International Journal of Scientific Research and Modern Education (IJSRME)
International Peer Reviewed - Refereed Research Journal, Website: www.rdmodernresearch.com
Impact Factor: 7.137, ISSN (Online): 2455 - 5630, Volume 9, Issue 1, January - June, 2024

AN OVERVIEW OF SECURITY THREATS AND COUNTERMEASURES IN VEHICULAR AD HOC NETWORKS

Dr. Vikram Singh* & Sitaram**
***** Professor & Dean, DCSE, Chaudhary Devi Lal University, Sirsa, Haryana
****** Research Scholar, Part Time M.Tech., DCSE, Chaudhary Devi Lal University, Sirsa, Haryana

Cite This Article: Dr. Vikram Singh & Sitaram, "An Overview of Security Threats and Countermeasures in Vehicular Ad Hoc Networks", International Journal of Scientific Research and Modern Education, International Peer Reviewed - Refereed Research Journal, Volume 9, Issue 1, January - June, Page Number 47-54, 2024.

Abstract:

Vehicle-based ad hoc networks, or VANETs, are becoming more and more important in automatic transportation systems. Their main goal is to make roads safer and more efficient for movement of traffic. In order to do this, they make it easier for cars and facilities to talk to each other. When it comes to cars, using digital contact adds new risks to the safety of riders. This study looks into both the actions that have been taken to fix the problems that have been brought up and the many security holes that have been caused by VANETs. The poll will start by putting security threats into a lot of different groups. Some of these types of privacy breaches are information leaks, message hacking, denial-of-service attacks, and position privacy breaches. Each class is carefully looked at, with a focus on the ways it could be attacked and the harm these attacks could cause in the VANET setting. The study then gives an overview of the various defenses and solutions that have been created to keep VANETs safe from harmful actions. Each countermeasure is put into a category based on how well it works against a certain type of attack. Some of these defenses are cryptographic protocols, intruder detection systems, safe direction-finding methods, and privacy-enhancing strategies. The poll also looks into how these defenses affect how well VANETs work and how much they cost to run. This lets the study look at the natural trade-offs that exist between how well the system works and how safe it is right now.

Key Words: Mobile Ad Hoc Network, Vehicular Ad Hoc Network; Inter-Vehicle Communication, Routing Protocols

Introduction:

Intelligent transportation systems have both fixed structures and nodes that are made up of moving vehicles. A "virtual area network" (VANET) is short for a "intelligent transportation system." The setting it works in is a scenario that is always changing and hard to predict. In a VANET, which is a type of MANET, each car is seen as a transmission point below the network. It is feasible for every vehicle in the network to join with each other without having to be screened or know anything about the other sites first. You can connect with yourself. The On Board Unit (OBU) of the car and the Road Side Unit (RSU) of the route are two separate groups that can be used to sort these nodes. Operations and Business Units (OBUs), which are placed inside the vehicles and are situated within the vehicles, are in charge of the less stable parts of the network design. The RSUsprimary function is to act as routers between cars and which are manufactured and positioned along the side of the road. Last ten years, there has been rise in the processing capacity of vehicles,a rapid growth in the development of autonomous vehicles, and an increase in the use of internet-based communication inside vehicles. Countries such as the UK have made investments in the research and development of an automated system of this kind. The development of VANET technology is the UK, which is a supporter of the technology and also the one of the world's leading countries. They have initiated the procedure that will provide permission for automobiles that are equipped with this technology to be sold on the market. The call for evidence system was created to enhance the safety of motorists and low-speed vehicles by providing more information.The system aims to maintain control of a car at low speeds, enhancing driver comfort and safety for others on the road. [1] Due to the fact that nodes in VANETs are characterized by their high degree of mobility and dynamic topology, communication becomes more precarious. In addition to this, wireless communication is very susceptible to security flaws wherever they are present. The fact that this information is being sent in real time must not alter. In such case, it might be catastrophic for the efficient functioning of VANETs and have an impact on the safety of drivers on the road. As a result, it is the most important thing for researchers who are concerned with security [2]. claimed that distributed denial of service attacks (DDOS) targeted around 79 nations, with 95.14 percent of assaults being carried out in the top 10 countries [3]. VANETs are more likely to be hit by large-scale attacks, like distributed denial of service attacks, which use peer-to-peer links to stop the car from connecting. These kinds of attacks happen more often on VANETs than on other types of networks. For this reason, the car can be attacked in many different ways, and all of them could have very bad results. Virtual private networks, or VANETs, can be attacked in a number of different ways, which can be roughly grouped by what the Central Intelligence Agency says. Numerous types of attacks can be used to break secrecy.

These types of attacks include listening in on conversations, man-in-the-middle attacks, home attacks, and social attacks. The aim of this study is to look into and rate the different attacks and defenses that are currently in place against virtual access networks (VANETs). It will also focus on VANETs' most important features and major flaws. Furthermore, it handles risks such as denial-of-service attacks, spam, and black holes, which are all very worrying when it comes to VANET security.

Security in Mobile WSN:

Sensor nodes are regularly deployed in dangerous an area, which necessitates the implementation of severe security, measures for mobile wireless sensor networks (WSN). The control of node mobility, energy limits, and the dynamic nature of network designs are some of the challenges that mobile wireless sensor networks (WSNs) face in comparison to stationary WSNs. The following are some of the essential security concerns and solutions that need to be taken in order to handle these issues:

Data Confidentiality and Integrity:

- Encryption: Now, encryption methods are being added to the system to make sure that contact between sensor nodes is safe and that no one else can get to important data without permission.
- Message Authentication Codes (MACs): MACs are deployed to ensure that the integrity of messages that are sent between nodes is preserved, hence preventing any tampering or alteration of data while it is being transmitted.
- Node Authentication:
- Secure Node Initialization: The network is protected by putting in place secure initialization procedures, which limit access to only those nodes that have been permitted to be there.
- Public Key Infrastructure (PKI): PKI makes sure that nodes can only connect to the network if they have the right keys.
- Secure Routing:
- Intrusion Detection Systems (IDS): When it comes to identifying and stopping unwanted actions such as compromised nodes or routing assaults, the adoption of intrusion detection systems (IDS) is very necessary.
- Trusted Routing Protocols: The implementation of routing protocols that are resistant to several types of attacks, including selective forwarding, blackhole, and grayhole assaults.
- Energy-Efficient Security:
- Lightweight Cryptography: A reduction in the amount of energy that resource-constrained sensor nodes use is suggested by the research, which suggests the utilization of lightweight cryptographic methods.
- Energy-Aware Key Management: Implementing critical management strategies that include the energy constraints of mobile sensor nodes.
- Location Privacy:
- Anonymity Techniques: Pseudonyms and random node movements are used in order to ensure that the location privacy of sensor nodes is preserved.
- Secure Localization: ensuring the security and impermeability of the mechanism that is used to physically locate nodes in the network.
- Resilience to Node Compromises:
- Byzantine Fault Tolerance: The implementation of techniques that is able to resist and recover from Byzantine failures, which occur when nodes display behavior that is malicious.
- Redundancy and Diversity: Implementing robustness and plurality throughout the network to mitigate the consequences of hacked nodes.
- Secure Data Aggregation:
- Secure Aggregation Protocols: The implementation of protocols that assign dedicated nodes to continuously aggregate data while simultaneously verifying the validity and security of the information that has been consolidated while doing so.
- Homomorphic Encryption: Utilizing homomorphic encryption to provide safe processing on encrypted data while aggregating.
- Dynamic Key Management:
- Periodic Key Updates: Regularly upgrading cryptographic keys to enhance security and resilience against possible key compromise.
- Key Distribution Protocols: Deploy efficient key distribution algorithms that consider the changing characteristics of mobile Wireless Sensor Networks (WSNs).

VANETs Architecture:

VANETs, which are recognized as a pioneering and cutting-edge technology, make it possible to connect millions of cars located all over the globe. The architecture of a VANET is comprised of three primary communication models: the communication between a vehicle and another vehicle, which is referred to as Vehicle to Vehicle (V2V), the communication between a vehicle and the local infrastructure that is situated

along the road, which is referred to as Infrastructure to Vehicle (I2V), and the communication between a vehicle and the infrastructure that is located along the road, which is defined as Vehicle to Infrastructure (V2I). cars that are equipped with a transmission that is referred to as vehicle-to-vehicle (V2V) have the capability to connect with other cars in two different ways: either directly at a short distance or via a technique of communication that involves a number of hops at a longer distance. When the delivery of essential information comes, single hop might be used for communication. A substantial change in traffic is directly linked to information, such as accidents, traffic congestion and highway bottlenecks, this particular category would be included.In addition, any extra information that would be directly tied to the benefits of the secure transportation of autos, mobility, and other environmental concerns would be included in the document. On the other hand, communication that does not include important information may be accomplished using multi-hop communication [3].

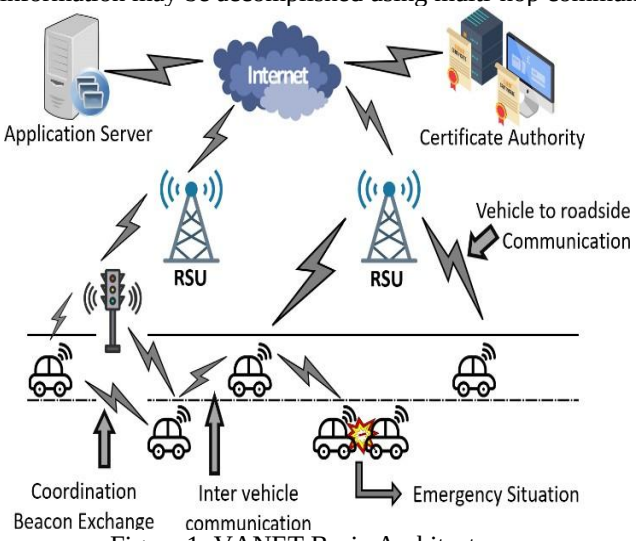

Figure 1: VANET Basic Architecture

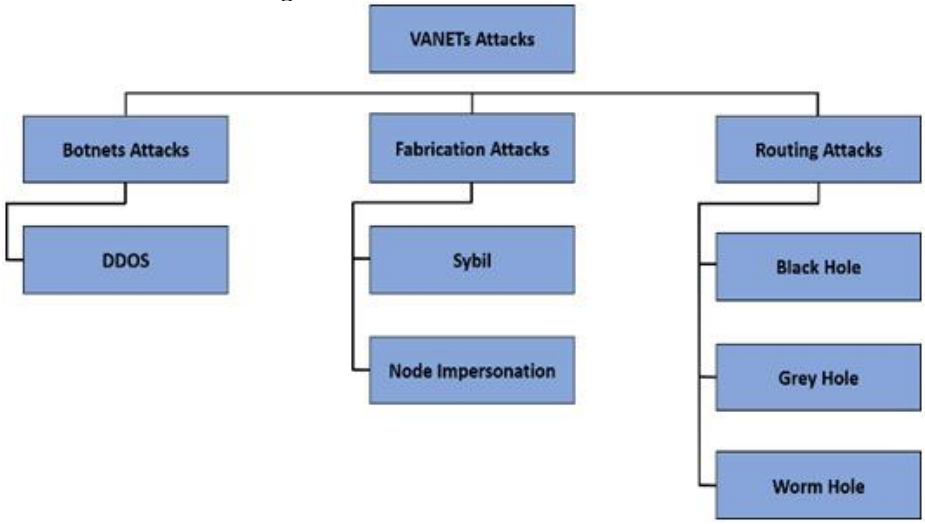

Figure 2: VANETs Attacks

Vehicle-to-infrastructure (V2I) communication involves the transmission of data from cars to remote source units (RSUs), mostly consisting of operational data and data about safety. The primary purpose of this data collection will be to enhance the mobility and safety of drivers, and it will be collected at those RSUs. Through the implementation of algorithms that subsequently make use of the data that has been gathered from the cars, the roadside infrastructure is able to carry out a variety of calculations that have the potential to anticipate potentially hazardous and high-risk circumstances in advance. It is possible that this will lead to the RSUs developing and disseminating warnings to drivers in order to avert the occurrence of the situations that have been forecasted. As seen in Figure 1, the fundamental architecture of VANETs is shown. A real-time analysis of the whole communication traffic might be performed in order to facilitate effective traffic flow, which would ultimately result in a large reduction in the amount of traffic congestion [4]. In the event that Traffic Light Controllers (TLCs) are able to transmit information about their present state to cars on the section of the road that they regulate, this is something that may be accomplished. It is also possible for cars to trade beacons with one another. It is possible for drivers to make judgments that are correct and would enhance the efficiency of traffic by combining the data that is received from TLCs and beacons on the road.

VANETs Attacks and Countermeasures:

In this part, we will discuss the numerous attacks that may be launched against VANETs by taking advantage of the inherent weaknesses that they possess. Additionally, the section examines the recommended remedies (countermeasures), as well as the advantages and disadvantages of each kind of remedy. The VANET attacks that were discussed in this research are shown in Figure 2.

- **Botnet Attacks:**

It is common practice to use botnet assaults in order to disrupt the typical operation of networks and servers. Because of these harmful attacks, a network of botnet devices is set up, and each of these devices helps one or more bots do their job. After that, a lot of devices that have been attacked are used to attack a website or other devices. Criminals in the internet use botnet attacks to carry out distributed denial of service attacks and other types of large-scale hacking.

A type of attack that is often called a distributed denial of service attack (DDoS)! A distributed denial of service attack, or DDoS attack, is a different type of attack in which many people launch an attack at the same time. This assault is carried out by a number of hacked nodes, which are referred to as Zombies, and serves as a source of attack traffic. Considering the nature of VANETs, they are very susceptible to distributed denial of service assaults. Through the use of this attack, communication between V2V and V2I may be undermined. The performance of the network, including its bandwidth, processing power, throughput, and operating system, may be significantly impacted by distributed denial of service assaults [5]. Attacks using distributed denial of service (DDoS) represent a threat to public safety in VANETs; they have the potential to cause major accidents, traffic jams, and other deplorable situations in ITS. As a result, a number of studies have been conducted with the purpose of safeguarding VANETs from this detrimental assault. In the next part, several approaches that have been suggested by researchers as potential solutions to this issue are presented and discussed.

- **Countermeasures:**

In [6], a straightforward method for detecting and mitigating distributed denial of service attacks was presented. A method is used to figure out how much data each node is using. When the bandwidth goes over a certain level, both the channel with the high bandwidth and the node with the high data rate are found. The last thing that needs to be done to stop the attack is to cut off the newly found node from the rest of the network. However, this method is used for talking between cars and not between vehicles and people. Another problem with this method is that it can't find spread denial of service attacks that happen slowly. As an example, the writers of [7] came up with a method that is similar to the one we are talking about here. The number of bits sent from a single node is taken into account in this method. When a node gets packets from different places, these packets are sent to the counter module, which has a number of 10 seconds set as the clock. The number of the counter is changed immediately to show what time it is. Because of this, the counter module's job is to keep track of how many packets each source sends over the course of ten seconds. If the total number of packets gets too high, the Alarm Message Module (AMM) will get the IP address of the person who sent the message. Two separate jobs are supposed to be done by the AMM. So that it can start talking, the first thing it will do is give the OBU of that car the affected node's IP address. We will now be able to talk to each other. It will also connect to the RSU it is linked to in order to give it details about the attacker. This is going to happen in the second place. In order to stop any new vehicles from linking with the fake IP address, the RSU has asked that the contact be done by other vehicles. A spread denial of service attack can't get through this way. Despite this, though, it doesn't work when dealing with Slow DDoS. To protect against widespread denial of service threats, the people who made [8] used the widespread Network Intrusion Detection System. After that, the network traffic engine will use the Random Forest (RF) algorithm to find the Distributed Denial of Service (DDOS) data. This machine will be the first to pick up network data. Any DDOS message found by the system's filters will quickly cause a warning to be sent out. The authors used the datasets NSL-KDD and UNSW-NB15 on their own computers to do the experiments. The data shows that RF is better than all other machine learning models, with a success rate of 98.7%. That being said, this experiment took place outside, where the deepest point was twenty trees. An exponential rise in the number of trees will cause the amount of time needed to do the math to grow exponentially. In [9], it is shown that the Multivariant Stream Analysis (MVSA) method is used to find and stop widespread denial of service attacks. The Motor Vehicle Safety Administration (MVSA) will divide the traffic into two groups: safe and unsafe. Services for fun, lowering fuel use, electronic tolls, and other uses are examples of uses that don't have to do with safety. Safety apps are those that have knowledge about how to keep people and cars safe. It is necessary to compute each and every message in order to compute network records. Each packet's network trace shows its content, hop count, time to live, and how often it is sent. The trace also shows how long you have left to live. The node that is responsible for finding and stopping the spread denial of service attack is also the one that will be responsible for keeping these records. Following that, the multi-variant stream factor must be calculated for any number of different time frames from the choices that are given. The multivariant stream weight will be found with this method by using the stream factor as a guide. MVSA will classify the DDoS packet and router based on the situation. Then, the company will take steps to lessen the effects of the DDoS attack.

- **Fabrication Attacks:**

A hostile node adjusts certain packet information in order to inflict catastrophic harm in the network, such as congestion and excessive latency. Fabrication attacks are impersonation-based assaults that entail the modification of packet information. The primary objective of the attacker is to either cause confusion inside the network or to interrupt the communication that occurs between the nodes of the network connection. The most common sorts of assaults that fall under this category are known as Sybil and Node impersonation.

- **Sybil Attack:**

[10] In VANETs, wireless connection is often the sole method that is used for communication activities. By using a Sybil attack, an adversary may take advantage of this characteristic. When an attacker generates many bogus identities and takes control of the network, they are committing the sort of assault known as a Sybil attack. Some people refer to these fictitious identities as Sybil nodes or virtual nodes [11].

- **Routing Attacks:**

As they transport the data that is required for information extraction, the routing protocols are an essential component of the VANETs network, which permits multi-hop in the network [23, 24]. One of the goals of an attack on a routing protocol is to stop communication between the source node and the destination node for the attacker. Black hole attacks are another prevalent kind of attack on routing protocols. In this type of attack, the attacker would discard all of the packets, which would result in connection and communication failure. The assaults on the black hole, grey hole, and wormhole are broken down into their component parts in the following sections.

- **Blackhole Attack.**

One of the most important aspects of VANETs is the Ad hoc AODV, which is an acronym that stands for On-demand Distance Vector. In spite of the fact that it is often used as a reactive routing protocol, it does not provide any security characteristics in the majority of instances [13]. An AODV node is able to send data to a receiving node in a network by first generating a Route REQuest (RREQ) packet and then broadcasting that packet throughout the network. This provides the AODV node with the ability to send data. In order for an adversary to carry out a black hole attack, they will enter the network using a malicious node that they have introduced. to become r. This particular node is able to redirect Packet Data Units (PDUs) to the node that the attacker desires to connect with since it is able to fulfill the role of a free receiving node and prescribe a short path for the destination. Consequently, the attacker has the capacity to enhance the impact of the attack by raising the number of malicious nodes that are present inside the network during the attack.

- **Wormhole Attack:**

The reactive routing system in VANETs may potentially be subject to a wormhole attack, which is another sort of assault. The malicious node is responsible for this attack, in which it takes the data from packets and sends it to another malicious node that is located a few hops away. Wormholes are famously difficult to identify in a network due to this quality. One of the most significant dangers posed by a wormhole assault is that it may quickly interrupt the multicasting and broadcasting routing networks, as well as furnish cars with incorrect information. In this way, genuine routes are prevented, and the security of the routing protocol is put in jeopardy.

Literature Survey:

Although VANET is not a new concept, it still continues to present new problems and problems in science [14]. The primary purpose of VANET is to help the network to set up and manage the communication network between vehicles without the use of central or monitoring stations. Some of the major uses of VANET are in critical medical situations with little support, although it is important to share relevant knowledge to save lives. the people. However, despite the large application, VANET has its problems and new issues. The disadvantage of VANET housing is that it puts a lot of load on the car. Each vehicle is part of the network, and network communication is often performed according to its own privacy rules. [15]

Ghada Abdelmoumin et. al. (2022) deep learning-based intrusion detection systems (DL-IDSs) outperform anomaly-based machine learning-enabled intrusion detection systems (AML-IDSs) in terms of detecting intrusions in the Internet of Things (IoT), demonstrating higher performance and prediction accuracy. For example, AML-IDS systems that use basic models for Internet of Things (IoT), such as the principle component machine (PCA) technique and the one-class support vector machine (1-SVM) method, are less successful in identifying intrusions compared to DL-IDS systems that employ the two-class neural network (2-NN) approach. AML-IDS, PCA, and DL-IDS all have different identification rates. AML-IDS and PCA might not work as well as DL-IDS depending on the size and number of features or variations in the dataset. The AML-IDS model may not work well and make accurate predictions because of a number of problems, including using a single-learner model, an unbalanced dataset, and a low similarity score between the training and testing data. A smart intrusion detection system (IDS) is less effective right away because of the problems that come with the single-learner hypothesis. Because the data used for training and tests are not the same, AML-IDS also have a higher rate of false positives (FPs). While DL-IDS are very accurate and rarely give fake warnings, they are also very predictable. Along with other methods, this is different. To make single-learner AML-IDS work better, this

study looks at how optimization techniques can be used. One-scalar support vector machine (SVM) and principal component analysis (PCA) are the AML-IDS models that we are most interested in. It is important to create improved intrusion detection systems (IDS) for the Internet of Things (IoT) that can properly spot and stop unauthorized entry. The AML-IDS models are tested by fine-tuning hyperparameters and finding the best ways to use ensemble learning on the Microsoft Azure ML Studio (AMLS) platform. These two types of data are used to look at both bad and good Internet of Things (IoT) network traffic, as well as industrial IoT (IIoT) network traffic. For the Internet of Things, we also compare AML-IDS models based on how well they worked compared to what was expected.[16]

Ngan Tran et.al. (2022) one of the most important responsibilities in order to safeguard the cyber environment from potential dangers is the detection of intrusions. However, despite the efforts of several research to develop complex models for identifying intrusions from vast amounts of data, they have failed to consider the significant influence of insufficient data quality on the effectiveness of intrusion detection systems. Instances of inadequate data quality include mislabeled, erroneous, incoherent, irrelevant, inconsistent, duplicated, and overlapping data. Other examples include data that lacks uniformity. We performed a series of tests on eleven datasets pertaining to host-based intrusion. We used a total of eight machine learning models, including two pre-trained language models: BERT and GPT-2. The aim of these research was to examine the impact of data quality on the effectiveness of machine learning. The experimental findings are as follows: BERT and GPT-2 consistently achieved better results than the other models on all datasets. Data duplications and overlaps in a dataset have discernible effects on the performance of pre-trained models and conventional machine learning models. Pre-trained models exhibited a reduced likelihood of encountering duplicate and overlapping data in comparison to conventional machine learning models. 3. The effectiveness of pre-trained models on most datasets might possibly be improved by removing duplicate and overlapping data from the training set, while still maintaining a reasonable range of sequence similarities. Nevertheless, in datasets containing very similar sequences, this might have a detrimental impact on the model's performance. 4. The existence of duplicate items in the testing data might compromise the precision of the model assessment. There seemed to be a negative correlation between the degree of overlap between the normal class and the intrusion class, and the effectiveness of the pre-trained models in detecting intrusions. Given the outcomes, we have devised a systematic approach for selecting models and guaranteeing the integrity of data in order to construct a top-notch intrusion detection system using machine learning.[17]

Giovanni Apruzzese et.al. (2022) Applying supervised machine learning (ML) to enhance Network Intrusion Detection Systems (NIDS) is a formidable task. In order to perform operations that need data with properly labeled benign and malicious samples, ML-NIDS must undergo training and assessment. The need for costly specialized knowledge to handle these labels results in a scarcity of practical implementations. Furthermore, publications often rely on outdated data, resulting in a dearth of authentic implementations. Recently, some projects have published their annotated datasets, leading to a positive impact on the current situation. However, most earlier studies regarded these datasets just as another test environment, disregarding the extra possibilities that their availability presents. Alternatively, we suggest using pre-established labeled data to do cross-evaluation of ML-NIDS. This technology has garnered little attention and requires a customized approach owing to its intricacy. Thus, we provide the first version of cross-evaluation. Our model showcases the wide array of real-life situations that may be analyzed via cross-evaluations, enabling us to discover novel attributes of cutting-edge machine learning and network intrusion detection systems. It is possible to increase the sensing area of these devices without incurring any further costs for labeling. Performing such cross-evaluations, meanwhile, is a demanding undertaking. Hence, we provide XeNIDS, the first framework designed for conducting dependable cross-evaluations using Network Flows. We showcase the unexplored potential of cross-evaluations in Machine Learning Network Intrusion Detection Systems (ML-NIDS) by using XeNIDS on six well acknowledged datasets. However, we also provide an overview of the hazards associated with these evaluations.[18]

Bing Gao et.al. (2022) An instance of a standard cyber physical system used in urban rail transportation is the communication-based train control system. The train-ground communication system, an integral part of the CBTC system, utilizes wireless communication protocols to convey control directions. However, it is vulnerable to a limited number of potential risks to the security of information. The objective of this study is to propose an intrusion detection methodology that utilizes machine learning and state observer techniques. The objective of the technique is to identify and recognize different types of assaults in order to guarantee the information security of the train-ground communication system. The detection system not only identifies deviations in the data sent over the wireless network, but also detects abnormalities in the physical state of the train components. This approach comprises of two distinct steps. The first layer utilizes machine learning methodologies, namely the random forest algorithm and the gradient boosted decision tree algorithm, to identify and categorize intrusions on wireless networks. The identification and detection of such factors is within the purview of this layer. For the purpose of identifying any anomalous physical circumstances that may arise while the train is in operation, the second layer makes use of a state observer. Merging the findings from the levels that were

mentioned before is done in order to accomplish complete intrusion detection. Based on the results of the simulation, it can be concluded that the proposed method is not only efficient but also practicable.[19]

Saikat Das et.al. (2022) Having the right security measures in place is very important when it comes to online and keeping network security safe. In order to offer quick network security against network weaknesses and data theft, these solutions are made to protect you. For important systems to stay safe from being hacked or viewed by people who aren't supposed to, there needs to be a detailed plan for setting up an effective intrusion detection system. The goal of this project is to use machine learning (ML) to come up with and put into action a complete security system that can find and stop network attacks. There are several ways to choose features in this method, which uses an ensemble approach for guided machine learning. We also look into the ways that the different machine learning models and feature selection methods are alike and how they are different. The goal of this project is to create a uniform detecting system that improves precision and lowers the number of false positives (FPR). For the project to work, the datasets NSL-KDD, UNSW-NB15, and CICIDS2017 are used. The data shows that our monitoring system can correctly identify intrusions 99.3 percent of the time, while also sending out an incredibly low number of fake reports. By measuring efficiency, this shows that our method is better than other options that are currently out there.[20]

Muawia A. Elsadig 2023 It is probable that the rapid expansion of wireless sensor networks (WSNs) across a wide range of industries might be attributed to the fact that these networks exhibit exceptional performance and feature unique characteristics. Denial-of-service assaults, often known as DoS attacks, are an incredibly prevalent occurrence in some networks. Despite this, these networks are particularly vulnerable to a broad range of security risks, including DoS attacks. The purpose of this article is to provide light on the limits, vulnerabilities, and security threats that are associated with wireless sensor networks (WSNs), with a particular emphasis on denial of service attacks. Following an in-depth analysis of novel approaches to detecting denial of service (DoS) assaults, researchers have assessed the advantages and disadvantages that are associated with these techniques. This was accomplished after they had conducted the inquiry. As a result of this, we are in a position to get vital knowledge on the most recent research that has been conducted in this particular field. An simple machine learning approach is shown in this article. This technique has the potential to be used in the identification of Denial of Service (DoS) assaults that are carried out in Wireless Sensor Networks (WSNs). Within the framework of this methodology, both the Gini feature selection method and a decision tree (DT) algorithm are used [21].

Conclusion:

The capacity to create future autos has been gained thanks to the vehicle messaging talent. The VANET makes it easier for cars to communicate with one another or during road construction. This work focuses on the analysis of challenges and requirements involved in the design of steering processes in VANETs. Additionally, a comprehensive evaluation of several steering methods was conducted. We have developed a protocol classification approach based on VANET characteristics. This method categorizes the processes into two groups: (1) vehicle-to-vehicle routing protocol and (2) vehicle-to-vehicle steering protocol. This course explores the characteristics, performance metrics, and routing values of all protocols assigned to a class of similar methodologies. This material potentially encompasses the most recent findings about the VANET routing protocol. The grouping of key steering values may simplify the effort of system designers when choosing the VANET routing strategy to be employed in certain scenarios. We have confidence that our study will provide significant value to the scientific community and serve as a foundational resource for anyone interested in pursuing VANET research and applications. Based on this extensive analysis, we can deduce that the primary differentiating factor among the different VANET protocols is in the approach used to categorize or establish steering between source and destination pairs. Several routing methods have been developed to address the most crucial issues in VANET technology. The majority of these protocols are unable to handle dynamic topologies and often disconnected networks, which is seen as a significant difficulty. We addressed specific concerns pertaining to these agreements and proposed analogous remedies. Location-based routing and geographic transmission are often more efficient than other VANET routing techniques due to environmental limitations. Furthermore, steering protocols that rely on substructure are particularly well-suited for VANET messages.

References:

1. GOVUK, "Safe Use of Automated Lane Keeping System (ALKS) Summary of Responses and Next Steps," 2021. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/980742/safe-use-of-automated-lane-keeping-systemalks-summary-of-responses-and-next-steps.pdf
2. S. Popoola, B. Adebisi, R. Ande, M. Hammoudeh, K. Anoh, and A. Atayero, "Smote-Drnn: A Deep Learning Algorithm for Botnet Detection in the Internet of Things Networks," Sensors, vol. 21, p. 2985, 04/26 2021, doi: 10.3390/s21092985. [3] Kaspersky, "DDoS attacks in Q1 2018," 2018. [Online]. Available: https://securelist. com/ddos-report-in-q1-2018/85373/

3. M. Hammoudeh, A. Kurz, and E. Gaura, "MuMHR: Multi-path, Multi-hop Hierarchical Routing," in 2007 International Conference on Sensor Technologies and Applications (SENSORCOMM 2007), 14-20 Oct. 2007 2007, pp. 140-145, doi: 10.1109/SENSORCOMM.2007.4394911.
4. P. Kaur, D. Kaur, and R. Mahajan, "Wormhole Attack Detection Technique in Mobile Ad Hoc Networks," Wireless Personal Communications, vol. 97, no. 2, pp. 2939-2950, 2017/11/01 2017, doi: 10.1007/s11277-017-4643-z.
5. C. Guleria and H. K. Verma, "Improved Detection and Mitigation of DDoS Attack in Vehicular ad hoc Network," in 2018 4th International Conference on Computing Communication and Automation (ICCCA), 14-15 Dec. 2018 2018, pp. 1-4, doi: 10.1109/CCAA.2018.8777539.
6. M. Shabbir, M. A. Khan, U. S. Khan, and N. A. Saqib, "Detection and Prevention of Distributed Denial of Service Attacks in VANETs," in 2016 International Conference on Computational Science and Computational Intelligence (CSCI), 15-17 Dec. 2016 2016, pp. 970-974, doi: 10.1109/ CSCI.2016. 0186.
7. Y. Gao, H. Wu, B. Song, Y. Jin, X. Luo, and X. Zeng, "A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Vehicular Ad Hoc Network," IEEE Access, vol. 7, pp. 154560-154571, 2019, doi: 10.1109/ACCESS.2019.2948382.
8. R. Kolandaisamy et al., "A Multivariant Stream Analysis Approach to Detect and Mitigate DDoS Attacks in Vehicular Ad Hoc Networks," Wireless Communications and Mobile Computing, vol. 2018, pp. 1-13, 05/20 2018, doi: 10.1155/2018/2874509.
9. M. S. Potnis, S. K. Sathe, P. G. Tugaonkar, G. L. Kulkarni, and S. S. Deshpande, "Hybrid Intrusion Detection System for Detecting DDoS Attacks on Web Applications Using Machine Learning," in ICT Analysis and Applications, Singapore, S. Fong, N. Dey, and A. Joshi, Eds., 2022// 2022: Springer Nature Singapore, pp. 797-805.
10. N. C. S. N. Iyenger and G. Ganapathy, "Trilateral Trust Based Defense Mechanism against DDoS Attacks in Cloud Computing Environment," Cybernetics and Information Technologies, vol. 15, 07/03 2015, doi: 10.1515/cait-2015-0033.
11. O. Osanaiye, H. Cai, K.-K. R. Choo, A. Dehghantanha, Z. Xu, and M. E. Dlodlo, "Ensemble-based Multi-Filter Feature Selection Method for DDoS Detection in Cloud Computing," EURASIP Journal on Wireless Communications and Networking, vol. 2016, 05/10 2016, doi: 10.1186/s13638-016-0623-3.
12. R. Kolandaisamy, R. M. Noor, M. R. Z'aba, I. Ahmedy, and I. Kolandaisamy, "Adapted stream region for packet marking based on DDoS attack detection in vehicular ad hoc networks," The Journal of Supercomputing, vol. 76, no. 8, pp. 5948-5970, 2020/08/01 2020, doi: 10.1007/s11227-019-03088-x.
13. K. Adhikary, S. Bhushan, S. Kumar, and K. Dutta, "Hybrid Algorithm to Detect DDoS Attacks in VANETs," Wireless Personal Communications, vol. 114, no. 4, pp. 3613-3634, 2020/10/01 2020, doi: 10.1007/s11277-020-07549-y.
14. M. Hammoudeh and R. Newman, "Information extraction from sensor networks using the Watershed transform algorithm," Information Fusion, vol. 22, pp. 39-49, 2015/03/01/ 2015, doi: https://doi.org/10.1016/j.inffus.2013.07.001.
15. Y. Yao et al., "Multi-Channel Based Sybil Attack Detection in Vehicular Ad Hoc Networks Using RSSI," IEEE Transactions on Mobile Computing, vol. 18, no. 2, pp. 362-375, 2019, doi: 10.1109/TMC. 2018.2833849.
16. Ghada Abdelmoumin; Danda B. Rawat; Abdul Rahman On the Performance of Machine Learning Models for Anomaly-Based Intelligent Intrusion Detection Systems for the Internet of Things IEEE Internet of Things Journal Year: 2022 Volume: 9, Issue: 6 Journal Article Publisher: IEEE
17. Ngan Tran; Haihua Chen; Jay Bhuyan; Junhua Ding Data Curation and Quality Evaluation for Machine Learning-Based Cyber Intrusion Detection IEEE Access Year: 2022 Volume: 10 Journal Article Publisher: IEEE
18. Giovanni Apruzzese; Luca Pajola; Mauro Conti The Cross-Evaluation of Machine Learning-Based Network Intrusion Detection Systems IEEE Transactions on Network and Service Management Year: 2022 Volume: 19, Issue: 4 Journal Article Publisher: IEEE
19. Bing Gao; Bing Bu; Wei Zhang; Xiang Li An Intrusion Detection Method Based on Machine Learning and State Observer for Train-Ground Communication Systems IEEE Transactions on Intelligent Transportation Systems Year: 2022 Volume: 23, Issue: 7 Journal Article Publisher: IEEE
20. Saikat Das; Sajal Saha; Annita Tahsin Priyoti; EteeKawna Roy; Frederick T. Sheldon; Anwar Haque; Sajjan Shiva Network Intrusion Detection and Comparative Analysis Using Ensemble Machine Learning and Feature Selection IEEE Transactions on Network and Service Management Year: 2022 Volume: 19, Issue: 4 Journal Article Publisher: IEEE
21. Muawia A. Elsadig (2023) Detection of Denial-of-Service Attack in Wireless Sensor Networks: A Lightweight Machine Learning Approach Digital Object Identifier 10.1109/ACCESS.2023.3303113 Volume 11, 2023