International Journal of Engineering & Technology, 7 (2.8) (2018) 145-148

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Misbehavior detection of nodes in mobile ad-hoc networks using cluster overheads

Rampati Purnasai [1] *, Vasanthadev Suryakala [1], Ramya. T [1], Kolangiammal. S [1]

[1] Department of Electronics and Communication Engineering, SRM University, Chennai, India
**Corresponding author E-mail: purnasai32@gmail.com*

Abstract

In this paper we mainly discuss about the problem of identifying the misbehaving nodes in a multi hop ad-hoc network. Misbehaving nodes identification is done using co-operative incentive based approaches. We are considering a cluster based system for identifying misbehaving nodes in a network. A cluster overhead is selected in each cluster for communicating with other clusters. Proposed system is capable of detecting misbehaving nodes using the cluster formation and also the degradation of network lifetime is decreased when compared to the existing protocol. By selecting the cluster over-head we have marginally reduced the time-delay and packet loss ratio in (network simulator 2) simulation environment. Acknowledgement schemes are used to identify selective packet droppers.

Keywords: *AMD; FMR; LTP; Function Point.*

1. Introduction

Mobile Ad-hoc networks are self-configuring wireless nodes placed randomly in the environment. In mobile ad-hoc networks communication between nodes is done in the form of packets. Successful delivery of packets between the intermediate nodes helps in the completion of transmitting data from sender node to the receiver node. As mobile ad-hoc nodes changes their position with respect to time this causes delay in packet transmission and changes its link to new nodes. Due to this dynamic nature of the nodes route discovery has become difficult and insecure. To resolve this problem various routing and security protocols are been proposed. These routing protocols are of two types proactive and reactive. Among these routing protocols we are considering AODV and DSR routing protocols based on our requirement. TCP/IP protocol is used for communication between nodes.

AMD audit based misbehavior detection protocol is been used for identifying misbehaving nodes in a network. AMD protocol identifies the misbehaving nodes by auditing the nodes present in the network. Auditing of the nodes can be termed as calculating the number of packets transmitted by the transmitting node and the number of packets received by the intermediate nodes. The number of packets received by every intermediate node during the transmission is been calculated. Based on the transmission of more number of packets by an intermediate node to the successive node with less packet loss ratio is identified as a reputed node in that network.

Credit based system is also used in this protocol. Credit based systems are known for providing credits to the nodes for transmitting packets. They will not provide any credit to the malicious nodes in our system.

This helps in reducing malicious nodes in the network. If a node in the network is not responding up to particular time and not forwarding packets then the node is identified as a misbehaving node and no credit is provided. That type of nodes are avoided in the future transmission of packets. Acknowledgement scheme is used for knowing successful reception of packets by the receiver. However AMD fails to detect packet droppers effectively and causes delay for finding the alternative routing path. A security algorithm is also been implemented in the AMD protocol in which encryption of data is done at the transmitter end and decryption is done at the receiver end to avoid the loss of data by the malicious node. Malicious nodes are otherwise categorized as unwanted nodes which are not part of our network joins into our network without our knowing. These nodes maybe included into our network by the attackers seeking information of our network. Implementation of encryption and decryption techniques reduces some malicious nodes entering into our network. There are many encryption and decryption techniques are present among them RSA algorithm is been used in the implementation of audit based misbehavior detection protocol.

2. Misbehaving nodes identification

Audit based misbehavior detection provides misbehaving node identification eliminating those nodes from a certain network. Identification of these nodes can be resolved in the two modules reputation module, route discovery module a) reputation module: It is responsible for computing the reputation of nodes in a network. A decentralized approach is implemented in which each node maintains its own view of reputation of remaining nodes in a network b) route-discovering-module: Malicious nodes with low reputation causes the loss of time and a new routing path has to be detected to avoid this a new routing path with highest number of trust worthy nodes has to be identified.

Incremental intrusion works on the basis of both signature based detection and anomaly detection. It also helps to detect unknown pattern of anomaly. It is assumed that network of sensor nodes are deployed in a network and then passes through the various phases: Cluster formation phase, Cluster head and Function point nomination phase, sensor nodes grouping phase, intrusion detection phase, decision making phase. i) Cluster formation phase: In this approach, sensor nodes are randomly deployed in a network and group of nodes are formed into networks and these group of networks are formed into cluster. ii) Cluster head and Function point nomination phase: In a certain network cluster head identification is done by broadcasting a message to all nodes in a network to respond with their respective energy levels. The node with the highest residual energy within a cluster will be chosen as Cluster Head and the node with second highest energy will be chosen as Function point of the cluster. There can be more than one function point in a cluster iii) Sensor node grouping phase: Within a cluster sensor nodes are grouped. In other case we are forming the pairs of sensor nodes, in that case when a new sensor node is deployed in to a network it cannot be able work without forming a pair with other node sensor nodes very close to each other will form a group. When a group is formed, then an acknowledgment message is sent to the cluster head. Once the cluster head receives all the acknowledgements it identifies the function point which works as an IDS agent within a network. IV) Intrusion Detection Configuration phase: It configures the nodes to detect security threats in a network

a) Key Based Authentication Between Nodes

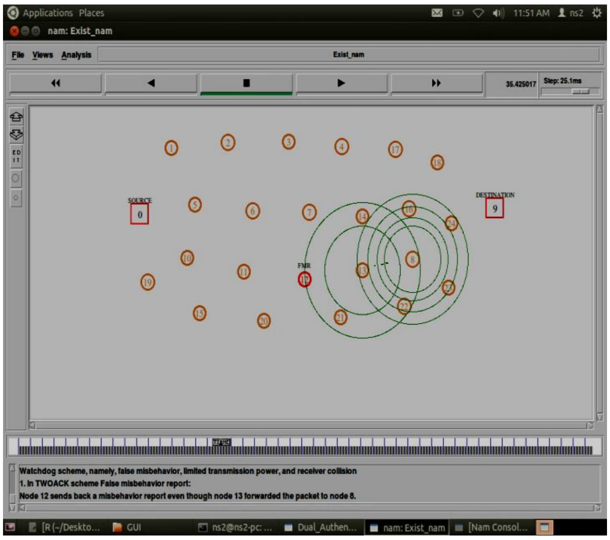
In the proposed protocol we are implementing a key based security system between the nodes in the network. The basic functionality of this key based system is that each message that has to be transmitted by the transmitter to the receiver undergoes encryption and decryption techniques. This encryption and decryption technique is the most commonly used security measure for the nodes. Here in this case we are providing a key based security system by assigning a key for every transmission that occurs in the network. Every individual correct node knows the key to be entered to transmit the packets. If the individual node doesn't know the key and causes mismatch of key then it takes alternative routing path avoiding that node and marks that as a faulty or misbehaving node. This key based system helps in identifying and eliminating the misbehaving nodes more effectively. Each individual node in the cluster or the selected routing path key is shared among them to forward packets without any loss in packets. This also helps in reducing the no of packets lost and helps in reducing the delay time for identifying new path and sending the data securely. In other way we can improve the security by applying authentication for each nodes transmission in that case each node sends a authentication message to the master or the cluster overhead whether to accept the data or not the master should authenticate each node by giving access to participate in the communication process but rather this is a time consuming process and results in increasing the delay time and that leads to the loss of packets increasing with respect to the delay caused. Various new security protocols are also being developed to improve the security of the packets.

b) Proposed Protocol Implementation

The proposed protocol has be designed to overcome the short comes of the existing protocol in such a way that it provides a more reliable secure and safest path by reducing the delay time and reducing the packet loss ratio. The designed protocol provides better results when compared to existing protocols in the following parameters reduced delay time, increased throughput, increased channel frequency, increased source and destination frequencies, and it also provides better results in terms of reduced packet loss ratio and increase in no of packets received at each individual intermediate node and the overall protocol frequency has also been increased. The implementation of the proposed protocol is carried out by considering a group of nodes or a network and we are forming nodes as clusters and we are assigning cluster overheads to cluster based on their energy levels. While considering the cluster overheads each node in the cluster communicates with the remaining nodes in that cluster based on the packets received, frequency of each node and energy levels one node is elected as a cluster overhead and the node with second highest energy level is considered as fraction point. These clusters are dynamic in nature and changes from one place to another with respect to time. After formation of these clusters each cluster in the network communicates with all the other clusters and the status of each node in the network is obtained after the communication of clusters we are identifying the misbehaving nodes, LTP (low transmitting power) nodes, FMR (false misbehavior report authentication) nodes and the nodes capable of transmitting high no of packets are identified.

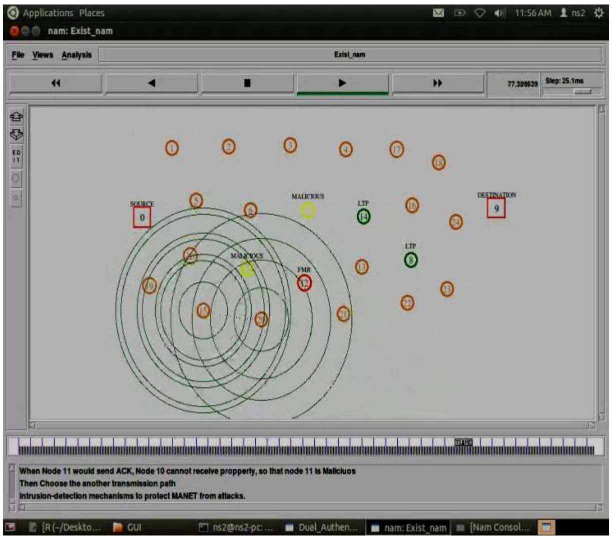
Now we are starting a transmission between the nodes implementing single acknowledgment scheme and starting transmission of packets. In this single acknowledgment scheme firstly the source and destination nodes are identified and packets are being forwarded to the next intermediate trustworthy node while receiving packets from source each intermediate node must provide a key which has been provided by the source before the transmission the nodes capable of providing the key are only allowed to participate in the transmission. In this protocol the intermediate nodes does not prefer shortest path it takes only the longest path to reduce the time delay it is possible because we are selecting the intermediate nodes with high energy levels. Upon successful transmission the destination sends an acknowledgment to the source that it has received the packets successfully. In another case we are considering two-acknowledgment scheme and starting transmission by identifying the source and destination nodes in the two acknowledgment scheme each intermediate node participated in the transmission sends an acknowledgment to the previous node regarding the transmission of packets the source node receives acknowledgments from each and every node participating in the transmission.

3. Experimental results



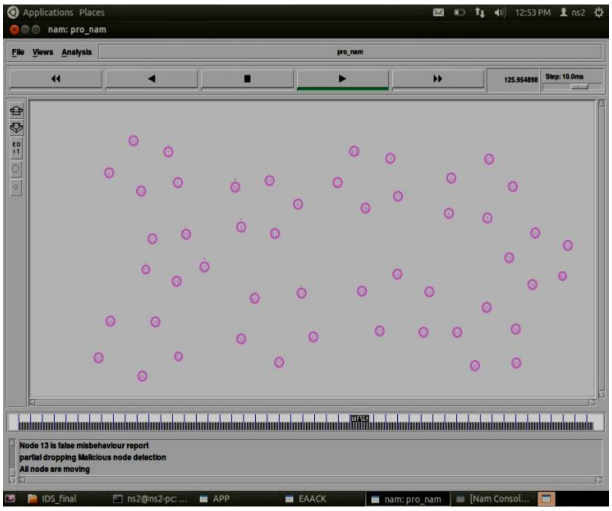
Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision
1. In TWOACK scheme False misbehavior report:
Node 12 sends back a misbehavior report even though node 13 forwarded the packet to node 8.

Fig. 1: Network Formation Considering 20 Nodes and Implementing Audit Based Misbehavior Detection.



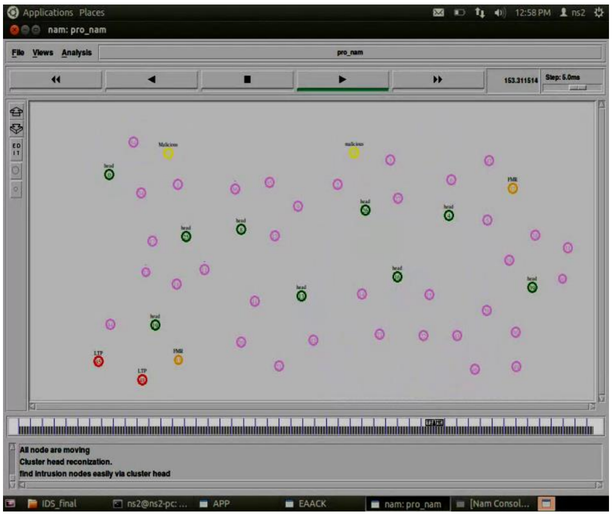
When Node 11 would send ACK, Node 10 cannot receive propperly, so that node 11 is Maliciuos
Then Choose the another transmission path
intrusion-detection mechanisms to protect MANET from attacks.

Fig. 2: Identification of Malicious and Misbehaving Nodes Using AMD.



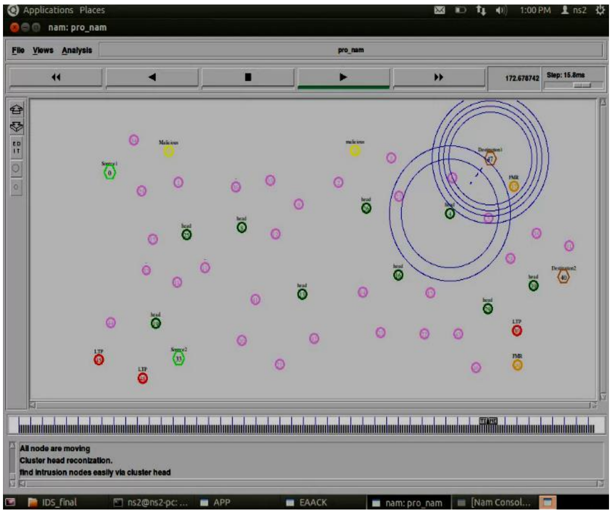
Node 13 is false misbehaviour report
partial dropping Malicious node detection
All node are moving

Fig. 3: Implementation of Proposed Protocol by Forming Clusters



All node are moving
Cluster head reconization.
find intrusion nodes easily via cluster head

Fig. 4: Cluster Overhead Identification and Obtaining Individual Nodes Status.



All node are moving
Cluster head reconization.
find intrusion nodes easily via cluster head

Fig. 5: Implementation of the Proposed Protocol and Transmitting Packets between Source and Destination Using Single Acknowledgment and Two Acknowledgment Schemes.

X-axis- Individual nodes delay time.
Y-axis- Simulation time.

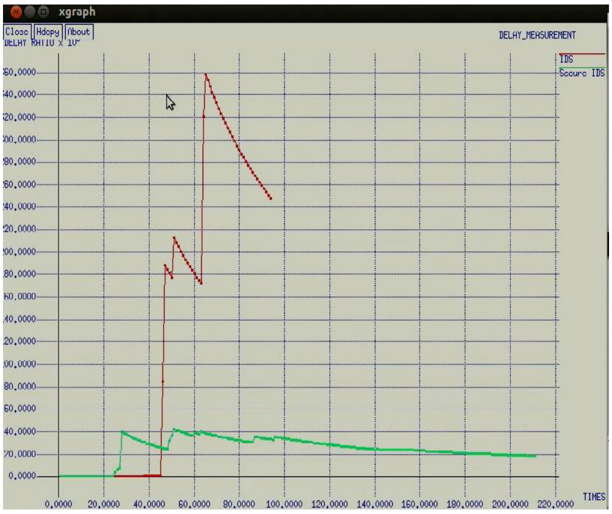


Fig. 6: Comparison in Delay Ratio of Networks with and without Cluster Formation.

X-axis- No of packets.
Y-axis- Simulation time.

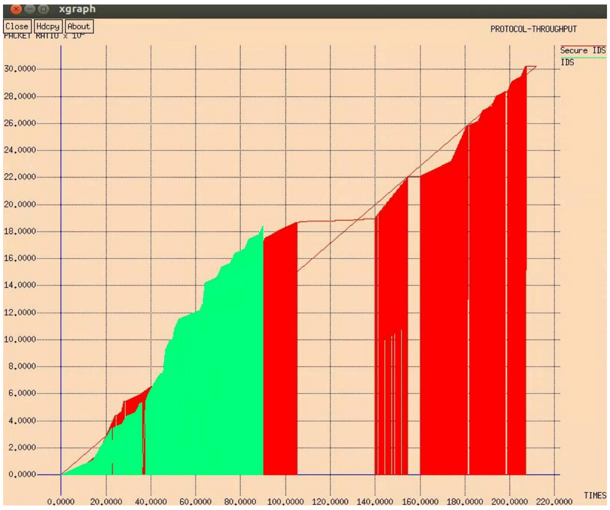


Fig. 7: Comparison in Throughput of Networks with and without Cluster Formation.

X-axis- Frequency of the channel.
Y-axis-Simulation time.

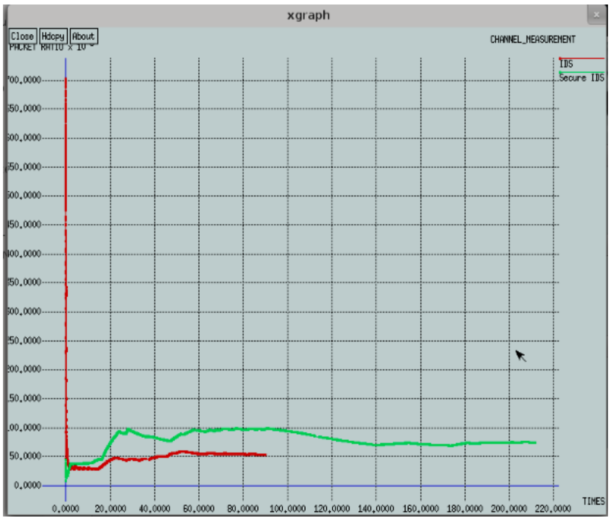


Fig. 8: Comparison in Channel Frequency of Networks with and without Cluster Formation.

X-axis-Frequency at source.
Y-axis-Overall channel frequency.

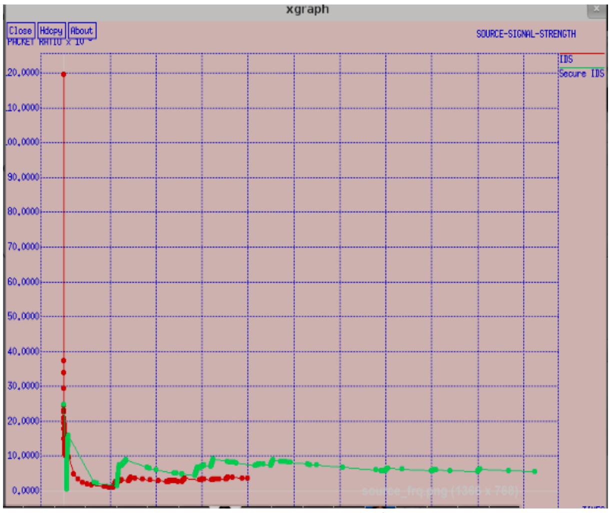


Fig. 9: Comparison in Frequency at Source of Networks with and without Cluster Formation.

X-axis-Frequency at destination.
Y-axis-Overall channel frequency.

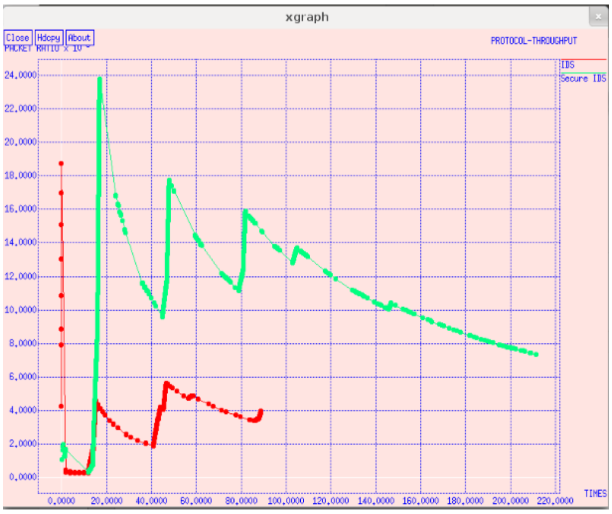


Fig. 10: Comparison in Frequency at Destination of Networks with and without Cluster Formation.

4. Conclusion

In the proposed protocol effectively and more efficiently reduces packet droppers in a network. The malicious nodes detection in the paths between the sender & receiver and basic encryption and decryption are done and shortest path available among optimized paths is done in the form of the cluster. Delay ratio has been reduced. The proposed protocol gives better performance in terms of less packet loss ratio and improved energy level and frequency range and thus increases the network life time. The throughput ratio had been improved after the formation of cluster head in a given network.

Acknowledgment

The authors would like to acknowledge Dr. T. Rama Rao, Head of the Department, Dept. of Electronics and Communication engineering for providing the opportunities and facilities required. The authors are thankful to the Department of Electronics and Communication engineering for giving us an opportunity to do this work and the management of the University and for their Support and help throughout this work. I am grateful to my project guide S chithira for constant support and guidance that helped me to carry out this project successfully.

References

[1] G. Acs, L. Buttyan, and L. Dora, "Misbehaving Router Detection in Link-State Routing for Wireless Mesh Networks," Proc. IEEE Int'l Symp. a World of Wireless, Mobile and Multimedia Networks (WoWMoM '10), pp. 1-6, 2010.

[2] Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens,“ODSBR: An on-demand secure byzantine resilient routing protocol for wireless Ad Hoc networks,” ACM Transactions Information Systems. Security, vol. 10, no. 4, pp. 11–35, 2008.

[3] K. Balakrishnan, J. Deng, and P. K. Varshney, “Twoack: Preventing selfishness in mobile Ad Hoc networks,” in Proc. IEEE Wireless Communication Networks. Conference, 2005, pp. 2137–2142.

[4] S. Buchegger and J.-Y. L. Boudec, “Self-policing mobile Ad-Hoc networks by reputation systems,” IEEE Communications, volume. 43, no. 7, pp. 101–107, Jul. 2005. https://doi.org/10.1109/MCOM.2005.1470831.

[5] J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring, “Modelling incentives for collaboration in mobile Ad Hoc networks,” in Proceedings. Workshop Model. Optimization Mobile Ad Hoc Wireless Networks, 2003, pp. 427–439.

[6] Y. Dong, H. Go, A. Sui, V. Li, L. Hui, and S. Yiu, “Providing distributed certificate authority service in mobile Ad Hoc networks,” in Proc. 1st Int. Conf. Security Privacy Emerging Areas Commun. Netw. 2005, pp. 149–156.

[7] S. Ganeriwal, L. Balzano, and M. Srivastava, “Reputation-based framework for high integrity sensor networks,”ACM Trans. Sensor Netw., vol. 4, no. 3, pp. 1–37, 2008. https://doi.org/10.1145/1362542.1362546.

[8] Q. He, D. Wu, and P. Khosla, “SORI: A secure and objective reputation-based incentive scheme for Ad Hoc networks,” in Proc. IEEE Wireless Commun. Netw. Conf., 2004, pp. 825–830.

[9] W. Kozma and L. Lazos, “Dealing with liars: Misbehavior identification via R#nyi-Ulam games,” in Proc. 5th Int. ICST Conf. Security e Privacy Commun. Netw, 2009, pp. 207–227.

[10] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, “An acknowledgment-based approach for the detection of routing misbehavior in manets,” IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007. https://doi.org/10.1109/TMC.2007.1036.

[11] T. Shu and M. Krunz, “Detection of malicious packet dropping in wireless Ad Hoc networks based on privacy-preserving public auditing, “ in Proc. 5th ACM Conf. Security Privacy Wireless Mobile Netw., 2012, pp. 87–98.

[12] S. Zhong, J. Chen, and Y. R. Yang,”Sprite: A simple cheat-proof, credit-based system for mobile Ad-Hoc networks, “in Proc. 22nd IEEE Annu. Joint Conf. Comput. Commun, 2003, pp. 1987–1997. https://doi.org/10.1109/INFCOM.2003.1209220.

[13] T. Padmapriya and V.Saminadan, “Handoff Decision for Multi-user Multiclass Traffic in MIMO-LTE-A Networks”, 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016) – Elsevier - PROCEDIA OF COMPUTER SCIENCE, vol. 92, pp: 410-417, August 2016. https://doi.org/10.1016/j.procs.2016.07.364.

[14] S.V.Manikanthan and V.Rama“Optimal Performance of Key Predistribution Protocol In Wireless Sensor Networks” International Innovative Research Journal of Engineering and Technology, ISSN NO: 2456-1983, Vol-2, Issue –Special –March 2017.

[15] Meka Bharadwaj, Hari Kishore "Enhanced Launch-Off-Capture Testing Using BIST Designs" Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.12, Issue No.3, page: 636-643, April 2017.