Journal of Engg. Research Vol. 11 No.(1A) pp.126-132 **DOI:10.36909/jer.11881**

An intelligent transportation system for forecasting wireless communication network issues with cyber attacks

M. Khaleel Ullah Khan*

Research scholar, ECE Department, K L University, Vaddeswaram, Guntur, A.P, India.

Corresponding Author: mkkcr9@gmail.com

Submitted: 04-10-2020

Revised: 25-10-2021

Accepted: 06-11-2021

ABSTRACT

This paper proposes a method to design an "Intelligent Transportation System" for forecasting wireless communication network issues with cyber attacks. wireless communication networks(WCN) is a broadly classified and critical gateway for any communication devices because the wireless communication networks is operated at various frequency ranges in different locations. In order to maintain its performance and also to prevent any attacks due to its high data handling, we need an Intelligent transportation system (ITS) to analyse and detect the cyber-attacks before going to implement it in real time transportation. In general wireless communication networks is an IEEE 802.11 standard which can be operated at physical Transfer control protocol/Internet protocol(TCP/IP) layer as well OSI model. In this paper a novel approach to design, analyse and detect cyber-attacks is proposed for wireless communication networks transport system, called Intelligent transportation system (ITS) based cyber-attack detection. Stacked firewall system is used for reducing fake attacks and detecting real time attacks in transportation system. Hence any fake attacks or real time attacks captured by the ITS will be informed to the system controller to make decision to whether it is a false-positive or real attack. ITS is the main process of the stacked firewall system which in turn take responsible to control, maintain, and prevent any cyber-attack.

Keywords: Communication: Cyber-attack: Intelligent systems: Networks: Transport: Wireless.

INTRODUCTION

With the origination of keen city changing urban areas into advanced social orders, making the life of its resident simple in each aspect, ITS turns into the imperative segment among all. In any city portability is a main thing; be it going to school, class and office or for some other reason residents use transport system to go inside the city. Utilizing residents with an ITS (Intelligent Transport System) can extra their time and create the city like very brilliant. ITS plans to achieve traffic effectiveness by restrictive traffic problems. It improves clients with earlier data about traffic, neighbourhood comfort ongoing running data, and seat accessibility and so on which decreases travel season of employees as updates their safety and comfort. The usage of 'ITS' is mostly recognized with used in many countries nowadays. The usage is not just limited to data and gridlock control, however also for road security and actual foundation usage. Due to its unlimited prospects, ITS has now become a multidisciplinary conjunctive field of work and consequently numerous associations around the globe have created answers for giving ITS applications to address the issue. Intelligent Transport System gives normal data to the everyday suburbanites about open transports, timings, seat accessibility, the flow area of the transport, time taken to arrive at a specific objective, next area of the transport and the thickness of travelers inside the transport. A proposed intelligent transportation system is shown in figure 1. Transport administrators in the city have the sensors in their transports. Thus, if the transport will be right on time to the following bus station the transport is incidentally and marginally is eased back down at the red light minimal longer than it ought to be to ensure the transport is on schedule and don't ahead of the timetable". The system has been planned so cleverly that travelers and even drivers are uninformed of the postponement as they are almost no deferrals.

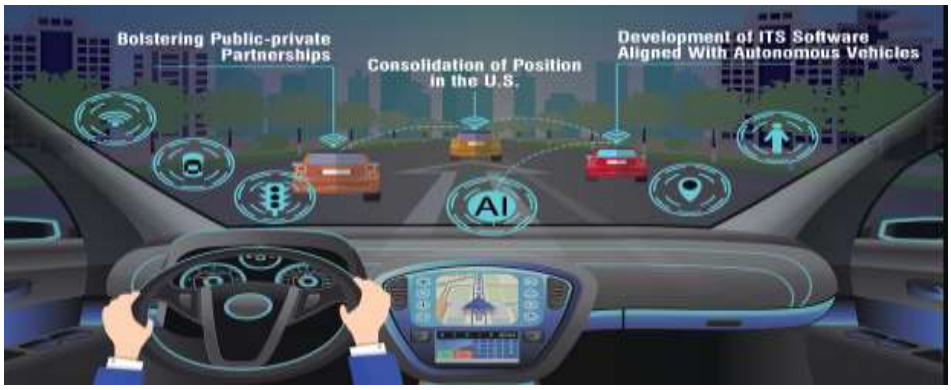

Figure 1. Intelligent transportation system

Wireless Communication Networks

Wireless communication includes the transmission of data over a separation without the assistance of wires, links or some other types of electrical channels. Wireless communication is a broad term that consolidates all techniques and types of associating and imparting between at least two gadgets utilizing a wireless sign through wireless communication advancements and gadgets. The development of wireless innovation has carried numerous advancements with its viable highlights. The sent separation can be anyplace between a couple of meters (for instance, a TV's controller) and a great many kilometers (for instance, radio communication). Wireless communication can be utilized for cell communication, wireless admittance to the internet, wireless home networking, etc. Different instances of sterilizations of radio wireless innovation incorporate GPS units, carport entryway openers, wireless PC mice, consoles and headsets, headphones, radio beneficiaries, satellite TV, broadcast TV and cordless phones. Wireless communication includes move of data with no physical association between at least two focuses. In view of this nonattendance of any physical foundation, wireless communication has certain advantages. This would frequently incorporate crumbling separation or space. Wired communication involves the utilization of association wires. In wireless networks, communication does not need expound physical foundation or upkeep rehearses. Thus the expense is diminished. Any organization giving wireless communication administrations does not acquire a ton of expenses, and therefore, it can accuse efficiently of respect to its client charges. Wireless communication empowers individuals to convey paying little heed to their area. It is not important to be in an office or some pay phone so as to pass and get messages. Diggers in the outback can depend on satellite telephones to call their friends and family, and accordingly, help improve their overall government assistance by keeping them in contact with the individuals who mean the most to them. Wireless communication gadgets like mobile telephones are very basic and along these lines permit anybody to utilize them, any place they might be. There is no compelling reason to genuinely associate anything so as to get or pass messages. Wireless communications administrations can likewise be found in Internet advances, for example, Wi-Fi. With no network links hampering development, we would now be able to interface with nearly anybody, anyplace, whenever.

Cyber-Attacks

WCN access used to be something you had to pay for, yet now free WCN is something numerous individuals underestimate. Guests to an inn, coffeehouse, bar, retail outlet, or café now expect WCN to be without given of charge. The choice to utilize a specific foundation is regularly affected by whether free WCN is accessible, however progressively the nature of the association is a factor in the choice cycle. The nature of the WCN on offer isn't only an issue of there being sufficient transfer speed and quick internet speeds. Guardians frequently decide to visit foundations that furnish secure WCN with content control, for example, organizations that have been confirmed under the Friendly WCN conspire. So as to be licensed under the plan, organizations more likely than not actualized suitable sifting controls to guarantee minors are kept from getting to age-wrong material. The gigantic ascent in cyber-attacks through open WCN networks and admonitions about WCN chances in the traditional press have seen numerous shoppers decide to visit foundations that offer secure WCN access. On the off chance that you maintain a business and are giving WCN to clients or on the off chance that you are thinking about adding a WCN hotspot to draw in more clients, make certain to think about the security of the network. The recent years have seen numerous attacks on WCN

networks and clients who utilize those wireless administration. The expansion in WLAN attacks implies WCN security has never been so significant. Before covering probably, the most widely recognized wireless attacks, it is beneficial investigating a portion of the regular wireless weaknesses that can be misused to listen in on traffic, taint clients with malware, and take delicate data. Recorded underneath are probably the most widely recognized wireless network weaknesses and steps that can be taken to keep the weaknesses from being abused. These wireless network weaknesses could undoubtedly be misused in certifiable attacks on wireless networks to take touchy information, assume responsibility for a switch or associated gadget, or introduce malware or ransom ware. WCN passages are dispatched with a default SSID and secret key which should be changed, yet very frequently, those default passwords are left set up. That makes it simple for an attacker to login and assume responsibility for the switch, change settings or firmware, load malignant contents, or even change the DNS worker so all traffic is coordinated to an IP possessed by the attacker. Default passwords must be changed to forestall anybody inside scope of the sign from interfacing and sniffing traffic. In the event that wireless regulators are utilized to oversee WCN passageways by means of web interfaces, ensure the default passwords are additionally changed. These default passwords can be handily discovered on the web and can be utilized to attack wireless networks.

LITERATURE REVIEW

Muhammad Sameer Sheik (2019): Proposed that "Vehicular Ad hoc Networks (VANETs)" are a rising kind of "Mobile Ad hoc Networks (MANETs)" with powerful applications in intelligent rush hour gridlock the executives systems. VANET has drawn huge consideration from the wireless communication research network and has gotten one of the most noticeable exploration fields in "Intelligent Transportation System (ITS)" on account of the possibility to give road wellbeing and careful steps for the drivers and travellers. In this review, we talked about the essential diagram of the VANET from the engineering, communication techniques, guidelines, attributes, and VANET security administrations. Second, we introduced the dangers and attacks and the ongoing cutting edge techniques for the VANET security administrations. At that point, we exhaustively inspected the confirmation plots that can shield vehicular networks from pernicious hubs and phony messages. Third, we talked about the most recent reproduction apparatuses and the exhibition of the validation plans as far as recreation instruments, which was trailed by the VANET applications. In conclusion, we recognized the open exploration challenges and gave future examination headings. In total, this study fills the hole of existing overviews and sums up the most recent exploration improvement. All the security attacks in VANETs and their associated counter-measures are examined as for guaranteeing secure communication. The validation plans and far reaching applications were presented and dissected in detail. In addition, open exploration difficulties and future examination headings were given.

Nishu Gupta (2020): Proposed tha the combination of Vehicular Ad hoc Network (VANET) with the Internet of Things (IoT) leads to the idea of the Internet of Vehicles (IoV). IoV structures a strong spine for Intelligent Transportation Systems (ITS), which prepares for advancements that better clarify about traffic productivity and their administration applications. IoV design is viewed as a major part in various territories, for example, the automobile business, research associations, savvy urban communities and intelligent transportation for different business and logical applications. Be that as it may, as VANET is defenceless against different kinds of security attacks, the IoV structure ought to guarantee security and productive execution for vehicular communications. To address these issues, in this article, a confirmation based convention (A-MAC) for brilliant vehicular communication is proposed alongside a novel structure towards an IoV design model. The plan requires hash tasks and uses cryptographic ideas to move messages between vehicles to keep up the necessary security. Execution assessment helps investigating its quality in withstanding different sorts of security attacks.

PROPOSED METHODOLOGY

In this chapter we are going to implement ITS cyber-attack and false positive detection in the simulated environment called Network Simulator. To simulate the working model of the ITS we are going to use network simulator. NS software consists of all required components in built in to it. We have various alert signal to which it is given to our ITS and output signal from the ITS will be given to the destination or remote vehicle. To implement this solution in to the ITS we have the following settings to make a precise decision under balanced wireless frequency. In general, for ITS design we have various control signal generated by the system will be analysed intelligently for further processing. With respect to the settings we have derived the results in the simulation part. We have been using in built tool boxes available in NS software such as signal processing, control and other systems etc. Our system was

designed as a closed loop system based on the attack control mechanism. The system consists of controllers, alert signals, GPS locations, destination route map, obstacle indicators, emergency indicators etc.

Intelligent Transportation System Building Blocks

System consists of two main block such as ITS block, cyber-attack detection block and other main components such as input signal, output signal, alert designing and interference frequency signal. In the input layer we are going to model input and traffic signal to the system. Based on the inputs stacked firewall system will control the ITS after checking and validating with the cyber-attack rules built in functions. Upon validation the processed input will be given to the ITS to achieve the precision and efficiency in the system ensuring no attack and false positive present.

The below block diagram represents an intelligent transport system for detecting WCN issue due to cyber-attacks. A typical block diagram of the intelligent transportation system is shown on figure 2.

- Prone Device – In non-protected zone prone to be easily attackable.
- Drone Device – To monitor live moments to reduce false positive alerts.
- Remote WCN – End host connection device.
- ITS Hub – Cyber-attack detection and smart transport management.

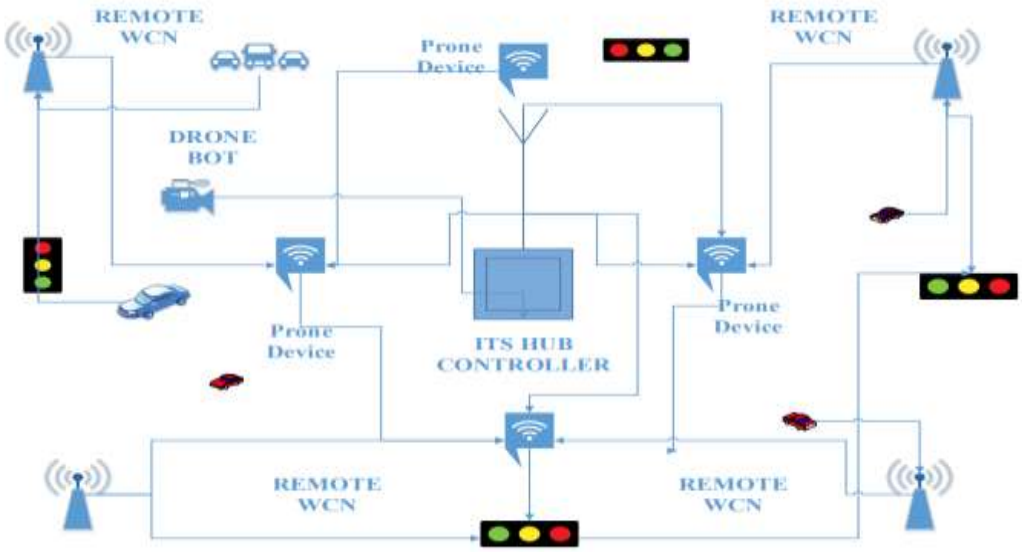

Figure 2. System blocks

Steps Involved in ITS for cyber-attack detection:

Step1: Nodes are sending and receiving data signal from ITS hub.

Step2: ITS hub continuously monitoring the edge WCN for intrusion and malware attacks.

Step3: In node is misbehaving or breaching the ITS rules will lead ITS to generate alert signal. Also ITS hub will parallel checking for drone bot confirmation and stacked firewall testing confirmation. Based on the comparison the node will be quarantined or will be in monitoring mode for some amount of time.

Step4: If cyber-attack identified ITS hub will disconnect the respective edge WCN from other network. Nodes will be handed over to next available WCN for further data processing and transportation control.

Proposed cyber-attack Methods for CIA triangle:

- Confidentiality – Decryption attacks.
- Integrity – Man in the middle attack.
- Availability – DDoS attack.

The above HUB regulator configuration comprises of end host, for example, vehicle, transport, emergency vehicle, traffic light WCN and automation bot. Information layer comprises of two data sources one from drone bot or reconnaissance camera and second info is from have and constrained by our ITS centre point system. The subsequent layer is the preparing layer, this layer have a few defers got from ITS hub during testing. The last layer is the output layer or called as Processed-ITS output layer, in this layer we will test and analyse the consequences of info sign and ITS hub output. To control ITS system utilizing stacked firewall hub procedures, we should assemble input/output getting ready data using examinations or entertainments of the system we have to show. When using stacked multi-vendor triple layer firewall, make or load the data and pass it to the arrangement signal information dispute. While using ITS attack and bogus positive recognition plan, in the Load data portion, select program testing, and subsequently to stack data from a record, select archive to stack data from the network test system workspace, select net sim work environment. As a cycle, stacked firewall testing (SFT) planning capacities admirably if the readiness data is totally illustrative of the features of the data that the readied plan is proposed to illustrate. To decide our readiness data, make a show in the network test system workspace. Each line contains a data point, with the last area containing the output regard and the remainder of the portions containing input caution and crisis signal. We would then have the option to pass this data to the readiness Data input conflict of the Stacked firewall Testing (SFT) ITS attack and bogus positive identification fashioner application. Load the data from an .nsim record. Each line of the record contains a data point with values disconnected by clear territory. The keep going and impetus on each line is the output, and the remainder of the characteristics are the data sources.

EXPERIMENTAL RESULT

A simulation environment is created using network simulator 2.35 simulator and intruder nodes are introduced to attack the in proposed system and Stacked firewall testing (SFT) output file is obtained. The set of components such as controller, ITS, input and output signal etc are evoked. They are initiated first using the NS software components viewer command panel. Once the simulation is completed, the exhibition attributes are seen on the particular extensions. The reaction signals of attack detection, false positive, input and output signal, will be printed here. The below two figures represent the output printed for each blocks of the system design. The figure 3 shows that the output signal from ITS and SFT output respectively. It has been observed that the proposed SFT signal accurately analyse the attacks and false positive. SFT signal and actual ITS signal overlap with each other and hence we can conclude that stacked firewall testing (SFT) detect and analyse the output under predefined conditions.

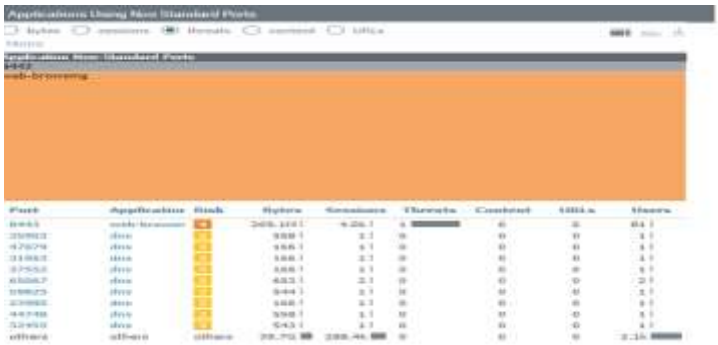

Figure 3. Thread Detection

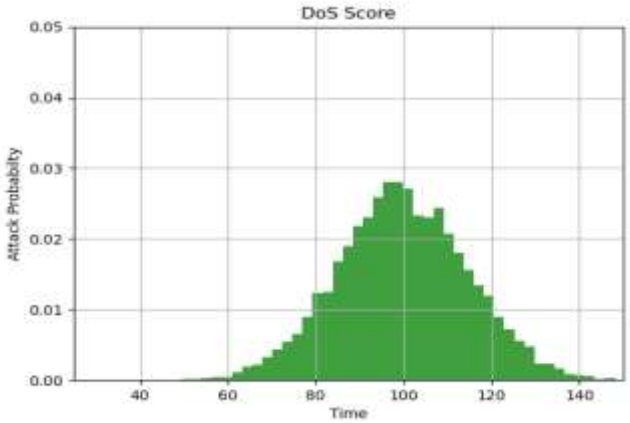

Figure 4. DoS attack probability

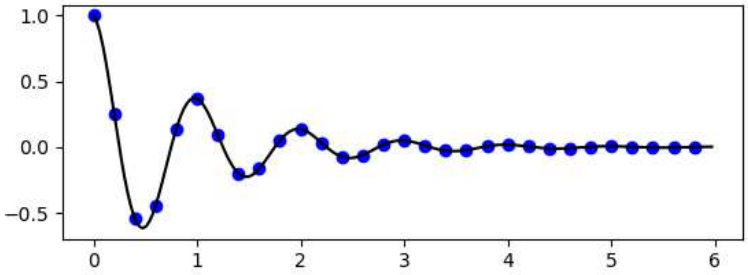

Figure 5. Node compromise vector

The figure 4 represents Denial-of-service attack probability based on the incoming request to the wireless communication networks. Our firewall continuously monitoring for live cyber-attacks for the probability of 0 to 1.

The figure 5 represent node compromise probability based on the behaviour of the nodes. If the node got compromised means it will not be in control with our WCN hub. The figure 6 represents monitoring of connected nodes for all day and time.

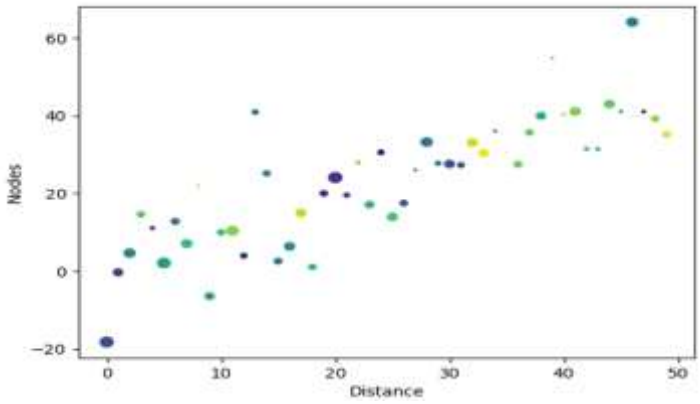

Figure 6. Node attack behaviour

CONCLUSION

In this paper we implemented ITS cyber-attack detection in WCN using Stacked firewall testing (SFT) system to control and stabilize the ITS system to utilize its performance at high level at high data transfer rates. Also we have proved our system capability by simulating and printing the result of SFT process. Here with we have concluded that we have completed our design of stacked firewall testing (SFT) to achieve maximum attack vector detection and false positives. Output from ITS is tested using Stacked firewall testing (SFT). Based on the simulation output we can conclude that our system work better to produces high accuracy and extreme precision in detecting attacks in ITS-WCN. So for each and every false positive signal detected at the output was given as a feedback to our ITS hub controller mechanism. Based on the feedback, controller was able to make decision in finding cyber-attacks in the ITS-WCN at very high data transfer speeds. At last we proved the following capabilities ITS capabilities, Stacked firewall testing (SFT) for false positive and cyber-attack detection.

REFERENCES

Muhammad Sameer Sheikh. 2019 "A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs)" https://doi.org/10.3390/s19163589,1132-1140.

Nishu Gupta 2020 "Authentication-Based Secure Data Dissemination Protocol and Framework for 5G-Enabled VANET" https://doi.org/10.3390/fi12040063,299-308.

Muhammad Arif. 2020 "SDN-based VANETs, Security Attacks, Applications, and Challenges" https://doi.org/10.3390/app10093217. 101-106.

Nidhal, M.; Ben-othman, J.; Hamdi, M. Survey on VANET security challenges and possible cryptographic solutions. Veh. Commun. 2014, 1, 53–66.

Raya, M.; Hubaux, J. Securing vehicular ad hoc networks. J. Comput. Secur. 2007, 15, 39–68.

Biswas, S.; Mišić, J.; Mišić, V. DDoS Attack on WAVE-enabled VANET through Synchronization. In Proceedings of the IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, USA, 2012; pp. 1079–1084.

Hasrouny, H.; Ellatif, A.; Bassil, C.; Laouiti, A. VANet security challenges and solutions: A survey. Veh. Commun. 2017, 7, 7–20.

Dua, A.; Kumar, N.; Bawa, S. A systematic review on routing protocols for Vehicular Ad Hoc Networks. Veh. Commun. 2014, 1, 33–52.

Mohaisen, L.F.; Joiner, L.L. Interference aware bandwidth estimation for load balancing in EMHR-energy based with mobility concerns hybrid routing protocol for VANET-WSN communication. Ad Hoc Netw. 2017, 66, 1–15.

Noor, M.B.M.; Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. Comput. Netw. 2019, 148, 283–294.

Trihinas, D.; Pallis, G.; Dikaiakos, M.D. ADMin: Adaptive monitoring dissemination for the Internet of Things. In Proceedings of the IEEE INFOCOM 2017-IEEE Conference on Computer Communications, Atlanta, GA, USA, 1–4 May 2017., 1127-136.

Trihinas, D.; Pallis, G.; Dikaiakos, M. Low-Cost Adaptive Monitoring Techniques for the Internet of Things. IEEE Trans. Serv. Comput. 2018,89-98.