5G Network: Attacks on vehicular adhoc network and mitigation

Presented by Muhammad Ishfaq REG\_num:220328

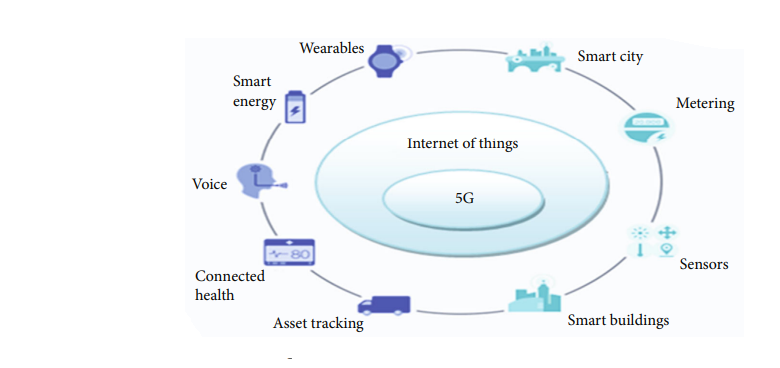
**Abstract:**

5g technologies have been launched for some time now, but the new technology has also become a new way for malicious people to attack the users. THESE people are just common people in real life but are legends in Virtual world. 3GPP standards are developed [1] for connecting previous 3G or 4G technology with 5G networks. This has made users life very easy now users have deployed IOT devices for their security. These Devices are SMART home appliances, user’s vehicles, and other smart gadgets. In this paper we have researched upon user’s vehicles and 5G network connectivity, their common issues and attacks that can be made by malicious people. We will propose a solution using machine learning and other ways to control these attacks .OUR proposed solution will help user’s to overcome these attacks and it will ensure robust security as well as users USERS software protection. AS we know software defined network service is the main part of 5G network. Attacker is always trying to find a way to enter to rob off user & to affect profits obtained by the users.

**INTRODUCTION :**

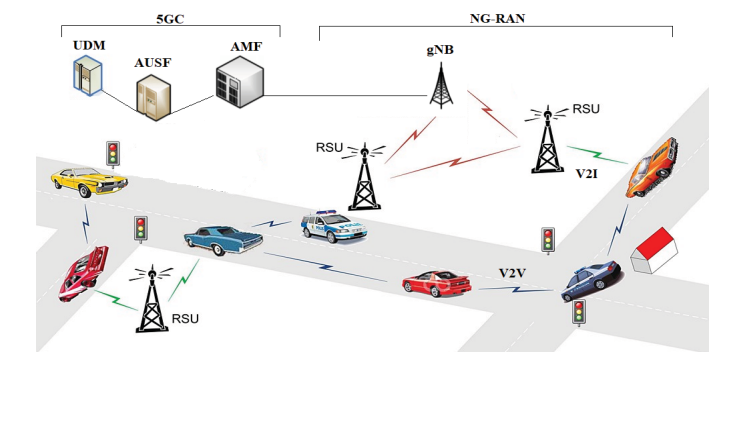
ADVANCEMENT in technology is the only way of developing our societies. Today every single person in a society has a smart phone .this smart phone is a very good technology, we can use this tech to monitor our different appliances. Smart vehicles are being introduced in societies just to make our life easy. BUT this easy way of life has too many problems.AS old machines were costly but did not have any scenarios for privacy protection .They were simple & required 0 or no application for usage . But today every smart vehicle also has a mobile application by which we can monitor our vehicles route and even drive them. Application’s are very easy to use and are more vulnerable to attacks. ATTACKERS are of two types 1)attacker who just need to impress user & 2)those who want some ransom or other intentions. First type of attacker only want user to know that they have been hijacked but 2’nd type malicious people only want to hurt the target by demanding ransom .

In today’s world Cyber-Security is the main and most important form of security. Today everyone is using smart appliances and these appliances have become more and more important as network has evolved from simple wired network to wireless networks. Long ago when we were using wired networks we used to prevent malicious people by using firewalls .firewall might be old but it is still a very good way to prevent attacks.

FIGURE 1 :relation b/w 5G and IOT

During past few years advancement in AI(artificial ) has led to development of societies, but it also paved way for attackers. Today everything is connected with internet .

NETWORK ARCHITECTURE:FIGURE 2 shows a network architecture between vehicles and 5G network.there are 2 types of communications.road and vehicles are both connected with wireless communication devices known as on boards



THESE on-boards are connected with internet and thus they can communicate in this way over the internet in background & will notify users if aany thing was about to happen

1)vehicle to vehicle :THIS is a 2 way communication in which user can communicate with other vehicles like they can easily get info about type of vehicle ,distance of vehicle, speed of vehicle and get info about how much traffic is running on certain route.

2)vehicles to ON-boards:On-boards are actually wireless communication devices that are installed on vehicles . their main purpose is to let vehicles connect with internet so that they can communicate with other devices accordingly.

PROBLEMS TO BE DISCUSSED IN THIS PAPER: The vehicle network can also be attacked like MITM(man in the middle) this means that attacker stops the services of the vender and client cannot attain his /her services, Redirectional attack means that destination of client is compromised and sometimes their rout towards destination is changed so that they can be extra CHARGED OR they can be robbed off. Sign change attack means signs that are along side of the road are changed for to create the chaos among peoples figure 4 shows how sign change can effect normal users and public.



FIGURE4 :SIGN CHANGE ON ROAD SIDE

PROPOSED SOLUTION: Machine learning is an easy way to deal with these kind of problems . We can use network slicing technique provided by researchers to over come these issues[5]. According to researchers the devices now support 5g network communication but their authentication mechanism is very low , and they do not address any standards for 5g network authentication. WHEN research was made for the authentication of the 5G network only integrated techniques were proposed for them by authors[6]. The latter author proposed the first 5G-AKA MODEL [7].ACCORDIG TO THIS MODEL WE need to authenticate our systems with Access control list to communicate . To over come MITM we need to make our network secure as a shell. This can be easily done by using secure network connection and vpn.

We can optimize our sdn controller because it is the main point for the attacks , This can be achieved by machine learning and using cross slice authentication ,the author proved in his search that this can help us prevent ddos attack on the network and thus by teaching data set (NSKLDD DATA SET) SHOWED 99% ACCURACY [8] the XGBOOST algo dose have high accuracy so we can use it to train our system.OUR system under testing phase provided 99% detection of attacks and notified user in time.

SECURED network connection means that user and vendor must have an agreement ,when connection is established using that isp provider that isp provider must not share credentials with outsiders.

Mitigation for redirectional attacks: To prevent redirectional attack authenticated user must have the privileges to control his route. The admin should only give best route option where as the destination and the route must be the choice of user. The administrator and traffic along the route must be true in case of error re-authenticate with network.

CONCLUSION: WE have provided some tricks that can help user to resolve his/her privacy and integrity of the software. MITM is happen upon negligence of users .TO get free internet access users simply connect themselves with rouge routers. THIS in return lead them to become vulnerable to many attacks and data theft.REDIRECTIONAL attackis only possible when we use free internet ,If we use our proposed solution they can prevent users from those attacks And notify user in time.

FUTURE work: ALTHOUGH our system is very best but every best thing has some things left behind.IN future we can teach our sys dynamic threshold attacks as our system doesnot detect attacks made by dynamic threshold.SO new researcher can do research and make system more protective.

**REFERENCES:**

**[1]:** [**https://www.ijcaonline.org/archives/volume174/number14/alamri-2021-ijca-921027.pdf**](https://www.ijcaonline.org/archives/volume174/number14/alamri-2021-ijca-921027.pdf)

**[2]:** **https://aginginplace.org/technology-in-our-life-today-and-how-it-has-changed/**

**[3]:** Y. Bengio, “Learning Deep Architectures for AI,” Found. Trends Mach. Learn Foundations and Trends® in Machine Learning, vol. 2, no. 1, pp. 1–127, 2009.

**[4]:** [**https://link.springer.com/chapter/10.1007/978-3-030-27192-3\_11**](https://link.springer.com/chapter/10.1007/978-3-030-27192-3_11)

**[5]:** [**https://ieeexplore.ieee.org/document/8597639**](https://ieeexplore.ieee.org/document/8597639)

**[6]:** [**https://dl.acm.org/doi/abs/10.1109/TNSM.2021.3052208**](https://dl.acm.org/doi/abs/10.1109/TNSM.2021.3052208)

**[7]:** D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, “A formal analysis of 5G authentication,” in Proc. ACM SIGSAC Conf. Comput. Commun. Security, 2018, pp. 1383–1396.

**[8]**: <https://www.ijcaonline.org/archives/volume174/number14/31744-2021921027>