iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XII **Month of publication:** December 2017

DOI:

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 XII December 2017- Available at www.ijraset.com

A Collaborative Approach for Detection of Blackhole, Rushing and Selfish Node attack in Reactive Protocol Environment

Vasu Sharma[1], Pawan Luthra[2], Gagandeep[3]
[1]*M.TECH CSE (Part-Time), DCSE, SBSSTC Ferozepur, India*
[2, 3] *Assistant Professor, Dept. of CSE, SBSSTC Ferozepur, India*

Abstract: ***Nowadays, Wireless Adhoc Networks (WANET) are widely used in various commercial and governments organizations. At commercial level, these networks are used to establish a temporary network for the smooth conduct of events such as Conference, Seminars and by the security of the Organization. In government sector, these networks are used within Defence, Army, Scientific experiments and space shuttle launch operations and by the rescue teams in situations like natural (floods, earthquakes etc.) and un-natural disaster (bomb blasts, riots etc.). As these networks are very fast in working, easy to install and handle, they are also come with several issues from the very beginning of these networks. They also have features like Open Access, No Administration and Dynamic Topology, which makes it fast, reliable and smooth, functioned. But these feature also come with lots of compromises in Security, Power and Bandwidth of the network established. As much as Telecommunication companies are very much investing in making the devices faster, cheaper and reliable but the software is still have old fashion. From the very much beginning of Adhoc Networks, the networking devices became much faster, small, and durable but the communication strategy is still old. Adhoc Networks have variety of networking protocols for different area and use of the network but not all are efficient for secure communication between sender and receiver. Lack of central admin and other features of the network give rise to various threats and attack for the network communication. In this paper, I have represented the impact of some network layer attack over the normal operations of the AODV protocol of Adhoc Networks.***
Keywords: AODV, NS2 Simulation, Selfish node, Rushing attack, WANET Security.

I. INTRODUCTION

In tele-communication, networking is significant area, which is answerable for source to destination transmission. With the support of computer networks two nodes are able to communicate with each other from the different or same physical positions and able to share any type of data or info between them. In present days due to every day developments in facilities, speediness, functionality and hardware technology computer networking is the highest emerging arena. As Computer Networks are basic building block of networking, they provide the platform for improved communication between contributing nodes. A network is graphical representation of networking devices Routers, Cables, and Switches etc. computer systems or nodes and links between all of contributing nodes. The networks which are established using air as medium and there is no physical path is present between two nodes of the network and nodes are communicate with each other through Electromagnetic waves or Radio waves such networks are called as Wireless Networks. In Wireless Networks, nodes communicate with each other through air. Wireless networks can be established using two approaches: Fixed and Mobile. In Fixed**,** networks are designed using a particular topology or a well-organized arrangement is used to connect nodes. A predefined protocols and strategies follow for the actual communication between two nodes. In this approach, there is one base station node such as Router, Switch or Access Point etc., which remains fixed at one position, allow other nodes such as Mobiles, Laptops, or Tablet to connect with it inside an assured physical area, and established the network through air. It offer the platform for the communication between two nodes of the network. Other nodes may change its location in the network within the range of the base station. All the communication between two nodes of the networks is takes place through the base station only. In Mobile**,** nodes communicate with each other in unstructured way. There is no a exact design is follow to connect the nodes of the network with each other. All nodes can communicate with each other as they arises under each other's range. Communication is takes place if both the nodes are decide to communicate with each other. There is no base station presents, all the nodes may change its position at any time (WANET's). Nodes communicate with each other by using a specific procedure or tactic according to the application or area of the network, which is being formed. As there is no strategy follows for these types of networks and the nodes are exit or linking the networks constantly so these types of networks are often considered as

Wireless Adhoc Networks. Nodes are allow to connect with each other as they comes in their individual antenna range. At any stage, a node may leave or join the networks without any approval. From the last decade, WANETs becomes very general in our life. These days in tele-communication these Wireless Adhoc Networks becomes very general to connecting with each other within a particular region for the various applications. As this field as growing up very fast, it comes with new problems, dares and boundaries for the actual communication between the nodes with full accuracy. With the rapid development in wireless technology, ad hoc networks have emerged in many forms. These networks operate in the license free frequency band and do not require any investment in infrastructure, making them attractive for military and selected commercial applications. However, there are many unsolved problems in WANETs; securing the network being one of the major concerns. Secure communication is always most important in wired or wireless networks. In this paper after the detailed introduction about WANET in section-I, section-II discuss about the Routing Protocol (AODV) which is being used for simulation, section-III defined about security threats of network layer of adhoc networking which are being implemented on AODV protocol to measure its performance, section-IV will be of simulation and result into the last section I concluded the paper with some future facets to this paper.

II. USED ROUTING PROTOCOL: - ADHOC ON-DEMAND DISTANCE VECTOR PROTOCOL (AODV)

Routing protocols in wireless ad-hoc networks describes how the actual communication between two nodes of the network takes place practically. There are so many protocols, are introduced in present time such as AODV, DSDV, DSR, ZRP etc. In this paper, I will describe the attacks in AODV protocol.

A. AODV (Ad-Hoc on Demand Distance Vector)

In AODV, links between nodes are establish according to the need of nodes. Communication never started between nodes until Sender node willing to do so. Sender node firstly broadcast a route request (RREQ) to the entire network for the discovery of best-known route to the destination. Any intermediate or receiving node can make reply to route request by sending route reply (RREP) message to Sender or with the information about Route Discovery. If Sender receives Positive route reply, node then it start the actual data transfer to the destination via best-known route or directly to destination if the destination node present within the range of source node. In case of no route found the intermediate nodes reply with route error message to the initiator [1].

B. So AODV protocols works in three processes.

Initially a source node sends a request to find particular destination, secondly destination node or other node of the network reply with availability or non-availability of route towards destination and if the route is available, the source node starts the third process of AODV protocol, which is actual data transfer. Due to open access to network, AODV cannot define about malicious node initially, so we cannot control whether our request are going to genuine node or to some malicious node. So attacker can easily target at route request to misguide or misuse it for attacking purposes at network layer.

III. LITERATURE REVIEW

A. Attacks and threats

1) *Selfish Node Attack:* In this attack the attacker node does not reply any route request (RREQ) received by it. Selfish node attack is exactly opposite to it. It just receive the request and remain idle in the network. It does not participate in the network to find genuine Receiver of the message. Due to its selfish nature Sender and Receiver has to follow a long route, which result in consumption in more power and bandwidth. [8]
2) *Black Hole Attack:* In Black hole attack a malicious nodes can misguide the all other node throughout the network with black hole attack. Same as wormhole node, a Blackhole node can also influence very badly to the network. The black hole attack make the network disturbance with two methodologies: Initial, the node exploits the mobile ad hoc routing protocol, such as AODV, to publicize itself as having a valid route to a target node, even though the route is spurious, with the intention of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding [3] [5]. In both of Blackhole node activities intruder consume bandwidth by making wrong reply and take information from the network without the awareness of the network nodes. This attack degrade the performance in very ruthless way.
3) *Rushing Attack:* In this attack, malicious node consumes battery and bandwidth by excessive route discovery or by forwarding unnecessary packets to victim node [3]. For example, suppose in the example of Blackhole attack, the Blackhole node reply to each and every route request (RREQ) send by any node of the network with fake route reply (RREP) it always results in wastage of so much energy of each and every node and bandwidth of the network which results in deficiency of the network

and poor performance. As the route request received by the attacker node from any other genuine node of the network, attacker node forward the route request in very massive way and in number of repetition to make rush in the network. This action of the attacker leads to consumption of network bandwidth and nodes energy. With the infection of this attack genuine nodes are not able to stay in network for longer time.

IV. SIMULATIONS AND RESULTS

Simulation can be defined as the artificial structured of the operation of a real-world process or system over time. For the development of networks scenario and to perform communication operations using nodes to create wireless networks I used Network Simulator-2 (NS2). All the tests are done using this simulator and results are also analysed using some tools of NS-2.
The performance of the Network Scenario is measure using widely used matrices like:

A. TCP Good put (Throughput)

Good put is defined as the number of unique packets delivered to an end host in a given amount of time. It refers to the amount of data moved successfully from one place to another in a given time period.

Throughput=Packet Delivered/ Time taken

B. Average End- to- End Delay

It refers to the time taken for a packet to be transmitted across a network from source to destination.

Average E2ED=Average time taken by a nodes to transfer data to destination

C. Packet Delivery Ratio (PDR)

The packet delivery ratio is defined as the ratio of number of packets received by the destination to that of the number of packets sent by the source.

Packet Delivery Ratio=Total Packet received/Total Packet Generated

D. Average Consumed Energy (Per Node)

The average consumed energy per node is defined as the ratio of total energy consumed in simulation (to send, received and forward) by total number of node.

Avg. Consumed energy (per node) = Total energy consumed/No. of nodes

E. Packet Delivery Ratio Analysis

As described PDR is the ratio of total packet received by destination (single or multiple) to the total packet send by source. In simulation of normal AODV with 20 nodes in the network show the maximum value for PDR (98.08%), as AODV simulated under Selfish node and Rushing Node Attack within 20 nodes in the network the value of PDR is decreased up to 47.23% (in case of Selfish node attack), 44.89% (in case of Rushing attack) and 19.01% (in case of Blackhole Attack) due to malicious nodes.

TABLE-1
Simulation Parameter Used

Parameters	Values
Protocol	AODV
No. of nodes	20, 40, 60
No. of attacker node	3
Area	1500*1000m
MAC	802.11
Maximum Packet in ifq	50
Simulation time	200 seconds
Traffic Source	FTP/CBR
Transmission Protocol	TCP
Packet Size	1500 bytes
Mobility	20m/s Random
Transmission Range	550
Maximum Data rate	11Mb

Basic Data rate	0.1Mb
Mobility	Random Way Point

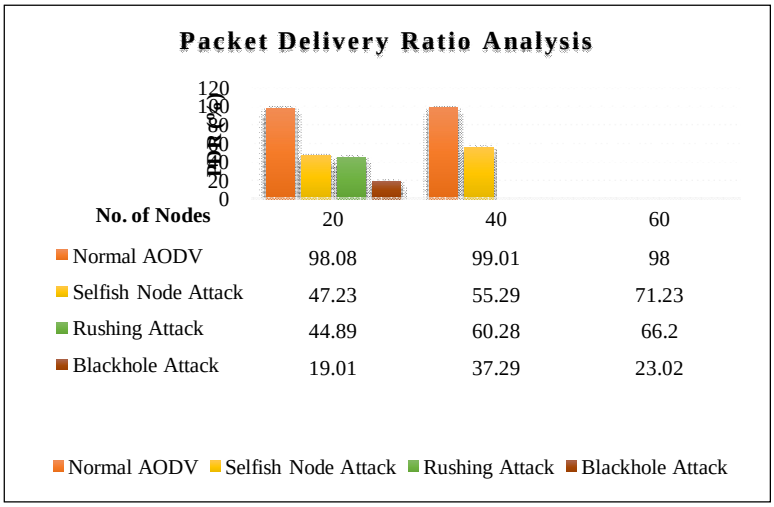


Figure-1: Packet Delivery Ratio Analysis

In 40 nodes simulation scenario maximum PDR value is 99.01% in normal AODV operation, but this value decrease with Selfish Node attack (up to 55.29%), with Rushing attack (up to 60.28%) and with Blackhole Attack (up to 37.29%). In Simulation scenario of 60 nodes the PDR value for normal AODV less (98%) then the simulation of Selfish node attack (71.23%), Rushing attack (66.20%) and Blackhole Attack (23.02%) in 60 nodes network.

F. End-to-End Delay Analysis

In normal AODV simulation of 20 nodes the value of E2ED is 160ms, it increases in the Selfish node simulation (198.702ms), also in Rushing attack simulation (180.674) and in Blackhole Attack (6.79ms). It is very surprising value under Blackhole Attack, the reason behind this is that there are three Blackhole Attack nodes which are replying so fast to consume the packet so as the request made, the malicious node immediately reply with fake address to consume all the packets. Throughput value in 20-Node scenario is surprising in attacks because of short interval of simulation time. But as we go to other scenario the value of throughput in attacks is so small as compared to the Normal AODV scenario.

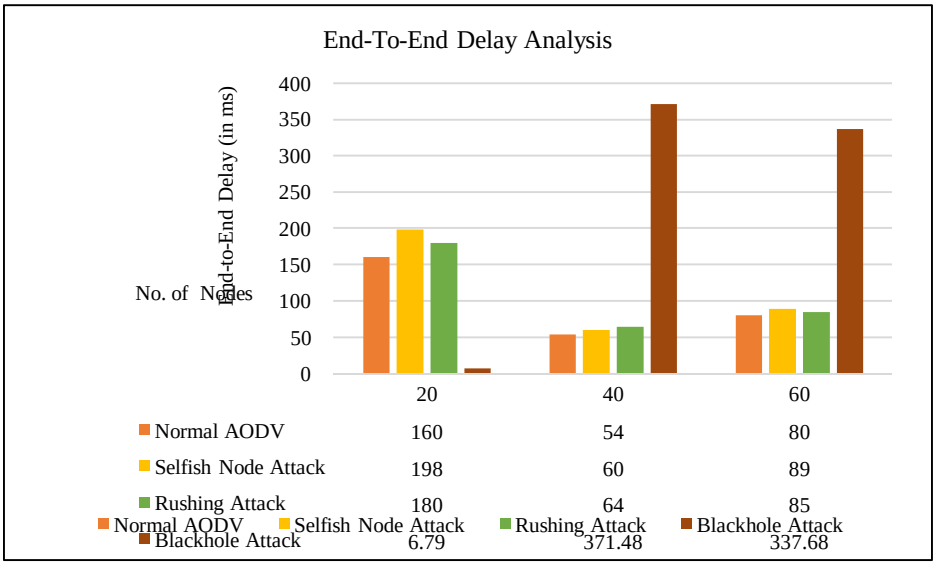


Figure-2: End-to-End Delay Analysis

In normal AODV simulation of 40 nodes the E2ED is 54.386ms and it decreased in simulation of Selfish node (up to 60.06ms) and increased in the simulation of rushing attack (up to 64.447) and very much increased in Blackhole attack. On the other hand in normal AODV of 60 nodes simulation the E2ED value is larger than other all simulation scenarios because of more number of intermediate nodes available to transfer the data to the desired destination. The Value of E2ED increases in the simulation of Selfish Node (up to 89.9622ms) and in Rushing attack simulation (up to 85.2937ms) and in Blackhole Attack (up to 337.68) into the 60 nodes simulation network.

G. Throughput Analysis

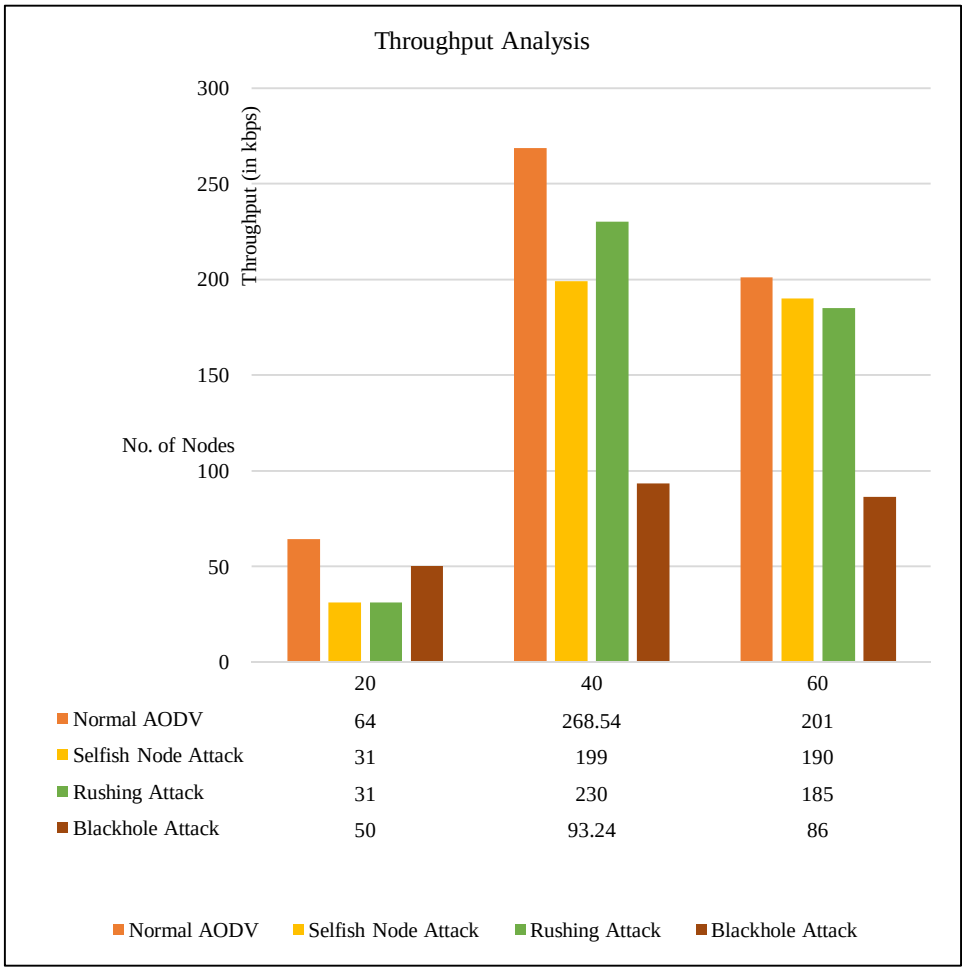


Figure-3: Throughput Analysis

As we can see in figure-3, in case of Blackhole attack the throughput is negligible because as discussed earlier in PDR and E2E delay analysis that attack node do not forward any packet to next hop or to destination, due to which no communication takes place between sender and receiver. As we increase the number of nodes in the network it rise up, but not considered because the increment is too less. Into the normal AODV simulation of 20 nodes the Throughput value is 64.4Kbps, it decreases up to 31.69Kbps in simulation of Selfish node and in simulation of Rushing attack into the network of 20 nodes. In other scenario throughput of normal AODV is good.

H. Average Energy Analysis

As I calculated avg. energy consumed by each node by dividing whole consumed energy to transfer, received and forward packet in the network, to the number of nodes present in the that network scenario.

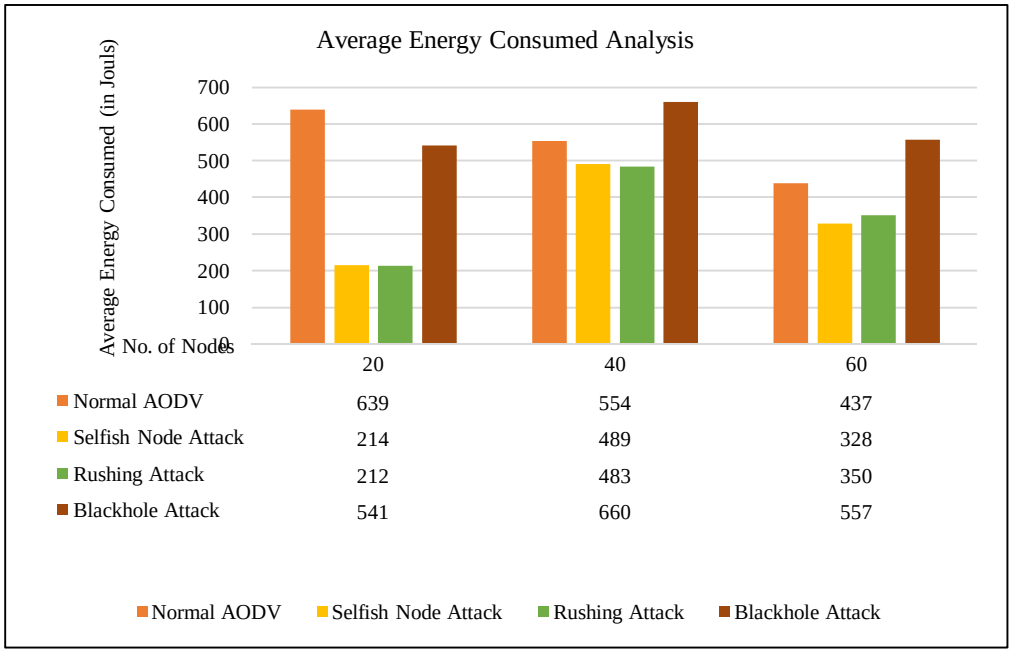


Figure-4: Average Energy Consumed Analysis

So as we look on 20 nodes simulation scenario in normal AODV operation. The Avg. is 639J, in case of Selfish node attack it is recorded as 214J due to not participating in the transmission operation by the senders of the network, in case of Rushing attack it is 212J due to presence of three malicious nodes as they are try to make rush in network there is no transfer takes place properly so the consumed energy s quit low.

But as in Blackhole attack the transfer is happened between sender and malicious node so the avg. consumed energy 660J.

V. CONCLUSION AND FUTURE WORK

In WANETs due to exposed entrance of the network an attacker can easily go in into the normal operations of the network, attacker node can add itself to the network without any validation or approval because there is no administration in the network. Results analysis of Selfish node, Rushing attack and Black Hole attack in AODV routing show that up to how much value these attacks can degrade the performance of the network. These attacks infects the value of PDR, E2ED and Throughput very badly and make the network inefficient and unsecure. These attacks also results in deficiency of the network, wastage of bandwidth, wastage in energy of the nodes, poor communication channel in the network.

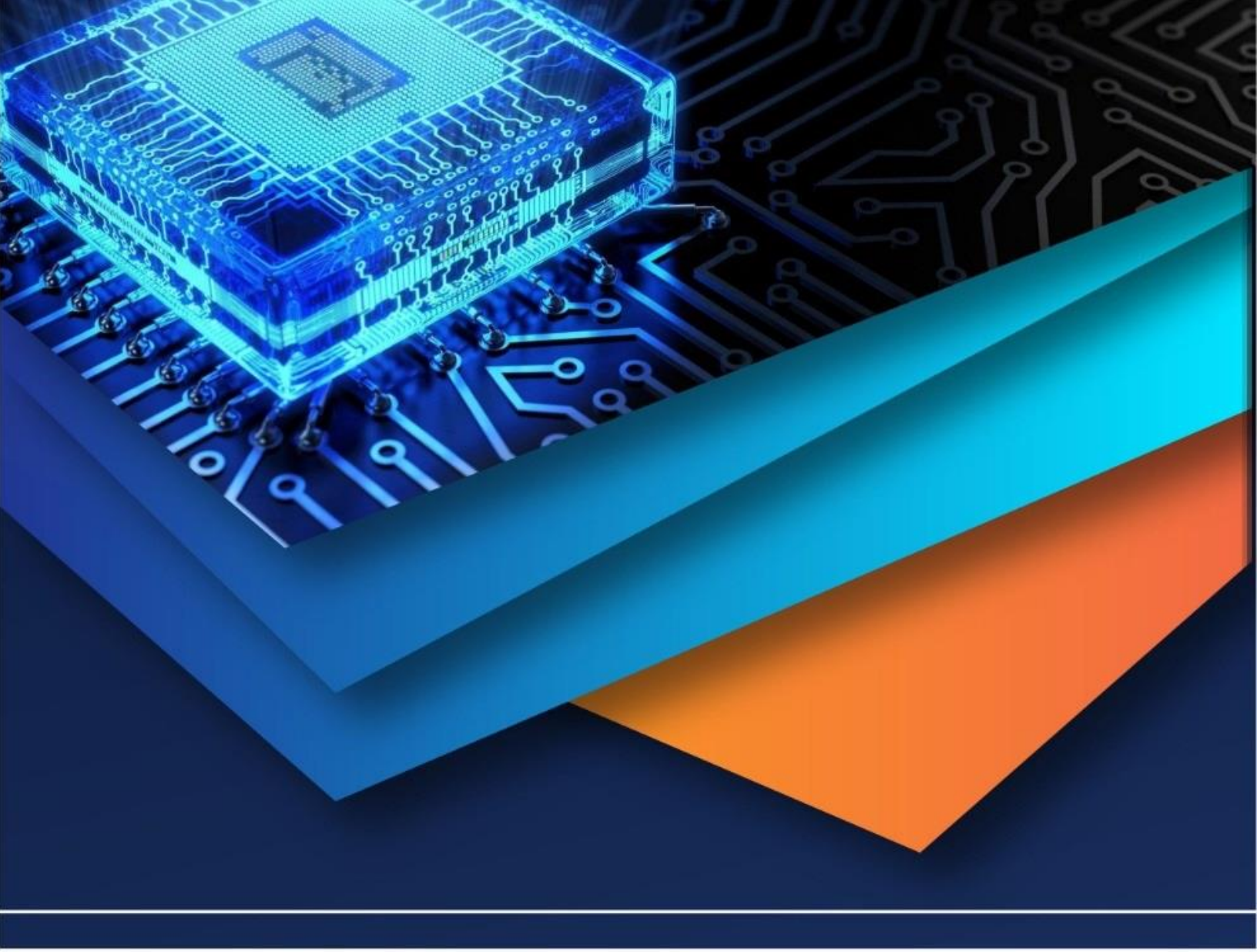
WANETs are much popular for their features and always be the research topic for many commercial and business organizations. In future, we can elaborate the impact of some other security issues and threats over the other layers of communication process in the network. We can also find or developed an excellent routing protocol which restrict the entry of malicious node into the network.

REFERENCES

[1] Syed Fakhar Abbas, Ghulam Yasin, Muhammad Akram Mujahid and Dr. S R Chaudhry, “Metric Base Analysis and Modeling Experiments of Routing Protocols in MANETs and VANETs Wireless Network using Real Time Scenarios”, IJCSI, Sept. 2013
[2] Andrew S. Tanenbaum, “Computer Networks”, Prentice Hall, New Jersey 2003. Page no. 281-285.
[3] David B. Johnson, David A. Maltz and Josh Broch, “DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks”, Computer Science Department Carnegie Mellon University Pittsburgh, PA 15213-3891
[4] Gurjinder Kaur, V.K.Jain and Yogesh Chaba. “Wormhole Attacks: Performance Evaluation of On Demand Routing Protocols in Mobile Adhoc Networks”, IEEE-2011.
[5] S. Mahajan and A. Jindal, "Security and Privacy in VANET to reduce Authentication Overhead for Rapid Roaming Networks," 2010 International Journal of Computer Applications, vol. 1, 2010.
[6] J. Nzouonta, et al., "VANET Routing on City Roads using Real-Time Vehicular Traffic Information," 2008.
[7] S. Medjiah, et al., "AGEM: adaptive greedy-compass energy-aware multipath routing protocol for WMSNs," presented at the the 7th IEEE conference on Consumer communications and networking conference 2010.
[8] S. Sharma and D. R. Gupta, "Simulation Study of Blackhole Attack in the Mobile Ad hoc Networks," presented at the International Conference on Network Applications, Protocols and Services 2008.

[9] H. Hasbullah, et al., "Denial of Service (DOS) Attack and Its Possible Solutions in VANET" World Academy of Science, Engineering and Technology, 2010.
[10] Manveen Singh Chadha, Rambir Joon and Sandeep, "Simulation and Comparison of AODV, DSR and AOMDV Routing Protocols in MANETs", "International Journal of Soft Computing and Engineering", IJSCE, July 2012.
[11] Preeti Nagrath and Bhawna Gupta, "Wormhole Attacks in Wireless Adhoc Networks and their Counter Measurements: A Survey", IEEE, 2011.
[12] Abhijit Das, Soumya Sankar Basu and Atal Chaudhuri, "A Novel Security Scheme for Wireless Adhoc Network", IEEE, 2011.
[13] Gilles Guette and Bertrand Ducourthial, "On the Sybil attack detection in VANET", IEEE, 2007.
[14] Farzad Sabahi, "The Security of Vehicular Adhoc Networks", "Third International Conference on Computational Intelligence, Communication Systems and Networks", IEEE, 2011.

Vasu Sharma is a student of M.Tech CSE (Part-Time) pursuing final year of his Post-Graduation from Shaheed Bhagat Singh State Technical Campus (SBSSTC) Ferozepur.
Pawan Luthra is an Assistant Professor in department of CSE at Shaheed Bhagat Singh State Technical Campus Ferozepur. He has 11 years of experience in Teaching, Guiding and mentoring the students in various fields of Computer Science.
Gagandeep is an Assistant Professor in department of CSE at Shaheed Bhagat Singh State Technical Campus Ferozepur. He has 5 years of experience in Teaching and guiding students in Wireless Network Security.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY