*IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*
*e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 12, Issue 4, Ver. II (Jul.-Aug. 2017), PP 07-12*
*www.iosrjournals.org*

# Improving the Efficiency of the Network Attack Detection Using Global Inspector

*Adarsh D. Mamidpelliwar[1], Vijay G. Roy[2], Sunil Kuntawar[3]
[1](Electronics and Communication Eng. /Gondwana University, India)
[2](Electronics and Communication Eng. /Gondwana University, India)
[3](Electronics and Communication Eng. /Gondwana University, India)
Corresponding Author: Adarsh D. Mamidpelliwar*

***Abstract :*** *The wireless communication has experienced phenomenal growth over the past decades, especially in the areas of mobile ad-hoc network (MANET) and in wireless sensor network (WSN). WSN is broadly used in the field of environmental monitoring, industrial process monitoring and tactical systems. So, the security and the efficiency of the network are the major concern in the wireless communication. The attack occurs during interaction between the trading peers as a transaction takes place. In this paper we develop an energy efficient and secure scheme against malicious attacks. For that we create a powerful method called as global inspector (GI) and powers are given to that. So it can identify malicious node by verifying trust of the node. Transmission should be through GI only, without GI communication between source to destination will not take place. The experiments were simulated using ns-2.*

***Keywords:*** *GI, Malicious Node, MANET, NS-2, Wireless Communication, WSN.*

---

Date of Submission: 12-07-2017 Date of acceptance: 24-07-2017

---

## I. Introduction

Wireless Sensor Networks (WSNs) consist of small sensor nodes working together to monitor and obtain data about an environment. Sensor nodes have limited resources in terms of energy, computation, storage, transmission range and available bandwidth. They are typically deployed in a remote or hostile location and are left unattended to perform monitoring and reporting tasks as in [6]. Therefore, limited resources of nodes need to be utilized efficiently in order to prolong network lifetime and obtain better throughput. These networks have been successfully deployed in a wide range of applications such as military surveillance, health care and environmental monitoring is few to mention. Most WSNs are deployed for mission-critical tasks for an unspecified duration of time. Therefore, security considerations need to be in place at the time of network design. The resource-constrained nature of these networks coupled with their unique characteristics, such as dynamic topology, in-network processing, error-prone communication links and scalability makes security provisioning challenging and complicated. In addition, these networks are left unattended without human intervention and base station supervision. Instead, sensor-collected data is harvested intermittently by a base station. Since the information is retained on individual sensors, securing this information is both important and challenging. Sensor nodes operating in unattended environments face a higher risk of security breaches. If any one of these nodes is compromised, its sensitive data and security parameters will be retrieved by an adversary to participate in malicious activities. When a malicious node uses multiple identities or claims fake IDs, the WSN suffers from an attack called Sybil attack. The node replicates itself to make many copies to confuse and collapse the network. The system can attack internally or externally. External attacks can be prevented by authentication but not the internal attacks. There should be one to one mapping system between source to destination in WSN.

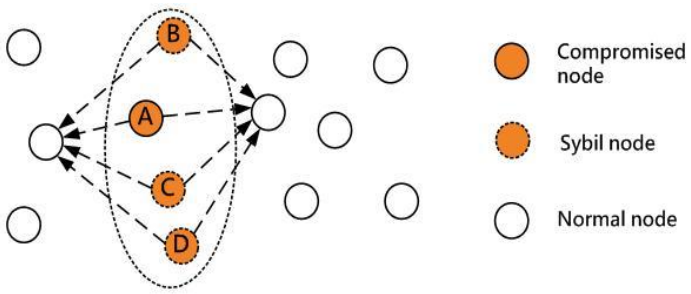


**Fig.1** Sybil attack in WSN

Authentication is a very crucial security requirement in WSNs, as sensor nodes are often deployed in unattended environment and thereby vulnerable to attacks. Authentication ensures a receiver that data, mobile code or control data such as route updates, location information and key management messages originate from the correct source. If a strong authentication mechanism is not included, then an adversary can often spoof others identity, generate fake data packets and force sensor node to relay those packets, draining their energy. A pretend message will cause device nodes to simply accept and transfer wrong info that successively makes device nodes susceptible to numerous attacks. Different authentication problems stem from the kind of node deployment. Just in case of a static deployment, the nodes never move. Such nodes are vulnerable to replay attacks and node capture, as the nodes are easily traceable as in [7]. On the other hand, in case of a dynamic deployment, issues such as re-authentication of mobile nodes, intractability of nodes movement and message integrity may arise. To secure the communication over WSN, we want an authentication technique which might make sure that unauthorized nodes cannot be a part of the network also as they cannot transmit any information over the network.

## II. Literature Survey

In this section we review the previous methods used for securing the data and detecting the attacks in the network, A paper published as in [10] by Prof. mukund joshi and renuka karkade had discussed about network security and cryptography concept to protect network and data transmission over wireless networks for that they used various cryptography techniques to increase the security of the network. However this technique can protect data for low level attacks because there are many computational algorithms are available to decrypt that data. In [14] Authors proposed a method for improving reliability against security attacks by identifying reliance node in MANET. For that they used monitor based intrusion detection technique for monitoring packets transmission. If any node found as harmful node then with the help of reliance node, source will avoid transmission of packets through that node and create the alternate path to reach its destination. Hence this technique provides reliable and efficient data transmission. In [4] Authors proposed a survey on solution to Sybil attacks. They presented the overview of work related to analyzing or solving the Sybil attacks, in which one entity appears as or control many different identities. The attacks additionally presents drawback for peer-to-peer network, mobile network. By showing kind of solutions we are able to limit or forestall the attacks in many individual application domains. A paper revealed as in [16] by T. Yao, S. Fukunaga and T. Nakai had mentioned regarding Reliable broadcast message authentication in wireless sensor networks. They projected an authentication protocol for broadcasting messages exploitation a method key chain and secure acknowledgements. But the drawback is there is no sync of time and whole broadcasting would be disrupted with single malicious node because of unknowing key chain.

## III. Proposed Methodology

Practically network attack prevention is not that simple. One of the ways in which of preventing the attack is by having a central Authority, like an administrator who acts as a certifying authority. Administrator will guarantee that every person contains a single identity. But in practice, this is very difficult to ensure on a large scale and would require costly manual attention. Many algorithms on detecting and defending such attack other than having a central authority have been proposed. In this paper a new method called Global Inspector (GI) has been proposed and authenticate node Trust. This approach is expected to give better performance for controlling the attacks. For node verification issue AODV protocol is used instead of AOMDV because transaction should be carry out by path detected by GI only. The flow chart for the network attack detection using global inspector as shown below,

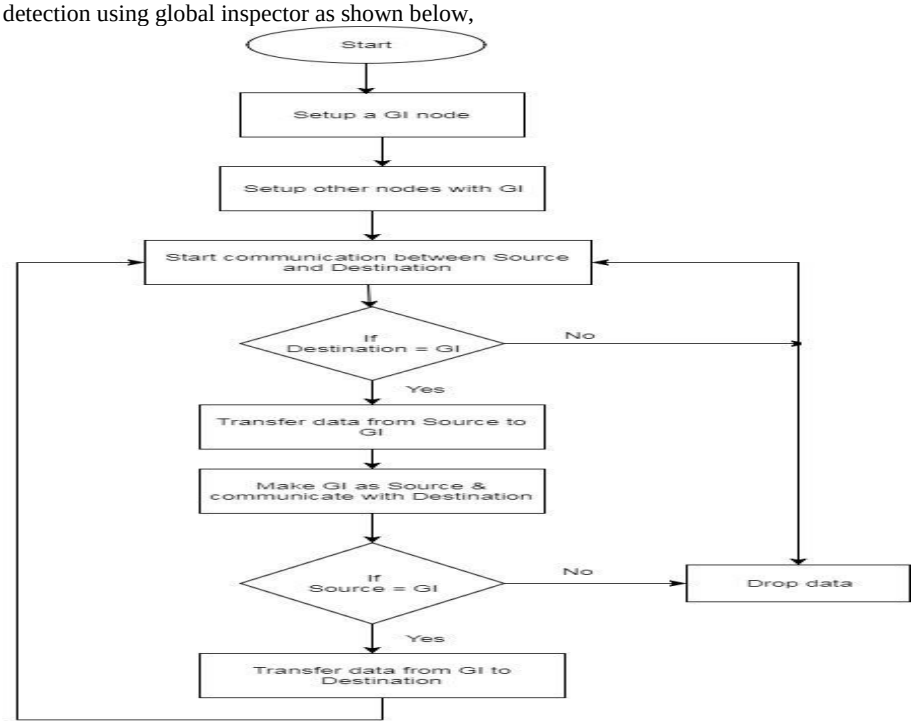


**Fig.2** The flow chart for the network attack detection using global inspector

In this paper the new scheme is proposed to provide network security between Source and destination. The scheme is based on the GI- Global Inspector. In the proposed scheme, after forming the network, Packets from the source to destination is transmitted through Global inspector and untrusted communication will detected by the system. For that we used neighbor table base mechanism, we defined single and multiple GI and it will verify the nodes which we will register during the operation and it will check that the coming packet is from trusted node or not if the communication without GI takes place it will detect, in multiple GI the source and destination will communicate through nearest GI for better routing. The global inspector is responsible for examine whether the packet is eavesdrop or not by the adversary. If the message is eavesdrop then it will get detected otherwise global inspector will pass it ahead. At the destination node, it will be checked if the packet has come from the trusted node i.e. global inspector.

## IV. Simulation Result

The network simulator covers a really sizable amount of applications of various kinds of protocols of various network varieties consisting of various network parts and traffic models. Network simulator is a package of tools that simulates behavior of networks such as creating network topologies, log events that happen under any load, analyze the events and understand the network. Platform required running network simulator UNIX and UNIX like systems Linux (Use Fedora or Ubuntu versions) Free BSD SunOS/Solaris Windows 2000/XP Backend Environment. In this section, the performance is analyzed by comparing single GI and multiple GI in the group by taking mean values of different parameters for different node values. The result of comparison is analyzed by throughput, energy, delay, attack detection and jitter as shown in Figure 3, Figure 4, Figure 5, Figure 6 and Figure 7 respectively.

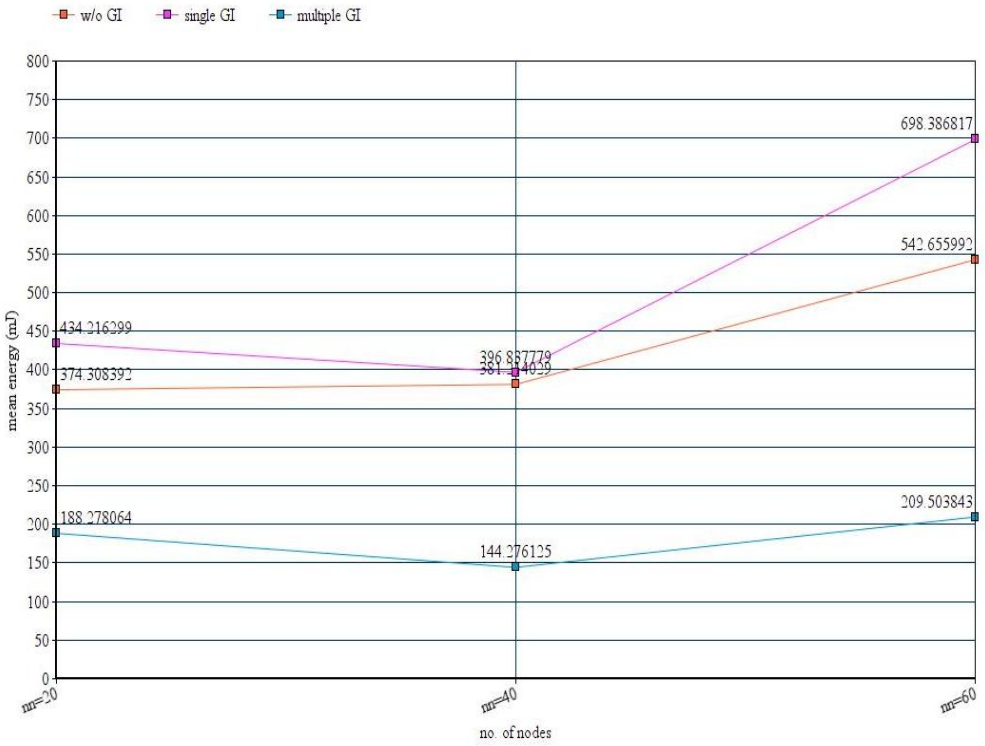


**Fig.3** The graph of mean energy

The Fig.3 shows energy consumption in m-Joules for a given network when the number of nodes is varied within the network. As the nodes multiplied within the given network, energy consumed also will increase. X- Axis represents range of nodes and y- axis represents mean energy consumption. The graph show that the energy consumption of network having 20 nodes, 40 nodes, 60 nodes, when there is only one GI in the network then energy consumption is higher than energy consumption when there is multiple GI in the network.

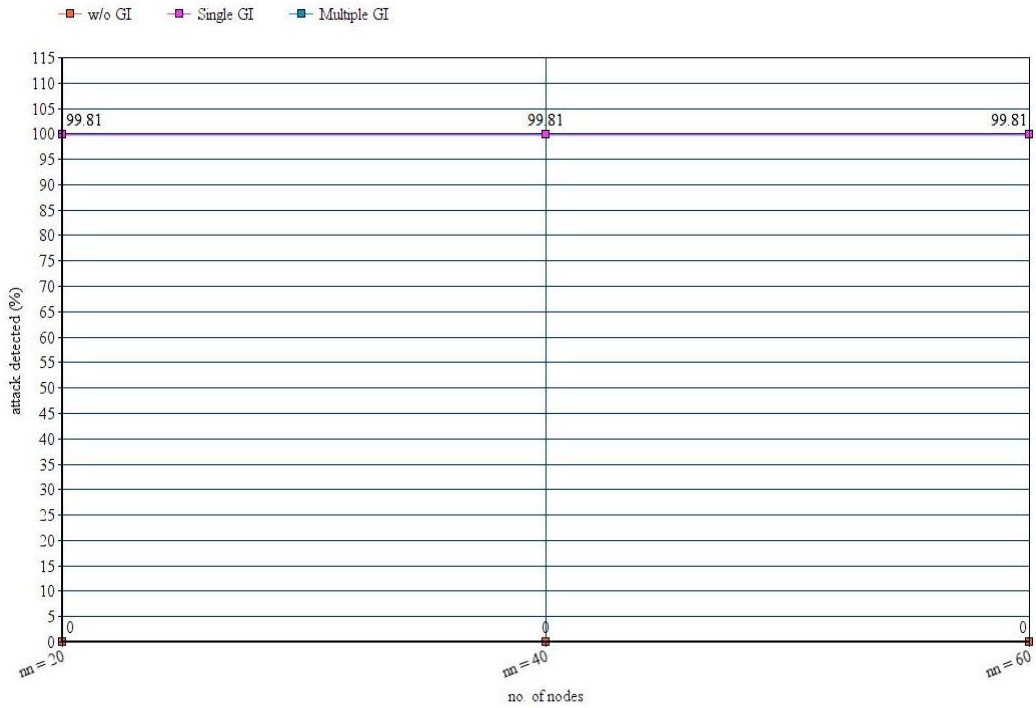


**Fig.4** The graph of network attack detected by GI for fixed no. of malicious node

The Fig.4 shows attack detected by the GI in % for a given wireless sensor network. It shows result for fixed no. of malicious attack removed in both time, detection rate can vary if we set random attack communication in the network but still the detection rate is very high. X- Axis represents number of nodes and y- axis represents attack detected. The graph shows the attack detection for network having 20 nodes, 40 nodes, 60 nodes. It shows that when there is no GI is activated in the network then attack is not detected and as GI is activated then the attack will be detected in the network.

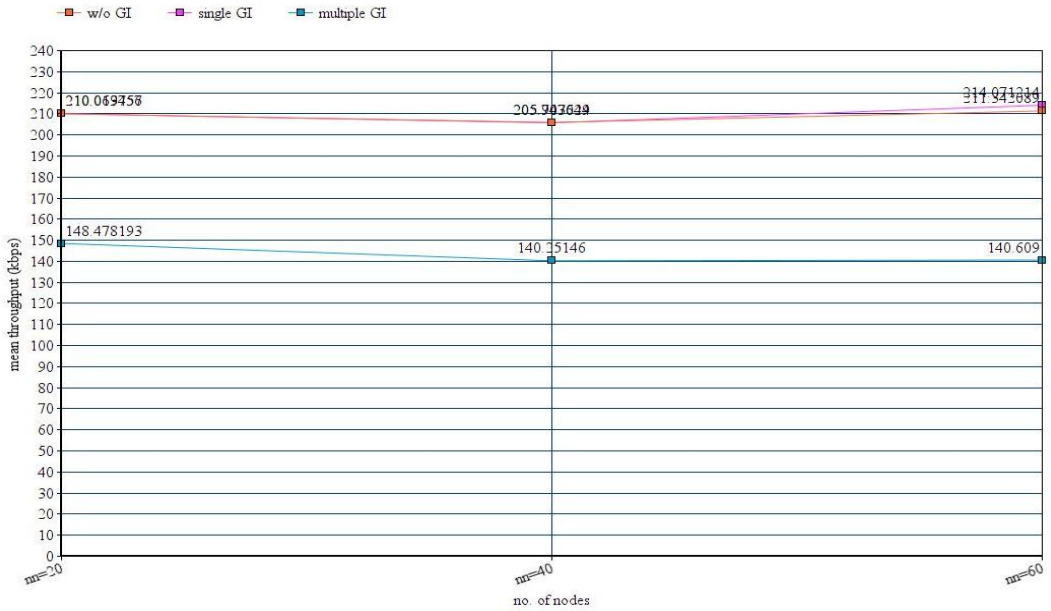


**Fig.5** The graph of mean throughput

In Fig.5 X- Axis represents number of nodes and y- axis represents mean throughput. As throughput measure the transmission efficiency in terms of successfully delivered packets in unit time for a specified channel bandwidth. The above graph shows the result by comparing single GI and multiple GI. The graph interprets that result of single GI better than that of multiple GI, because in the multiple GI overhead is increased which slows things down.

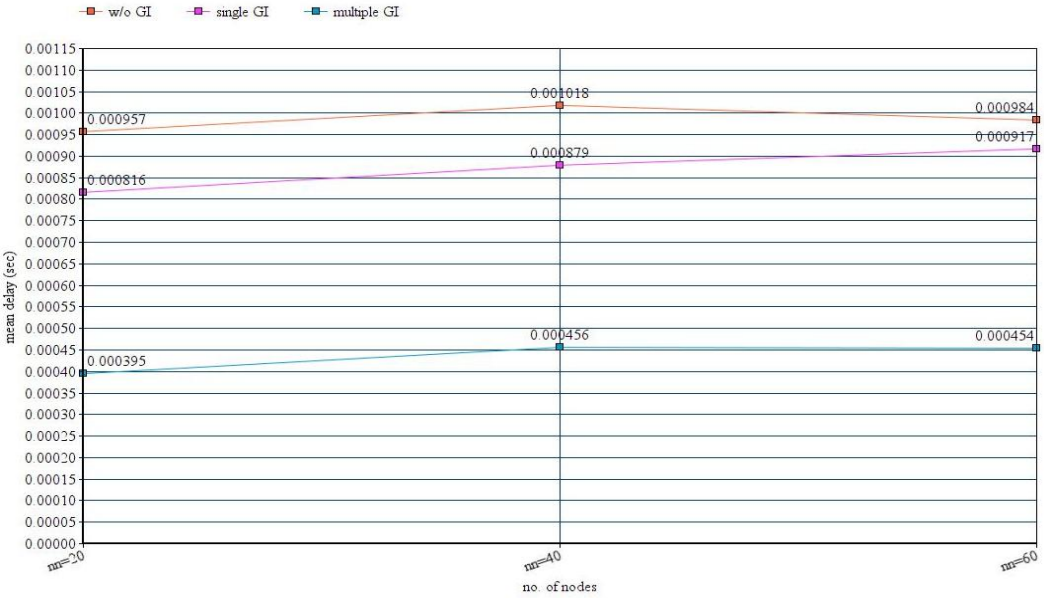


**Fig.6** The graph of mean delay

In Fig.6 X-axis denotes number of nodes and Y-axis denotes mean delay. The graph shows mean delay in network by comparing single GI and multiple GI. As shown in Fig.6 the delay of multiple GI is lower than single GI.

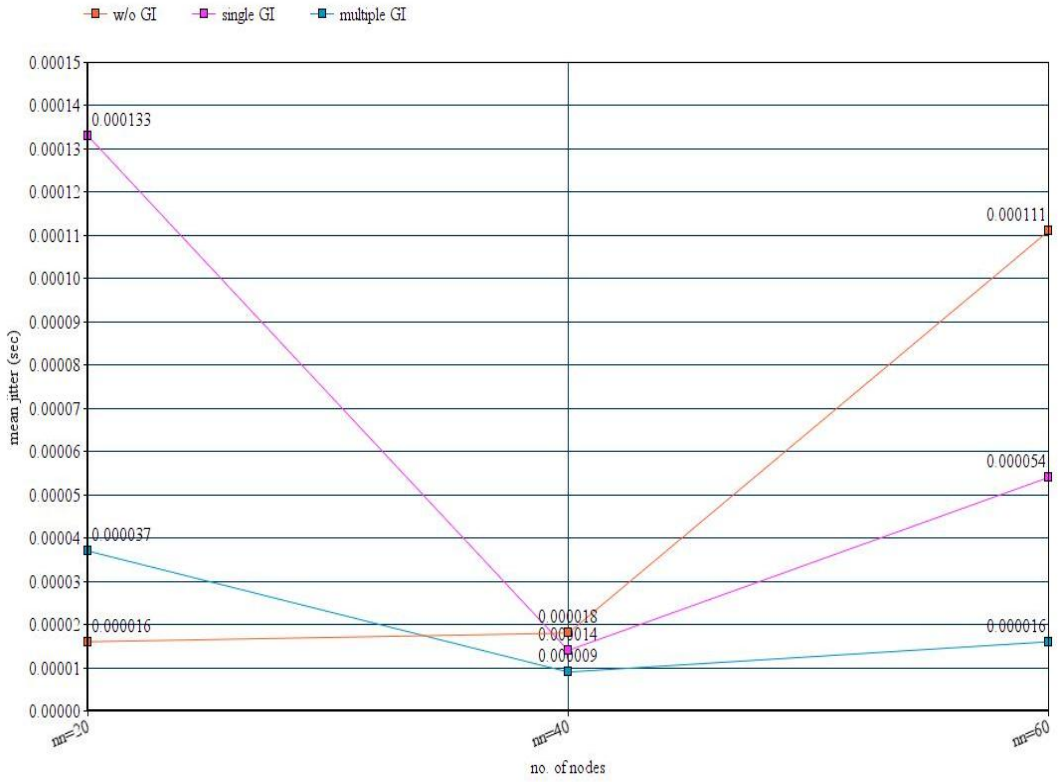


**Fig.7** The graph of mean jitter

In Fig.7 X-Axis represents no. of nodes and Y-Axis represents mean Jitter in sec. As shown in graph the jitter of multiple GI is lower than that of single GI. Thus from all these output graph we tend to conclude that the network having multiple GI perform so well than single GI.

## V. Conclusion

A number of existing methodologies for the detection of attacks have been studied and algorithms were proposed for the same in the wireless sensor network. In this paper we are introducing Global Inspector (GI) which acts as a network pass through and helps in authentication and proper communication. We have run the simulation for comparing single GI and Multiple GI in the network and also analyzed its result. It is found that the output is improved sufficiently in many factors by using multiple GI in the network.

## Acknowledgements

This research was supported by publisher of this paper. We thank our colleagues from Ballarpur institute of technology who provided expertise that greatly assisted the research. Also, for sharing their pearls of wisdom with us during the course of this paper.

## References

[1] A. Perrig, R. Szewczyk, J. Tygar, V. Wen and D. Culler, "SPINS: Security Protocols for Sensor Networks," Wireless Networks, Volume 8, Issue 5, pp. 521-534, 2002.
[2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Ad Hoc Networks, Volume 1, Issue 2-3, pp. 293-315, 2003.
[3] A. Abduvaliev, S. Lee and Y.-K. Lee, "Simple hash based message authentication scheme for wireless sensor networks," in 9th International Symposium on Communications and Information Technology, ISCIT 2009, Icheon, South Korea, 2009.
[4] Technical Report of Univ of Massachussets Amherst 2006–052: BN LevineC. ShieldsBN Margolin2006A survey of solutions to the sybil attack.Technical Report of Univ of Massachussets Amherst2006–052.
[5] N. Sastry and D. Wagner, "Security considerations for IEEE 802.15.4 networks," in Proceedings of the 2004 ACM workshop on Wireless security - WiSe '04, Philadelphia, PA, USA, 2004.
[6] I. Akyildiz, W. Su and E. Cayirci, "Wireless sensor networks: a survey," Computer Networks, pp. 393-422, 2002.
[7] W. Dargie and C. Poellabauer, Fundamentals of Wireless Sensor Networks: Theory and Practice, West Sussex, United Kingdom: John Wiley & Sons Ltd., 2010.
[8] J. Deng, R. Han, and S. Mishra, "Enhancing Base Station Security in Wireless Sensor Networks," Department of Computer Science, University of Colorado, Tech. Report CU-CS-951-03, 2003.
[9] J. N. Al-Karaki and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks:a survey," IEEE Wireless Communications, Volume 11, Issue 6, pp. 6-28, December 2004.
[10] Mukund R, Joshi J, Karkade RA. Network security with cryptography. IJCSMC. 2015; 4(1):201–04.
[11] Y. Zou, J. Zhu, X. Wang, and V. Leung, Improving physical-layer security in wireless communications through diversity techniques, IEEE Network, vol. 29, no. 1, pp. 42-48, Jan. 2015.
[12] Tuomas Aura , Pekka Nikander , Jussipekka Leiwo, DOS-Resistant Authentication with Client Puzzles, Revised Papers from the 8th International Workshop on Security Protocols, p.170-177, April 03-05, 2000.
[13] M. E. Hellman, "An Overview of Public Key Cryptography," IEEE Commun. Mag., vol. 16, no. 6, May 2002, pp. 42–49.
[14] G. Arulkumaran and R. K. Gnanamurthy, "Improving Reliability against Security Attacks by Identifying Reliance Node in MANET," Journal of Advances in Computer Networks, Vol. 2, No. 2, June 2014.
[15] J. Golbeck, B. Parsia, and J. Hendler, "Trust networks on the semantic web," Cooperative Information Agents VII, pp. 238–249, 2003.
[16] Taketsugu Yao, Shigeru Fukunaga and Toshihisa Nakai, "Reliable Broadcast Authentication in Wireless Sensor networks", LNCS, vol.4097, pages 271-280, 2006.
[17] J. Dinger and H. Hartenstein, "Defending the sybil attack in p2p networks: Taxonomy, challenges, and a proposal for selfregistration," in ARES '06: Proceedings of the First IEEE International Conference on Availability, Reliability and Security, 2006.
[18] Guojun Wang, Felix Musau, Song Guo, Muhammad Bashir Abdullahi" Neighbor Similarity Trust against Sybil Attack in P2P E-Commerce" in Proc. IEEE Transactiom on Paralle and Distributed Systems, VOL. 26, NO. 3 MARCH 2015.

IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) is UGC approved Journal with Sl. No. 5016, Journal no. 49082.

Adarsh D. Mamidpelliwar. "Improving the Efficiency of the Network Attack Detection Using Global Inspector." IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) 12.4 (2017): 07-12.