iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 5 **Issue:** VIII **Month of publication:** August 2017

**DOI:** http://doi.org/10.22214/ijraset.2017.8147

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:6.887*
*Volume 5 Issue VIII, August 2017- Available at www.ijraset.com*

# Security of Wireless Mesh Network from Denial of Service Attack

Shweta Nijhawan[1], Sunita Rani[2]
*M.Tech Student[1], Assistant Professor[2] , BPS Mahila Vishwavidyalaya Khanpur Kalan (Sonipat)*

***Abstract: Wireless Mesh Networks (WMN) is an integral broadband wireless network who provides high bandwidth internet service to users. It is a kind of multi-hop network having many to many connections with the capability of dynamic signify network topology WMN's utility network performance can cause a massive fall. Channel your physical security vulnerabilities, due to the dynamic changes of topology is a major challenging issue. Self –Configuration is a wireless mesh network self-organized nature make it vulnerable to various type of more attacks .In this paper we have discussed Some attacks that TCP / IP model are performed at different layers of security challenges, analyzing the counter remedies and protection mechanisms in place various attacks listed. Some attacks that TCP / IP model, are performed at different layers of security challenges, analyzing the counter remedies and protection mechanisms in place various attacks listed.***
***Keywords: Wireless Mesh Networks, Wormhole attack, Grey Hole attack, Security, Attack, Challenges***

## I. INTRODUCTION

Wireless Mesh Networking is a rise innovation. A remote Mesh Network originates mesh hubs which frame the foundation of the network[1].Nodes consequently design organize availability and powerfully reconfigure the system "self-form" and "self-mending" highlights are to keep up returns. Akyldiz [3] expressed that WMNs are grow to retutation confinements and to enhance the execution of Ad-hoc arranges. Concentrated administration [2] should act naturally adequate on account of the connection between the work hubs are evacuated .Various applications [4] of remote work organize as

*A.* Broadband home network
*B.* Community and vicinity networking
*C.* Diligence Network
*D.* Building Automation
*E.* Transportation System
*F.* Health and Medical System
*G.* Security and Surveillance system
*H.* Emergency disaster network
*I.* Peer to peer communication

Security has turned into the principle worry to give secure correspondence. Different preferences of remote work system,forexample

*J.* Simple Installation and Low Cost
*1)* Nodes Self-connectivity
*2)* Network flexibility
*3)* Discovery of the newly added nodes

## II. CHARACTERISTICSOF WMNs

Remote Mesh Networks is dynamic, self-association, self-design and self-recuperating portrayed by adaptable joining, quick sending, empowering simpler support, Low costs, high versatility and dependable administrations. System arrangement and support is enormously diminished unpredictability and the capacity to sort out their own particular [3].
Remote Mesh systems comprise of

*A.* Mesh Clients (MC): Minimal versatility
*B.* Mesh Routers (MR): Static or Mobile in nature

WMNs are utilized to incorporate diverse sorts of system like Internet, Cellular, Wi-Fi systems, Wi-Max, Sensor systems and so forth. For the most part three sort of remote work systems can be characterized:

1) Infrastructure WMNs work switches offer system administrations to the customer clients. The system makes them mend attributes.
2) WMNs customers are impromptu systems shaped by another customer. None of committed switches or foundation exists with the goal that the self-arranging customer and customer WMN switches go about as movement to be. WMNs have two different points of interest of mixture WMNs.

Wireless Mesh Network are multi jump organizes and gives much scope go. Like on the off chance that one hub is fizzled or kills then through different hubs message can be transmitted to goal hubs that capacity gives the excess in the work organize. They have ability of self-recuperating and self-framing and self-association and offer help for Ad Hoc Networking. As we have multi-trusting so it accomplishes higher throughput, and more productive recurrence re-utilize. They give minimal effort to establishment in light of the fact that the diminishment of the quantity of get to focuses to web so the primary points of interest of WMNs is that effortlessness of arrangement. Numerous kind of system get to like help for web and p2p correspondence too. Furnish similarity with existing remote systems like WiMax, Wi-Fi, cell systems. It has adaptable system architecture

## III. SECURITY REQUIREMENTS

A remote work organizes security prerequisite can be named:

### A. *Data Validation*

To guarantee the information is started from the correct source.

### B. *Data Privacy*

To ensure that exclusive approved hubs can get the substance of the messages.

### C. *Data Integrity*

To ensure that any got message has not been adjusted or alteration by unapproved gatherings to send.

### D. *Availability*

To ensure that administrations offered by WSN or by a solitary hub ought to be accessible while essential.

### E. *Non Repudiation*

To guarantee a hub which sends a bundle to a goal hub can't refute that the parcels sent and got parcels to the goal can't deny.

## IV. SECURITY CHALLENGES IN WMNS

WMNs totally for a few reasons it is hard to be ensured. These security challenges are as beneath:

### A. *Multihop Nature*

Multihop to defer in location and treatment is expected for assaults[11]. Also since most of the one-jump out insurance plans are proposed for the system, one of them being assaulted are not adequate to secure the WMN

### B. *Multisystem Security*

WMNs incorporate different remote advancements, for example, IEEE 802.15, IEEE 802.16, IEEE 802.11 and so on. A security organize is required however it is difficult to give in the systems.

### C. *Multitier Security Framework*

[11] Security is should be ensured the customer hubs as well as the work switches and the work customers and work switches.

D. We expected the hub is being trade off because of absence of physical security[10]. In this manner the framework outside the system from vindictive assaults propelled from inside the system is powerless against assaults.

E. WMN has memory and computational limitations [10], the security are not connected to regular plans.

*F. Shared Remote Connections*

[12] since a solitary radio channel is used by work customers to send and receive data bundles spying or the replay assaults like MAC layer are possible to be back.

*G. Dearth of Affiliation*

Due to the impromptu idea of WMN change the put stock in relationship among hubs.

*H. Physical Risk*

The absence of physical security hub is probably going to settle.

*I. Resource Avail*

Security are not appropriate for conventional plans WMNs as a result of pool of computational requirements and memory [12].

## V. ATTACKS ON PROTOCOL LAYER

The attacks might appear in Physical layer,MAC layer, Network layer, Transport layer and Application layers of the protocol stack

*A. Security Attacks at the Physical Layer of WMNs*

There WMNs first physical layer comprises of various sorts of assaults. An aggressor could annihilate outside equipment simply the switches are introduced in the open air range. Such powerless switches are an aggressor can without much of a stretch concentrate the data. The pinpoint sticking, sticking at time, receptive jamming attacks can be connected in physical layer [13]. In pinpoint sticking assault assailant transmits the steady commotion. In occasional sticking assault (or scrambling assault) an assailant sends a little intermittent flag. In last receptive sticking assault at whatever point a hub identifies that an assailant has begun a transmission flag transmit an aggressor.

*B. Security Attacks in the MAC Layer of WMNs*

Many sorts of assaults are conceivable in the MAC layer and comprise of the accompanying:

1) *Passive Eavesdropping:* WMNs nature of broadcasting the transmission it falls inside the transmission scope of the aggressor uninvolved correspondence hubs is conceivable to dispatch the listening in. It can be launched in inner hubs and outside hubs. Inside listening in by noxious middle hubs keeps duplicate the information and forward to any hubs in the system without facilitate learning [14].
2) *Flooding Attack:* An assailant sends many messages to its neighboring hubs to control a few MAC. Due to the fairness of the medium is physically mishandled [15].
3) *MAC Spoofing:* If an assailant tries to change the MAC address of the casing is communicated.
4) *Jamming Attack:* Jamming assaults are likewise conceivable in MAC layer.

*C. SecurityAassaults in the Network Layer of WMNs.*

Many assaults on the system layer are likewise conceivable. These assaults are additionally ordered in two gatherings:
Control Plane or (steering) to concentrate on the directing usefulness of the system. Control Plane assaults is distinguished as underneath:

1) *Rushing Attacks:* On-request steering conventions an aggressor sends various directing parcels past the system in a short interval of time to keep hubs occupied.
2) *Routing Table Overflow:* The new courses are being made by an assailant enough to escape courses with the expectation of making invented hubs endeavors to manufacture new streets.
3) *Wormhole Attack:* In this attack malicious assailant to persuade two hubs utilize the way or connives with more malevolent hub is amid the establishment of a passage. A wormhole assault utilizing a fruitful correspondence medium. Once the casualty hubs enter the noxious hubs in the method for steering hubs the malignant hub starts dropping packets.

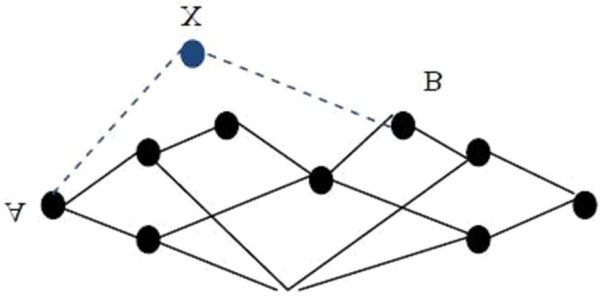



Fig. 1 Wormhole Attack

4) *Sinkhole (or Black hole) Attack:* In this assault a malignant parcel sending hubs starts to disclose to its neighboring hubs. That bundle to propel the most ideal hub. A district hub started to forward parcels noxious hub bundles are sent by the neighboring hubs goes.
5) *Grey Hole Attack:* Gray Hole assault is a variety of sinkhole assault [16]. Amid this assault they won't drop the whole parcel simply particular bundle drop [13].
6) *Location Disclosure Attack:* During this assault structure or system hub uncover data about the area [17].

Information Control Attack: Data control (or way sending) organizes assaults target way sending functionalities. These types of assaults are started by the hubs in the system mishandle. Bansal et. al. [18] isolated into two groups selfish hubs and malignant hubs. A ravenous hub tries to irritate the operation of an egotistical hub organize; even in the working expenses of alternate hubs is worried about his execution. Listening stealthily is a basic approach to control the attack.

*D. Security Attacks in the Transport Layer of WMNs*

An assailant may focus on the vehicle layer. Surge assaults are conceivable in the vehicle layer and desynchronization. In flooding assaults noxious hub to achieve a greatest point of confinement to the asset prerequisites can ask for another association. In desynchronization assault a pernicious hub may over and over fake the messages to ask for the retransmission of the edge with the goal that the host can come up short.

*E. Security Attacks in the Application Layer of WMN*

Application layer assaults infections and also worry in remote systems, noxious code, foreswearing of the application, worms and so forth.

## VI. PHYSICAL SECURITY THREATS

*A.* Conventional remote system deployments were inside physical and regulatory control of the chief or organization of an endeavor environment .Outdoor remote work systems work get to directs require toward be out of the administrator's physical control. Physical gadget security postures more difficulties for outside organization. Wireless mesh gets to focuses, lighting positions are moving away or outer structures, a situation where the organization of a wide zone arranges that is not under the control the administrator of the physical and overseers, such gadgets could be a few thousand.
*B.* Wired network get to focuses that required organize connectivity. Wired organize get to focuses once in a while media backhaul which can uncover delicate wired network associations is required.
*C.* Battery weariness assault 'lack of sleep assault' is known as a real threat and straightforward disavowal of service assaults more unsafe. Assault on CPU number may deny the accessibility of the dissent of administration while battery exhaustion can injure the casualty.
*D.* Security of client protection is an extremely striking issue in remote system correspondence. Be that as it may it is troublesome to ensuring security of the clients.
*E.* To realize the message are ensured inside the system as there are relatively few security arrangements or machine which ensure that learning approved gatherings themselves [19].

## VII. POSSIBLE COUNTER MEASURES

DoS in any shape against any system are respected as a genuine assault. Broadband remote system the consequences of various DoS assaults shift with the nature and sort of DoS assault. In the event that begin against a single node either to debilitate its battery to isolate it from the organize operation. Egotistical work switch assault in WMN and devilish BS assaults are utilized to make services unavailable to an objective zone in remote broadband networks.

### *A. DoS Assaults and Conceivable Counter Measures*

Requirements to be investigated to defeat it to some degree are these:

*1)* Cognitive radios usage at physical layer should be researching to deal with the jamming and scrambling sort of assaults, all of which are common in the broadband systems.
*2)* The current encryption systems utilized as a part of broadband systems WEP, DES, and AES, which are defenseless against assaults like eavesdropping. Improved and proficient encryption instruments need to be proposed only for each broadband technology as the effective listening stealthily office assailants to dispatch DoS assaults.
*3)* Intrusion location system to detect and react particularly for the system layer apprehend especially for WMN condition.
*4)* Location location instrument is premise on flag quality and AP test ask for spate of the assaults and de-confirmation sort with the capacity to recognize malevolent hub work remote switch should be prepared, a similar framework IEEE 802.16 systems can be utilized to distinguish fake enlistment ask for surges.
*5)* Improve directing conventions particularly for multi-jump WMNs are fancied.

### *B. Cryptography and Digital Signatures*

Hubs can create computerized marks and check them then arrangement is straight forward. The utilization of open key cryptography a hub can check the mark of alternate hubs, the two hubs will build up a typical mystery key signs innovation get to, and ensured by the mystery key messages will have the capacity to acknowledge. Be that as it may, a significant number of the hubs in a WMN have computation and absence of battery confirmation action that incorporates open key cryptography may not be implemented. However Elliptic Curve Cryptography (ECC) [20] gives some vitality and computation efficient methods in execute cryptographic algorithm which might be merit for portable clients.

### *C. Match Wise Key Sharing*

In WMNs symmetric cryptography is conceivable due to the topsy-turvy cryptographic system require less computation. A better arrangement Diffie-Hellman (D-H) key trade to be utilized [21].Diffie-Hellman(D-H) key exchange is a cryptographic protocol that permitting two gatherings that have no prior knowledge of each other the two gatherings usually build up an unsecured correspondences channel that permits shared key. The key is a symmetric key figure to encode interchanges utilizing the later can be utilized.

### *D. Secure Routing*

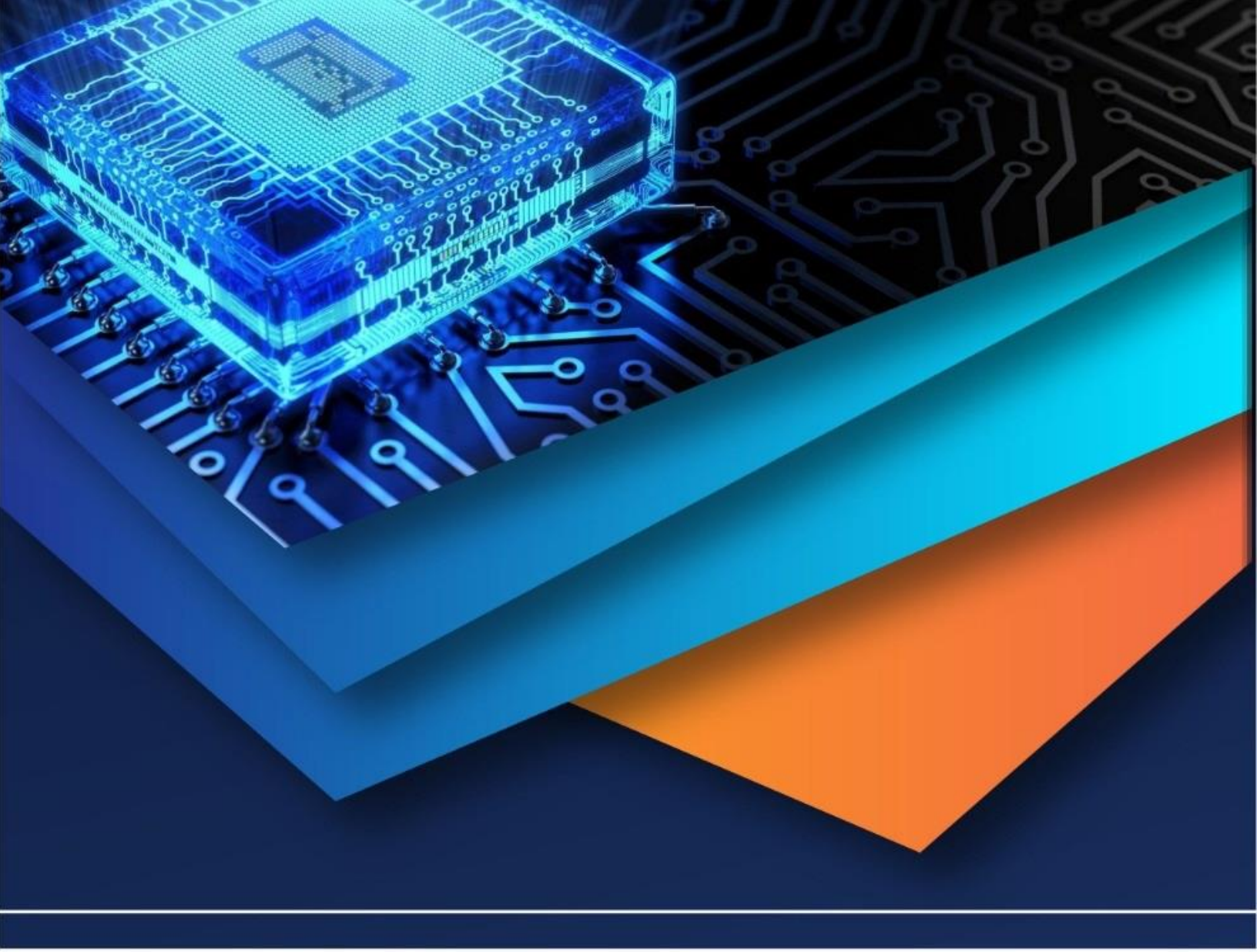
To accomplish accessibility both powerfully changing topology and steering convention must be strong against vindictive assaults. There are two sources of threats to directing conventions. To begin with come from external assailants and the second more serious sorts of dangers additionally originate from compromised nodes; wrong steering data might be promoted to different hubs. To forestall such attacks we can use certain properties of WMNs to achieve safe steering. Like Multipath directing [22] takes preferred standpoint of various courses in a productive manner without message retransmission. The first thought for blunder location and redress through extra courses to transmit data is pointless. Indeed, even if some course bargained the recipient may still have the capacity to approve messages.

## VIII. CONCLUSION

WMNs are able to provide seamless connectivity to the nature of self-healing system. WMNs successful implementation of secure conventional and enhanced security protocols required. Thwarting all security to prevent attacks on the network layer and above all security measures to maintain security is impossible. So far, the proposed security measures introduced in the various layers are not the solution for a variety of attacks. Network layer security attacks can be caused by events in the lower layers is caused. This is necessary to secure a cross-layer approach WMNs. The major security requirements threats and security risks are analyzed WMNs and finally some security mechanism are discussed.

## REFERENCES

[1] H.T. Cheng, H.Jiang and W.Zhuang ,"Distributed medium access control for wireless mesh networks",. Published online in Wiley InterScience, pp.845–864,2006.
[2] S.M.Cheng, P.Lin, D.W. Huang and S.R.Yang, "A Study on Distributed/Centralized Scheduling for Wireless Mesh Networks",Vancouver British Columbia, Canada., pp 599-604, 2006,
[3] F.Akylidz, X.Wang and W.Wang, "Wireless Mesh Networks: A Survey" Comput Net,47(4),pp.445-487, 2005.
[4] X.Xu, X.Wu, Z.Yu, "Application of Wireless Mesh Network in Campus Network", Second International Conference on Communication systems Networks and applications, pp.245-247,2010.
[5] T.karasi, M.S.Bhanu, "A Survey of Secure Routing Protocols for Wireless Mesh Networks", International Journal of Computer Applications, 97(6), 2014.
[6] Monika, "Denial of Service Attacks in Wireless Mesh Networks",International Journal of Computer Science and Information Technologies, 3(3), pp.4516-4522,2012.
[7] S.D.Kanawat, P.S.Parihar,"Attacks in Wireless Networks", International Journal of Smart Sensors and Adhoc Networks, 1(1),pp.113-116, 2011
[8] A.Khajuria1, R.Srivastava, "Attacks and Challenges in Wireless Networks A Literature survey", International Journal Of Enhanced Research In Management And Computer Applications, 2(3), pp.1-6, 2013.
[9] Yongguang Zhang and Wenke Lee, "Security in Mobile Ad-Hoc Networks," In Book Ad Hoc NetworksTechnologies and Protocols, Springer, 2005.
[10] M.S.Aswal, P.Rawat, T.Kumar, "Threats and Vulnerabilities in Wireless Mesh Networks", International Journal of Recent Trends in Engineering, 2(4), pp.155-158, 2009.
[11] Aamir Shaikh and Siraj Pathan, "Research on Wireless Sensor Network Technology", International Journal of Information and Education Technology, 2(5), pp. 476-479, 2012.
[12] A.K.Gankotiya, S.Seth, G.Singh, "Performance Analysis of Secure Wireless Mesh Networks" , Research Journal of Recent Sciences Vol. 1(3),pp. 80-85, 2012.
[13] S. Seth, and A. Gankotiya, "Denial of Service Attacks and Detection Methods in Wireless Mesh Networks", In the Proceedings of the 2010 International Conference on Recent Trends in Information, Telecommunication and Computing ,Koshi, Kerala, , pp. 238 – 240,2010.
[14] Mewada Shivlal and Singh Umesh Kumar, "Performance Analysis of Secure Wireless Mesh Networks", Research Journal of Recent Sciences, 1(3), pp.80-85, 2012.
[15] P.Sharma, "performance analysis of secure wireless mesh networks" International Journal of Research in Science and Technology (IJRST), 3(4), pp.65-75, 2013.
[16] M.Panda, "Security in Wireless Sensor Networks using Cryptographic Techniques", American Journal of Engineering Research (AJER),3(1) pp-50-56,2014.
[17] Edwin Prem Kumar Gilbert, Baskaran Kaliaperumal, and Elijah Blessing Rajsingh, "Research Issues in Wireless Sensor Network Applications: A Survey", International Journal of Information and Electronics Engineering, 2(5), pp.702-706, 2012.
[18] Y.C Hu, A.Perrig and D.B.JohnsonWormhole Attacks in Wireless Networks", IEEE Journal On Selected Areas In Communications, 24(2), pp. 370-380, 2006.
[19] D.MA, G.Tsudik "Security and Privacy in Emerging Wireless Networks", IEEE Wireless Communications, pp.12-21, 2010.
[20] D.Sharma, S.Verma, K. Sharma, "Network Topologies in Wireless Sensor Networks: A Review", 4(3), pp. 93-97, 2013.
[21] F.T.B.Muhaya, F.Hadi, A.Naseer, "Selfish node detection in wireless mesh network", International Conference on Networking and Information Technology, pp. 284-288, 2010.
[22] M.Imani, M.E.Rajabi, M.Taheri, M.Naderi, "Vulnerabilities in network layer at Wireless Mesh Networks (WMNs)", International Conference on Educational and Network Technology, pp. 487-492,2010.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY