IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

Hetnet Security Solution for Black Hole Attack In Millimeter Range Mobile Communication

D.V. Chikhale[1*], S.B. Deosarkar[2]

[1] Electronics and Telecommunication, Lokmanya Tilak College of Engineering, Navi Mumbai, India
[2] Electronics and Telecommunication, Dr. Babasaheb Ambedkar Technological University, Lonere, India

[*]*Corresponding Author: devidas.chikhale@gmail.com, Tel.: 9967081541*

Available online at: www.ijcseonline.org

Accepted: 06/Jun/2018, Published: 30/Jun/2018

***Abstract*—** In the world of network security, hetnet security is upcoming task in the era of evolution of fifth generation around 2020. The mobile device usage to handle cellular data which needs high level of security is increasing day by day.This data is used for various applications in different fields extensively, hence the attacks in an attempt to break security breach is also increasing. It is essential to provide security for network formed by small cells like picocell, femtocell and microcell. This paper deals with one of the approach to provide security to heterogeneous network from black hole kind of attack based on performance evolution using simulation of various network parameters in matlab to provide end to end authentication and security. The security to femtocell or picocell in hetnet not only help to send data at high speed in millimeter range but also increase coverage, capacity and efficiency of the network and reduce power requirement up to the greater extent. The heterogeneous network security solution focuses on how data level and network level security can be achieved by improving hetnet parameters to reduce the level of security breach and to achieve desired security.

Keywords— HetNet, Communication node, Attacks, Routing Protocol, Security

Nomenclature:-- SOLSR: Secured Open Link State Protocol, MPR: Main Primary Route, TTL: Time to Live Field. HetNet: Heterogeneous Network RSA: Rivest-Shamir-Adleman, asymmetric cryptographic algorithim. IoT: Internet of Things, M2M: Machine to Machine, WILL-ALWAYS: Field

I. Introduction

When macrocell is divided into microcell, picocell and femtocell, that network of small cells is called heterogeneous network. Initially transmission power requirement was very large because of usuage of only macro cell network. Now as cell is divided into small size and use of relays made communication faster with increased data handling capacity in 4G which will enhance the data rate [1]. It is supported by huge spectrum of millimeter wave technology in multipoint communication.The data and network security became very crucial as users and data demand is increasing exponentially. The security solution must take into consideration type of attack, level of security required based on security strength, available security mechanism, practicability and interoperability of available security mechanism. This is because wireless channel is highly insecure due to its time varying nature. Various types of attacks are possible on mobile network in the interest of modify, steal, replay, spoof and eavesdrop important and confidential data [15]. Black hole kind of attack is one good example of it. End to end communication security in millimeter range is vital from black hole type of attack for high speed, reliable, secure communication for maintaining confidentiality, integrity, and authenticity of the data which is need of applications like IoT, M2M communication in fifth generation. Secure optimum link state routing protocol is implemented to improve the network performance.Secured and shortest path is found by analysis of transgression of intermediate node before forwarding the packets. Compared with other approaches communication overheads are reduced and other parameters like packet detection ratio, packet delivery ratio are also improved than two hop acknowledgement, watchdog and other methods [5].

The rest of the paper is organized as follows. Related work information is explained in section II. Methodology or proposed algorithim is explained in section III. Results and related discussion is done in section IV.Concluding remarks are given in section V.

II. Related Work

In computer networks, end to end secure communication can be achieved by routing data from one node to another node

by finding best shortest path using algorithms like Dijkstra's and routing tables are updated accordingly. Link state protocol maintains routing table, topology table and neighbor table. Network performance for implemented security protocol can be tested using various network parameters against attacks like Black Hole. Same analogy is used in the existing paper for mobile network of small cells that is HetNet to route data to base station from mobile device through various relay nodes and vice-versa.Network parameters are improved in the implemented protocol SOLSR solution, when compared with the results in the computer network [5]. These are shown in figures of result and in tabular form.

III. Methodology

When two nodes want to communicate, it is possible that packet or message may get dropped, intercepted, modified, replay when transmitted by eavesdropper. Performance evaluation is done based on active and proactive approach [3]. Here data is encrypted as well as decrypted. Public and private keys are generated for a session by secured link state routing protocol. Private keys are used for signing and decryption while public keys are used for verification and decryption. Best path is found between source and destination using routing algorithim like Dijkstra's and after then data is send from source node to destination node through various intermediate nodes and routed to the base station. Secured link state routing protocol developed and implemented as one of the security solution in the heterogeneous network. Various parameters are simulated in matlab and their performance is compared with existing simulation results for improvement in security [5]. Proposed protocol is derived from mobile adhoc networks. Neighbor nodes and possible link failures are determined to choose best path between source and destination. Neighbour discovery route information, and neighbor table updated accordingly. Each node advertises link state packet for routing table or route updation. In our approach we have number of packets received, packet delivery ratio, average delay, and communication overhead like parameters which are analyzed with or without attack. While broadcasting information to nodes, fields used are packet type identifier, address of broadcasting node, IP address, time to live field(TTL) value for increment and decreament of counter after response when it is greater than zero, zone radius, link state matrix, sequence number, certification, which is done by certification authority, timestamp, expiry of certificate, signature and encryption key, verification and decryption key,source address, destination address, neighbor id, insert time, and route metrics. In mobile adhoc network nodes are arranged without strict top down administration. Each node within routing zone advertises link state packet. First key is acquired then encryption is done. Packet validity is verified and decryption is done before extraction. Then data is transmitted. In black hole attack, request is received, response is spoofed, destination address, sequence number is set to high value, and hop counter is set to small value. Intermediate node sends response to source.Source node updates routing table and uses new route. When intercepted, data will be dropped by black hole node. New path nodes between source and destination unable to communicate because of intermediate node attack is called black hole attack.The black hole node prepares 'HI' message in which the field willingness is set to 'WILL_ ALWAYS' from the black hole node X. The source node S selects X as Main Primary Route (MPR) and updates its routing table accordingly. In order to reach destination node D, packet must pass through X acting as intermediate node which will drop them. In cooperative black hole attack if node S asks X_2 which is the next hop of X_1 and if it is the valid route to the destination node D we can say X_2 is cooperating with X_1. Its further response will be positive. Consequently the source node S assumes that the route (S: X1: X2) are secure and starts sending packets through this unsecure route. Once intercepted, packet will be dropped by X1. The type of attack is called cooperative black hole attack. [5].

IV. Results and Discussion

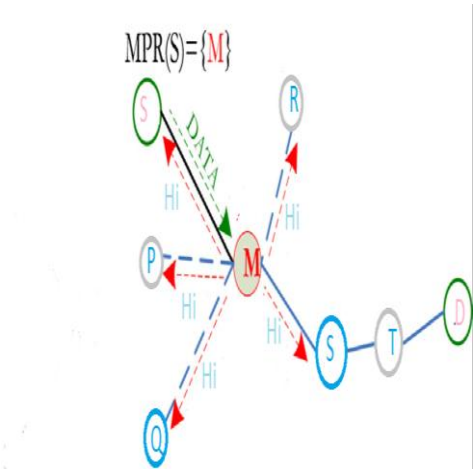


Figure 1. *Black hole attack* [5]

From figure1, among various routes, path chosen from source node S through node M-S-T as a main primary route to destination node D for data represented by word 'Hi.' Neighbour discovery packet helps to find neighbour node by sending link state packet. If Packet sent by eavesdropper detected, it will be dropped in the black hole kind of attack.

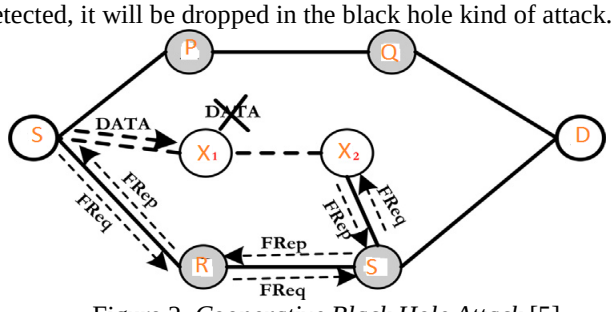


Figure 2. *Cooperative Black Hole Attack* [5]

From figure 2, if route is through S-R-S-D, but X1 in cooperation with X2 receives data as a trusted user for packet as S-X1-X2-S-D. But when detected packet will be dropped as acooperative black hole attack.

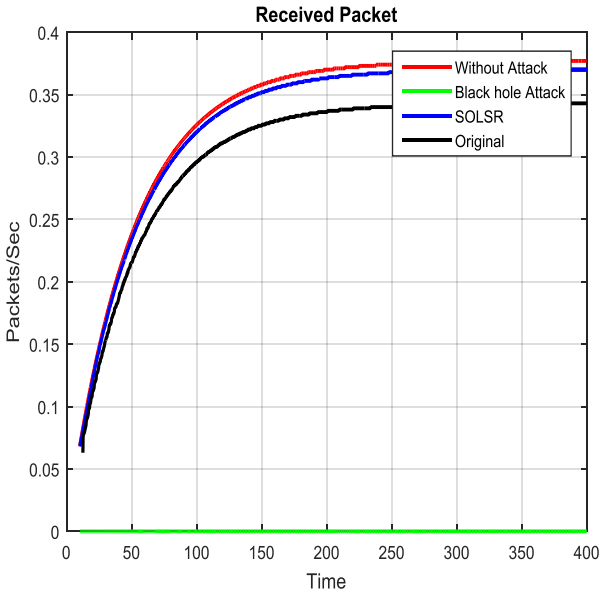


Figure 3. *Plot of Received Packets vs. Time*

It is clear from 'figure 3', when there is attack zero packets are received and received packets are increased at constant rate after certain time period that is 100seconds when original rate is compared with or without attack and using SOLSR.

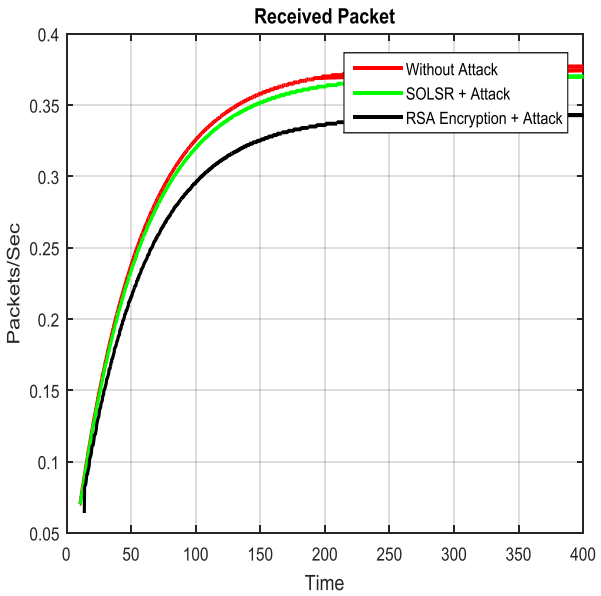


Fig. 4. *Plot of Received Packets vs. Time*

It is clear from 'figure 4' that inspite of attack on data packet encrypted with RSA,received packets are transmitted at constant rate after 100 seconds using SOLSR plus attack and without attack.

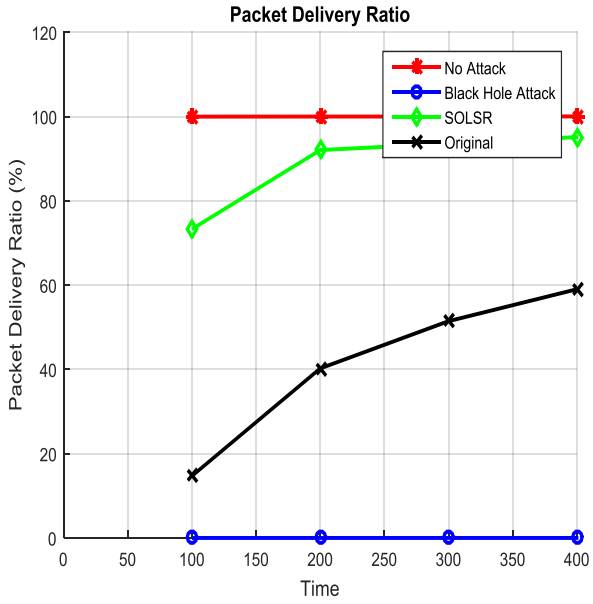


Fig. 5. *Plot of Packet Delivery Ratio vs. Time*

From 'figure 5' packet delivery ratio using SOLSR is more than 96% which is much better than original. While it is 100% when there is no attack. It is zero percent with attack.

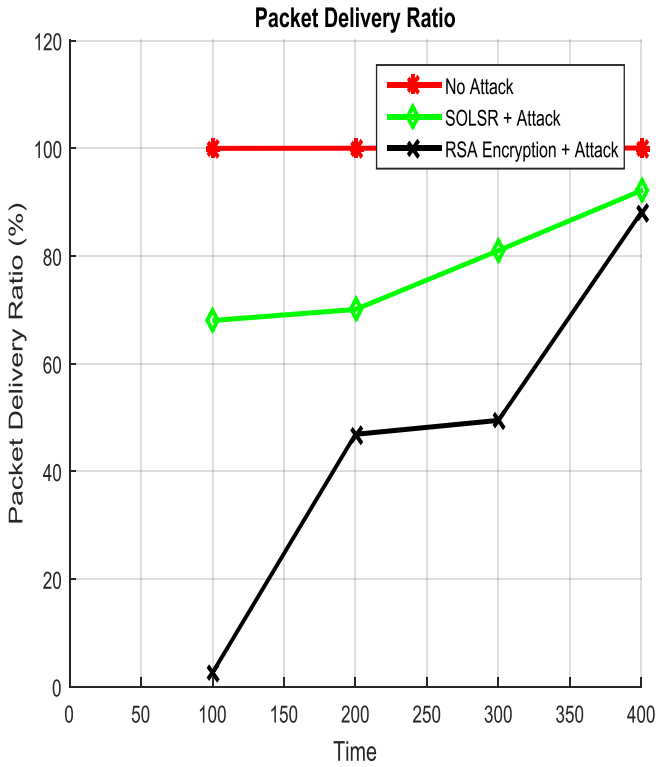


Fig. 6. *Plot of Packet Delivery Ratio vs. Time*

From 'figure 6' packet delivery ratio is above 80% after 300 seconds for SOLSR with attack which is better than RSA encryption plus attack. When no attack is there it is 100%.

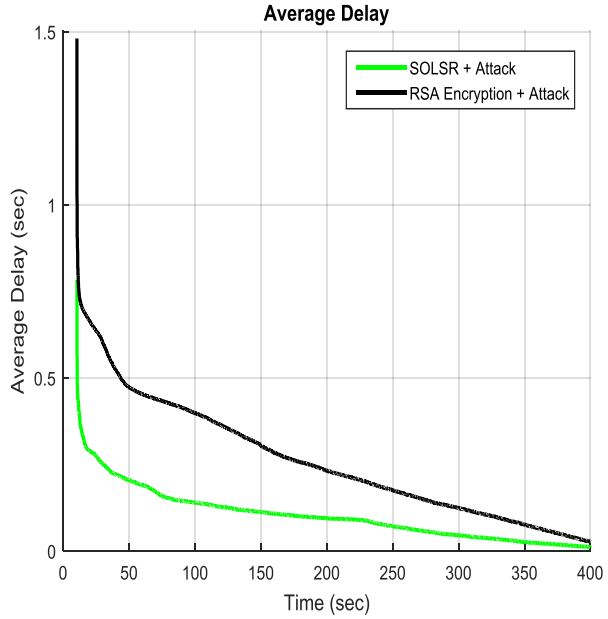


Figure 7. *Plot of Average Delay*

. From 'figure 7' average delay goes on reducing with implementation of optimum link state protocol with attack as compare to original delay with RSA Encryption in presence of attack.

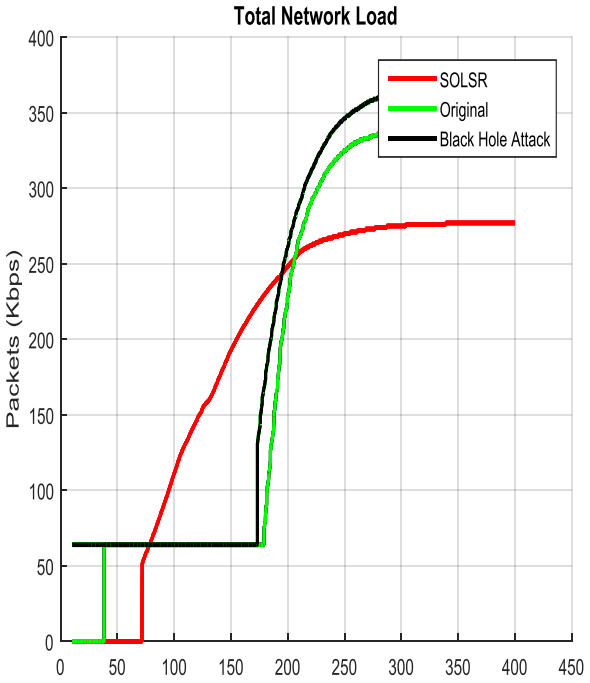


Figure 8. *Plot of Total Network Load*

From 'figure8' it is clear that total network load with implementation of SOLSR is less when compared with original and black hole attack. It is 275 kbps at 250 seconds for SOLSR and 350kbps at 250 seconds.

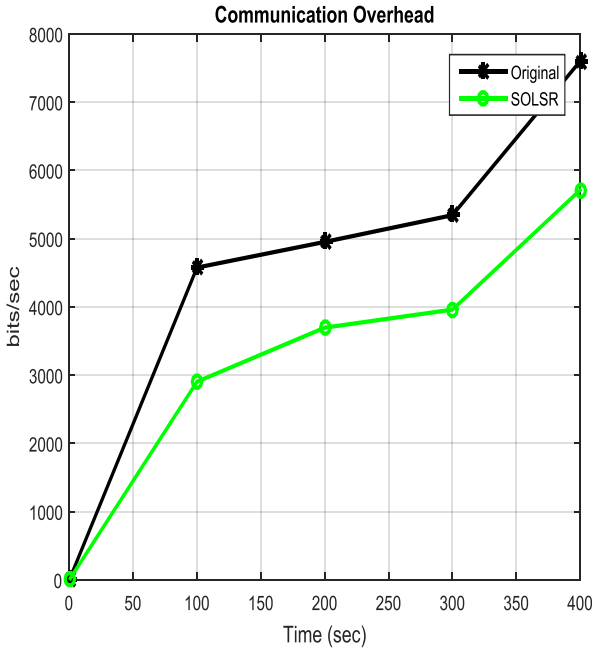


Figure 9. *Plot of Communication Overhead*

From 'figure 9' it is clear that communication overheads are less with implementation of SOLSR than original. It is 5700bits/sec at 400seconds while it is 7800bits per second at 400 seconds originally.

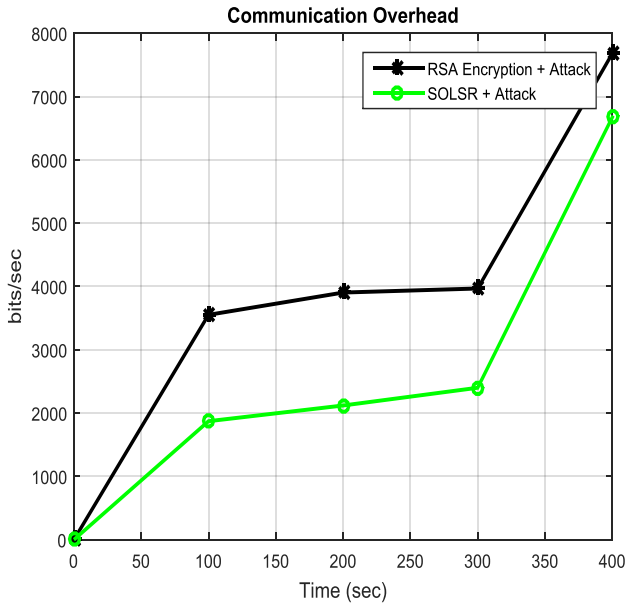


Figure 10. *Plot of Communication Overhead*

From 'figure 10' it is clear that communication overheads are less with implementation of SOLSR with attack than original with RSA Encryption and attack. It is 6800bits/sec at 400 seconds while it is 7800 bits per second at 400 seconds originally with RSA Encryption and attack.

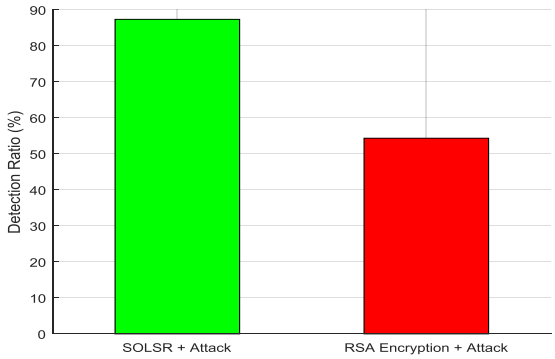


Figure 11. *Histogram Packet Detection Ratio*

From 'figure 11' it is clear that packect detection ratio is 88% with SOLSR in presence of attack while it is 55% with original in presence of RSA Encryption and attack. Table 1 and Table 2 show SOLSR with Attack.

Table -1 Simulation Results

Sr. No.	Time (Seconds)	Received Packet(Seconds)	Packet Delivery Ratio (%)
1	50	0.23	62(not shown)
2	100	0.32	65
3	150	0.35	68
4	200	0.37	70
5	250	0.375	78
6	300	0.38	80
7	350	0.38	85
8	400	0.38	90

Table-2 Simulation Results

Sr. No.	Average Delay	Total Network Load(Kbps)	Communication Overhead (Bits/sec.)	Communication Overhead (bits/sec.)
1	0.2	0	900	900
2	0.1	120	1900	1900
3	0.08	185	2000	2000
4	0.07	250	2100	2100
5	-,0.05	270	2200	2200
6	0.02	280	2300	2300
7	0.01	280	4500	4500
8	0.00	280	6800	6800

V. Conclusion and Future Scope

HetNet security is prime concern in next generation networks which can be achieved in different ways. One of the way which gives optimum security solution when compared with existing solutions is implementation of secured optimum link state routing (SOLSR) protocol. Simulation result obtained for important network parameters gives optimum results in presence of black hole type of attack. When compared with original, communication, overhead bits required are less. In cooperative mode instead of checking all acknowledgements few acknowledgements can be checked to improve packet delivery ratio, reduction of average delay and low network load can be maintained. Authenticated, end to end delay and acknowledgement based approach checks correct forwarding of packets by intermediate nodes. Packet detection ratio is above 85%. Thus security solution using SOLSR in this paper gives one of the optimum security solutions when implemented. Mobile network has to deal with various kinds of attack so it is always challenging to provide data and network security in HetNet. Though various security solutions are available by various information technology and telecom companies in the world and academics still it is open issue for research in next generation networks. In future handoff security task if achieved for Hetnet along with other securities in millimeter range, reliable, ultra high speed, secure, and hundreds of gigabits per second communication is possible in fifth and next generation networks.

Acknowledgment

We are grateful to NILIT research centre affiliated to Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, Lokmanya Tilak College of Engineering Navi Mumbai and Dr. Babasaheb Ambedkar Technological University, Lonere.

References

[1] Rose Hu,Yi Qian,Sastri Kota, Giovanni Giambene, *"Hetnets- a new paradigm for increasing cellular capacity and coverage"* IEEE Journel and Magazine, Vol-18,Issue-3,pp-8-9,June-2011.

[2] Pradeepkumar Sharma, Shivlal Mewada,Pratiksha Nigam,"*Investigation based performance of Black and Gray Hole Attack in Mobile Adhoc Network*" International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue 4, pp.8-11, Sep.-2013.

[3] Leena Pal,Pradeep Sharma,Netram Kaurav,and Shivlal Mewda "*Performance Analysis of Reactive and Proactive Routing Protocols for Mobile Ad-hoc –Networks*", International Journal of Scientific Research in Network Security and Communication, Vol.1, No.5, pp.1-4, Nov. 2013.

[4] Elamathi N, Dr. S. Jayshree, *"Security For Green Communication in Heterogeneous Wireless Networks"* International Journel of Innovative Research in Computer and Communication Engineering, Vol. 2, Jan. 2014.

[5] Abderrahmane Baadache, Alibelmehdi, " *Struggling against simple and cooperative blackhole attacks in multihop wireless adhoc networks"* ScienceDirect Journel of Computer Networks, Vol-73, pp-173-184,November 2014.

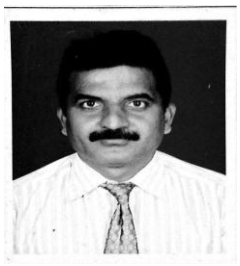
[6] Meenakshi Sharma, GNDE RC Jalandhar, *"Future Trends in the Cell Site Planning For Capacity Enhancement"* International Journel of Engineering Research and Management Technology, Vol. 2, March 2015.

[7] Sumant Kumohapatra, BiswaRanjan Swain, Pravanjan Das, *"Comprehensive Survey of Possible Security Issues on 4G Networks"* International Journal of Network Security and Its Applications, Vol. 7, No.2, March 2015.

[8] Xianbin Wang, Peng Hao, Lajos Hanzo, "*Physical Layer Authentication for Wireless Enhancement: Current Challenges*

and Future Developments", IEEE Journel and Communications Magazine, 2016.
[9] Javed Ahmad Shaheen, *" Wireless Network Architecture an Overview and Security Issues on 4G"* International Journel of Future Green Communication and Networking, Vol. 10, No. 1, pp 15-24, 2017.
[10] Lin C., Lee B., "Exploration of Routing Protocols in Wireless Mesh Network", In the Proceedings of the 2015 IEEE Symposium on Colossal Big Data Analysis and Networking Security, Canada, pp.111-117, 2015.
[11] Muhammad Omer Farooq Cormac J Sreenan and Kenneth N. Brown,*"*Research Challenges in 5G Networks : a Hetnets Perspective*"* International ICIN conference, Paris, March 2016.
[12] Makato Ando, Miao Zhang, Jiro Hirokawa, Kei Saka Guchi, Toru Taniguchi, Makoto Noda, Akira Yamaguchi, *"* Demonstration of mmWave Systems and Networks for the Hetnet in 5G Mobile Communication*"* URSI International Symposium on Electromagnetics Theory (EMTS), 2016.
[13] Hakima Chaouchi, Maryline Laurent-Maknavicius , "Wireless and Mobile Network Security:Security in On the shelf and Emerging Technologies." JohnWiley and Sons Publication, UK, pp. 409-435, 2010.
[14] Kan Zheng, Long Zhao, Jie Mei, Mischa Dohler, Wei xiang, Yuexing Peng, "10Gbs/s, HetsNets with Millimeter-Wave Communications Access and Networking – Challenges and Protocols." IEEE Communications Magazine , Jan. 2015.
[15] Silvere Mavoungou, Georges Kaddoum, Mostafa Taha, Georges Matar, *"* Survey on Threats and Attacks on Mobile Networks*"* IEEE Access, Vol. 4, 2016.

Authors Profile



Mr. D. V. Chikhale pursed Bachelor of Electronics Engineering from University of Kolhapur, India, in 1998 and Master of Electronics and Telecommunication Engineering from Dr. Babasaheb Ambedkar Technological University Lonere, India, in year 2008. He is currently pursuing Ph.D. from Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, India, and currently working in Lokmanya Tilak College of Engineering Navi Mumbai as a Assistant Professor in Department of Electronics and Telecommunication Engineering, University of Mumbai, since 2011. He is a member of IEEE & IEEE antenna and wave propagation society since 2014, and a life member of the ISTE since 2009. He has published more than 10 research papers in reputed international journals recognized by UGC and conferences including Springer and it's also available online. His main research work focuses on Mobile Communication,Wireless Networks, Computer Communication Netwotks, Network Security, Antenna and Wave Propagation and Computational Electromagnetics. He has 19 years of teaching experience.He has done Research Project under the 'Minor Research Grant' by University of Mumbai on topic " Impact of Environmental Parameters on Electromagnetic Signal Propagation" of 01 year duration.

Dr. S. B. Deosarkar pursed Bachelor of Engineering from Shree Sant Gajanan Maharaj College of Engineering, Shegaon, affilitated to Amravati University,India in 1988. He has done Master of Engineering from Sardar Guru Govind Singh(SGGS) College of Engineering and Technology, Nanded, India in 1990. He has completed his ph.D from Swami Ramanand Teerth Marathwada University (SRMTU), Nanded, India, in 2004. He is research guide of Ph.D. and currently working as Professor in Department of Electronics and Telecommunication, Dr. Babasaheb Ambedkar Technological University of Lonere,India. He has more than 30 research papers in his credit in the reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE, Springer and it's also available online. His main research work focuses on Communication and Networking, Network Security, Antenna and Wave propagation, Electromagnetic Interference and Computational Electromagnetics. He has 25 years of teaching experience .

APPENDIX

List of Figures: Pages

