Wi-Fi Protected Access Using Packet Filtering Method To Optimized the Delay Factor

Jaspreet Kaur[1], Amanpreet Singh Dhanoa[2]
[1]M.Tech (Scholar), [2]Assistant Professor
Department of University School of Engineering Technology, Rayat Bahra University, Mohali (Punjab)

Abstract **-** Wi-Fi innovation controls most home systems, numerous business neighbourhood and open hotspot systems. A few people wrongly name a wide range of remote systems administration as "Wi-Fi" when as a general rule Wi-Fi is only one of the numerous remote advances. Wi-Fi is configured in either of two modes i.e. ad-hoc mode Wi-Fi and infrastructure mode Wi-Fi. Almost all setups use infrastructure mode, where all devices within range can connect and communicate via a centralized wireless access point. Today, there are various gadgets that utilize and adventure remote innovation, enormously improving their utility and the significance of remote innovation. Routing protocols are designed to discover the communication track in between the transmitter and receiver. These are necessary and play the crucial role in a performance of the network. Routing protocols are the standards to authorize the nodes to decide a manner in which packet is transmitted among the devices in the network. A channel access controls depends on a multiplexing technique that permits a few information streams or flags to have a similar correspondence channel or physical medium. In this unique circumstance, multiplexing is given by the physical layer. Packet Filtering is the way toward passing or blocking parcels at a system interface in view of source and goal locations, ports or conventions. The procedure is utilized as a part of conjunction with bundle ravaging and Network Address Translation (NAT). It's a frequent part of a firewall program for shielding a neighbourhood organize from undesirable interruption. The main issues are fundamental needs that wireless network procedures should be further planned and modified to improve their communication efficiency. When the high rate is selected, the growth in retries also increases, which deals with higher consumption and utilization which lowers signal to noise ratio which increases the noisy environment. As a result of which the available time, capacity and throughput decrease. To implement the effective filtering of redundant packets approach to decrease the end delay, collision rates in wireless networks. To compare the proposed approach with the base approach and to evaluate the lifetime of the network.

Keywords- Wi-Fi Access Control, Packet Filtering, Network Address Translation and Channel Access.

I. INTRODUCTION

Wireless networks enable individuals to cooperate with email or peruse the Internet from an area that they lean toward. Remote systems utilize radio waves to interface gadgets, for example, workstations to the Internet, the business system and applications. At the point when workstations are associated with Wi-Fi problem areas in broad daylight puts, the association is set up to that business' remote system [1]. Various remote correspondence frameworks exist, however a recognizing quality of a remote system is that correspondence happens between PC gadgets. These gadgets incorporate individual advanced colleagues (PDAs), workstations, (PCs), servers, and printers. PC gadgets have processors, memory, and a methods for interfacing with a specific sort of system. Customary PDAs don't fall inside the meaning of a PC gadget; be that as it may, fresher telephones and even sound headsets are starting to join processing force and system connectors. In near future, all hardware will offer remote system associations [2]. Wi-Fi has emerged as the popular wireless network protocol of 21st century [3]. While different remote conventions work better in specific circumstances, Wi-Fi innovation controls most home systems, numerous business neighbourhood and open hotspot systems. A few people wrongly name a wide range of remote systems administration as "Wi-Fi" when as a general rule Wi-Fi is only one of numerous remote advances. The Wi-Fi Alliance is an association made up of driving remote hardware and programming suppliers with a mission of confirming every one of the 802.11-based items for interoperability and advancing the term Wi-Fi as the worldwide brand name [4]. As indicated by the insights made by Wi-Fi Alliance, in January 2016 around 12 billion Wi-Fi units have been delivered and conveyed in homes, workplaces, structures, processing plants, et cetera. Therefore, Wi-Fi has turned out to be a standout amongst the most productive advancements around the globe.

Table 1 . Comparison between Wireless Networks

Type	Range	Applications	Standards
Personal area network (PAN)	Within reach of a person	Cable replacement for peripherals	Bluetooth, ZigBee, NFC
Local area network (LAN)	Within a building or campus	Wireless extension of wired network	IEEE 802.11 (WiFi)
Metropolitan area network (MAN)	Within a city	Wireless inter-network connectivity	IEEE 802.15 (WiMAX)
Wide area network (WAN)	Worldwide	Wireless network access	Cellular (UMTS, LTE, etc.)[5]

II. RELATED WORK

LiFeng, at al., (2016) [6] proposed a model to identify the impact of settled delay on collision possibility, output and MAC delay. In wireless CPS, increased number of sensor are installed to transmit huge data, which need further amendments to enhance communication efficiency. The DCA (Delayed Channel Access) protocol is practically important to improvise channel utilization. Enhanced version of IEEE 802.11 DCF is DCA protocol, in which a node initially waits for additional delay before entering DCF's normal procedure. That additional delay influenced the execution of DCA, which was never investigated theoretically. They executed asymptotic analysis which can increase system output by calculating optimal deterministic delay. The performance of system is remarkably influenced with the connection among number of nodes and deterministic delay. Considerable NS2 simulations proves that suggested model is accurate and can achieve maximum throughput and beneficial for creating and executing the packet aggregation technology adopted by IEEE wireless standards that includes 802.11n and the latest 802.11ac. **Wenchao Xu et al., (2016) [7]** proposed an analytical model as per Markov Chain to essay the reliance of delay on several factors consists of radio network conditions, amount of vehicles that access AP services and recruited validation appliance like: WPA-2 prior shared key and WPA2-802.1X modes. Demand of in vehicle internet applications was increased with the provision of profitable and high performance Wi-Fi access to vehicle drivers. A user has to wait for specific time before accessing internet via Wi-Fi access points on road, until authentication and assignment of accurate parameters. They investigated that access delay is critical in vehicular environment, because bigger the delay, lesser the duration of internet connectivity on road Wi-Fi access point especially high speed vehicles. Simulated results spotlight the accuracy of proposed model. Results furnish useful specifications for creation of suitable network access methods in a vehicular environment. **Omar Nakhila, et al., (2016) [8]** presented a real-time client side detection model to detect ETA (evil twin attack) while the attacker counts on LAP for detection of WC data to internet. Free access Wi-Fi service is complimentarily offered by coffee shops, airports, etc. These free accesses are basically insecure where attacker can deceive the wireless system very easily by setting up RAP (rouge access point) and imitating LAP (legitimate access point). Due to which the wireless connection become easy target for data traffic snooping. The WC can recognize ETA by checking different Wi-Fi diverts in an irregular request searching for particular information bundles sent by a committed separate on the Internet. Once an ETA is distinguished, our plan can obviously recognize whether a particular AP is a LAP or a RAP. The accuracy of proposed recognition strategy was numerically displayed, and evaluated, all things considered, condition with a discovery rate approximates to 100%. **A.K.M. Nazmus Sakib, et al., (2012) [9]** presented suggestions to improvise WPA2 (Wi-Fi Protected Access 2) protocol. WPA and WPA2 is a confirmation program created by the Wi-Fi Alliance to show consistence with the security convention made by the Wi-Fi Alliance to secure remote systems. The Alliance characterized the convention in light of a few shortcomings specialists had found in the past framework: Wired Equivalent Privacy (WEP). Many advanced validation and encryption systems have been inserted into WPA2 yet despite everything it confronting a considerable measure of testing circumstances. In this paper we examine the advantage of WPA2, its defencelessness and shortcoming. **Miss.Prastavana, et al., (2016) [10]** discussed the technical needs and threats to remote system and stay away from such dangers utilizing the WPA2 convention used to secure correspondences in Wireless Networks over past conventions. In recent times we've immense improvement of remote innovation and getting more subjects. The security traditions proposed for the wired framework can't be extrapolated to remote frameworks. Programmers and interlopers can make usage of the escape clauses of the remote correspondence. They characterizes the distinctive remote security threats to remote framework and traditions at introduce available like wired proportionate security (WEP), Wi-Fi ensured access(WPA) and Wi-Fi secured access2 (WPA2) . WPA2 is greater security tradition when contrasted with Wi-Fi ensured get to (WPA) it uses the Advanced Encryption standard (AES) encryption. So as to dispose of dangers and to enhance security of remote system and discussed the available modes to secure a wireless network using the WPA2 protocol and finally explored its vulnerabilities.

III. CONFIGURATION AND ISSUES OF WI-FI

Wi-Fi is configured in either of two modes i.e. ad-hoc mode Wi-Fi and infrastructure mode Wi-Fi. Almost all setups use infrastructure mode, where all devices within range can connect and communicate via centralized wireless access point. Whereas in ad-hoc Wi-Fi, devices connected to each other directly without access point [11].

- ***Wi-Fi Hardware:*** Remote broadband switches generally used as part of home systems serve with different capacities as Wi-Fi to focus. Additionally, open Wi-Fi hotspots use minimum one access. Little Wi-Fi radios and receiving wires are installed inside cell phones, workstations, printers, and other devices enabling them to work as system.
- ***Wi-Fi Hotspots:*** Hotspots are an infrastructure mode designed for public access. Hotspots access point uses particular software to manage users and their authorizations.
- ***Wi-Fi Network protocols:*** Wi-Fi comprises of data link layer protocol that keeps running over any diverse physical later (PHY) joins. The information layer underpins a unique MAC protocol that utilizations impact evasion methods (CSMA/CA) to deal with numerous customers on system. Wi-Fi supports the idea of stations like TV's. Every Wi-Fi channel uses a

particular recurrence extends inside the bigger flag groups (2.4 GHz or 5 GHz). This permits neighbourhood organizes in close physical closeness to convey without meddling with each other.

No innovation is immaculate; Wi-Fi also has its own restrictions. Common issues faced with Wi-Fi networks consist of:

- ***Security:*** Network activity sent crosswise over Wi-Fi systems goes through outdoors making it inclined to snooping from noxious outsiders. A few sorts of security innovation have been added to Wi-Fi throughout the years to help address this issue, albeit some work superior to others. Progressively - Introduction to Wi-Fi Network Security
- ***Health concerns:*** Some individuals assert that broad presentation to remote radio signs like those from Wi-Fi systems cause cerebral pains, queasiness and other physical issues. Numerous industry specialists guarantee general society that Wi-Fi is protected, yet contention holds on as cases one way or the other are hard to demonstrate.
- ***Signal range:*** An essential Wi-Fi coordinate with one remote access point comes to at most just a couple of hundred feet (100m or less) toward any path. Growing the scope of a Wi-Fi organize requires introducing extra access directs designed toward speak with each other, which winds up plainly costly and hard to help, particularly outside. Similarly as with different remote conventions, flag impedance can bring down the viable scope of Wi-Fi and its general unwavering quality.

IV. PROPOSED METHODS

Packet Filtering is a firewall system used to control organizes access by checking active and approaching bundles and enabling them to pass or stop in light of the source and goal Internet Protocol (IP) locations, conventions and ports. System layer firewalls characterize parcel sifting guideline sets, which give profoundly proficient security components. It's otherwise called static filtering.

Packet Filtering is the way toward passing or blocking parcels at a system interface in view of source and goal locations, ports or conventions. The procedure is utilized as a part of conjunction with bundle ravaging and Network Address Translation (NAT). It's frequent part of a firewall program for shielding a neighbourhood organize from undesirable interruption.

Packet filtering lets you control (allow or disallow) data transfer based on:

- The address from which the data is (supposedly) coming from.
- The address to which the data is going to.
- The session and application protocols being used to transfer the data [12].

Packet Filtering has various advantages:

- Just one strategically setup router can protect an entire network, regardless of size of a site.
- It doesn't need user practical knowledge or cooperation from client machine.
- Packet filtering abilities are available in several software and hardware routing commodities available.

Table 2: Routing Protocols are compared [16] as:

Features	Reactive	Proactive	Hybrid
Routing Structure	Mostly Flat	Both Flat & Hierarchical	Hierarchical
Route Acquisition	On demand	Table driven	Combination of both
Routing Overhead	Low	High	Medium
Latency	High due to flooding	Low due to routing tables	Inside zone, Low outside similar to reactive protocols
Scalability	Not suitable for large networks	Low	Designed for large networks
Routing information	Available when required	Always available	Combination of both
Periodic Updates	Not needed	Yes whenever the topology of the network changes	Yes
Mobility	Route Maintenance	Periodic updates	Combination of both
Storage Requirement	Low	High	Medium
Bandwidth Requirement	Low	High	Medium

V. SIMULATION RESULT ANALYSIS

As the number of sensors being deployed upsurges, more data will be conveyed over wireless links. This fundamentally needs that wireless network procedures should be further planned and modified to improve their communication efficiency.

The objectives are:

1. To study the basic concepts of wireless networks and the consequences of multipath hoping in wireless communications.
2. To implement the network deployment scenario and an efficient routing in wireless channel networks.
3. To implement the effective filtering of redundant packets approach to decrease the end delay, collision rates in wireless networks.
4. To compare the proposed approach with the base approach to evaluate the lifetime of the network.

In this chapter, explained the results in the MATLAB 2016a simulation model used. An implement the wifi-access control with packet filtering approach to enhance the packet delivery rate as well as optimize the time consumption.

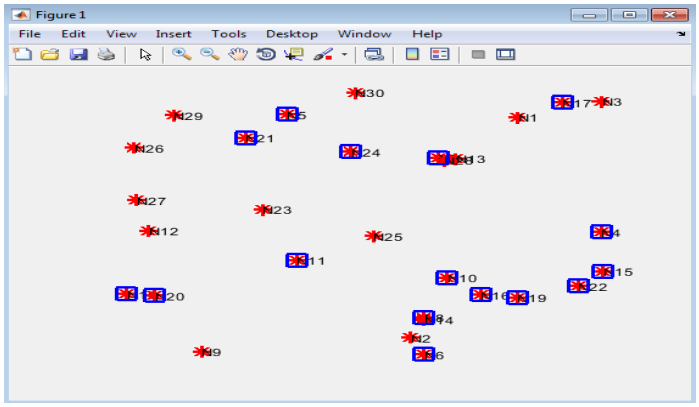

Figure no 1. Node deployment

The above figure shows the nodes deployment in which the netowrk area is defined having 1000 ×1000 meters. In the defined network deployement procedure takes place. The nodes are deployed which communicate packets to the neighbouring nodes and then neighboring nodes fed the tasks or packets to the target locations. In this proposed work three target nodes are considered.

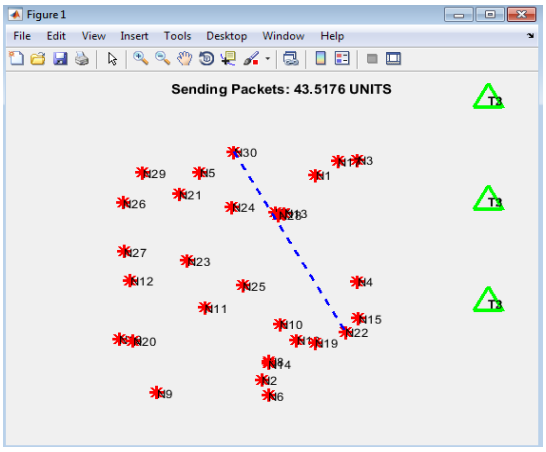

Figure no. 2 Packet Transferring

The above figure shows the tranferring of the packets among the route nodes and it is notices at the top of figure that how much units of the packets are tranferringfrom node id 30 to node id 22 which will further send packets to the target locations and the filteration of the packets are done and then taget locations will note the locations of the filtered packets and the packets units are extracted from that filtered locations.

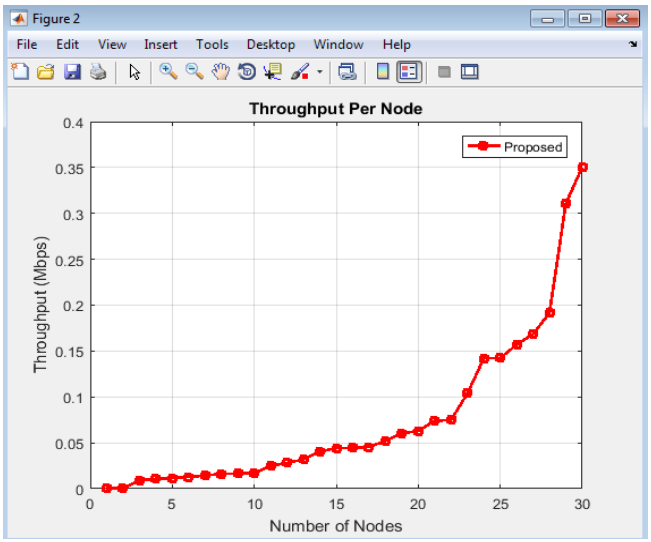

Figure no. 3 Throughput in proposed Work

The above figure shows the throughput per node which shows that the throughput per node is increasing to have high successful delivery of the packets with less delay and error probabilities and less collision rates.

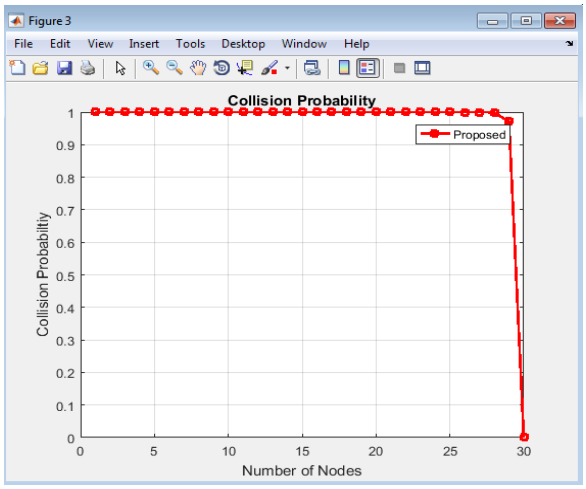

Figure no. 4 Collision Probabilities with Proposed Work

The above figure shows that the collision probability which shows that the collision probability is decreasing in such a manner which increases the lifespan of the network and also reducing the loss and overhead of the packets.

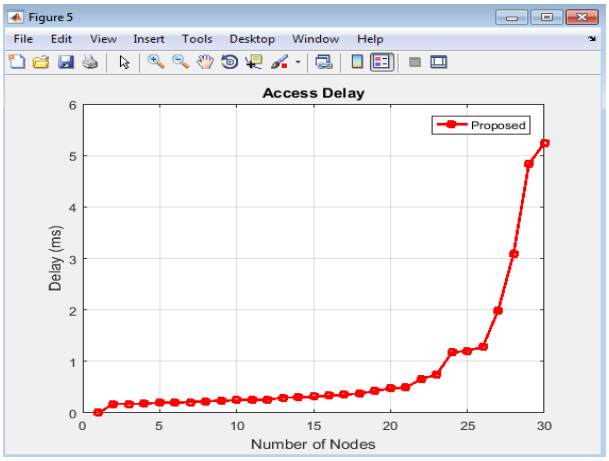

Figure no. 5 Access Delay with Proposed Work

The above figure shows the access delay in milliseconds and shows that our proposed approach is able to achieve less 5.5 ms in delivering of packets to the target locations in successful manner. The end delay must be low for high throughput and less overhead and collisions which increases the security and lifespan of the wireless networks.

Table: 3 Performance Comparisons

Parameters	Base	Proposed
Collision Probability	0.38	0.1
Delay	36 ms	5.5ms
Throughput per node	0.1 mbps	0.35 mbps

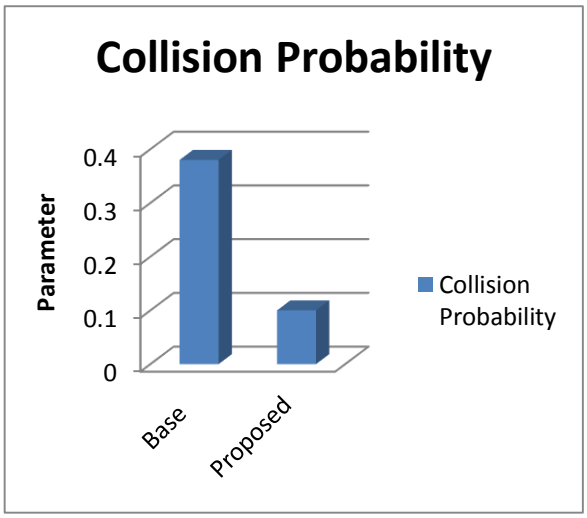

Figure no. 6 Comparison between Proposed and Base Paper (Collision Probability)

The above figure defined that the comparison between proposed and existing work collision probability. In proposed work in collision probability value is 0.1 and existing work in collision probability value is 0.38.

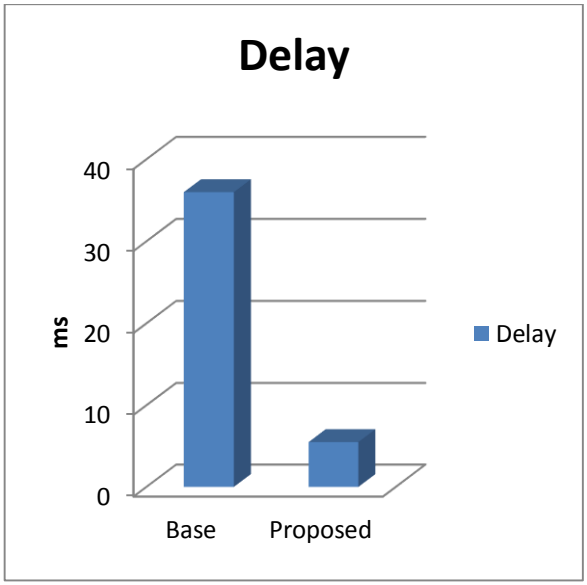

Figure no. 7 Comparison between Proposed and Base Paper (Delay)

The above figure defined that the comparison between proposed and existing work delay. In proposed work in end to end delay value is 5.5 ms and existing work in delay value is 36ms.

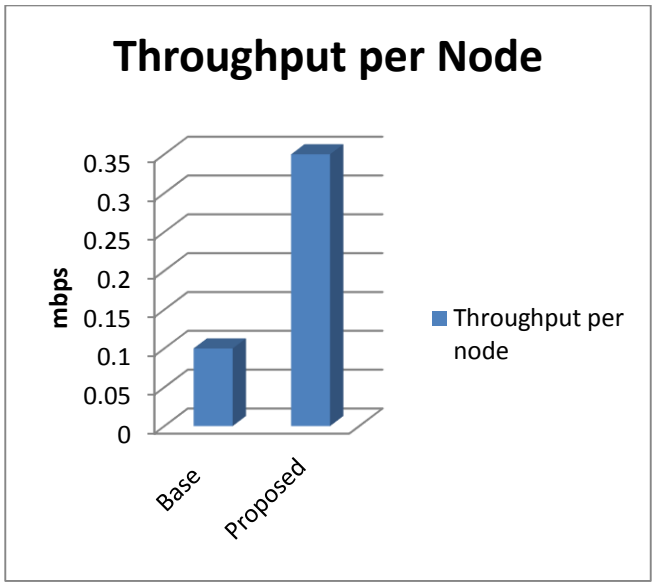

Figure no. 8 Comparison between Proposed and Base Paper (Throughput)

The above figure defined that the comparison between proposed and existing works Throughput. In proposed work in Throughput value is 0.35 mbps and existing work in delay value is 0.1mbps.

VI. CONCLUSION AND FUTURE SCOPE

With more and more data being transmitted in wireless cyber-physical systems, wireless network protocols should be further studied and amended to improve their transmission efficiency, throughput, and delay and collision probability. The main issues are fundamental needs that wireless network procedures should be further planned and modified to improve their communication efficiency. When high rate is selected, the growth in retries also increases, which deals with higher consumption and utilization which lowers signal to noise ratio which increases the noisy environment. As a result of which the available time, capacity and throughput decreases. The filteration approach deals with the filteration of authentic packets which are useful for our system. In filtertion process we have used secrete servlet ids and secrete servlet packet threshold. If the servelet packets are less than threshold limit which is configured to the centralized unit that will tell us the packet location in which the packets are transferring and that will be send to the target location by the secrete servlet. In this research work, to evaluate the routing scenario of the users with the access points and then evaluate the routing performance in terms of the overage area scenario. The number of packet losses increases then we will perform the scheduling approach in which the load balancing will be done and the execution of the requests will be achieved in the rapid manner.

The future work, we will develop an intelligent channel selection for MMAC-HR so that the network load is balanced over multiple channels, thereby enhancing the network performance.

REFERENCES

[1] Ho, Quang-Dung, Daniel Tweed, and Tho Le-Ngoc. "IEEE 802.11/Wi-Fi Medium Access Control: An Overview." In Long Term Evolution in Unlicensed Bands, pp. 31-41. Springer International Publishing, 2017.

[2] Kumar, G. Vijaya, Y. Vasudeva Reddyr, and Dr M. Nagendra. "Current research work on routing protocols for NETWORK: a literature survey." international Journal on computer Science and Engineering 2, no. 03 (2010): 706-713.

[3] Gupta, Parul. "A Litrature Survey of NETWORK." International Research Journal of Engineering and Technology 3, no. 02 (2016).

[4] Dhenakaran, Dr SS, and A. Parvathavarthini. "An overview of routing protocols in mobile ad-hoc network." International Journal of Advanced Research in Computer Science and Software Engineering 3, no. 2 (2013).

[5] Clausen, Thomas, and Philippe Jacquet. Optimized link state routing protocol (OLSR). No. RFC 3626. 2003.

[6] Murthy, Shree, and Jose Joaquin Garcia-Luna-Aceves. "An efficient routing protocol for wireless networks." Mobile Networks and applications 1, no. 2 (1996): 183-197.

[7] Feng, Li, Jiguo Yu, Xiuzhen Cheng, and Shengling Wang. "Analysis and optimization of delayed channel access for wireless cyber-physical systems." EURASIP Journal on Wireless Communications and Networking 2016, no. 1 (2016): 60.

[8] Wenchao Xu , Hassan Aboubakr Omar , Weihua Zhuang , Fellow, IEEE, and Xuemin (Sherman) Shen , Fellow, IEEE "Delay Analysis of In-Vehicle Internet Access Via On-Road WiFi Access Points", 2169-3536 (c) 2016 IEEE.

[9] Nakhila, Omar, and Cliff Zou. "User-side wi-fi evil twin attack detection using random wireless channel monitoring." In Military Communications Conference, MILCOM 2016-2016 IEEE, pp. 1243-1248. IEEE, 2016.

[10] A.K.M. Nazmus Sakib,Shamim Ahmed, Samiur Rahman, Ishtiaque Mahmud & Md.Habibullah Belali"WPA 2 (Wi-Fi Protected Access 2) Security Enhancement: Analysis & Improvement", Volume 12 Issue 6 Version 1.0 March 2012.

[11] Prastavana, Suraiya Praveen, and P. R. A. V. E. E. N. Suraiya. "Wireless Security Using Wi-Fi Protected Access 2 (WPA2)." International Journal of Scientific Engineering and Applied Science (IJSEAS)-ISSN (2016): 2395-3470.

[12] Selim, Gamal, Hesham M. El Badawy, and M. Abdul Salam. "New protocol design for wireless networks security." In Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference, vol. 1, pp. 4-pp. IEEE, 2006.

[13] Sobh, Tarek S. "Wi-Fi networks security and accessing control." International Journal of Computer Network and Information Security 5, no. 7 (2013): 9.