Investigatory Analysis of Attacks on DSR and AODV in Mobile Ad-hoc Network

Mehak Saini[1], Priyanshu Tripathi[2], Madhwendra Nath[3], Sanju Saini[4], K K Saini[5]
[1] Department of Electronics and Communication Engineering
Deenbandhu Chhoturam University of Science and Technology Murthal, Sonepat, Haryana, India
[2,3,5]Department of Electronics and Communication Engineering
Hindu College of Engineering Sonepat, Haryana, India
[4] Department of Electrical Engineering
Deenbandhu Chhoturam University of Science and Technology Murthal, Sonepat, Haryana, India
[1]mhk.saini1904@gmail.com [2]prk.tripathi@gmail.com, [3]madhwendra.711@gmai.com, [4]dphce2015@gmail.com, [5]sanjusaini.ee@dcrustm.org

***Abstract*- A Security threat in MANET (Mobile Ad hoc Network) is an important issue because of the numerous attacks. Its routing protocols are vulnerable to unattended installation of sensor nodes in the environment causes these security threats in the Ad-hoc networks. The security of the DSR and AODV protocol is threaded by some kind of attacks such as Black Hole attack and Gray Hole attack. In this work, a novel technique has been proposed to detect and prevent the two types of attacks (Black hole attack and Grey hole attack) which cause more damage to the routing performance of MANET. the impact of these attacks on MANET has been compared also. Here, the AODV routing protocol is improved and simulated in MATLAB.**

Index Terms- MANET, AODV routing protocol, Black hole, gray hole.

I. INTRODUCTION

The Ad-hoc network may be a assortment of infrastructure less nodes, co-operating dynamically to make a brief network that meets sure immediate wants. The shortage of infrastructure implies that the nodes square measure connected peer-to-peer. Therefore, every node plays its role as a number beside its role as a router [1, 2]. Just in case of rescue and emergency operations, putting in a centralized supporting system is time overwhelming. In-order to beat this drawback we've got Mobile unintentional Networks which might be quickly deployed in places wherever it's inconceivable otherwise. MANETs square measure essentially a group of mobile nodes that communicate wirelessly.

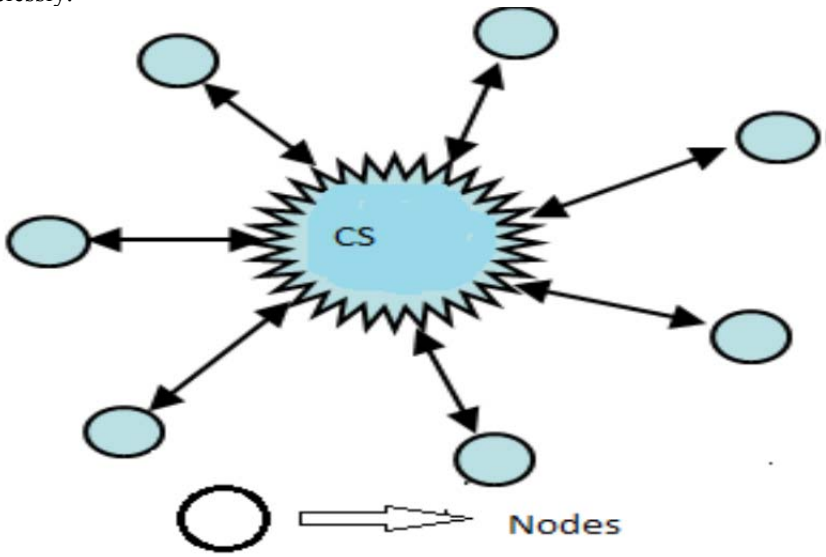

Fig.1.1 MANET with Centralized System [12]

Security in Mobile Ad-hoc Network is that the most significant concern for the essential practicality of

network. Convenience of network services, confidentiality and integrity of the information is achieved by reassuring that security problems are met. MANET typically suffer from security attacks attributable to the its options like open medium, dynamic its topology dynamically, lack of central observation and management, co-operative algorithms and no clear psychoanalytic process. These factors have modified the battle field scenario for the MANET against the safety threats. MANET works while not a centralized administration wherever node communicates with one another on the bottom of mutual trust. This characteristic makes MANET a lot of liable to be exploited by associate degree offender from within the network. Wireless links conjointly creates the MANET a lot of liable to attacks that make it easier for the offender to travel within the network and find access to the continuing communication [7].

1.1 Objectives of work:

- An elaborate study targeted on impact of black hole and gray hole attack in MANET.
- Comparative analysis of both the attacks on DSR by mistreatment AODV routing protocol – an energetic protocol.

1.2 Types of Attack:

- Black hole attack
- Grayhole attack
- Wormhole attack

Black hole attack:

In Black-hole-attack, a malicious node will impersonate a destination node by causing a spoofed route packet to a supply node that initiates a route discovery [5]. A black hole has two properties [4]:

a) The node exploits the unexpected routing protocol to advertise itself as having a sound route to a destination, despite the fact that the route is spurious, with the intention of intercepting packets.
b) The node consumes the intercepted packets. In a poster hoc network that uses the AODV protocol, a part node absorbs the network traffic and drops all packets. to elucidate the part attack we tend to add a malicious node that exhibits part behavior within the Fig.2.

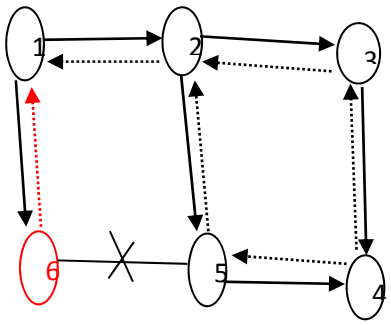

Fig1.2: Black hole attack in AODV

Gray Hole Attack:

This is a kind of active attack. within the starting, the assaulter nodes behave ordinarily and reply true RREP messages to the nodes that started RREQ messages. once it receives the packets it starts dropping the packets and launches Denial of Service (DoS) attack. It drops packets whereas forwarding them within the network. In another grey hole attacks the assaulter node behaves maliciously for the time till the packets square measure born so switch to their traditional behavior [8]. grey hole attack is additionally referred to as node misbehaving attack [6].

Wormhole attack:

The hollow assaulter creates a tunnel so as to records the continuing communication and traffic at one network position and channels them to a different position within the network [10].When the assaulter nodes produce an immediate link between one another within the network, the hollow assaulter then receives packets at one finish and transmits the packets to the opposite finish of the network. once the attackers square measure in such position the attack is thought as out of band hollow [9].

II. LITERATURE SURVEY

Hizbullah Khattak [1]: In this paper, the authors bestowed a hybrid approach for preventing black/gray hole attacks by choosing second shortest route for secure route choice and hash operate and timestamp base answer for consisting information transmission.

Ketan S. Chavda [2]: the Ad-hoc on-demand distance vector routing (AODV) is demand driven one in the entire simplest and widespread routing algorithmic program. AODV was severely stricken by well-known part attack during which a malicious node injects a pretend route reply message that it's a contemporary route towards destination. In this paper, a completely unique approach was projected that creates a modification in existing AODV routing protocol. A completely unique approach finds the safe route between causation and receiving node. The simulations shows that the projected approach was economical than traditional AODV with high packet delivery magnitude relation and turnout.

C. K. Nagpal [8]: Analysed a performance analysis of Ad-hoc networks within the presence of the part nodes. Mobile Ad-hoc Network (MANET) could be a self-organized wireless network, consisting of nodes (mobile devices) chargeable for its creation, operation and maintenance. The communication within the MANET is of multi-hop in nature because of absence of any fastened infrastructure. Associate in Nursing assailant might intrude simply into MANET by movement as legitimate intermediate node and gift numerous kinds of security attacks on information exchanges happening between supply and destination. In this paper we tend to study the impact of presence of part node on MANET performance on the idea of reachability, hop count, neighbor node density and path optimality. We tend to observe that because the share of part nodes will increase, the MANET performance degrades considerably.

Sweta religion [6]: bestowed a review on a serious class of co-ordinate attacks i.e. co-operative part / Grey Hole attack that are a heavy threat to Ad-hoc network security. In co-operative part attack multiple nodes conspire to cover the malicious activity of alternative nodes; thence such attacks were harder to find. In this paper a survey of assorted security mechanisms that had been projected within the literature for diction of such attacks was bestowed. The limitation of this prompt work was that it doesn't find co-ordinate attacks that successively greatly reduced the system performance during a touch of your time and resulted as a bigger injury.

R. Sivakami [3]: projected that MANETS were a spontaneous network that may be established with none infrastructure. Issues were moon-faced whereas fixing and employing a MANET that was each reliable and secure. Transmittal message over multiple ways can increase the protection Associate in Nursingd dependability of transmission in an open cooperative MANET surroundings wherever any node will maliciously or egotistically disrupt and deny communication of alternative nodes.

Fidel Thachil [11] projected a trust based mostly cooperative approach to mitigate part nodes in AODV protocol for MANET. In this approach each node monitors neighboring nodes and calculates trust price on its neighboring nodes dynamically. If the trust price of a monitored node goes below with relevance predefined threshold, then the observance node assume it as a malicious and avoided that node from the route path. The experiment disclosed that the projected theme secures the AODV routing protocol for MANET by mitigating and avoiding part nodes.

III. PROPOSED MODEL AND RESULTS

In order to simulate each the attacks we've got changed the AODV protocol by making a machine in MATLAB. In this simulation the supply node (chosen randomly) broadcasts a RREQ request within the network. The request contains destination node address. Currently each node that receives the request has got to send a RREP back to the sender of RREQ. If the receiver is itself the destination, then the search ends and RREP is shipped back to the sender. Otherwise, the receiver more broadcasts the RREQ to its neighbors within the network. The sender when causing the RREQ sends a check packet to all or any nodes that received the RREQ. The receiver has got to resend the packet back to the sender. Currently if the receiver is associate offender node, it'll drop the packet; this detects the region offender node. Currently the sender stores in its cache the address of this receiver as a region and sends equivalent information to neighboring nodes throughout successive request.

Some nodes drop packets by selection whereas routing the opposite packets. The sender involves fathom the standing as a Grey Hole only a packet is born.

In Fig.3, a synthetic MANET machine is formed thus on discover the attack. The inexperienced color dots square measure nodes within the networks that contain some worth of energy like E0 = zero.005 and also the transmitter state energy ETX = 50*0.000000001 and receiver state energy ERX = 50*0.000000001. Because the knowledge is transmitted and also the variety of rounds will increase the energy is reduced and also the nodes square measure dead. At conclusion the red colored cross square measure dead nodes with zero energy. The black colored dots depict region attack that happens once a malicious node act as associate intermediate node and destroys the info packets. The blue color dots represents the gray Hole attack in which the attacker misleads the network by agreeing to forward the packets in the network.

The on top of Fig.4 shows the amount of black holes attacks detected in every spherical. The image

shows region attack that is merely one attack most as a result of every spherical show single transfer of knowledge from supply to destination associated if an attack detected, the info doesn't reach its destination.

In Fig.5, the amount of grey hole attacks detected in every spherical is incontestable. The amount of nodes typically reaches quite one offender nodes in a very spherical as a result of the grey hole nodes don't continuously kill the info. Typically they are doing enable the packets to have them to the destination. Thus there's an opportunity that grey hole offender node is encountered later within the path.

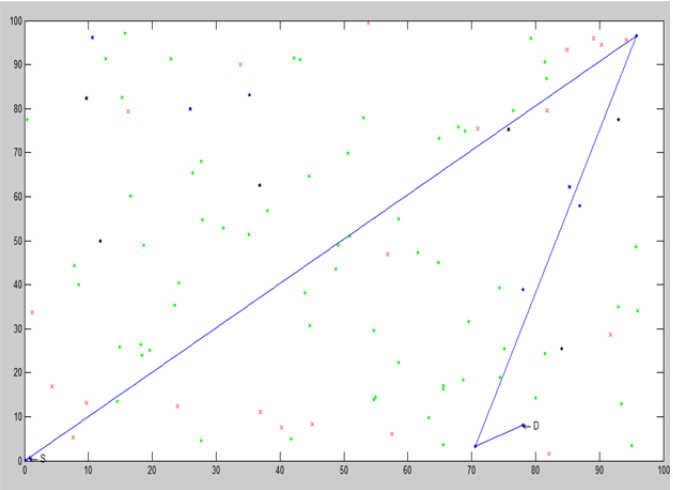

Fig.3: MANET Simulaton

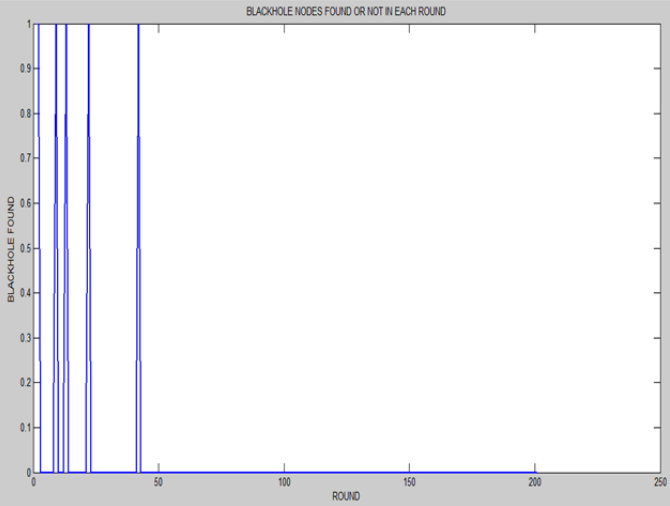

Fig.4: No of black hole found in each node

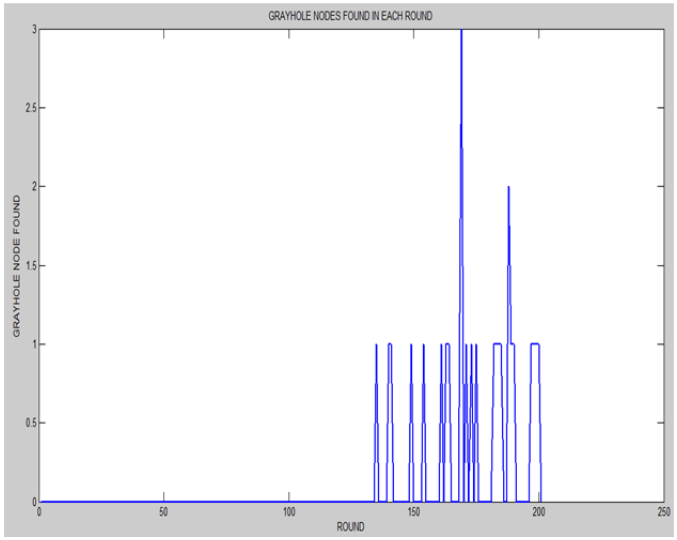

Fig.5: No of Gray hole found in each node

Fig.6 shows the graphical analysis of variety of dead nodes fashioned in every spherical is conferred here. Whereas iteration takes place when attack is performed within the system, the nodes concerned lose their energy and ultimately it ends up in a dead node. Because the variety of rounds will increase there's an excellent increase within the variety of dead nodes to be fashioned. There's an oversized decrease within the quantity of energy of nodes when a hundred and forty rounds that cause the rise within the variety of dead nodes of the system.

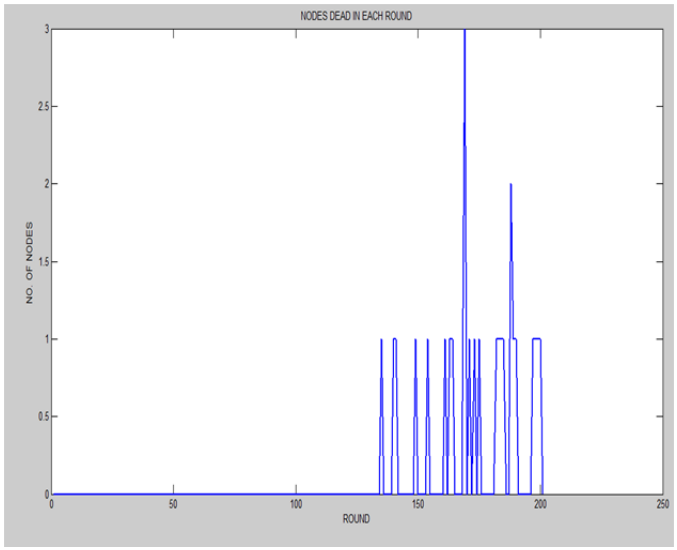

Fig.6: Graph for dead nodes in each round after attack

The amount of energy consumed in every spherical is hyperbolic because the system iterates. In Fig.7, there's an oversized increment within the quantity of energy consumed when every spherical. The pointer shows an excellent increment ranging from first spherical to two hundred rounds. Because the energy is lost when every spherical this indirectly shows the energy consumption of the system

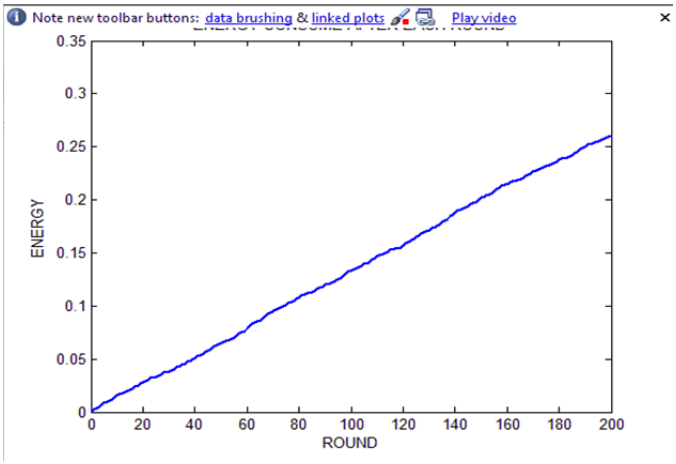

Fig.7: Graph for energy consumption in each round

IV. CONCLUSIONS AND FUTURE SCOPE

In this paper, we've got overviewed the challenges and solutions of the protection threats in MANET. As shown within the graphs the region attacks area unit additional vulnerable than grey Hole attacks as a result of the packet drop quantitative relation is high for region attacks compared to grey Hole attacks. Compared to the quantity of energy consumption within the system, it's additional within the case of any attack performed within the system instead of while not attacked system.

Significant analysis in MANET has been in progress for several years, however still in AN early stage. Resource consumption DoS attack remains unclear to the researchers. Additional analysis is required on secure routing protocol, sturdy key management.

ACKNOWLEDGEMENT

The work reported in this paper was supported by Worthy Director-Principal, faculty & Staff members of Hindu College of engineering and the Honorable management of "The Sonepat Hindu Educational and Charitable Society Sonepat.

REFERENCES

[1] HizbullahKhattak, Nizamuddin "A Hybrid Approach for Preventing Black and Gray Hole Attacks in MANET", IEEE, 2013.
[2] Ketan S. Chavda and Ashish V. Nimavat "Removal Of Black Hole Attack In Aodv Routing Protocol Of MANET", 4th ICCCNT – 2013.
[3] R.Sivakami and Dr.G.M.Kadhar Nawaz "Reliable Communication for MANETS in Military through Identification and Removal of Byzantine Faults", IEEE ,2011.
[4] Latha Tamilselvan, Dr. V Sankaranarayanan,"Prevention of Black hole Attack in MANET"; IEEE, The 2nd International Conference on Wireless Broadband and Ultra Wideband Communication (AusWireless 2007) India,2007.
[5] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto. "Detecting Black hole Attackon AODV ASED Mobile Ad hoc networks by Dynamic Learning Method". International Journa of Network Security. Vol.5, No.3, PP.338-346, Nov 2007.
[6] Sweta Jain, JyotiSinghai, Meenu Chawla " A Review Paper on Co-operative Blackhole And Grayhole Attacks in Mobile Ad hoc Networks", IJASUC Vol.2, No.3, September 2011.
[7] Hussein Al-Bahadili and Rami Jaradat "Performance Evaluation of an OMPR Algorithm for Route Discovery in Noisy MANETs" International Journal of Computer Networks & Communications (IJCNC), Vol. 2, No. 1, January 2010.
[8] C. K. Nagpal, Chirag Kumar and Bharat Bhushan "A Study of Black Hole Attack on MANET Performance" I.J.Modern Education and Computer Science, 2012.
[9] R.Sivakami and Dr.G.M.Kadhar Nawaz "Reliable Communication for MANETS in Military through Identification and Removal of Byzantine Faults", IEEE ,2011.
[10] Chiranjeev Kumar, Gourav Kumar, and Puja Rani "Efficient-Dynamic Source Routing (E-DSR)", International Symposium on Communications and Information Technologies (ISCIT), 2012.
[11] Fidel Thachil and K C Shet "A trust based approach for AODV protocol to mitigate black hole attack in MANET", International Conference on Computing Sciences, 2012.
[12] Pradeep Kumar Sharma, Shivlal Mewada and Pratiksha Nigam "Investigation Based Performance of Black and Gray Hole Attack in Mobile Ad-Hoc Network" International Journal of Scientific Research in network security and communication, 2013.
[13] Wang W, Bhargava B, Linderman M, "Defending against Collaborative Packet Drop Attacks on MANETs", International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009), New York, USA, 27 September 2009.
[14] Sanju Saini, K.K. Saini, " Comparative analysis of various mobility generators techniques in VANETs", IJEC, Vol. 5, No. 2, 2013, pp. 113-117.
[15] Sanju Saini and J.S. Saini , "Chaotic queue-based genetic algorithm for design of a self-tuning fuzzy logic controller," 6th Global Conference on Power Control & Optimization, 6-8 August 2012, Las-Vegas, U.S.A.
[16] Min Z, Jiliu Z, "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks**",** International Symposium on Information Engineering and Electronic Commerce, Ternopil, Ukraine, 16–17 May 2009.

[17] Sanju Saini, Dr. J.S.Saini, "Secure Communication Using Memristor based Chaotic Circuit", Proceedings of IEEE International Conference on Parallel, Distributed and Grid Computing, Waknaghat, Solan, H. P., India, December 11-13, 2014, pp.159-163.
[18] Raj PN, Swadas PB, "DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET", International Journal of Computer Science 2009.
[19] Vijay Rohilla, Sanju Saini et. al., "Identification of suitable LFC structure optimized by GA with SMES in deregulated environment", International journal of applied engineering research, Vol. 7, No. 11, 2012.
[20] Jaisankar N, Saravanan R, Swamy KD, "A Novel Security Approach for Detecting Black Hole Attack in MANET'', International Conference on Recent Trends in Business Administration and Information Processing, Thiruvananthapuram, India, 26–27 March 2010.
[21] Snehlata, Mrs.Sanju Saini, "Chaotic Search Based Genetic Algorithm for Economic Load Dispatch Problem", Proc. of Int. Conf. on Emerging Trends in Engineering and Technology, DOI: 03.AETS.2013.3.142_34© Association of Computer Electronics and Electrical Engineers, 2013.
[22] Mistry N, Jinwala DC, IAENG, Zaveri M, "Improving AODV Protocol Against Blackhole Attacks", International MultiConference of Engineers and Computer Scientists, Hong Kong, 17–19 March, 2010.
[23] Pawan, Sanju Saini, " Matlab Simulation of Chaotic System and its Application in Secure Communication with AWGN Channel", International Journal of Electrical, Electronics and Data Communication, vol. 1, Issue 4,pp. 56-59, ISSN:2320-2084, 2013.
[24] Oliveira R, Bhargava B, Azarmi M, Ferreira EWT, Wang W, Lindermann M, **"**Developing Attack Defense Ideas for Ad Hoc Wireless Networks"**,** Dependable Network Computing and Mobile Systems (DNCMS 2009), New York, USA, 27 September 2009.
[25] Sanju Saini, Dr. J.S.Saini "GA Optimized Time Delayed Feedback Control of Chaos in a Memristor Based Chaotic Circuit", Proceedings of IEEE Symposium on Computational Intelligence for Engineering solutions 2014 , Orlando, Florida, U.S.A, 9-12 Dec. 2014, pp. 74-80.
[26] Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K, **"**Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks" *International Conference on Wireless Networks, Las Vegas, Nevada, USA, 23–26 June 2003* .
[27] Weerasinghe H, Fu H, **"**Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", *Future Generation Communication and Networking, Jeju-Island, Korea, 6–8 December 2007.*
[28] Sanju Saini, J.S.Saini, "Chaos Embedded Optimization Algorithms : State of the Art", Proceedings of International Conference on Interdisciplinary Research & Technological Developments, Chandigarh , India, 1st November, 2014.
[29] Yu CW, Wu T-K, Cheng RH, Chang SC, **"**A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network"**,** *PAKDD workshops, Nanjing, China, 22–25 May 2007.*
[30] Megha Tiwari, Sanju Saini et. al., "Multisim Implementation & application of Chua's circuit in secure communication", National conference on contemporary techniques & technologies in Electronics Engineering, D.C.R.U.S.T, Murthal, Sonepat, 13-14 March, 2013.
[31] Sanju Saini, KK Saini, " Based new WiMax simulation model to investigate Qos with OPNET modeler in sheduling environment", Journal of AIP Conference Proceedings, Vol. 1499, Issue 1, 2012, pp. 234-238.
[32] Djenouri D, Badache N, **"**Struggling Against Selfishness and Black Hole Attacks in MANETs**",** *Wireless Communications & Mobile Computing* 2008..

BIOGRAPHIES

Ms. Mehak Saini is B.Tech (ECE) and pursuing M.Tech from Deenbandhu Chhoturam University of Science and Technology Murthal, Sonepat ,Haryana, India. She is a young Technocrat and Researcher. She has published 6 research papers in National/ International Journals. Her area of Interest is Watermarking Techniques, Optical Communication and Advanced Communication System.

Mr. Priyanshu Tripathi is B.Tech., M.Tech from N.I.T. Jalandhar, Punjab, India. He is a young Technocrat and researcher. Currently, He is working as an Assistant Professor in Hindu college of Engineering Sonepat, Haryana, India. His area of Interest is Robotics and image processing. He has published various research papers in International journals and IEEE international conferences.

Mr. Madhwendra Nath is B.Tech, M.Tech from N.I.T. Jalandhar, Punjab, India. Currently, He is working as an Assistant Professor in Hindu college of Engineering Sonepat, Haryana, India. His area of Interest is Signal Processing and image Biometric Security. He has published various research papers in National, International and IEEE international conferences.

Dr. Sanju Saini is B.Tech.., M.Tech. & PhD in Electrical Engineering. Currently, She is Assistant Professor in Deenbandhu Chhoturam University of Science and Technology Murthal, Sonepat ,Haryana, India. His area of interest is Control Syatem, Chaos based Nonlinear Dynamic System and Artificial Neural Networks. She has published more than 30 research papers in various reputed National and International journals and conferences. She has guided Dissertation of more than 20 M.Tech. Students

Dr. Kamalesh Kumar Saini is B.E., M.Tech. & PhD in Electronics & Communication Engineering. Currently, He is Director-Principal of Hindu College of Engineering Sonepat, Haryana, India. His area of interest is Optical Communication, Chaos Communication, Satellite Communication and Reliability Engineering. He has published more than 500 research papers in various reputed National and International journals and conferences. He has guided Dissertation of more than 100 M.Tech. students and 7 Ph.D. scholars. For more detail kindly visit the website www.drkksaini.com.