

[8] P. Liu, Z. Tao, S. Narayanan, T. Korakis, and S. Panwar. A Cooperative MAC protocol for Wireless LANs. *JSAC*, 25(2), Feb 2007.

[9] Bahl et al. Opportunistic Use of Client Repeaters to Improve Performance of WLANs. Technical Report MSR-TR-2008-149,Microsoft Research, 2008.

[10] Kai Zeng, Wenjing Lou, and Hongqiang Zhai. On end-to-end throughput of opportunistic routing in multirate and multihop wireless networks. In Infocom, Phoenix, AZ, April 2008.

[11] Henri Dubois-Ferriere, Matthias Grossglauser, and Martin Vetterli. Least-cost opportunistic routing. Technical Report LCAV-REPORT-2007-001, School of Computer and Communication Sciences, EPFL, 2007.

[12] D. De Couto, D. Aguayo, J. Bicket, and R. Morris. A high-throughput path metric for multi-hop wireless routing. In *Proceedings of ACM MobiCom Conference*, September 2003.

[13] A. Le and A. Markopoulou, "Locating Byzantine Attackers in Intra-Session Network Coding Using SpaceMac," Proc. IEEE Int'l Symp. Network Coding (NetCod), 2010

[14] S.-Y. R. Li, R. W. Yeung, and N. Cai. Linear Network Coding. IEEE Transaction on Information Theory, 49(2):371–381, Feb. 2003.

[15] J. Dong, R. Curtmola, and C. Nita-Rotaru. Practical Defenses Against Pollution Attacks in Intra-flow Network Coding for Wireless Mesh Networks. In WiSec '09: Proceedings of the second ACM conference on Wireless network security, pages 111–122, 2009.

[16] C. Gkantsidis, W. Hu, P. Key, B. Radunovic, P. Rodriguez, and S. Gheorghiu. Multipath Code Casting for Wireless Mesh Networks. In CoNEXT '07: Proceedings of the 2007 ACM CoNEXT conference, pages 1–12, New York, NY, USA, 2007. ACM.

[17] S. Biswas and R. Morris. Opportunistic Routing in Multi-hop Wireless Networks. SIGCOMM Comput. Commun. Rev., 34(1):69–74, 2004.

[18] I. Akyildiz and X. Wang. A Survey on Wireless Mesh Networks. IEEE Radio communication, 43(9):S23–S30, September 2005.

[19] P. Gupta, P.R. Kumar, The capacity of wireless networks, IEEE Transactions on Information Theory 46 (2) (2000) 388–404.

[20] R. Ahlswede, N. Cai, S.-Y.R. Li, and R.W. Yeung, "Network Information Flow," IEEE Trans. Information Theory, vol. 46, no. 4 pp. 1204-1216, July 2000.