iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** II **Month of publication:** February 2022

DOI: https://doi.org/10.22214/ijraset.2022.40349

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue II Feb 2022- Available at www.ijraset.com

Online Health Care System: A Survey

Nijhum Mohapatra[1], Dr. Bhuvana J[2]

[1]*Student, Department of Master of Computer Applications School of Computer Science IT, Jain Deemed to Be University, Jayanagar 9th Block, Bengaluru, Karnataka– 560041, India.*

[2]*MCA Coordinator, Department of Master of Computer Applications School of Computer Science & IT, Jain Deemed to Be University, Jayanagar 9th Block, Bengaluru, Karnataka– 560041, India.*

Abstract: Today`s technology offers many online services in almost every field. From those fields Healthcare is one of them. However, in this pandemic it is very difficult to obtain the consultation with the doctor for every health problem so to overcome this problem Online Healthcare System can be implemented. This Web application contains features like manage patient details, doctor`s detail, schedule appointments, view reports, online payment and some additional features like videos for "yoga and exercise" and a "Chatbot", Which is a type of software that used to redirect the conversation between human beings and users which will help people to provide details according to their quires in an productive way.

I. INTRODUCTION

Online Healthcare System is a way of obtaining medical care for the problem with minimum hospital visits. It gives us advantages like booking Appointments, consulting a doctor, viewing test report right from the comfort of our homes without actually going to the hospital. Online Healthcare system provides us with an option for different users using the website like Patients, Doctors, Administrator, Pathologist, Pharmacist, etc. As a Patient we can get solution from looking for a doctor for treatment to booking appointment for getting a check-up, viewing reports of the tests performed, getting consultation of doctors about the report and present health status, booking medicines according to the prescription suggested by the doctor and also getting yoga, exercise suggestions from the doctors. Once registered the patients can get benefits of all this function from anywhere anytime from any device that they login. As, a doctor this project helps them to keep a record off their patients with all their medical details and their current status with their reports and prescription. As a administrator user, they will be able to manage doctors, patients data along with all other data like appointment, pathologist, etc. As a pathologist, they can login, see the test request, upload the test reports after completion of tests. As a pharmacist they can view prescription about medicines request, ships with the necessary medicines to the patients. Another feature of this project is chatbot integration which provide instant 24*7 solution to all the queries that the users of the website have regarding any process. The last module is physical activity where a patient gets access to videos and other content according to their doctor's recommendations and practice it. makes them exposed enough to be attacked by any attacker deploying more resources than any individual node or base station, which may not be a difficult job for the attacker. A typical sensor network may be comprised of potentially hundreds of nodes which may use broadcast or multicast transmission. The broadcast nature of the transmission medium is the reason why wireless sensor networks are susceptible to security attacks.

II. RELATED WORKS

A variety of literature is available related to intrusion detection in wireless sensor networks for selective packet dropping, wormhole, and Sybil attacks. A few of the related work is discussed below.

The paper entitled "The Sybil Attack in Sensor Networks: Analysis & defences" presents systematically analyses the threat posed by the Sybil attack to wireless sensor networks. Authors demonstrate that the attack can be exceedingly detrimental to many important functions of the sensor network such as routing, resource allocation, misbehaviour detection, etc. authors establish a classification of different types of the Sybil attack, which enables to better understand the threats posed by each type, and better design countermeasures against each type. Author then propose several novel techniques to defend against the Sybil attack, and analyses their effectiveness quantitatively [10].

The sensor networks are especially susceptible to attacks is because of their specialized communication pattern. Since all packets share a similar ultimate destination (in networks with just a single base station), a compromised node needs just to give a single brilliant route to the base station so as to influence a potentially large number of nodes. In WSN, nodes have particular properties, for example, stable neighbor's information that aides in detection of anomalies in network. Nodes monitor their neighbourhood and collaborate with cluster head to detect malicious conduct.

©IJRASET: All Rights are Reserved

Despite the fact that nodes don't have worldwide view however they can in any case detect an intrusion with certain probability and report to cluster head. This paper introduces a specification based Intrusion Detection System for wireless sensor networks. The proposed scheme tries to optimize the local (information collected by watch dogs) into worldwide information (decision taken by cluster head) so as to compensate the communication pattern in network [11].

The paper entitled "Survey On Selective Forwarding Attack in Wireless Sensor Networks", have discussed about selective forwarding attack, its types and some countermeasure schemes. Author concludes that Secure and on time transmission of packets is the basic need in wireless sensor network. One of the attacks that violate this need is Selective Forwarding attack. In this attack, a malicious node is dropping packets which make information unavailable. They have discussed some of the mitigation schemes to defend this attack and had given analysis on every scheme. This analysis will help us to know the drawbacks in the previous schemes and may helpful to overcome the drawbacks in the future [12].

The paper entitled "A Comparison of Link Layer Attacks on
Wireless Sensor Networks", focus on security of WSNs, divide it (the WSNs security) into four categories and consider them, include: an overview of WSNs, security in WSNs, the threat model on WSNs, a wide variety of WSNs' link layer attacks and a comparison of them. The work by authors enables to identify the purpose and capabilities of the attackers; furthermore, the goal and effects of the link layer attacks on WSNs are introduced. Also, the paper discusses known approaches of security detection and defensive mechanisms against the link layer attacks; this would enable IT security managers to manage the link layer attacks of WSNs more effectively [13].

The paper entitled "Prevention of wormhole attack in wireless sensor network" investigate the techniques dealing with wormhole attacks and an approach for wormhole prevention is proposed. The approach proposed in the paper makes RREP packet forwarding conditional. By checking the validity of the two-hop neighbour node that has forwarded the packet, a node lets it to move further towards the source. Wormhole end is detected when the identity of the two-hop neighbour is found illegal. Authenticity checking of such two-hop neighbours is carried out using a preloaded secret key. By comparing the memory requirement for various numbers of neighbours, it can be concluded that by spending more on setup cost, higher scalability can be achieved. The proposed scheme focuses on the type of wormhole with out-of-band channel. It can be extended to detect other types of wormhole attacks also. [14].

The proposed in this paper that proposed in this paper wormhole is a sort of attack in Wireless Sensor Network (WSN) that needs not to crack encryption key, which has awesome harm. Aiming at characteristics of Wormhole attack, the paper presented a sort of wormhole attack defence strategy of WSN in light of neighbour nodes verification. Under this strategy, when every normal node received control packet, it will monitor the packet to figure out if it originates from its normal neighbour nodes to avoid Wormhole attack effectively. Modelling and simulation of WSN in view of OMNeT++ shows that the AODV added neighbour nodes verification effectively implement effective defence. Wormhole needs not to crack encryption key, which has extraordinary harm. Mature security protocol in traditional wired and wireless ad hoc networks can't be copied to WSN, so it needs to research on various sorts of unique potential security attack form in WSN and their defence strategies. Aiming at characteristics of Wormhole attack, the paper presented a sort of wormhole attack defence strategy of WSN in view of neighbour nodes verification. Under this strategy, when every normal node received control packet, it will monitor the packet to figure out if it originates from its normal neighbour nodes to avoid Wormhole attack effectively. Modelling and simulation of WSN in view of OMNeT++ shows that the AODV added neighbour nodes verification effectively implement effective defence [15].

The paper entitled "Detection of Packet Droppers in Wireless Sensor Networks Using Node Categorization Algorithm" proposes a simple yet effective scheme to catch packet droppers. In this scheme, a Tree on DAG (ToD) structure rooted at the sink is first established. When sensor data is transmitted along the tree structure towards the sink node, each packet sender or forwarder adds a small number of extra bits, which is called packet marks to the packet. Based on the packet marks, the sink node can figure out the dropping ratio associated with every sensor node, and then runs authors proposed node categorization algorithm to identify nodes that are packet droppers for sure, suspicious packet droppers, or no packet droppers. Proposed scheme has the following features: (i) being effective in detecting the dropping packets, (ii) low communication and energy overheads, (iii) being compatible with existing false packet filtering schemes. Extensive simulation on ns2 simulator is conducted to verify the effectiveness [16].

Wireless Sensor Network (WSN) is vulnerable to various types of security attacks where the attackers could undoubtedly intrude into the network and could bring about inexplicable destruction by disrupting the expected functionalities of the network. Severe seepage of battery may happen because of the attacks and as a result, the lifetime of the network may decrease drastically. In this paper, an energyeffective integrated Intrusion Detection System (IDS) is proposed to identify network layer Sybil attack. Our scheme spots out accurately and purges out the Sybil node which may falsely act as a genuine node.

The experimental results demonstrate that the critical factor in WSN, energy is conserved more proficiently by the proposed scheme than the existing alternative methods. Likewise, accurate detection of the malicious node is conceivable spending relatively less energy. The reduction in energy consumption for the networksetup confirms to be extremely significant for WSN. The proposed approach comes extremely convenient even with densely deployed networks. In this work, detecting the presence of a solitary malicious node in the network is essentially focused. The idea could likewise assist in detecting colluding nodes in the network [17].

Wireless Sensor Network (WSN) is an emerging technology that offers awesome guarantee for various applications. The sensing capabilities combined with relatively small processing power and wireless communication makes it one of the fundamental technologies to be exploited in the future. Despite its attractive features, WSN is vulnerable to various security attacks. The constraints of WSN, for example, limited energy and memory make the security problem considerably more critical. One of the security issues of WSN is it is susceptible to Sybil attack. In this attack, the adversary forges multiple entities to disrupt the whole network. This paper addresses the problem by developing a lightweight trust system utilizing energy as a metric parameter for a hierarchical WSN. The performance evaluation of this system shows efficiency and scalability for detecting Sybil attacks in terms of true and false positive detection in a heterogeneous WSN. Besides, this system reduces the communication overhead in the network by scratching off feedback and recommendations among sensor nodes (SNs) [18].

The paper has proposed various intrusion detection systems to detect various types of active attacks on wireless sensor networks (WSNs). Selective forwarding and delay attacks are two straightforward yet compelling attacks that can disrupt the communication in WSNs. We propose two parameterized collaborative intrusion detection systems and optimize their parameters for given situations utilizing extensive simulations and multi-objective evolutionary calculations. Besides, we test the whole pursuit space to enable evaluation of evolution performance. We assess the influence of changes of the quantity of malicious nodes on the intrusion detection performance. The approach where we can choose from a set of non-dominated solutions based on current WSN application, security and different requirements anytime after the advancement process can be effortlessly adjusted to practical applications. In any case, the streamlining ought to be performed on a deliberately configured simulator with an accurate model of target WSN. Both detection methods can be effectively combined into single IDS recognizing selective forwarding and delay attacks [19].

III. PROBLEM FORMULATION

The wireless sensor networks are the self-configuring network in which sensor nodes sense the environmental conditions and pass the sensed information to base station. The size of the sensor nodes is very small due to which its battery is also very limited. In the recent times, various techniques have been proposed to reduce energy consumption of the network. Among the proposed techniques LEACH is the most efficient protocol for data aggregation. The modification is required to increase security of the LEACH protocol. Due to less security of the existing LEACH protocol the various types of attacks are possible which reduce the network performance in terms of various parameters. In this work, improvement in the LEACH protocol will be proposed to detect and isolate these attacks in the network.

IV. PROPOSED SCHEME

In this work, we are working on three network layer attacks. These selective packets dropping, Sybil and wormhole attacks which greatly affects the network performance in terms of battery consumption, throughput and delay. The novel framework had been proposed through which these three attacks can be isolated from the networks. This framework will work on the wireless sensor networks. The basic assumption for the framework is that all the sensor nodes are static and location based clustering will be done in the network. The second assumption is that the cluster head will chosen using LEACH protocol and all the information sensor nodes which are within the cluster head are stored on Cluster head. The stored information is node id and distance from the cluster head in meters.

The proposed framework will first test the network for hello flood attack. The distance of each sensor node from cluster head is stored on cluster head. The new equation will be proposed through which distance between cluster head and sensor node will be calculated, if any node passing wrong distance information will be detected as malicious node. When whole network pass the hello attack test, the test is to detect malicious node which will be responsible for Sybil attack. I assume that all the nodes are registered to its cluster head and cluster heads maintain a registration table. The sink maintains the registration table to every cluster head and correspond their sensor nodes. The authentication mechanism will be proposed to verify the identity of the sensor nodes at cluster heads and cluster heads identity at sink node. The wormhole attack is the attack which increase delay in the network. To detect nodes which are responsible for triggering wormhole attack are detected with the watchdog technique. The figure 3.1 shows the flow diagram of research methodology carried out.

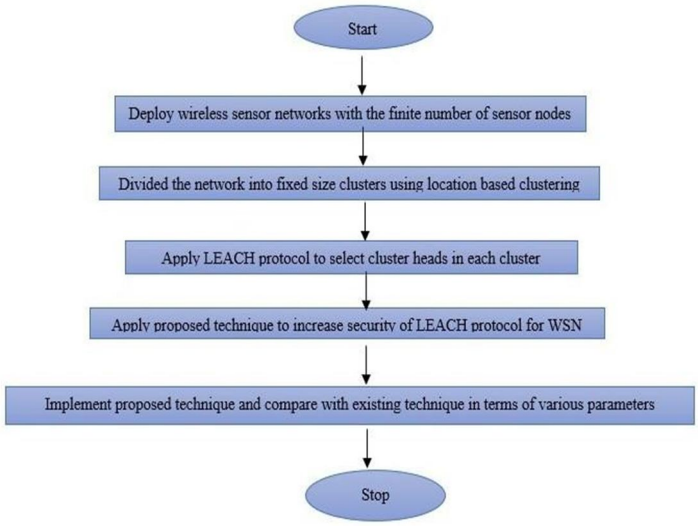


Figure 3.1: Flow diagram

V. CONCLUSION

In this paper, the sensor networks are particularly susceptible to attacks is due to their specialized communication pattern. Since all packets share the same ultimate destination (in networks with only one base station), a compromised node needs only to provide a single high-quality route to the base station in order to influence a potentially large number of nodes.

we defined the Sybil attack and establish a taxonomy of this attack by distinguishing different attack types. The definition and taxonomy are very important in understanding and analysing the threat and defences of a Sybil attack. We present several novel methods by which a node can verify whether other identities are Sybil identities, including radio resource testing, key validation for random key redistribution, position verification and Registration. The most promising method among these is the random key pre-distribution which associates a node's keys with its identity. Random key predistribution will be used in many scenarios for secure communication, and because it relies on well understood cryptographic principles it is easier to analyse than other methods.

These methods are robust to compromised nodes. We have shown that in the multi-space pair wise scheme with each node storing 200 keys, the attacker would need to compromise 400 nodes before having even a 5% chance of being able to fabricate new identities for the Sybil attack.

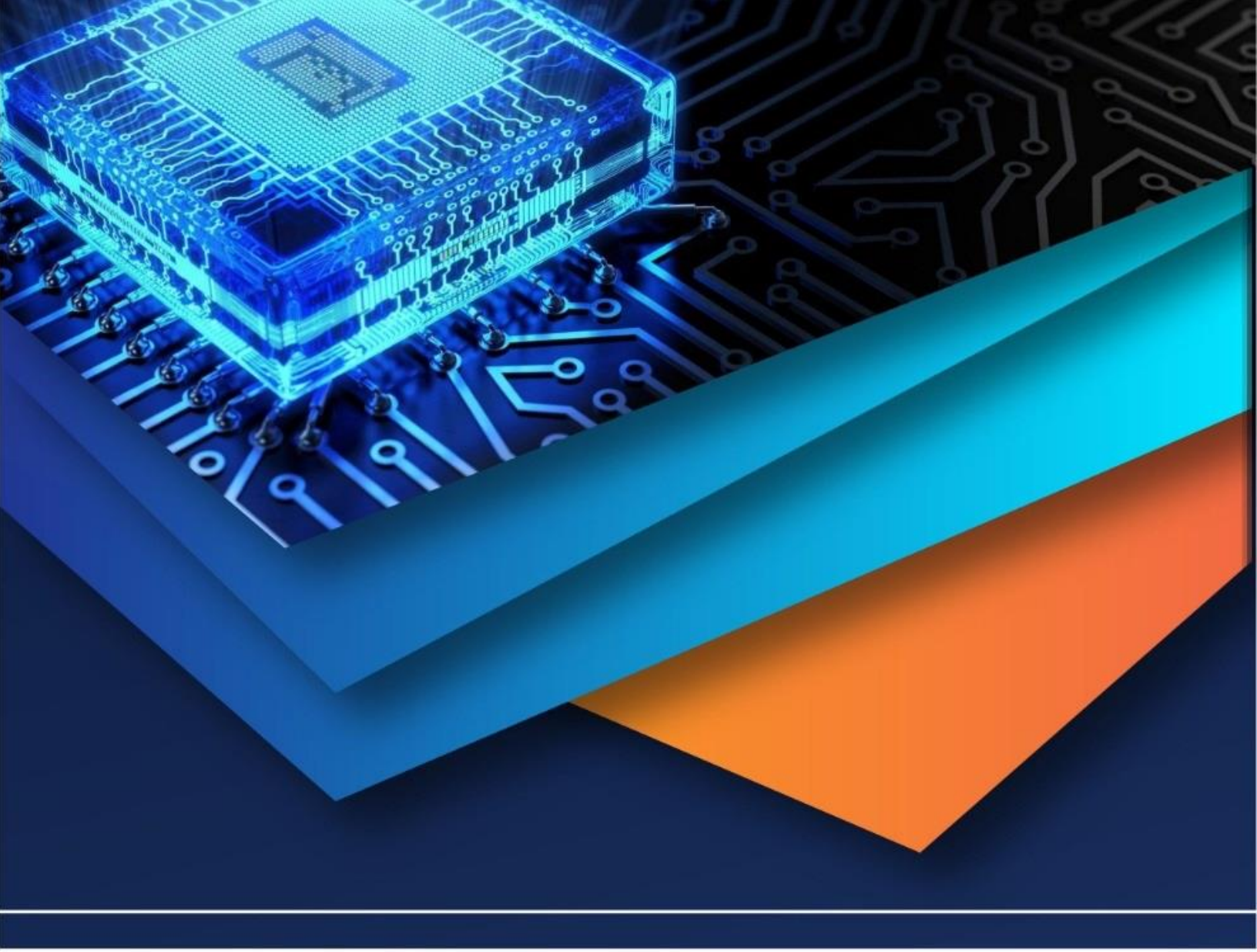
LEACH is a MAC protocol, it contains many advantages like it does not need any control information, it saves energy.

REFERENCES

[1] Winnie Louis Lee, Amitava Datta, and Rachel Cardell-Oliver “Network Management in Wireless Sensor Networks,” 2010, School of Computer Science & Software Engineering, The University of Western Australia.
[2] Ray Hunt, Network Security: The Principles of Threats, Attacks and Intrusions, part1 and part 2, APRICOT, 2004.
[3] Su-Chiu Yang, Flow-based Flooding Detection System, APRICOT,2004.
[4] Chu-Fu Wang, jau-Der Shih, Bo-Han Pan and Tin-Yu Wu, “A Network Lifetime Enhancement method for Sink Relocation and Its Analysis in Wireless sensor Networks”, 2014, IEEE Sensors Journal, Vol. 14, No. 6, 1932 - 1943.
[5] WU Xiaoping, LIN Hong and Li Gang “An Improved Routing Algorithm Based On LEACH Protocol”, 2010, Ninth International Symposium, IEEE, 259- 262.
[6] Maciej Nikodem and Bartosz Wojciechowski, “Upper Bounds on Network Lifetime for Clustered Wireless Sensor Networks”, 2011, 4th IFPI International Conference, IEEE, 1-6.
[7] Chi-Tsun Cheng, Chi K. Tse, and Francis C. M. Lau, “A Delay- Aware Data Collection Network Structure for Wireless Sensor Networks”, 2011, IEEE Sensor Journals, Vol. 11, No. 2., 699-710.
[8] Zijan Wang, and EyuphanBulut, “Energy Efficient Collision Aware Multipath Routing for Wireless Sensor Networks”, 2009, International Conference on Communications, IEEE, 1-5.
[9] Aashima Singla and Ratika Sachdeva “Review on Security Issues and Attacks in Wireless Sensor
[10] Networks,” 2013, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, ISSN: 2277 128X. Research Paper available online at: www.ijarcsse.com
[11] James Newsome, Elaine Shi, Dawn Song, and Adrian Perrig “The Sybil Attack in Sensor Networks: Analysis &Defenses,”2004, IPSN’04, April 26–27, Berkeley, California, USA.
[12] Mukesh Tiwari, Karm Veer Arya, Rahul Choudhari, Kumar Sidharth Choudhary,” Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information”, 2009 Fourth International Conference on Computer Sciences and Convergence Information Technology

[13] Leela Krishna Bysani and Ashok Kumar Turuk "A Survey On Selective Forwarding Attack in Wireless Sensor Networks," 2011, International conference on Devices and Communications, 24-25 February, Mesra, India. 978-1-4244-9190-2/11 ©2011 IEEE
[14] Shahriar Mohammad, Reza Ebrahimi Atani, and Hossein Jadidoleslamy "A Comparison of Link Layer Attacks on Wireless Sensor Networks," 2011, Journal of Information Security, 2, 69-84 doi:10.4236/jis.2011 .22007 Published Online April 2011 (http://www.scirp.org/journal/jis). [14] Dhara Buch and DeveshJinwala "Prevention of wormhole attack in wireless sensor network," 2011, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5
[15] Jin Guo, Zhi-yong Lei," A Kind of Wormhole Attack Defense Strategy of WSN Based on Neighbor Nodes Verification", 2011, IEEE
[16] N. Vanitha, G.Jenifa," Detection of Packet Droppers in Wireless Sensor Networks Using Node Categorization
[17] Algorithm," 2013,International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, ISSN: 2277 128X. Research Paper available online at: www.ijarcsse.com
[18] A. BabuKaruppiah, J. Dalfiah, K. Yuvashri," A Novel Energy-Efficient Sybil Node Detection Algorithm for Intrusion Detection System in Wireless Sensor
[19] Networks", 2014, IEEE
[20] Noor Alsaedi, FazirulhisyamHashim, A. Sali," Energy Trust System for Detecting Sybil Attack in Clustered Wireless Sensor Networks", 2015, IEEE
[21] Martin Stehlik, VashekMatyas, Andriy Stetsko," Towards Better Selective Forwarding And Delay Attacks Detection in Wireless Sensor Networks", 2016,
[22] IEEE 13th International Conference on Networking, Sensing, and Control
[23] MostefaBendjima," Wormhole Attack Detection in Wireless Sensor Networks", 2016, SAI Computing Conference.
[24] Rupinder Singh, Jatinder Singh, Ravinder Singh," TBSD: A Defend Against Sybil Attack in Wireless
[25] Sensor Networks", 2016, IJCSNS International Journal of Computer Science and Network Security, 90 VOL.16 No.11
[26] Ju Ren, Yaoxue Zhang, Kuan Zhang, and Xuemin (Sherman) Shen," Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks", 2016, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. [23] Parmar Amish, V.B.Vaghela," Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol", 2016, Procedia Computer Science 79, 700 – 707.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)