# DoS Attack Prevention Technique DSR Protocol based on Signal Strength

Rakesh Dhatarwal
Computer Science Engineering
Govt. Engineering College, Bikaner

D. M. Nagar
Information Technology
Govt. Engineering College, Bikaner

## ABSTRACT

Ad Hoc network is a network that is not any fixed physical structure and is established with mobile nodes using wireless connections. Ad Hoc network is highly flexible and use dynamic network topology. Thus, the efficiency of the routing protocol will affect the all network performance. Dynamic Source Routing (DSR) is one of the extensively used routing protocols for packet transfer from source to destination. It relies on maintaining most recent information, for which, each ad-hoc node maintains hop count and sequence number field. Mobile ad hoc networks carriage many types of security problems, initiated by their open systems and nature of collaborative by limited accessibility of resources.

In this paper, his propose an improved version of DSR routing protocol using neighbor monitoring Scheme which prevents dos attack and accomplishes in maintaining Integrity Security Standard by following minimum hop count path. In GDSR a neighbor monitoring has been detected the routing and packet forwarding vulnerabilities for an incoming demand that helps to stabile its security and efficiency of incoming messages. GDSR DSR routing scheme is evaluated by simulation and results show that improved FPR, throughput and ETE delay can be obtained using simulator.

## Keywords

Security, Integrity, DSR, MANET, DOS, Neighbor Monitoring.

## 1. INTRODUCTION

Mobile ad hoc network is self-governing system of mobile node connected through wireless link, every node has operates an end system and a router for all other nodes in a networks. Thus, the efficiency of the routing protocol will affect the overall networks performance. Routing protocols have long been researched in fixed communication networks. With the development of wireless networks in recent, more and more researches have been focusing on routing protocols for wireless networks [12],[18].

Nodes in mobile ad-hoc network are random and organize themselves in an expert manner. Each user is free to communicate with others. The path between each pair of the users may have many links and the radio between them can be distinct. This allows an association of various links to be a part of the same network. A mobile ad-hoc network is picking up mobile nodes forming an ad-hoc network without any fixed centralized structures. These networks introduced a design of network establishment and can be well suited for an environment where either the substructure is lost or where substructures extend is cheap[1].

Mobile ad-hoc networks can work to connecting "anyplace and anytime" into reality. Ad-hoc applications include a disaster recovery or a military operation. A mobile ad-hoc network introduced a new design of network installation and can be well compatible for an environment where either the infrastructure is missing or where an infrastructure extends is cheap. The "WI-FI" protocol is able to give ad-hoc network facilities at base level, when no access point is available. Nodes are fixed to send and receive information but do not route anything thence forward the network. Mobile ad-hoc networks can be operated in a stand-alone manner or could possibly by connecting to a larger network such as the Internet.

## 2. ROUTING PROTOCOLS FOR MANET

Ad-Hoc Routing Protocol can be classified depending on routing mechanism employed by a given protocol. In Reactive Protocol, route path is set up on demand, i.e., path is set up only when node has data packets to send.eg: Dynamic Source Routing (DSR) [1]. Proactive Protocol practices a table driven approach. It tends to waste bandwidth and power in network because of need to broadcast the routing. e.g.: Distance Sequenced Distance Vector (DSDV) [2]. Hybrid Protocol is combination of both the protocols in order to achieve higher performance. Reactive protocol is used at global network level while employing Proactive protocol in node’s local neighborhood. e.g.: Zone Routing Protocol (ZRP), Hybrid Ad-Hoc Routing Protocol (HARP) [11], [24].

### 2.1 DSR Routing Protocol

DSR routing protocol functions on a pure on- demand route acquisition system, i.e., nodes that do not lie on active path does not maintain any routing information nor take part in any periodic route table exchanges [1]. DSR protocol mainly involves 3 packets: - Route Request (RREQ) is broadcasted by source code to its neighbors whenever it has data packets to transfer. Route Reply (RREP) is sent by destination to source when route is established. The Route Error (RERR) is sent by either destination or intermediate nodes when there is no path to destination or when the link breaks in valid path to destination[2][25].

## 3. SECURITY CHALLENGES

The DSR routing protocol uses a reactive approach but this DSR have some disadvantage. The disadvantage of this protocol is that the route maintenance mechanism does not locally repair a broken link. Stale route cache information could also result in inconsistencies during the route reconstruction phase. The connection setup delay is higher than in table- driven protocols. Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility. Also, considerable routing above is involved due to the source-routing mechanism employed in DSR. This routing above is directly is directly proportional to the path length.

The primary concern of any security solution for DSR should be to satisfy security standards, mainly, Integrity, Authentication, Confidentiality and non-repudiation [6], [15] and [24]. To achieve these standards, the designed security solution must safeguard against attacks possible at each layer. Table describes some security attacks.

## 3.1 Attacks on Ad-hoc Network

Ad-Hoc Network being wireless in nature is vulnerable to many attacks, which are mainly categorized as:

- Routing Loop: By sending forged routing packets an attacker can create a routing loop. This will result in data packets being sent around consuming both power and bandwidth for a number of nodes. The packets will not reach their intended recipient and thus can be considered a sort of denial-of service attack.

- Grey Hole Attack: In this case, the attacker introduce itself as cooperating node, it participate in route request and route reply mechanism, it make sure that it will be available on the path. After the route discovery mechanism, when source node transmit data packet at that time malicious user just drop all the data packet. In other words, such attacker does not allow that all of packets arrive at real destination.

- The goal of security solutions for MANET's is eventually to render services such as integrity, authentication, confidentiality, non-repudiation and availability. No single mechanism exists that could provide all the security services for MANET's. In this paper, we have focused on ensuring Integrity of Data being transferred by introducing an improvement in DSR Routing Protocol. It ensures that message being transmitted is never corrupted and maintains Integrity Standard over a minimum hop count path.

## 3.2 Secure Multi-hop neighbor Monitoring Mechanism DSR

In this work he look at DSR in detail, study and explain various attacks possible on it. His proposed work is extension of GDSR, which includes change strategies and improving its performance. In This thesis report on the research to develop a routing protocol algorithm to solve the problem of malicious node and secure data transmission in mobile ad hoc network. As Dynamic source routing protocol establishes routes only when the source node is going to send data packets to a destination node. The proposed method, called modified DSR protocol (GDSR), is developing by modifying the DSR protocol.

The first part of the proposed security mechanism is built on the model of neighbor monitoring to detect the mischievous nodes in the network. Acting as a message sender or relay node, each node should change its channel not only depending on multi-hop neighbors. The neighbor monitoring has detected the routing and packet dispatching vulnerabilities. The detail is described as follows.

He implements the DSR protocol and gets the result. First of all calculate the G value and Now compare G value and table result and get that the malicious node is available in this process or not so the packet transmission process in DSR done by just sending RREQ message broadcasting again and again. But in comparison to G value the node first finds the neighbor node and the neighbor list of the packet. Then it rebroadcast the RREQ message to the nodes which are not getting the message. After that we compute two performance metrics and by these we transmit the data without any malicious process.

In this thesis we goals a developed a secure path transmission and efficient routing protocol. So that work we divided the process into parts as

1. Develop an adaptive GDSR routing protocol of the secure DSR protocol extension.

2. Develop the secure routing protocol to solve the problem of malicious node through G value calculating.

Then destination nodes receive several RREQ messages for the same communication flow. When a node meets a transmission problem, it removes the route from its route cache and generates a route error message. The route error message is sent to each node that has sent a packet routed over the broken link. When a node receives a route error message, it removes the hop in error from its route cache. He makes sure that the RREP message sent by the destination node will flow the reverse route that is created during the RREQ propagation phase. Then the RREP is received by the source node. In the proposed G-DSR protocol, each node selects a radio link with the lowest G value from the available set of neighbor links it has during the route discovery process between a source-destination pair. An info field called G-info is added in the RREQ (Route Request) message of DSR routing protocol. The value of the G of a received message is calculated using its received hope count value which is exacted from RREQ message format [4], [3].

The hope count is calculated as a number of received RREQ signals. The information about the queue load of each node of the received RREQ message is then used by the network layer during the route discovery process to select the route that consists with the links that has the lowest load as compared to the other routes available between the source destination pair for which the route discovery phase is initiated. Two additional data structures that are used in the implementation process of our proposed G-DSR protocol. The first data structure is a modification in the DSR protocols RREQ control message. In this, i add a G-info field is added whenever it receives a RREQ message. In the G-info field adds the request message queue load information of the received RREQ message which is then extracted from hope count value when this RREQ is reached at the network layer. The second data structure is the RREQ_BUFFER that is created at each node during the route discovery process [2], [3].

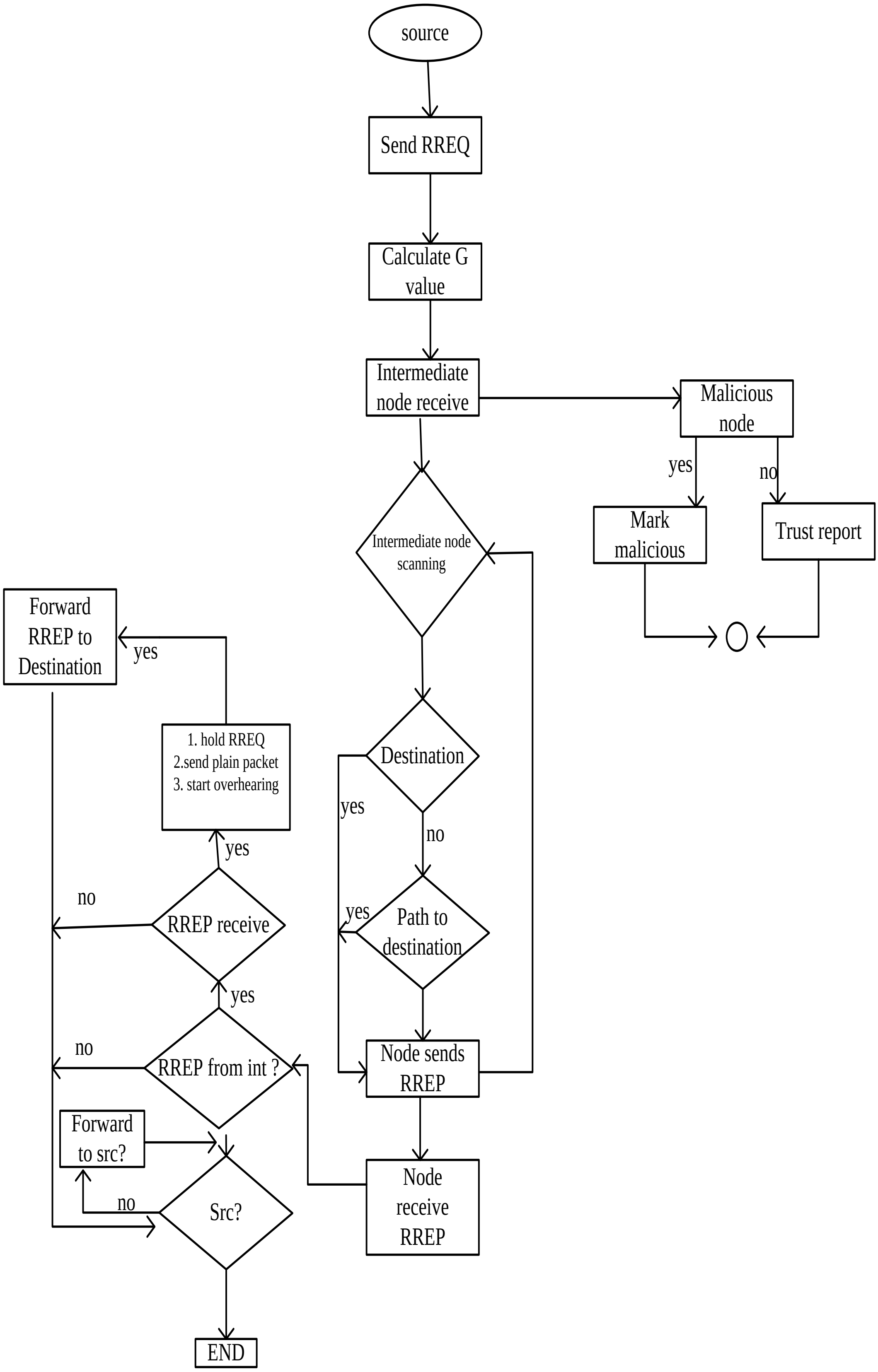

**Fig 1: Flow Chart Of DSR Protocol**

# 4. EVALUATION METHOD

## 4.1 Simulation Setup

A simulation model was developed using EXATA where assessment was done by examining the performance result of two conditions 1) using normal DSR Protocol 2) using proposed GDSR Protocol. Overall simulation parameters are summarized below:

**Table 1: Simulation Setup**

| PARAMTER | VALUE |
|---|---|
| Simulator | EXATA |
| Simulation Time | 300sec |
| Number of nodes | 40-120 |
| Terrain | 1200m*1200m |
| Traffic type | Random |
| Packet Size | 512 B |
| Packet Generation Rate | 4 packet/sec |

## 4.2 Routing Metrics

The metrics mentioned below is used in our evaluation:

1. Average ETE Delay: Average of all packets' time delay from source node to destination node, which in turn manifests the efficiency of a routing protocol.

2. Throughput: Refers to the rate of successful message delivery over a communication channel. The larger the throughput, the more reliable the network is.

ETE Delay and Throughput metrics is evaluated over two factors, namely, network mobility and network load.

## 4.3 Simulation Results

The performance of the proposed GDSR and default DSR are compared. Four runs with different random seed numbers were conducted for both the metrics.

Fig. 2 and Fig. 3 showcase how ETE Delay and throughput varies against network mobility. In Fig. 2, ETE Delay initially has higher value for DSR when compared to GDSR. GDSR outperforms DSR as network mobility increases due to less rerouting and high integrity.

In Fig. 3, throughput for GDSR is far better in earliest stages of network mobility. Throughput of DSR has wide fluctuations whereas GDSR maintained a constant rate because of packets dropped in very less when compared to DSR. When node mobility is higher than 18, throughput of GDSR is approximately 23%/30% greater than DSR.

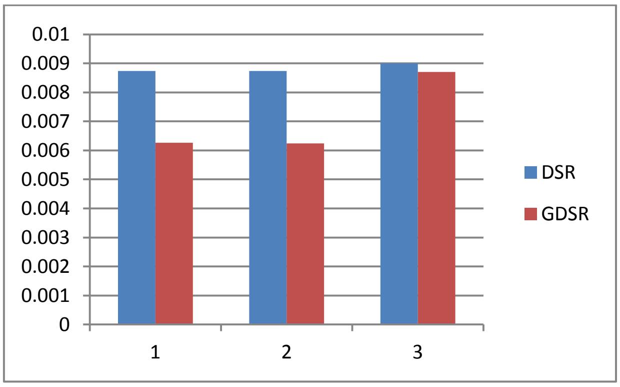

**Fig 2: End To End Delay N/W Mobility**

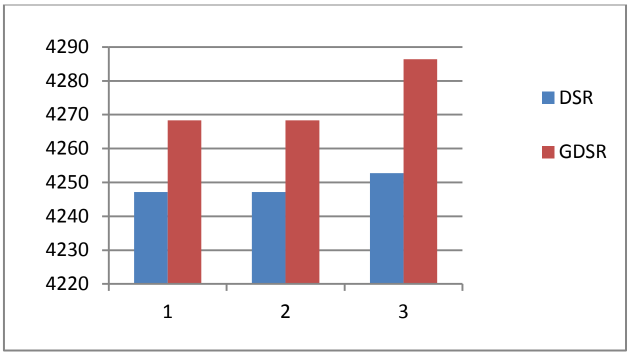

**Fig. 3: Average Throughput with Increase In Network Mobility**

Fig. 4 and Fig. 5 show how ETE Delay and throughput varies against network load. In Fig. 3, DSR has high ETE Delay when network load is less than 10. It drops sharply as network load increases, but GDSR proves to be better and maintains a considerable effective ETE Delay as compared to its counterpart DSR. In Fig. 5, throughput obtained in case of GDSR is far better than DSR when network load is 20 throughput of GDSR is approximately 4.54% greater than GDSR.

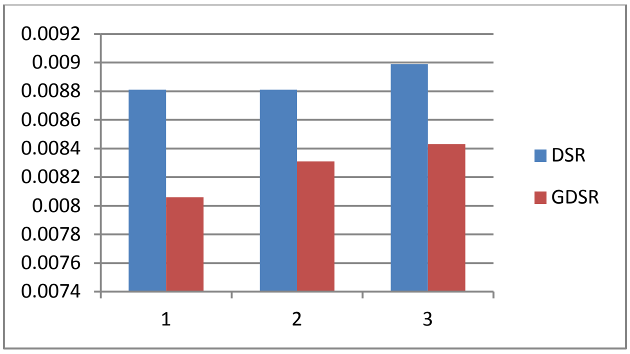

**Fig 4: End To End Delay N/W Load**

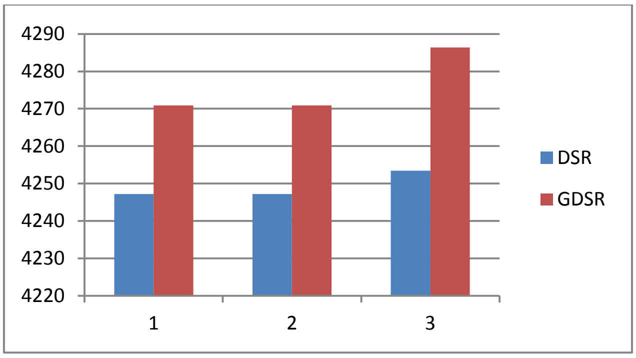

**Fig 5: Average Throughput with Increase in Network load**

# 5. CONCLUSION AND FUTURE WORK

In the DSR routing protocol the performance of these parameters as the first packet received, throughput and end to end delay but the modified DSR that is improve the performance much in this process so that routing protocol is show as GDSR routing protocol. In this paper the malicious node is find out and remove the malicious nodes through the G value. He evaluated the behavior of DSR protocol developed in this research, analyzed its performance and compared it to the original DSR protocol in ad hoc network environments. The simulation results show that the modified DSR protocol achieves higher network performance than the original DSR protocol.

In this research, present a new method to improve performance of the DSR protocol using the G value in Ad-hoc network. This method is not only used in DSR routing protocol but also use in other Ad-hoc network routing protocols. In the research, focus is on the data transmission. The simulation done in this research, when source node receives a RREP from the destination node, and data transfer to the destination node. He tried to discover and analyze the impact of DOS attack in MANETS using DSR and GDSR protocols. There is a need to analyze DOS attack in other MANETS routing protocols such as AODV, TORA and GRP. Other types of attacks such as wormhole, jellyfish and Sybil attacks are needed to be studied in comparison with DOS attack. They can be categorized on the basis of how much they affect the performance of the network.

## 6. REFERENCES

[1] Rahiman, M. Abdul, et al. "Code Aware Dynamic Source Routing for Distributed Sensor Network." International Conference on Communication Systems and Network Technologies (CSNT-2013), Gwalior, India. 2013.

[2] Hamad, S.; Noureddine, H.; Al-Raweshidy, H., "LSEA: Link Stability and Energy Aware for efficient routing in Mobile Ad Hoc Network,"14th International Symposium on Wireless Personal Multimedia Communications 2011(WPMC'11), pp.1-5, Oct. 2011.

[3] AbdJali, Kamarularifin, Zaid Ahmad, and Jamalul-Lail Ab Manan. "Mitigation of Black Hole Attacks for DSR Routing Protocol." (2011).

[4] T. Jin, G. Noubir, B. Thapa, "Zero Pre-shared Secret Key Establishment in the Presence of Jammers", MOBIHOC 2009, New Orleans, Louisiana, USA, 2009, pp. 219-228.

[5] Yafeng Zhou; Sang-Hwa Chung; Lihua Yang; "A Link-Quality Aware Routing Metric for Multi-hop Wireless Network," International Conference on Communication Software and Networks, 2009(ICCSN'09)., pp.390-394, 27-28 Feb. 2009.

[6] D. Boneh, D. Freeman, J. Katz, and B. Waters, "Signing a linear subspace: Signature schemes for network coding," in Public Key Cryptography- PKC 2009, ser. Lecture Notes in Computer Science 5443.Springer Verlag, 2009, pp. 68–87.

[7] Effatparvar, M.R.; Yazdani, N.; Lahooti, F.; EffatParvar, M., "Link Stability Approach and Scalability Method on ODMRP in Ad Hoc Networks," Communication Networks and Services Research Conference, 2009(NSR '09)., pp.416-421, 11-13 May 2009.

[8] J. Dong, R. Curtmola, and C. Nita-Rotaru, "Practical defenses against pollution attacks in intra-flow network coding for wireless mesh networks,"in ACM conference on Wireless network security - WiSec '09.ACM, 2009, pp. 111–122.

[9] D. Charles, K. Jain, and K. Lauter, "Signatures for network coding," International Journal in Information and Coding Theory, vol. 1, no. 1,pp. 3–14, 2009.

[10] "Secure network coding for wireless mesh networks: Threats,challenges, and directions," Computer Communication, vol. 32, no. 17,pp. 1790–1801, 2009.

[11] Wu, C.; K.; Kato,"AMANET protocol considering link stability and bandwidth efficiency", International Conference on Ultra-Modern Telecommunications & Workshops, 2009(ICUMT '09), pp.18, 12-14 Oct. 2009.

[12] A. Dhananjay, H. Zhang,"Practical, Distributed Channel Assignment and Routing in Dual-radio Mesh Networks", SIGCOMM 2009, Aug 2009, pp. 99 – 110.

[13] H. Huang, X. Cao, and X. Jia, "Channel assignment using block design in wireless mesh networks", Computer Communication, vol.32,2009, pp.1148-1153.

[14] S. Katti, H. Rahul, W. Hu, D. Katabi, M. M´edard, and J. Crowcroft, "XORs in the air: practical wireless network coding," IEEE/ACM Transactions on Networking, vol. 16, no. 3, pp. 497–510, 2008.

[15] P. Dutta, S. Jaiswal, R. Rastogi, "Globally Optimal Channel Assignment for Non-Cooperative Wireless Networks", INFOCOM 2008, pp. 2216-2224.

[16] Peng Yang, "QoS Routing Protocol Based on Link Stability with Dynamic Delay Prediction in MANET," Pacific-Asia Workshop on Computational Intelligence and Industrial Application, 2008. ,vol.1, pp.515-518, 19-20 Dec. 2008.

[17] P. Sarkar, "A New Universal Hash Function and Other Cryptographic Algorithms Suitable for Resource Constrained Devices," Cryptology ePrint Archive, Report 2008/216, 2008.

[18] P. Dutta, S. Jaiswal, R. Rastogi, "Globally Optimal Channel Assignment for Non-Cooperative Wireless Networks", INFOCOM 2008, pp. 2216-2224.

[19] Kar, K., Luo, X., Sarkar, S, "Throughput-Optimal Scheduling in Multichannel Access Point Networks Under Infrequent Channel Measurements", INFOCOM 2007, 26th IEEE International Conference on Computer Communications, May 2007, pp. 1640 –1648.

[20] YingZhiZeng, JinShu Su, Xia Yan, BaoKang Zhao, QingYuan Huang. "LBKERS: A New Efficient Key Management Scheme for Wireless Sensor Networks". the 3rd International Conference on Mobile Ad-hoc and Sensor Networks (MSN), Beijing, China, 2007,pp. 772-783.

[21] A. Haq, A. Naveed and S. S. Kanhere, "Securing Channel Assignment in Multi-Radio Multi-Channel Wireless Mesh Networks",in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC - 2007), Hong Kong, March 2007, pp.3113-3118.

[22] Lin, X., Rasool, S.A, "Distributed Joint Channel-Assignment, Scheduling and Routing Algorithm for Multi-Channel Ad-hoc Wireless Networks"., 26th IEEE International Conference on Computer Communications (INFOCOM 2007), May 2007, pp. 1118 –1126.

[23] C. Gkantsidis and P. Rodriguez, "Cooperative Security for Network Coding File Distribution," in IEEE INFOCOM 2006. IEEE, 2006.

[24] A. Naveed, S. S. Kanhere, "Security Vulnerabilities in Channel Assignment of Multi-Radio Multi-Channel Wireless Mesh Networks",Globecom 2006, Nov. 2006.

[25] Jenn-Hwan Tarng; Bing-Wen Chuang; Fang-Jing Wu, "A Radio-LinkStability-based Routing Protocol for Mobile Ad Hoc Networks," IEEE International Conference on Systems, Man and Cybernetics,2006(SMC'06). , vol.5, pp.3697-3701, 8-11 Oct. 2006.

[26] Rupinder Gill, Jason Smith, Mark Looi and Andrew Clark. "Passive Techniques for Detecting Session. Hijacking Attacks in IEEE 802.11 Wireless networks".In proceedings of AusCERT2005, Gold Coast, Australia, May 2005, pp. 26-38.

[27]Chunxiao Chigan, Leiyuan Li, Yinghua Ye, "Resource-aware selfadaptive security provisioning in mobile ad hoc networks". In proceedings of Wireless Communications and Networking Conference, March 2005, pp. 2118 -2124.

[28] Yan Xia, Ren-Fa Li, Ken-Li Li, "Intrusion Detection Using Mobile Agent in AD Hoc Networks", Proceedings of the International Conference on Machine Learning and Cybernetics, Volume 6, Aug. 2004, pp. 3383-3388.

[29] M. Alicherry, R. Bhatia, L. Li,"Joint Channel Assignment and Routing for Throughput Optimization in Multi-radio Wireless Mesh Networks", MOBICOM 2005, Cologne, Germany, Aug 2005, pp. 58-72.

[30] M. N. Krohn, M. J. Freedman, and D. Mazi`eres, "On-the-Fly Verification of Rateless Erasure Codes for Efficient Content Distribution," in IEEE Symposium on Security and PrivacyS&P2004.IEEEComputer Society, 2004, pp. 226–240.