Detection and avoidance of Security attacks in Vehicular Ad hoc Networks

PROJECT PHASE-1 REPORT
Submitted by

N.S.V Chaitanya (1BM16CS053)

Naveen R (1BM16CS055)

Nikhil Srinivas M (1BM16CS058)

in partial fulfillment for the award of the degree of
BACHELOR OF ENGINEERING
in
COMPUTER SCIENCE AND ENGINEERING

Under the Guidance of
Dr. Nandhini Vineeth
Assistant Professor, BMSCE

B. M. S. COLLEGE OF ENGINEERING
(Autonomous Institution under VTU)
BENGALURU-560019

2019-2020

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

Certified that the project entitled "**Detection and Avoidance of Security Attacks in Vehicular Adhoc Networks**" is a bonafide work carried out by N.S.V Chaitanya (1BM16CS053), Naveen R (1BM16CS055), Nikhil Srinivas M (1BM16CS058) in partial fulfilment for the award of Bachelor of Engineering in Computer Science and Engineering of the Visvesvaraya Technological University, Belagavi during the academic year 2019 -2020. The project report has been approved as it satisfies the academic requirements in respect of project work prescribed for the said degree.

Guide

Dr. Nandhini Vineeth,
Assistant Professor,
Dept of CSE,
B.M.S. College of Engineering

Head of Department

Dr. Umadevi V,
Associate Professor and HOD,
Dept of CSE,
B.M.S. College of Engineering

Principal

Dr. B. V. Ravishankar
B.M.S. College of Engineering

External Viva

Name of the Examiners	Signature with Date
1.	
2.	

Table of Contents

Abstract

In the current generation, road accidents and security problems increase dramatically worldwide in our day to day life. In order to overcome this, Vehicular Ad-hoc Network (VANETs) is considered as a key element of future Intelligent Transportation Systems (ITS). With the advancement in vehicular communications, the attacks have also increased, and such architecture is still exposed to many weaknesses which led to numerous security threats that must be addressed before VANET technology is practically and safely adopted.

Distributed Denial of Service (DDoS) attack and Sybil attacks are the significant security threats that affect the communication and privacy in VANET. As simulators are being used in our work, we have discussed about OMNET++ which is a new modernized latest mobility and network simulators as well as data network simulator. This is also integrated with the road traffic simulator SUMO with Veins, an open-source framework for VANET simulation.

An in-depth survey of a new innovative technology called as Vehicular Cloud Computing (VCC) which has an enormous impression on ITS by utilizing the assets of vehicles such as internet, storage, Global Positioning System(GPS), computing power for creating a quick judgment including transmission of information between the cloud and VANET. In addition to providing the usage and approach of vehicular cloud, a short survey of the routing protocols, major security threats, attacks and even security solutions for the cloud computing have also been surveyed.

An extensive survey has been done on the architecture of VANET, existing protocols, prevalent security attacks etc. and after analyzing the pros and cons of the existing algorithms, the objective of this our work is to design an algorithm to detect and avoid various kinds of attacks using Vehicular Cloud computing. An analysis has also been done by applying four protocols on a existing scenario of real traffic simulator using OpenStreetMap and the best suitable protocol has been selected for further application.

DECLARATION

We, hereby declare that the Project Phase-1 work entitled "**Detection and Avoidance of Security Attacks in Vehicular Adhoc Networks**" is a bonafide work and has been carried out by us under the guidance of Dr**.** Nandhini Vineeth, Assistant Professor, Department of Computer Science and Engineering, B.M.S. College of Engineering, Bengaluru**,** in partial fulfilment of the requirements for the degree of Bachelor of Engineering in Computer Science and Engineering of Visvesvaraya Technological University, Belagavi.

We further declare that, to the best of our knowledge and belief, this project has not been submitted either in part or in full to any other university for the award of any degree.

Candidate details:

SL. NO.	Student Name	USN	Student's Signature
1	N.S.V Chaitanya	1BM16CS053	
2	Naveen R	1BM16CS055	
3	Nikhil Srinivas M	1BM16CS058	

Place: Bengaluru

Date:

Certified that these candidates are students of Computer Science and Engineering Department of B.M.S. College of Engineering. They have carried out the project work titled "**Detection and Avoidance of Security Attacks in Vehicular Adhoc Networks**" as Project Phase-1 work. It is in partial fulfillment for completing the requirement for the award of B.E. degree by VTU. The work is original and duly certify the same.

Guide Name Signature

Dr. Nandini Vineeth

Date:

Acknowledgment

We would like to express our gratitude to our beloved Principal, Dr. B. V. Ravishankar, the Head of the Department of CSE, Dr. Umadevi V and our project guide Dr. Nandini Vineeth who have given us this golden opportunity to work on this wonderful project titled "Detection and Avoidance of Security Attacks in Vehicular Adhoc Networks". During the course, we have gained knowledge of the previously unknown subjects through the tedium of research. We have been able to broaden our spectrum and redefine our conceptions on the current trends, technological advancements and the current needs in the market.

We would also like to appreciate those, who through the course of design and development of this project have made time to interact and guide us in numerous ways. We would also acknowledge the fact that there are plenty of mind-boggling breakthroughs that have occurred in the field over the past decade and also the numerous theories that are published and presently in development. We are really grateful to our faculty project guide, who believed in us and bestowed upon us with her time and knowledge to develop this project and bring our vision into reality.

Secondly, we would like to acknowledge the entire CSE Department of B.M.S College of Engineering for their constant and continuous support in the development of this project.

We also express a feeling of appreciation to our friends and family for believing in us and providing moral support in all phases of this project to make it a grand success.

We really had a great time working on this project and learning new concepts.

List of tables

List of figures

Chapter 1

Introduction

1.1 Overview

Vehicular Ad-hoc Network (VANET) provides smart transportation system owing to Vehicle to Infrastructure (V2I) and Vehicle to Vehicle (V2V) message dissemination with an objective to provide safety on roads. VANET in comparison to Mobile Ad-hoc Network (MANET) points to an exceptional kind of networking with high mobility nodes which are vehicles. Major applications of VANET include electronic brake light, parking management and point crash notification. The topology in VANET vary according to vehicle movement scenario such as traffic light, highway and urban road scenario. The contribution in area of VANET by research community on various layers is on the rise. The simulator close to the real time set up for VANET is preferred choice of researchers as it involves less cost in comparison to real set up.

Nearly 1.25 million people die each year and on an average 3,287 deaths a day is observed according to world health organization. Many engineers from different area of study such as vehicle designers and road engineers help in the reduction of the number of road accidents. VANETs are applicable in both rural and urban. Constraints of VANET is that the velocity of vehicles are purely depending on the speed limit of the roads they travel. Traffic signs and signals are bound to be followed by all vehicles which makes VANET less difficult than MANET.

1.2 Motivation

Challenges faced by VANET are classified as

1.2.1. **Technical Challenges:** Before deployment of VANET in real world, there are some technical challenges which need to be resolved. Some of the challenges which need to be addressed are given below:

1. Infrequent Connectivity: Due to structure of road and speeding limitations, network topology is changing rapidly. With these technicalities, we can't use structures like trees because setting them up is difficult.
2. Security: Privacy of user's data and their location is always at risk. While communicating, vehicles need to make sure that the other device is authentic and then decide which information is worth sharing and which is not. Detection of attacks and sensitive data is sent to cloud for analysis.
3. Environmental Impact: For communication between vehicle and infrastructure use electromagnetic waves which are affected by environment. Hence environmental impact on VANET is worth considering.
4. Dissimilar vehicle management: In future, a large number of new smart vehicles are expected on roads. Management of both varieties - new smart vehicles and old vehicles is a difficult task. These modern connections are upcoming challenges in VANET.

1.2.2. **Social and Economic Challenges:**

Social and economic challenges should be considered along with technical challenges to deploy VANET. Consumer will reject monitoring systems which conveys traffic violation and appreciates the police trap warning message. Manufactures gain incentives by deploying VANET.

In 2015, there were about five lakh road accidents in India, which killed about 1.5 lakh people and injured about five lakh people. India, as a signatory to the Brasilia declaration, intends to reduce road accidents and traffic fatalities by 50% by 2022. The Department for Transport estimates that an all-time high of 327.1 billion vehicle miles were driven in 2017.

Current transportation systems face great challenges due to the increasing mobility. There is an increase in the number of automobile accident fatalities due to increased traffic with unsafe driving behaviors. There is no proper communication between the vehicles, which is a major issue in causing accidents, traffic jam etc. The main applications of VANETS are used for safety issues such as alarm and warning messaging, traffic services and audio / video streaming in order to make the quality of transportation better through time-critical safety and traffic management applications.

1.3 Objective

We propose a system that comprises of:

- Improving customer safety and location awareness
- Detecting and prevention of DDoS attacks
- Improving reliability of DDoS and Sybil attack algorithm
- Using Vehicular Cloud Computing (VCC), where attacks can be detected in real time.
- Improving privacy and authentication of message.

1.4 Scope

Vehicular Ad Hoc Network is an important research area that provides ubiquitous short-range connectivity among moving vehicles. The main aim of this project is to protect VANET system from security threats. This project remotely diagnoses, detects DDoS attacks and Sybil attacks in VANET via RSU which is connected to cloud for real time data or information and also implements preventive measures.

1.5 Existing System

As discussed, under literature survey section, various security attacks have been discussed in VANET, among those the main DDoS attack is the most frequently occurring one in VANET. Machine learning algorithm has been used to detect a DDoS attack in VANET and mitigation process is done by simulating in Network simulator SUMO, traffic simulator OMNET++ with Veins.

1.6 Proposed System

To attain the user privacy, authenticity of data, trajectories are exploited to attain identity of vehicle. For the identification purpose, the authorized messages stored in the tables created in cloud are transmitted to the vehicles. The authorized message when transmitted in its original form affects the privacy. Hence the proposed technique in this work involves ambiguous signature scheme which results in location-hidden authorized message. Using the authorized messages from multiple tables, the proposed technique forms trajectory of the vehicle. Footprint mechanism detects the Sybil trajectories through the similarity definition of two trajectories. A protection scheme is proposed to detect the corrupted data in RSUs.

As the information about the current location is stored in the tables seen in the cloud, the reliability status of the accident sent by the same vehicle can be known by calculating the difference in the distance when the data is received. This technique is used for the DDOS attacks.

Attack is accurately detected by the location and speed information provided by the vehicle. Simulation is conducted using Network Simulator (NS-3) for evaluation of the efficiency of the proposed technique.

1.7 Work Plan

We have divided the project into phases. The initial phases deliver the basic and essential functionalities. We plan on working in two weekly cycles following agile practices.

Weeks 1 and 2	Implementation design
	List protocol used in VANET communication
	List types of analyses and methods
	List current work
	List Security attacks in VANET
	Survey on Recent research paper.
	Frameworks and Tools
	Understand how Simulation tools works

	Set up and configure project resources - GitHub repos, AWS service instances
Weeks 3 and 4	Analysis of Different communication medium
	Selecting best Communication Medium
	Analysis on both Dens traffic and Highway traffic
	Finalizing two Main attacks in VANET
	In Depth Research on selected attacks
	Comparing the attacks
	Designing new ideas
Weeks 5 and 6	nalysis of requirements (Functional and Non-Functional Requirements)
	Cost Estimation for Software tools and Frameworks
	Dividing the work among the team members
	Implementing with sample datasets
	List types of analyses and design the framework
	Work on the analyses
Weeks 7 and 8	Implementing and Detecting Better Protocol for the communication
	Complete the Implementation
	Analysis with real time traffic
	Start implementation using cloud computing
	Implementing Simulation tools
	Design and implementation of proposed algorithm.
Weeks 9 and 10	Testing with Real time Traffic analyses
	Graph analysis

Table:1.1 Work plan

Chapter 2

Literature Survey

Research done in the same domain are listed below:

The demand for vehicle networks has increased on a daily basis. In this paper, author discussedabout the different safety requirements of users in VANETs**.** Author also describes the contact procedures and different areas of VANETs, and it also addresses various categories of organizations, attackers, security threats and networks. At the end of the day, we heard about various security threats that cause a lot of problems[1].

Attacks	**Description**	**Attacks Involved**
1	Network attack	Denial of service Attack, Node Impersonation Attack. Black hole attack, Sybil attack, Masquerading attack. Brute force attack, Distributed Denial of service Attack GPS spoofing attack, Wormhole attack
2	Application attack	Bogus information attack safety application attack non safety application attack broadcast tampering attack Illusion attack Message alteration attack
3	Timing attack	Peer to peer timing attack Timing attack for authentication Extended level timing attack
4	Social attack	Social engineering attack
5	Monitoring attack	Man, in the middle attack Traffic analysis attack

Table: 2.1 Classification of VANET Security Attacks

The new threats and vulnerabilities of the security are classified in VANET. The systematic and compressive analysis of VANET securities and their breaches are done. The vulnerabilities and threats based on the security requirements in VANETs are classified around 20 different categories of threats are presented along with various attacks and security procedures in VANET. Each attack is provided with a security procedure. The paper presents attacks based on security requirements such as availability, confidentiality, integrity and attacks on non-repudiation discussed in depth [2].

An algorithm is found to detect malicious node which acts as genuine vehicle during the session of hijacking attack in VANET. The proposed algorithm forms a cluster in the vehicular network and the RSU assigns random ids to all the nodes in the cluster, then the session starts by measuring time gap between the nodes, the distance and traffic flow (TF). A Machine Learning algorithm is used to determine the registered table, where a vehicle is considered as honest vehicle if TF value is less than or equal to 1 and it is added to the registered table. A vehicle is tagged as malicious node if TF value is greater than 1. This result in high throughput, less end to end delay by detecting a malicious node and a smaller number of dropped packets [3].

The State-full network connection is required to maintain the reliable connection between V2V and V2I. The proposed system here is integrating the classic IEEE 802.11p standard and hybrid LTE network that forms a hybrid Cloud-VANET. This gives an efficient routing protocol with high reliability, less congestion and low network overhead in VANET. The suggested system uses the SUMO and OMNET++ to simulate the network scenario which demonstrates that a hybrid cloud-VANET develops the transmission authorization by hitting a low SNIR loss and low ratio of data and packet loss over the network. The proposed system shows that the network connectivity is improved in all traffic densities and is capable of implementing applications like shared storage and Streaming video. This hybrid Cloud-VANET with IEEE 802.11p-LTE based on VANET can be used for future analysis [4].

The Proposed system is centralized Software-defined network (SDN) architecture in VANET. In this network, the LTE which is used as a controller for a long-range network interface, in order to receive and request flow rules and it also controls all the vehicles and the RSU in the network. Author proposed a new algorithm called Sentinel, a new defense procedure which is used to find the source of spoofed packets and mitigate these attacks by creating a flow tree. The analysis of packet flow with respect to time is used to detect flooding attack. Results of mitigation method are promising. Even in different situations such as dense traffic network, the algorithm was able to detect and mitigate the attack. In detection phase, it helps us by avoiding false detections using generated flow rules and number of packets being processed together. When algorithm truly detects an attack, it starts the process by mitigating the attack which is achieved by building a flow tree to localize the bots. Sentinel is able to mitigate attacks even in the scenarios suck as high speed vehicles which didn't affect the results of the algorithm. The classical classification of the algorithm is replaced by new data

classification which uses machine learning. Finally, this algorithm achieves mitigation of 78% in all scenario [5].

To overcome infrequent connections between vehicles and to increase availability of VANETs, we need to efficiently mitigate DDoS attacks by using robust network detection system. The Proposed algorithm is used to detect a DDoS Attack in VANET. In this algorithm, we use big data technologies to detect DDoS attacks on system. This detection system has two components, they are- real-time network traffic collection module and network traffic detection module. To perfectly achieve this system, HDFS is used to store massive attack patterns. Spark is used to detect and increase the processing of packets. In order to evaluate algorithm for accuracy, which is divided into datasets containing NSL-KDD and UNSW-NB15, Random Forest classifier algorithm is used to classify results. When experiments are practically tested out, they show an accuracy of 99.95% and 98.75% in the two datasets respectively [6].

In VANET detection a greedy approach is used which detects and mitigates the DDOS attacks by creating the attack topology and network congestion. In this section, each node bandwidth consumption in the network is analyzed and previous data is evaluated to set the threshold for each node. If threshold is high it means that a node is detected. This node is sent to mitigate by separating that detected node from network. This proposed technique for detecting of malicious nodes in network is less complex than previous algorithm. The proposed method is demonstrated by developing the NS2 simulation, by creating a set of nodes. Finally, the proposed system shows that it is better than the previous techniques in these respective areas such as overhead, packet loss and better throughput. This methodology is used to represent DDoS attacks especially in V2V communication i.e. vehicle to vehicle communication [7].

The detection of an attacker node in a network can be achieved on the basis of frequency and velocity. This algorithm is used to detect both irrelevant and true data. In DDoS, multiple nodes attack different locations at the same time. This Algorithm has been able to detect these types of multiple nodes better than the previous algorithm which was used to detect attacks by a single node. The time span of this network is expanded by the identification of the above-mentioned nodes. The benefit of using this algorithm is that it has improved the identification of the packet algorithm and is able to show an effective difference between the current and previous algorithms [8].

In this proposed system, the packet loss properties of VANETs have been analyzed. The traffic number, the road speed limit and the causes for the failure of the kit were deemed to be empirical considerations. The simulation results show that the packet loss rate of the VANETs varies significantly with the vehicle length, and that the vehicle's moving speed is far lesser than the transmitting speed of the radio waves, which is not the main reason for packet loss. Thanks to the movement of the car, there are random variations in the outcome of the simulation. As the traffic number increases, the capacity decreases slowly [9].

In this proposed system the VANET ID-based system was introduced. Many real-time scenarios like high density traffic combined with much more complex scenarios are evaluated in the simulation. Drawbacks of this system are focused primarily on protecting the integrity of authentication in VANET. In order to keep Master Secrets safe, the keys are spread between two, Low-level TA and Upper level TA during broad deployment of VANET. By using clustering hierarchy, it tremendously reduces responsibility of the credentials. This hierarchical scheme is not sufficient protection throughout a collision and it is not completely secure [10]**.**

.

The defense analysis of the proposed scheme shows that it is secure against numerous recorded attacks and gives additional security features, such as mutual authentication, RSU secrecy properties, and intractability properties. This scheme showed us low latency, high security level and high packet transmission when compare with existing protocols in performance analysis. Opportunistic adaptive neighbor selection-vehicle localization (OANS-VL) protocol and public key encryption is successfully adapted into VANET secured routing using lightweight authentication. In practical analysis, we used different network parameters by using ns2. Therefore, this scheme is suitable for future generation applications in VANET such as E-health, smart transportation and physical societies [11].

Sybil attacks on VANET may be nullified by identification and avoidance techniques. The advantages and disadvantages of each approach published in recent years have been reviewed. In VANET, tool monitoring techniques alone are not enough to uncover Sybil attack with high accuracy and precision. The accuracy, reliability and credibility of the data are enhanced by authentication techniques. Appropriate techniques shall be used in cities for the useful applications of the above classification of the data. Preventing the transfer of false data / information from threats on the network is achieved by combining two approaches that have generated considerable results. The work is not over, but it needs to be done in the future [12**].**

The proposed system is based on Blockchain and MEC. The VANET security architecture is divided into three layers - vision layer, edge processing layer and operation layer. Security of VANET data in contact process is ensured by knowledge layer using blockchain. Second layer namely layer of edge processing offers services and resources such as cloud and computing in cognition layer. Lastly service layer uses Blockchain and standard cloud infrastructure to ensure data security [13].

The proposed system uses standard real-time systems provide discrete resources based on given set of flows and their corresponding metric intensities. In addition, we have shown that the proposed heuristic can be used to provide different facilities and to enhance quality of service (QoS) in VANETs. The proposed system gives priority to the analysis of VANET flows based on their respective strengths. The problem which occurred as PMKP has been shown as NP-Hard. This algorithm is polynomial time because of the complexity in PMKP. In real time, this PMKP formulation is desired to carry out prioritization. This method is a baseline for non-prioritized processing approach, and it is tested against PMKP solution **[**14**].**

Falsified location information in VANET with regional routing protocols contributes to loss of network performance and helps attackers to spread non authentic information. Firstly, the distribution of false information in the network is studied in this proposed study. The identification systems are then used to detect nodes that depends on their location using beacon signals. When simulation is over, the results that obtained reveals about nodes that spread non-authentic information using this verification system and this method reduces the spread of false information. This strategy will not prevent a false attack completely, but will reduce the spread of false position. Major drawback in this system is that it cannot be implemented in real-time scenario. With implementation of much more sensors, better scenarios can be including in this system in future **[**15**].**

The mechanism is used for C-ITS and in detection of new Sybil attacks. Initially, CAM messages provided by neighbors detects attacks using algorithms and it even estimates vehicle velocity based on road segment fundamental design. If the speed of a node is greater than estimated speed and is different from real one, it is used to detect and mitigate attacks by broadcasting an alert message to other nodes. In order to consider it as an attack and not a false one, the trigger node waits for neighbors to send confirmation when an attack is detected. This proposed procedure proved its worth in many scenarios such as high-density scenarios by mitigating 90% of attacks and it can be implemented easily. In future, this design can fight against the attacks by developing counter measures and identifying the attackers **[**16**]**.

For implementing smart transport using VANET, fuzzy logic plays an important role. There is a rapid growth of urban population. Traffic management in areas with denser traffic and at road junction points, is a complex task. Yet security and threat problems remain to be the main obstacles for smart transport. This analysis report mainly focusses on various ways of controlling traffic at road junction points and how to approach various types of attacks. In this paper, introduction part mainly based on how to make transport better by preventing attacks on GA, PSO, ANN and AIS strategies. In second section of this article, Fuzzy logic based VANETs have been expanded. Several smart transport systems which consists of fuzzy logic explained in detail. It explains about two methods i.e. fuzzy controller with traffic signal and without traffic signal. Defects in this system are, there is no importance to cyclists, ambulances and traffic control **[**17**]**.

The simulation of the two protocols listed above shows that the EDAODV protocol exceeds the performance of the AODV protocol except in the case of the performance of the throughput. This is because EDAODV attempts to predict it in advance instead of coping with congestion reactively Ad hoc On Request Vector Routing (AODV) is a reactive vector routing protocol available on request. Its working is in two stages, discovery of the route and maintenance of the lane. The node that wants to send the data to the destination in the routing table looks for an existing route. If no path is identified, the source node will send RREQ messages to all its neighboring nodes, which will refresh their routing table. In maintenance, each node sends a HELLO message here to ensure that there is a working path to the destination after the node receives it. The Early Congestion Detection and Control Route Protocol (EDAODV) is an on-demand route protocol for VANETs. It acts in three stages i.e. Route discovery, early detection of congestion and exploration of the bi-directional way. Connection node looks for the path to the destination when the RREQ message is sent and the RREP message is received. Through the process of route searching, done through sending a BIRREQ packet and, if it reaches an uncongested neighbor node, a BIRREP will be sent to the primary path of the first uncongested neighbor node [18].

Chapter 3

Requirement Analysis and Specification

3.1 Functional requirements

- Real time connection to cloud server. Data is stored and retrieved in real time.
- To implement better protocol for communication between vehicles in VANET system. We have generated real traffic scenario using open street map where number of vehicles, traffic signals has been added.
- We have used SUMO tools to demonstrate the real-world network scenario which is generated by Open Street Map.
- We have done comprehensive analysis in sumo by analyzing throughput, network overhead, congestion between nodes and delay between nodes.
- For better communication, we have used 4 different protocols named as follows (DSR, OLSR, AODV, DSDV)
- We convert the SUMO scenario to the mobility of the .tcl file that includes node attributes Id, node-id, node-speed, node-frequency, protocol)
- Finally, an in-depth analysis of the nodes was carried out using a network simulator (NS-3) where communication between each node analyzed and the node throughput was calculated for the protocol used in each node.
- Graphical analysis of each protocol is done using the gnuplot that gives DSR as the best protocol with a high throughput plus the less delay.

3.2 Non-Functional Requirements

Non-functional requirements address the constraints on the services or functions offered by the application. Some non-functional requirements we look to address are listed below.

- Authentication: The data generated by the user is checked for authentication. In VANET, the data transmitted between nodes must be true and the authentic user must be created.
- Reliability: Data passing through the network is true and error-free and ensures that false information / data is removed.
- Availability: This system handles data transmission between clouds and nodes and ensures that these systems are available for an authentic node.
- Anonymity: System data is generated by vehicle owners. Data privacy of all nodes must therefore be ensured.
- Confidentiality: Important data generated by node is not available to unauthorized

user who is present in network.

- Performance: Performance of system depends upon velocity and distance of system. Performance of system is low when vehicle is stationary.

3.3 sHardware Requirements

The proposed system follows a modularized microservices architecture. The features are deployed as microservices - these services need always-on servers to accept and process requests. We use cloud service provider, such as AWS. The cloud service provider will handle the provisioning and maintenance of the servers and processors.

3.4 Software Requirements

- A Linux based environment for development.
- SUMO, OMNET++, Veins.
- Python3, C++.
- AWS command line interface - to use the cloud services.

3.5 Cost Estimation

The approximate cost estimation of the AWS services is shown in the table.

AWS service	Price	Free tier eligible	Count	Cost
S3 bucket	$0.025 per GB	Yes	3	0
EC2 - t2. medium	$0.0496 per Hour	No	2	$0.0992 per Hour
EC2 - t2. micro	$0.0124 per Hour	Yes	2	0
API Gateway	$3.5 per million API calls	Yes	1	0
EKS	$0.20 per hour	No	1	$0.20 per hour
AWS amplify	$8.08 per month	Yes	1	0
DynamoDB	$5.83 per month	Yes	3	0
SQS	$0.5 per million requests	Yes	2	0

Lex	$0.004 per voice request, and $0.00075 per text request	Yes	1	0
Cognito	$0.0055 per monthly active users	Yes	3	0
Cloud Search	$0.094 per Hour	No	1	$0.094 per Hour
Transcribe	$0.0004 per second	Yes	60	0
Lambda	$10 to $15 per month	Yes	10	0
			Total	$0.3932 per hour

Table 3.1: Cost estimation

Developers	**Effort per week (in hours)**	**Total effort per week (in hours)**
3	12	24

Table 3.2: Effort estimation

Chapter 4

Design

High level design

4.1.1 System Architecture

VANET's are sub class of manet which consists of moving or stationary vehicles are connected by wireless networks. VANET is also known as Intelligent Transport System (ITS) which is trying to achieve safety, efficient flow of traffic and as well as additional traveler. information. Communication between cars is achieved by these protocols such as vehicle to vehicle (V2V), Vehicle to infrastructure(V2I) and vehicle to network(V2N). Most important aspect of VANETs is vehicles move in direction of road and velocity based on speed. The architecture can be divided into three domains namely Management, Mobile and Infrastructure domains.

1. Mobile unit domain:

As name suggests, it consists of units which are capable of moving like vehicles. Between these units, communication can happen in two ways

1. Communication between one vehicle to another vehicle is achieved by V2V communication model.
2. Communication between vehicles to infrastructure is achieved by V2I communication model.

2. Infrastructure domain:

This type of architecture consists of the mainly Road-side units (RSU) and other devices which can establish connection with internet, transceiver which are installed to aid in the vehicle communication. This type of Communication is done by V2I model.

3.Management domain:

This type of domain contains management systems like supervision applications and the cloud servers. When a vehicle sends a message to server about accident or traffic jam, this message is checked for reliability and server sends alert messages to all vehicles in range coming in same way. These kinds of information are so useful for vehicles to deal with the situation.

This architecture even includes OBUs, Application Units (AU):

- Ad-hoc environment: It elaborates on intelligent vehicles that contain basically 2 components.
- OBU (On Board Unit): OBU has four crucial parts which as wireless communication module, GPS module, human-machine interface module and Central control module (CCM). Central control module includes decision making, information transceiver, Judgement making, processing of serial port information and memory. The OBU unit can establish communication between other OBU units and infrastructure. The communication of vehicle with RSU via Dedicated short -range communication (DSRC) radios is achieved by this system where this communication is recognized as mainly assuring standard of wireless to join I2V and V2V.
- AU (Application Unit): For OBU to communicate is facilitated by AU by implementing this program. Connection between OBU and AU is accomplished in two ways i.e. wired and wireless. OBU could be endured by the AU in a particular physical component.

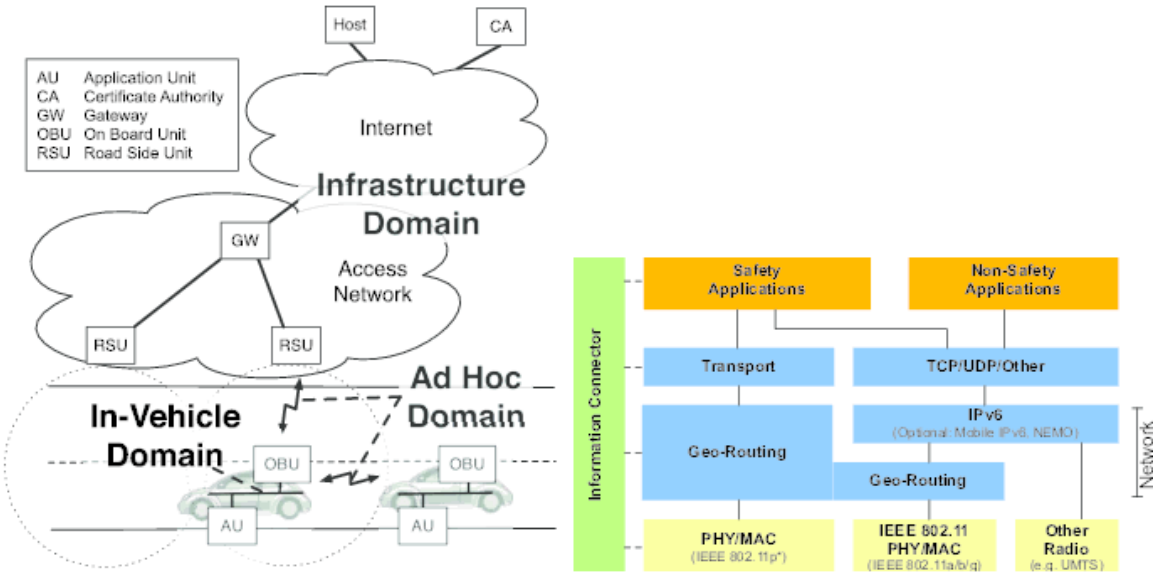

Figure 4.1: VANET Architecture

4.1.3 Interface Design:

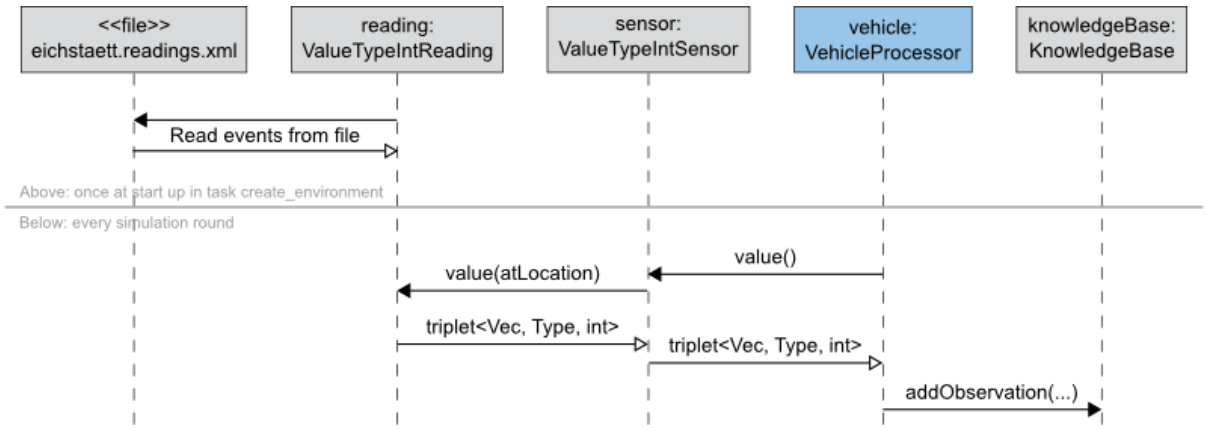

Figure 4.2: Sequence diagram of VANET Architecture

4.2 Methodology:

4.2.1 Generating Real world Scenario using OpenStreetMap.
4.2.2 Integrating with SUMO Tool.
4.2.3 Simulation using SUMO.
4.2.4 Analysis using Network Simulator (NS3).
4.2.5 Graph Analysis using GNUPLOT.

Chapter 5

Conclusion and Future Enhancements

5.1 Conclusion

This report highlights how the VANET environment can be improved by improving driving experience, navigation services, road safety and other roadside services. Due to the characteristics of the VANET system and its architecture, VANET is vulnerable to many security attacks. There is a need to develop security solutions in the VANET environment. Many previous security efforts have applied the same old traditional security solutions without taking into account any special aspects of VANETs. We have studied the security challenges faced by VANETs and their architecture for our literature, which have helped us to come up with this solution to detect and prevent DDoS.

5.2 Future Enhancements

All recent studies in this field focus more on DDoS and Sybil attacks, such as how to detect and prevent them, from the security point of view of VANET. In addition, the report provides various security solutions for various attacks in VANETs using machine learning capable of detecting patterns in attacks. As part of our future work, we create an environment by using simulation tools that help us produce datasets that are greater than general and public datasets by using VCC (Vehicular Cloud Computing). By using this dataset, we can create a real-time context that lets us detect threats. We put forward to provide a solution for detecting and prevent DDoS attacks in VANET along with its prevention rate, detection rate and its own design.

References

[1] Nice Mathew, V. Uma, "VANET Security -Analysis and survey," International Conference on Control, Power, Communication and Computing Technologies (ICCPCT), 2018.

[2] Jeevitha. R, N.Sudha Bhuvaneswari, "Malicious node detection in VANET Session Hijacking Attack," ICECCT.2019.8869452 IEEE 2019.

[3] Mohammad Syfullah, Joanne Mun-Yee Lim, "Data Broadcasting on Cloud-VANET for IEEE 802.11p and LTE Hybrid VANET Architectures," 3rd IEEE International Conference on "Computational Intelligence and Communication Technology" (IEEE-CICT 2017).

[4] Gabriel de Biasi, Luiz F. M. Vieira, Antˆonio A. F. Loureiro, "Sentinel: Defense Mechanism against DDoS Flooding Attack in Software Defined Vehicular Network," IEEE International Conference on Communiciations (ICC-2018).

[5] Ying gao, Hongrui wu, Benjie song, Yaqia jin, Xiongwen luo,Xing zeng, "A distributed network intrusion detection system for ddos detection in vanet," Proceedings of the Second International Conference on Computing Methodologies and Communication (ICCMC 2019) IEEE Conference Record # 42656; IEEE Xplore ISBN:978-1-5386-3452-3.

[6] Charu Guleria, Harsh Kumar Verma. "Improved Detection and Mitigation of DDoS Attack in Vehicular ad hoc Network," 4th International Conference on Computing Communication and Automation (ICCCA) 2018.

[7] Sushil Kumar, Kulwinder Singh Mann, "Prevention of DoS Attacks by Detection of Multiple Malicious Nodes in VANETs," 2019 International Conference on Automation, Computational and Technology Management (ICACTM) Amity University 2019 IEEE.

[8] Yutong Liu, Kai Shi "Analysis of Packet Loss Characteristics in VANETs" 4th International Conference on Computing Communication and Automation (ICCCA) 2018).

[9] Roshini T V, "An Efficient Privacy Preserving Scheduling in VANET using NS-2" ((ICETIETR-2018).

[10] D. Kiruba Sandou, N.Jothy, K.Jayanthi, "Secured Routing in VANETs Using Lightweight Authentication and Key Agreement Protocol" Proceedings of the Second International Conference on Computing Methodologies and Communication (ICCMC 2018) IEEE Conference Record # 42656; IEEE Xplore ISBN:978-1-5386-3452-3.

[11] Salman Ali Syed, B.V.V.S Prasad, "Merged technique to prevent SYBIL Attacks in VANETs," 3rd IEEE International Conference on "Computational Intelligence and Communication Technology" (IEEE-CICT 2019).

[12] Zhang, X., Li, R., & Cui, B. (2018), "A security architecture of VANET based on blockchain and mobile edge computing". 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN).

[13] Ala Al-Fuqaha, "Severity-Based Prioritized Processing of Packets with Application in VANETs" 3rd IEEE International Conference on "Computational Intelligence and Communication Technology" (IEEE-CICT 2017).

[14] A. Asline Celes and N. Edna Elizabeth, "Verification Based Authentication Scheme for Bogus Attacks in VANETs for Secure Communication" 4th International Conference on Computing Communication and Automation (ICCCA) 2018

[15] Marwane Ayaida, Nadhir Message, Geoffrey Wilhelm, "A Novel Sybil Attack Detection Mechanism for C-ITS," 4th International Conference on Computing Communication and Automation (ICCCA) 2019.

[16] Harsha Vardan Maddiboyina, "Fuzzy Logic Based VANETS: A Review on Smart Transportation System", 3rd IEEE International Conference on "Computational Intelligence and Communication Technology" (IEEE-CICT 2019)
[17] Ahmed Yasser, "VANET routing protocol for V2V implementation: A suitable solution for developing countries" Second International Conference on Communiciation and Computational Technologies 2018.
[18] P Sailaja, Banoth Ravi. Jaisingh, "Performance Analysis of AODV and EAODV Routing Protocol Under Congestion Control in VANET", 2018 Second International Conference on Communiciation and Computational Technologies

APPENDIX A: Details of publication:

Author Names: N.S.V Chaitanya, Naveen R, Nikhil Srinivas M, Dr. Nandhini Vineeth

Paper Title: Detection and Avoidance of Security Attacks in Vehicular Adhoc Networks.

Name of the Conference or Journal:

The Paper is to be submitted to

Eleventh international conference on recent trends in information telecommunication and computing -ITC 2020 which will be held during Feb 28-29, 2020 in Bangalore, India.

APPENDIX 2: PROGRAM OUTCOMES

BMS College of Engineering.
Department of Computer Science and Engineering.
Attainment of POs and PSOs

Batch no. :23 Date:01-01-2020
Project Title: **Detection and Avoidance of Security Attacks in VANET's**

PO	Level (3/2/1) 3-High 2-Medium 1-Low	Justification if addressed
PO1	2	Engineering knowledge: Applying the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
PO2	3	Problem analysis: Identify, formulate, review research literature, and analyses complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
PO3	2	Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
PO4	2	Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
PO5	3	Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.
PO6	3	The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

PO7	2	Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
PO8	2	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
PO9	3	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
PO10	2	Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
PO11	3	Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
PO12	3	Life-long learning: Recognize the need for and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

PROGRAM SPECIFIC OUTCOMES

PSO	**Level (3/2/1) 3-High 2-Medium 1-Low**	**Justification if addressed**
PSO1	1	Apply Software Engineering Principles and Practices to provide software solutions
PSO2	3	Design and Develop Network, Mobile and Web based Computational systems under realistic constraints
PSO3	2	Design efficient algorithms and develop effective code.

Submitted by:

USN	NAME	SIGNATURES
1BM16CS053	N.S. V Chaitanya	
1BM16CS055	Naveen R	
1BM16CS058	Nikhil Srinivas M	

APPENDIX C: Plagiarism report