Secure Multicasting Protocols in Wireless Mesh Networks—A Survey

Seetha Surlees and Sharmila Anand John Francis

Abstract Security is considered as one of the most significant constraint for the recognition of any wireless networking technology. However, security in wireless mesh networks (WMN) is still in its infancy as little attention has been given to this topic by the research society. WMN is a budding technology that provides low-cost high-quality service to users as the "last mile" of the Internet. Multicasting is one of the major communication technologies primarily designed for bandwidth (BW) conservation and an efficient way of transferring data to a group of receivers in wireless mesh network. The goal of secured group communication is to ensure the group secrecy property such that it is computationally infeasible for an unauthorized member node to discover the group data. In this article, the comparative study on existing approaches has been carried out; in addition to it, the fundamental security requirements and the various security attacks in the field of secure multicasting in WMN have also been discussed.

Keywords Wireless mesh networks · Multicasting · Security

1 Introduction

Wireless mesh networks (WMNs) are multihop, dynamically self-organized and self-configured network, with the nodes in the network automatically establishing an ad hoc network and maintaining the mesh connectivity. Fig. 1 illustrates the

S. Surlees (✉)
Department of IT, Karunya University, Coimbatore, India
e-mail: sitakaru@karunya.edu

S. A. John Francis
Department of MCA, Karunya University, Coimbatore, India
e-mail: sharmila@karunya.edu

G. S. S. Krishnan et al. (eds.), *Computational Intelligence, Cyber Security and Computational Models*, Advances in Intelligent Systems and Computing 246,
DOI: 10.1007/978-81-322-1680-3_27,

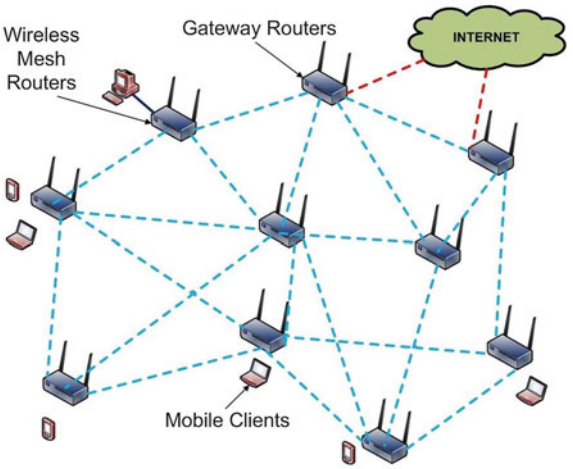

Fig. 1 Wireless mesh architecture—MR, mesh clients, and gateway node

architecture of WMN. WMNs are consisting of two types of nodes: mesh routers (MR) (wireless access points) and mesh clients. A mesh router is usually equipped with multiple wireless interfaces built on either the same or different wireless access technologies [1]. Routers in WMNs are usually stationary and form the mesh backbone for mesh clients. The additional gateway/bridge functionalities in MR enable the integration of WMNs with various other networks. Unlike in MANET, there is no power or computational constraints in WMN and the MR are stationary in most cases where as in MANET the nodes are mobile always [2]. WMN offers enormous applications like broadband home networking, community networking, transportation systems, public safety, and disaster recovery.

Group communication based on multicasting is considered to be a well-known communication paradigm in WMN due to the broadcasting nature of wireless communications. Multicasting is a bandwidth (BW)-conserving technology that helps at reducing the consumption of many applications. More internet users like to watch football matches and TV dramas on the internet as a substitute of traditional TV. Plentiful multicasting applications were foreseen to be deployed in WMNs, such as video on demand, Webcast, distance education, online games, video conferencing, and multimedia broadcasting [3]. These multicasting applications have one or more sources that distribute data to a group of changing receivers. The messages are delivered only once and duplicated only at branch points where links to the destination split.

The multicasting applications use multicast routing protocols that effectively deliver data from a source to multiple destinations organized in a multicast group. Multicasting is especially useful in wireless environments where there is scarce BW and many users are sharing the same wireless channels [4]. A major goal for multicasting is providing data confidentiality among the group members [5]. Based

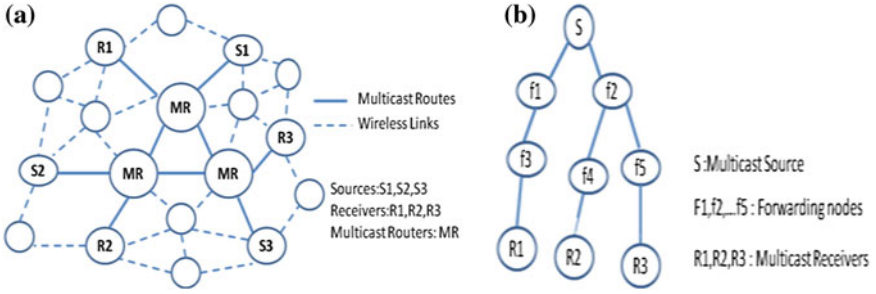

Fig. 2 **a** Mesh-based multicasting, **b** tree-based multicasting

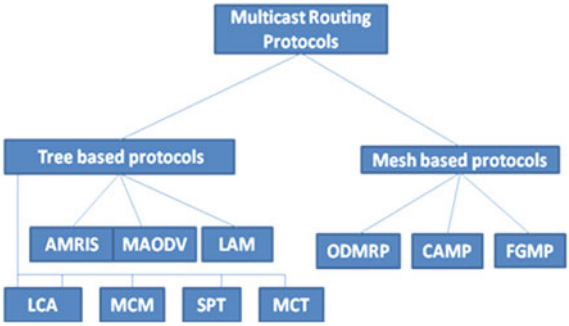

Fig. 3 Classification of multicasting protocol

on the way of creating the routes among the members of the multicast group, the multicasting routing protocols categorized into mesh-based and tree-based protocols that are shown in Fig. 2a and b. The tree-based protocol does not always offer sufficient robustness where as a mesh-based protocol addresses robustness, reliability requirements with path redundancy. However, tree-based protocols have been widely used in WMN because of its resilience characteristics that withstand the failure of the nodes in the network. Fig. 3 shows the different kinds of protocols under tree-based and mesh-based approaches.

The features of wireless medium, dynamic changing topology, and cooperative routing protocols of the WMN demand the security measures for authenticating the members in the multicast group [6]. To ensure secured group communication, the forward secrecy and backward secrecy [7] should be followed for the newly joined members and revoked members in a group.

The rest of the paper is organized as follows: In Sect. 2, we briefly review the related works for secure multicast routing in WMN. In Sect. 3, the performance analysis of different secure multicasting protocols is being compared. The article concludes with Sect. 4.

2 Existing Approaches to Secure Multicast Routing

Very few researchers have focused toward secure multicasting in wireless mesh network. The existing approaches that deal with security aspects of multicast routing in WMN have been discussed below.

2.1 Secure On-Demand Multicast Routing Protocol [8]

The recently developed secure multicast protocol focused on selecting a path based on high-quality metric such as expected transmission count (ETX) and success product probability (SPP) rather than using traditional hop-count metric to maximize the throughput of the network. On-demand multicast routing protocol (ODMRP) is a multicast protocol that source periodically recreates the multicast group by sending a JOIN QUERY and JOIN REPLY messages. The aim of this approach is to detect the metric manipulation attacks, namely local metric manipulation (LMM) and global metric manipulation attack (GMM) that results against high-quality metrics in multicasting of WMN.

In Fig. 4, a malicious node C1 maintains that SPP metric value of $B_1 \rightarrow C_1 = 0.9$ instead of the correct metric of 0.6. Therefore, C_1 gathers an incorrect local metric for the link $B_1 \rightarrow C_1$ and advertises to R about the metric $S \rightarrow C_1 = 0:9$ as a replacement of the correct metric. The route $S \rightarrow A_1 \rightarrow B_1 \rightarrow C_1 \rightarrow R$ is highly preferred than the correct route $S \rightarrow A_3 \rightarrow B_3 \rightarrow C_3 \rightarrow R$. The limitation of this approach is that the node is detected as an attacker only when the specified threshold value is met. This leads to some attackers being unnoticed if the difference between expected PDR (ePDR) and perceived PDR (pPDR) is less than threshold value. In addition to it, the approach restricts to accuse only one node at a time. Therefore, it is difficult to secure a network despite of the fact that the majority of the nodes are attackers.

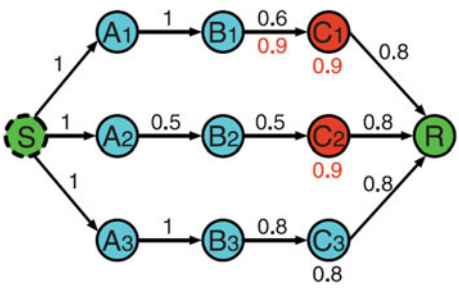

Fig. 4 Metric manipulation attack [8]

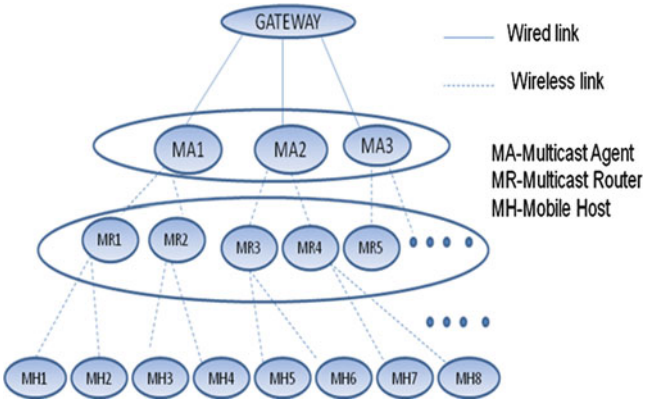

Fig. 5 Two-level hierarchical system model

2.2 Hierarchical Agent-Based Secure Multicast HASM [9]

This approach deals with the secure mobile multicast by ensuring only the authenticated mobile users to access the multicast data that are exchanged among the members of the multicast group. This approach proposed HASM protocol that efficiently ensures secured mobile multicasting in WMNs. Fig. 5 shows a gateway at the higher level of hierarchy in which multicast tree is rooted which connect MRs that serve as multicast agents (MA). Each multicast group member, i.e., Mobile Host (MH), is being registered with and serviced by an MA.

The objective of HASM is to minimize the overall network communication overhead incurred for security, group membership maintenance, and mobility management tasks. This method guarantees both backward and forward secrecy properties but lacks addressing the security attacks that arise within the group.

2.3 Bandwidth-Efficient Key Distribution for Secure Multicast in Dynamic Wireless Mesh Networks [7]

Data confidentiality in group communication is achieved by encrypting the message with a group key that is known to all the group members. To ensure secure group communication, the group key must be updated when there is a change in the membership of the multicast group. This situation is termed as rekeying. Dipping the BW utilization of rekeying is a central problem to guarantee enough BW for reliable data delivery when multicast-based services are provided over wireless networks. This approach defines the metric that represents the expected BW consumption of rekeying for given key tree. The adaptive and bandwidth-reducing (ABR) tree is a BW-efficient key tree management approach designed for

WMN when the group membership is dynamically changed. When a new member joins the group, this scheme assigns to the new member the proper KEKs to keep the expected BW consumption of the key tree as low as possible. Using this approach, ABR tree effectively reduces the actual BW consumption used for re-keying compared to traditional key tree management schemes. The demerit of this approach is that the deletion event is not optimized to a minimum cost level.

2.4 Design of Certification Authority Using Secret Redistribution and Multicast Routing in Wireless Mesh Networks [10]

In common, public key infrastructure (PKI) has a certification authority (CA), which is trusted by all the nodes in a network. But there is no trusted third party (TTP) in self-organizing networks such as WMNs. As a result, CA functions should be distributed over MR. MRs in WMNs are with enough power and capacity, so they are all able to participate in CA function distribution, and actively participating MRs can be changed from time to time. In order to achieve secret sharing and redistribution, the fast verifiable share redistribution (FVSR) scheme works for threshold cryptography and minimizes the possibility of secret disclosure when some shareholders are compromised by adversaries. This method adopts multicasting based on Ruiz tree that optimally reduces the operation overhead. It can update, revoke, and verify certificates of WMN nodes in a secure and well-organized manner. The demerit of this approach incurs additional overhead and cost due to Transferring MeCA functions.

2.5 Secure Group Overlay Multicast [5]

This approach provides data confidentiality such that only valid group members are allowed to access to the data sent to the group and to secure the primary protocols and effective designing of key management schemes. This approach uses ODMRP as a multicast routing protocol. Every authenticated client has a pair of public/private keys and a client certificate that maps its public key to its user ID. The CA is responsible for authorizing clients by issuing them a group member certificate. This member certificate binds the client to the group ID (group IP address) that provides proof of the client's membership. The goal is to ensure group secrecy property such that it is technically infeasible for outside adversaries to discover the group data. In addition to it, it also ensures forward and backward secrecy properties. The advantages of this approach is that it incurs less computational overhead, communication overhead, and latency without compromising the security. The limitation of this approach is that it lacks consideration of attacks against the multicast protocol itself.

2.6 An Improved Security Mechanism for High-Throughput Multicast Routing in Wireless Mesh Network Against Sybil Attack [11]

The objective of this approach is to detect Sybil attacks against high-throughput multicast protocols in WMN. In Sybil attack, a node maliciously claims multiple identities. Each node identity in the multicast group is validated using random key pre-distribution (RKP) technique, in which nodes create secure links to neighboring nodes. Using RKP, a random group of keys to each node is being assigned in such a way that each node can compute common keys that it share with its neighbors. These are called secret session keys that are used to ensure node-to-node secrecy. The limitation of this technique is not scalable when the attacker increases to high level.

3 Performance Analysis

This section analyzes the performance of existing approaches of secure multicasting in WMN against different parameters, viz. multicast protocol, routing metric, performance metrics, security issues addressed, merits and demerits. Table 1 shows the comparative study of existing approaches in secure multicasting protocols of WMN.

In S-ODMRP [8], the high-throughput metric (ETX, SPP) leads to increase in the ratio of attacker, but the defense mechanism is very effective against drop-only, LMM and GMM attack with the PDR of 95 %. The overhead of S-ODMRP is due to the periodic flooding of authenticated query packets that is common in all scenarios. In HASM [6], the total communication cost is much smaller than SPT due to the hybrid hierarchical multicast structure. The ABR tree [7] is effective for reducing the BW consumption of rekeying, and it achieves around 80 % reduction in total BW consumption compared to conventional tree approach. MeCA [10] minimizes the secret key discloser and improves the efficiency by incorporating multicasting but incurs high control overhead due to transferring MeCA functions over several MRs. The SeGrOM [5] offers high delivery ratio with minor encryption overhead, but the security attack against the multicast protocol is not addressed. Finally, RKP [11] tries to overcome the drawbacks of S-ODMRP, but it fails to scale for many attackers.

The analyses of multicasting protocols are performed using multicast routing metrics and performance metrics. The description of the multicast routing and performance metrics is as follows:

Table1 Comparison of existing approaches

Secure protocols	Multicast protocol	Routing metric	Security issues addressed	Performance metrics	Advantages	Drawbacks
SODMRP [8]	ODMRP	ETX, SPP	Resource consumption, mesh structure, data forwarding attacks	PDR-95 %, BW overhead-0.95 kbps, data-transmission efficiency-2–3 pkts	High throughput, security	Single accusation at time, detection is based on threshold value
HASM [6]	HASM	Hop count	Forward and backward secrecy	Avg. total communication cost/sec-low (10–20 times)	Minimizes the overall communication cost	Security attacks from within group not addressed
			User mobility		Ensure forward and backward secrecy	Reliability, QOS requirements not addressed
BW-efficient key distribution [7]	ABR tree	Expected BW consumption for rekeying	Data confidentiality	Total BW consumption-80 % reduction	Reduces network BW consumption of rekeying	Deletion event needs to be optimized
Design of CA using secret redistribution (MeCA) [3]	MCT	Hop count	Exposure attack, compromise attack	Control overhead-high, data overhead-small	Strengthens security, improves efficiency	Transferring MeCA functions incurs much overhead
SeGrOM [5]	ODMRP	Hop count	Data confidentiality	Delivery ratio is very high. computation, BW, latency overhead of join and leave events—increases linearly with data rate	Higher performance, smaller overhead	Attacks against multicast protocol are not considered
RKP [11]	S-ODMRP	ETX	Sybil attacks	PDR-high, BW overhead-low	High throughput, high security	Not scalable

3.1 Multicast Routing Metrics

In multicasting, route selection is carried out based on the metric designed to improve throughput. The commonly used routing metrics for multicasting are defined below.

(a) Expected Transmission Count

ETX is the total number of transmissions needed to successfully deliver a packet over a link from a source to destination [12].

$$\text{ETX} = 1/d_f \tag{1}$$

where d_f is the loss rate of the link in forward direction.

(b) Success Probability Product

SPP is used to provide the probability for the receiver to receive a packet over a link. SPP value for a path of j links between a source S and a receiver R is [8],

$$\text{SPP}_{S\to R} = \prod_{i=1}^{j} \text{SPP}_i \tag{2}$$

where $\text{SPP}_i = d_f$ and d_f is defined in ETX.

(c) Expected Transmission Time

ETT is the product between ETX and the average time required to deliver a single data packet. Let S be the size of the probing packet and B be the measured BW of a link; then, the ETT of this link is defined as follows [12]:

$$\text{ETT} = \text{ETX} * S/B \tag{3}$$

(d) Hop Count

A hop-count metric is a metric that counts router hops.
The description of the performance metrics is as follows:

3.2 Performance Metrics

The following metrics are frequently used to evaluate the performance of a secure multicast protocol:

(a) *Packet delivery ratio*

The amount of packets that are received successfully at the receiver to the total number of packets that are sent by source.

(b) *End-to-end delay*

The average time taken for a packet to reach the destination after it leaves the source.

(c) *Routing overhead*

The amount of control messages that every multicast router sends on average per unit of time.

(d) *Avg. total communication costs*

It is the number of wireless transmissions needed per operation of multicast members. It consists of cost of mobility management, the cost for security key management and the cost for group membership management.

4 Conclusion

The research in secure multicast routing in WMN is still in its infancy. In summary, the major security requirements, routing metrics, performance metrics, multicast protocol and their merits and demerits for the efficient secure multicast routing protocols in wireless mesh network are analyzed. In addition to this, various security issues in the WMN are discussed. WMN is a technology suitable for next generation wireless networking stimulating the application setups to its rapid development. Nevertheless, to make stronger market penetration, more research is needed in the area of secure mobile multicasting which accomplishes QOS for different application services with least cost, less BW consumption, and high throughput on WMN.

References

1. Ian F. Akyildiz, Xudong Wang, Weilin Wang. “Wireless mesh networks: a survey”, Elsevier transactions on computer networks, 2005.
2. Guokai Zeng, Bo Wang, Yong Ding, Li Xiao, Matt W. Mutka, “Efficient Multicast Algorithms for Multichannel Wireless Mesh Networks”, IEEE Transactions on Parallel and Distributed Systems, vol 21, no 1 January 2010.
3. Uyen Trang Nguyen, “On multicast routing in wireless mesh networks”, Elsevier Computer Communications, pp 1385-1399, January 2008.
4. Pedro M.Ruiz, Francisco J.Galera, “Efficient Muticast Routing in Wireless Mesh Networks connected to Internet”, IEEE, 2006.

5. Jing Dong, Kurt Erik Ackermann, Cristina Nita-Rotaru, "Secure Group Communication in Wireless Mesh Networks", IEEE conference on World of Wireless, Mobile and Multimedia Networks, 2008, pp.1-7.
6. Yinan Li, Ing-Ray Chen, "Hierarchical Agent- Based Secure Multicast for Wireless Mesh Networks", proc.IEEE Communication Society, Proceedings of IEEE International Conference on Communications, 2011.
7. Seungjae Shin, Junbeom Hur, Hanjin Lee, Hyunsoo Yoon, "Bandwidth Efficient Key Distribution for Secure Multicast in Dynamic Wireless Mesh Networks", proc IEEE Communication Society, 2009
8. Jing Dong, Reza Curtmola, Cristina Nita-Rotaru, "Secure High Throughput Multicast Routing in Wireless Mesh Networks", IEEE Transactions on Mobile Computing, vol 10 no 5, pp 653-667, May 2011.
9. Yinan Li, Ing-Ray Chen, "Hierarchical Agent- Based Secure Multicast for Wireless Mesh Networks", proc.IEEE Communication Society, Proceedings of IEEE International Conference on Communications, 2011.
10. Jong Talc Kim, Saewoong Bahk, "Design of certification authority using secret redistribution and multicast routing in wireless mesh networks".
11. P.Anitha, G.N.Pavithra, P.S.Periasamy, "An Improved Security Mechanism for High Throughput Multicast Routing in Wireless Mesh Network Against Sybil Attack", proc International Conference on Pattern Recognition, Informatics and Medical Engineering, pp 125-130, March 2012.
12. Sabyasachi Roy, Dimitrios Koutsonikolas, Saumitra Das, and Y. Charlie Hu, "High-throughput Multicast Routing Metrics in Wireless Mesh Networks", IEEE, 2006.
13. Weichao Wang,Bharat Bhargava,"Key Distribution and Update for Secure Inter-group Multicast Communication".
14. Adarsh. R, Ganesh Kumar.R, Jitendranath Mungara, "Secure Data Transition over Multicast Routing In Wireless Mesh network", International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol 1 Issue 3, pp 98-103, August 2012.
15. Adrian Perrig, Dawn Song J.D Tygar, "ELK, a New Protocol for Efficient Large-Group Key Distribution.
16. Jing Dong, Kurt Erik Ackermann, Cristina Nita-Rotaru, "Secure Group Communication in Wireless Mesh Networks", IEEE conference on World of Wireless, Mobile and Multimedia Networks, 2008, pp. 1-7.
17. S.Sasikala Devi, Dr.Antony Selvadoss Danamani, "A Survey on Multicast rekeying for secure group communication", International Journal of Computer Tech Application, vol 2(3) pp 385-391.
18. Jing Dong, Cristina Nita Rotaru, "Enabling Confidentiality for Group Communication in Wireless Mesh Networks".
19. Shafiullah Khan, Kok-Keong Loo, Noor Mast, Tahir Naeem, "SRPM: Secure Routing Protocol for IEEE 802.11 Infrastructure Based Wireless Mesh Networks"
20. M.Iqbal, X.Wang, S.Li, T.Ellis, "Qos scheme for multimedia multicast communications over wireless mesh networks", IEt Commun, vol 4, Issue 11, pp 1312-1324, 2010
21. Guokai Zeng, Bo Wang, Yong Ding, Li Xiao, Matt W. Mutka, "Efficient Multicast Algorithms for Multichannel Wireless Mesh Networks", IEEE Transactions on Parallel and Distributed Systems, vol 21, no 1 January 2010
22. Sung-Hwa Lim, Young-Bae Ko, Cheolgi Kim, Nitin H.Vaidya, "Design and Implementation of multicast for multi-channel multi-interface wireless mesh networks", Springer, pp 955-972, February 2011.
23. Qin Xin, Fredrik Manne, Yan Zhang, Xin Wang, "Almost optimal distributed M2 M multicasting in wireless mesh networks", Elsevier, Theoretical Computer Science, pp69-82, March 2012.
24. Goukai Zeng, Bo Wang, Matt Mutka, Li Xiao, Eric Torng, "Efficient Multicast for Link-Heterogeneous Wireless Mesh Networks".

25. Uyen Trang Nguyen, “On multicast routing in wireless mesh networks”, Elsevier Computer Communications, pp 1385-1399, January 2008.
26. Sung-Ju Lee, Mario Gerla, Ching-Chuan Chiang, “On-Demand Multicast Routing Protocol.”
27. Ashish Raniwala, Tzi-cker Chiueh, “Architecture and Algorithms for an IEEE 802.11-Based Multi-Channel Wireless Mesh Network”
28. Huan-Wen Tsai, Hsu-Cheng Lin, Chih-Lun Chou, Sheng-Tzong Cheng, “Multicast-Tree Construction and Streaming Mechanism for Intra 802.16 Mesh Networks”, International Conference on Networking and Distributed Computing”.
29. Uyen Trang Nguyen, Jin Xu, “Multicast Routing in Wireless Mesh Networks: Minimum Cost Trees or Shortest Path Trees?”
30. Kyoung Jin Oh, Chae Y.Lee, “Multicast Routing Protocol with Low Transmission Delay in Multirate, Multi-radio Wireless mesh Networks”, proc IEEE Computer Society, 2010.
31. unaid Qadir, Chun Tung Chou, Archan Misra, “Exploiting Rate Diversity for Multicasting in Multi-Radio Wireless Mesh Networks”.
32. Brian Keegan, Karol Kowalik and Mark Davis, “Optimisation of Multicast Routing in Wireless Mesh Networks”.
33. Mingquan Wu, Hayder Radha, “Distributed network embedded FEC real-time multicast applications in multi-hop wireless networks”, Springer, pp 1447-1458, October 2009 .
34. Zheng Liu, Min Yang, Heng Dai, Jufeng Dai, “Concurrent Transmission Scheduling for Multi-hop Multicast in Wireless Mesh Networks”.
35. Vineet Khisty, “Link Selection for Point-to-Point 60Ghz Networks”.