**ATTACKER IDENTIFICATION & INTRUSION DETECTION IN VEHICLE NETWORK**

M.Malathi

Electronics And Communication Engineering

Adhiparasakthi Engineering College

,Melmaruvathur,Chengalpet,India

ecemalathi@gmail.com

J.Raja

Electronics And Communication Engineering

Adhiparasakthi Engineering College

,Melmaruvathur,Chengalpet,India

raja.stj@gmail.com

ABSTRACT

VANET is a form of Mobile Ad-Hoc Network which provides communication between vehicles and roadside base stations. The aim is to provide safety, traffic management, and infotainment services. The security of VANET is in concern state from early time. VANETs face several security threats and there are a number of attacks that can lead to human life loss. Existing VANET systems used detection algorithm to detect the attacks at the verification time in which delay overhead occurred. Batch authenticated and key agreement (ABAKA) scheme is used to authenticate multiple requests sent from different vehicles. Yet it does not provide any priority to the requests from emergency vehicles and a malicious vehicle can send a false message by spoofing the identity of valid vehicles to other vehicles leading to Sybil attack. Priority Batch Verification Algorithm(PBVA) is used to classify there quests obtained from multiple vehicles in order to provide immediate response to emergency vehicles with less time delay. This system also to prevent Sybil attack by restricting timestamps provided by RSU at a nearly stage itself.

**Key words – VANET, intrusion, attack, prevention algorithm**

# INTRODUCTION

The need for transportation is increasing day by day because of this; number of vehicles can also increase dramatically. So it is necessary to regulate vehicle traffic and improve safety for vehicles and human lives on roads. This initiates the development of new kind of network called Vehicular Ad-hoc Network (VANETs) .Vehicular communication network is one of the developing technologies to provide safety for human lives, management of traffic in roads and also disseminates messages to drivers and passengers. The concept of Vehicular Ad-hoc Networks (VANET) came into limelight which has opened new possibilities to avail the use of safety applications. VANET refers to a network created in an ad-hoc manner where different moving vehicles and other connecting devices come in contact over a wireless medium and exchange useful information to one another. A small network is created at the same moment with the vehicles and other devices behaving as nodes in the network. Whatever information the nodes possess is transferred to all other nodes. Similarly all the nodes after transferring their set of data receive the data being transmitted by other nodes. After accumulating all of such data, nodes then work to generate useful information out of the data and then again transmit the information to other devices. The communication between devices expands in such as way where nodes are free to join and leave the network i.e. it is an open network. The new vehicles being launched in the market are now coming with equipped on board sensors which make it easy for the vehicle to easily join and merge in the network and leverage the benefits of VANET.VANET is a variation of MANET (Mobile Ad-hoc Network). MANET comprises of nodes which communicate without central network and where nodes are equipped with networking capabilities. VANET on the other side has emerged as a challenging and more liable class or variation of MANET. The freedom of nodes to enter or leave the network in VANET calls for different routing protocols than MANET. This inter vehicle communication leads to passing and receiving of information so as to increase traffic efficiency, detect road conditions, decrease collisions, detect emergency situations and overall increase the 8884 Ravi Tomar, Manish Prateek and G. H. Sastry efficiency of the network. VANET transfers the information to distant devices as well with the help of multi hops. VANET can be characterized by following factors like dynamic topology, intermittent connectivity, mobility patterns, unlimited storage and onboard sensors. According to Zinxiang Bi (2019) et al., As the number and computational power of electronic computing units installed in standard automobiles continue to increase, contemporary motor vehicles face more cybersecurity threats than previous designs, while providing greater convenience and various useful features. Although vehicles are attacked at various entry points, eventually, attacks are injected into the in-vehicle controller area network (CAN) to cause vehicle anomalies. Currently, OEMs and research fields have implemented protection for the CAN bus in terms of external interfaces, internal protocols, and intrusion detection. Although the deployment of intrusion detection solutions is the most effective approach, the main challenges currently faced by automobile intrusion detection algorithms in practice involve limited computing resources, insufficient real-time responsiveness, and low recognition accuracy. In this study, we propose a novel intrusion detection method based on the message and time transfer matrix to address these difficulties, which can be applied to the vehicle Electronic Control Unit (ECU) to achieve real-time attack signal identification with high accuracy. Experiments on actual vehicles show that the proposed algorithm identified various attacks with high accuracy while consuming less computational and storage resources than previous methods. Moreover, the efficiency of the proposed algorithm is not affected by the attack injection frequency. Compared with other methods, the proposed method achieved better attack identification performance. Additionally, the message and time transfer matrix used by the algorithm can be used as a message transfer fingerprint of the CAN bus to discover anomalies. While the other researcher named **Malhi et al., (2020)**studies show thatVehicles equipped with significant computing, communication and sensing (also known as “smart” vehicles), are being focused by Intelligent Transportation Systems (ITS). The primitive target of Vehicular Ad-Hoc Networks (VANETs) is to deliver safer and efficient traffic conditions by providing real time traffic conditions to automobiles and involved trusted third parties. This paper reviews eminent safety solutions to address the security aspects for VANETs. Four ingredients of this paper are (a) attacks and security mechanisms in VANETs (b) comparative analysis of security schemes based on cryptography mechanism used (c) trust management schemes based upon discrete characteristics and intrusion detection systems (d) open issues which need a thorough consideration in the future. Here we discuss how the research reflects the evolutionary growth of security attacks with its future prophesy, based upon the past developments in the area of computer security.

# REQUIREMENTS

**HARDWARE REQUIREMENTS**

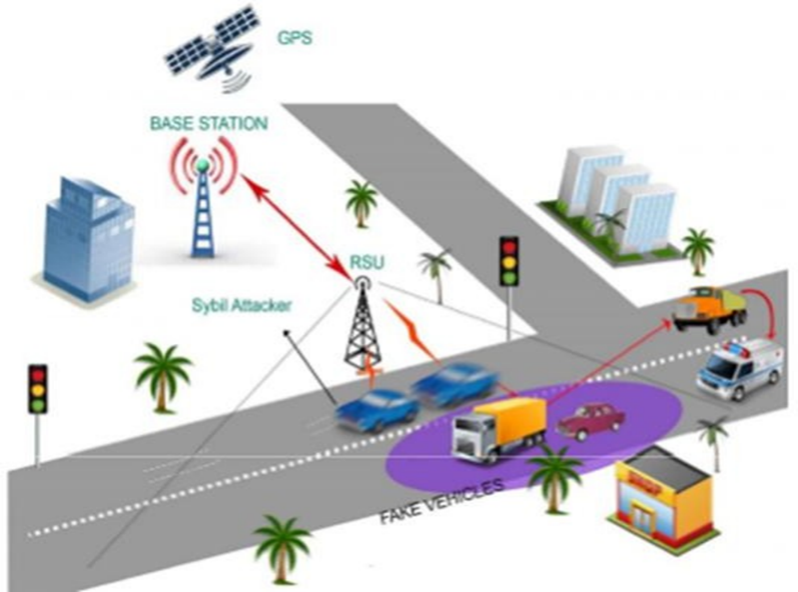
The hardware requirements of this paper serve as a tool for capturing the gestures of the user to be used for authentication by the system. The following are the hardware specifications, A system of Pentium IV 2.4 GHz, 40 GB hard disk, 44 MB floppy drive, a monitor of 15 VGA color, and a RAM of 512 MB.

**SOFTWARE REQUIREMENTS**

The software based requirements of this paper are pertinent to the tools used for the processing of the live input feed. The requirements are a Network simulator tool, Ubuntu OS, a Language TCL and a Backend C++.

# SYSTEM ANALYSIS

The existing system used to defend against the Sybil attack with only support of Road Side Unit (RSU). Whenever a vehicle passes the RSU it obtains a timestamp. If a vehicle wants to send a message to another vehicle, it incorporates the timestamp inside the message. The author finds it impossible for two vehicles to pass two or more RSUs at the same time, so there must be a small time difference between them. According to the timestamp provided by the RSU, a new kind of timestamp series mechanism is developed. It is difficult for two vehicles to obtain the same timestamp while crossing multiple RSUs. From this a Sybil attack can be detected. Secure batch verification is carried out to avoid the invalid or false message from the unauthenticated or even authenticated vehicles. By avoiding these false messages, road accidents and traffic jams can be prevented to continue the safe and secure transportation. A digital signature is used to ensure the identity authentication and message integrity. A vehicle signs the message with digital signature and then sends it to the RSUs for verification. They improve the scheme to prevent replay attack and forgery attack. The scheme includes key generation and pre-distribution phase, pseudo identity generation and message signing phase, identity tracing and message verification phase. Tracking of vehicle identity becomes difficult when the generation of pseudo identity for vehicle gets failed. There is also threat for replay and non-reputation of digital signatures. The identity of vehicle can be lost. The Sybil attack detection based on signature vectors (SADSIV) in VANETs. Each node gathers the digital signatures in their moving; then the algorithm detects Sybil attack by analyzing and comparing vehicle nodes’ signature vectors independently under the condition of inadequate infrastructures. While the Proposed system present an algorithm to detect the Sybil attack detection based on signature vectors (SADSIV) in VANETs. There are some distributed authority units (AUs) in a VANET system. These AUs are comprised of authorized RSUs and some mobile nodes, including police or public transport vehicles. It is assumed that these authorized units can provide the digital signatures with timestamp for the vehicle nodes periodically. And all vehicle nodes will record these digital signatures for the detection. And these legal nodes gather and record the signature vectors from different AUs in their movement. In contrast, Sybil nodes have the same locations and motion trajectories all the time. They always get the signatures from same AUs because of their consistent trajectories. The authorized units provide signatures with timestamp every one minute. In an algorithm when a detector wants to detect Sybil attackers around, it gathers the neighboring nodes signature vectors. A signature vector is more robust and it is obtained based on the collaboration of neighboring nodes. Each vehicle can independently detect Sybil attack by comparing the differences of neighboring nodes digital signature vectors; this algorithm is more feasible even less infrastructure resources.



**Fig 1.1** System Architecture

# MODULES

In this paper two modules have been used. One is Sybil attack prevention mechanism module while the other is priority batch verification algorithm.

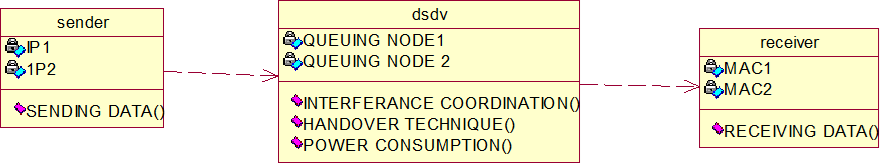
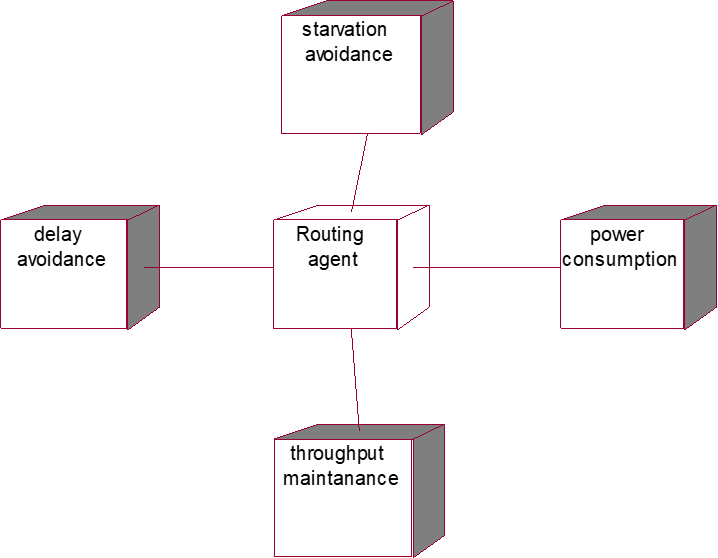
**Sybil attack prevention mechanism**

In safety applications, vehicles can send a message to neighbor vehicles, vehicles need a timestamp (denotes at which time a vehicle passes a particular RSU). It has to attach time stamps in every messages. When a vehicle obtains multiple timestamps from a single RSU then it may act as an attacker and send a Sybil message to other vehicles in order to deviate or slow them down. An attacker spoofs identities of legitimate vehicles. It sends a false message that contains the timestamp obtained from RSU by using these identities. While receiving multiple messages from different vehicles, legitimate vehicles decide that some accident or traffic has occurred and take another route or reduces it speed. It is not necessary to provide a timestamp to a single vehicle within a short period of time by RSU. Our attack prevention algorithm restricts the providing of continuous timestamps to the particular vehicle within a small time interval. The RSU sets the timer when it provides a timestamp to the vehicle for the first time. Before the timer expires a vehicle again sends a request for timestamp which means there is a chance that the vehicle may be an attacker then RSU denies to provide timestamp and discards the request and then tracks the vehicle to find whether the vehicle is an attacker or a legitimate vehicle.

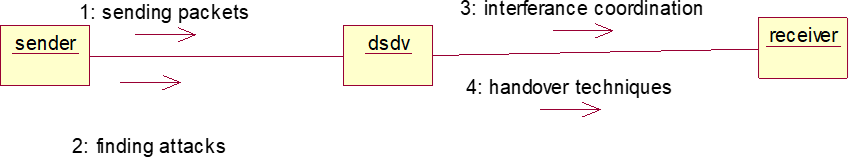
**Priority batch verification algorithm**

It is common multiple vehicles send request to single RSU at same time. Generally RSU perform operation on those received request by using batch verification algorithm. But it does not assign any priority and provide response to the request from emergency vehicles. It is very important to provide immediate services to emergency vehicles. The Proposed model Priority Batch Verification Algorithm (PBVA) is installed in each RSU. When RSU receives multiple requests at the same time, PBVA processes these requests in order to detect any request received from emergency vehicles.RSU classify the obtained requests by using the vehicle identifier found in the received requests. Each vehicle in the VANET has unique identifier by this only RSU identifies whether it is an emergency vehicles or other general vehicles. If RSU obtains requests from emergency vehicles our mechanism PBVA immediately processes these requests and sends necessary services to that vehicle without time delay.

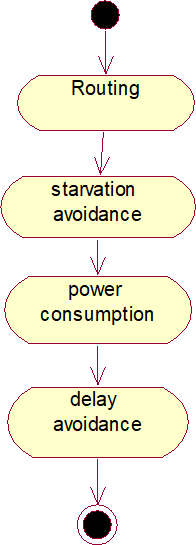
# CLASS DIAGRAM



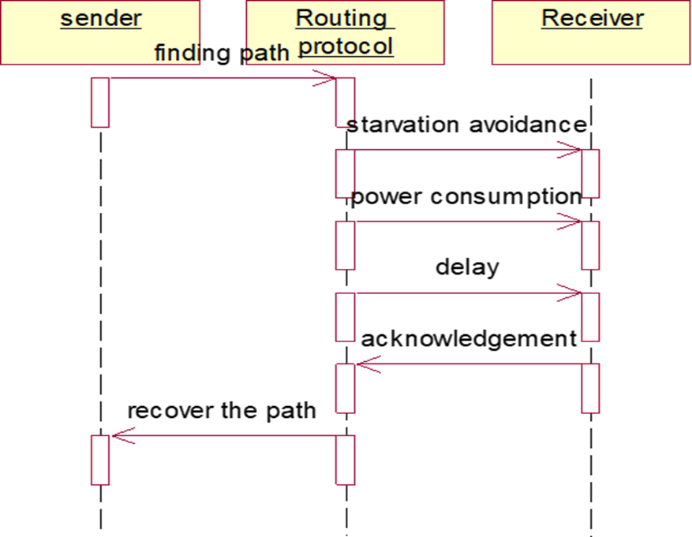
**Fig 2.1** Class Diagram **Fig 2.2** Collaboration diagram



**Fig 2.3** Activity diagram



**Fig 2.4**  Deployment diagram

****

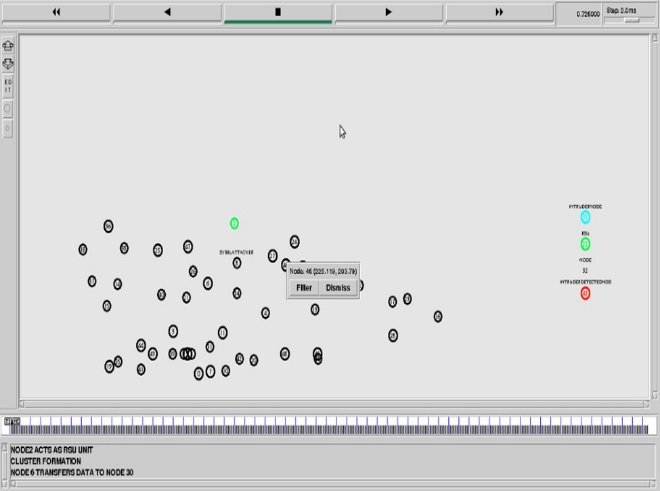
**Fig 2.5**Sequence diagram

**RESULTS**

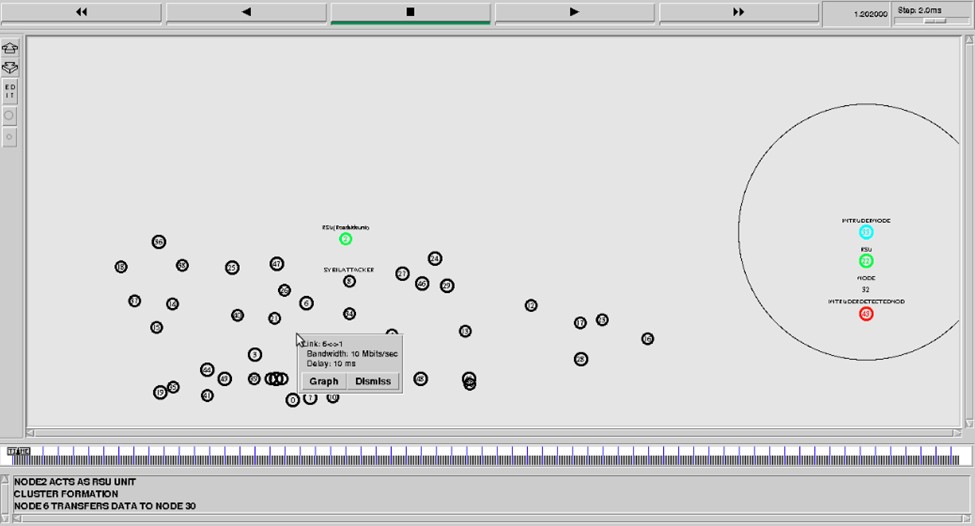
The screenshots of the roadside unit function has been attached below.



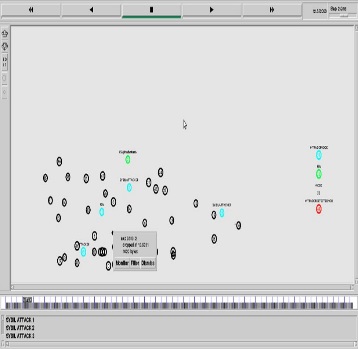
**Fig 7** Representation of **RSU**



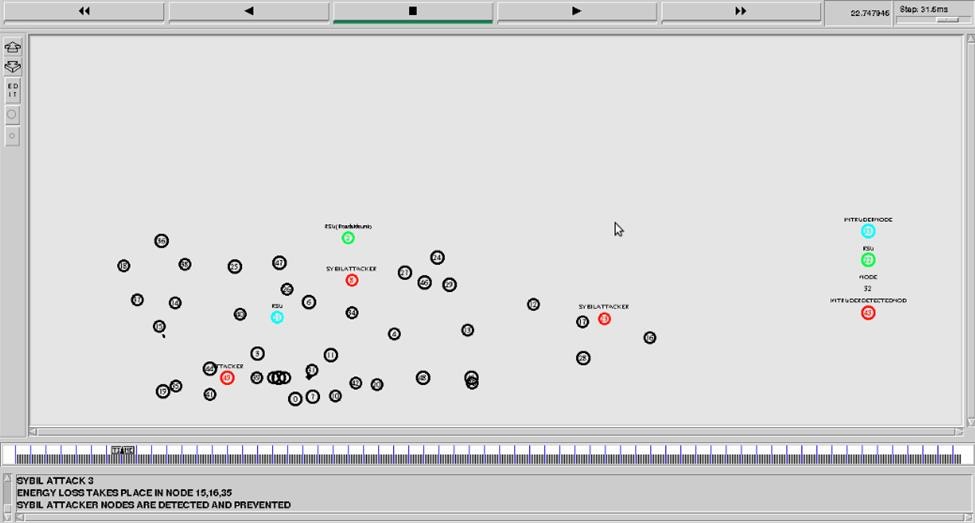
**Fig3.1** Representation of Router Table



**Fig 3.2**Bandwith Utilization



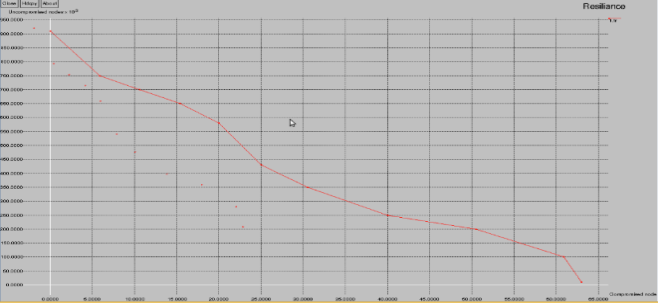
**Fig 3.3**Sybil attack

****

**Fig 3.4** prevented Sybil Attack

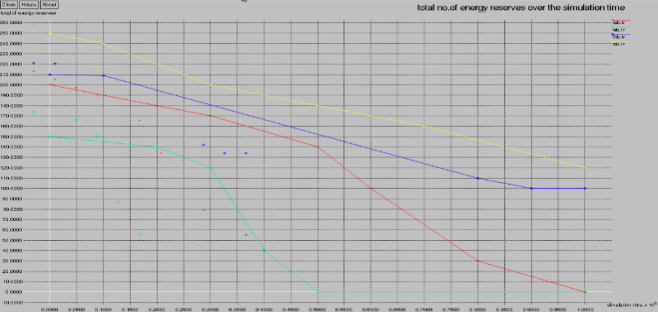
# PERFORMANCE EVALUATION

The performance evaluation was done. According to the studies the yellow line represents the proposed hybrid protocol, red line represents the Reactive protocol, blue line represents the proactive protocol, while the green represents the active trust protocol. After conducting certain tests, certain parameters have been checked and has been represented graphically. From **Fig 4.1**  it could be analyzed that the nodes are lesser resilient and they start decreasing with thw increase of the compromised nodes. Hence the uncompromised nodes are lesser resilient towards the compromised nodes.



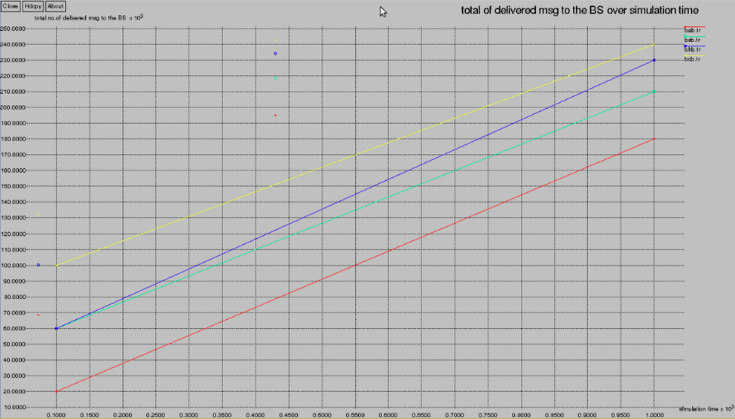
**Fig4.1**Graphical representation of Resilience.

From **Fig 4.2**it could be inferred that the proposed hybrid protocol has the highest energy reserves with respect to the simulation time. While Active trust protocol started to dropdown after it reached the certain simulation time.

****

**Fig 4.2**Total no. of energy reserves over the simulation time.

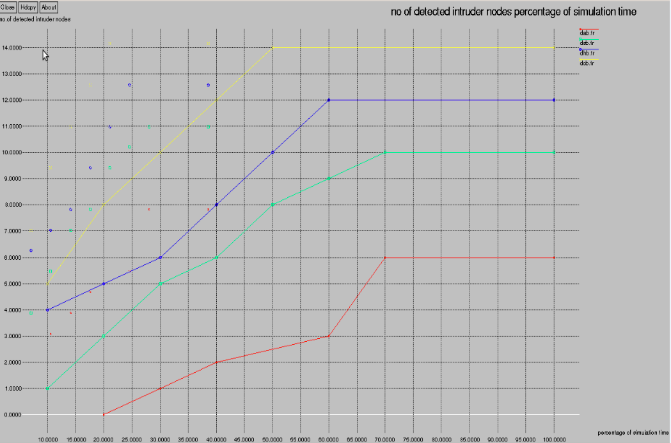
**Fig 4.3** inferred that the data rates of the proposed hybrid protocols were higher with respect to the simulation time while the reactive protocol was the slowest.



**Fig 4.3**Total no. of delivered messages to the BS over the simulation time.

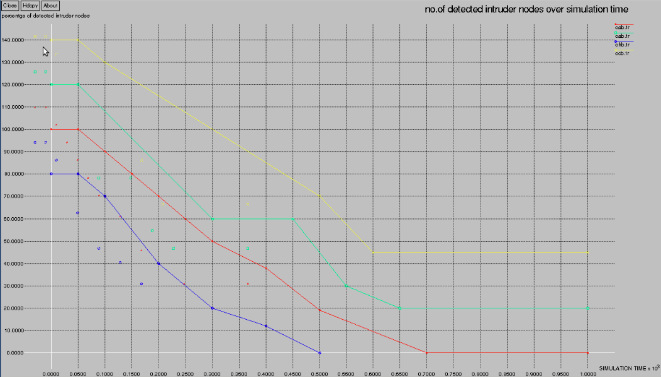
**Fig 4.4** refers to the detected malicious nodes.

According to the graph, the no. of detected malicious nodes percentages were higher in the proposed system. While all the other failed to detect it.



**Fig 4.4** Total No. of detected intruder nodes in percentage.

From **Fig 4.5** it could be said that the intruder nodes were detected higher in the proposed system.

****

**Fig 4.5** Total no of detected intruder nodes.

# CONCLUSION

Our proposed system PBVA algorithm is used to process multiple request at a single time and also to provide immediate response to the request from emergency vehicles. By using attack prevention mechanism, to prevent Sybil attack in early stages itself through restricting the time stamp.

# FUTURE WORKS

It is used to prevent attack, without restricting the provision of timestamps to vehicles. It is used to minimize the computation work of algorithm.

# REFERENCES

1. Abien Fred M. Agarap, 2018, “A Neural Network Architecture Combining Gated Recurrent Unit (GRU) and Support Vector Machine (SVM) for Intrusion Detection in Network Traffic Data,” Proceedings of the 2018 10th International Conference on Machine Learning and Computing, ACM.
2. Aburomman, Abdulla Amin and Mamun Bin IbneReaz, 2016, “A novel SVM-kNN- PSO ensemble method for intrusion detection system,” AppliedSoftComputing, Vol. 38, pp.360-372.
3. Al-Yaseen, WathiqLaftah, Zulaiha Ali Othman and MohdZakree Ahmad Nazri, 2017 “Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system,” Expert Systems with Applications Vol. 67, pp.296-303.
4. Ashfaq and RanaAamirRaza, et al., 2017 ,“Fuzziness based semi-supervised learning approach for intrusion detection system,” InformationSciences, Vol. 378, pp. 484-497.
5. Avleen Kaur Malhi, ShaliniBatra, Husanbir Singh Pannu, 2020,”Security of vehicular ad-hoc networks: A comprehensive survey, Computers & Security”.
6. Bamakan and SeyedMojtabaHosseini, et al., 2016, “An effective intrusion detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization,” Neurocomputing, Vol. 199, pp.90-102.
7. Cabaj, Krzysztof, MarcinGregorczyk and WojciechMazurczyk, 2018 ,“Software- defined networking-based crypto ransomware detection using HTTP traffic characteristics,” Computers & Electrical Engineering, Vol. 66, pp.353-368.
8. Eesa, Adel Sabry, ZeynepOrman and Adnan MohsinAbdulazeezBrifcani, 2015 ,“A novel feature-selection approach based on the cuttlefish optimization algorithm for intrusion detection systems,” Expert Systems with Applications ,Vol.42, No.5, pp.2670-2679.
9. Elhag, Salma, et al, 2015 ,“On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on intrusion detection systems,” Expert Systems withApplicationsVol.42,No.1,pp.193-202.
10. Elike Hodo, et al., 2017 “Shallow and deep networks intrusion detection system: A taxonomy and survey,” arXivpreprintar, Vol. Xiv: 1701. 02145.
11. GhassanSamara ,Wafaa A.H. Al-Salihy , R. Sures 2012 , “Security Issues and Challenges of Vehicular Ad Hoc Networks(VANET)”, IEEE Xplore.
12. and R. Sankar, 2014, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," in IEEE Communications Surveys & Tutorials.
13. I. Idrissi, M. Azizi and O. Moussaoui, 2020, "IoT security with Deep Learning-based Intrusion Detection Systems: A systematic literature review," 2020 Fourth International Conference On Intelligent Computing in Data Sciences (ICDS).
14. Jeong, EunHee and ByungKwan Lee, 2014, “An IP Traceback Protocol using a Compressed Hash Table, a Sinkhole router and data mining based on network forensics against network attacks,” Future Generation Computer Systems, Vol.33, pp.42-52.
15. Kevric, Jasmin, SamedJukic and AbdulhamitSubasi, 2017, “An effective combining classifier approach using tree algorithms for network intrusion detection,” Neural Computing and Applications, Vol. 28, No.1, pp.1051-1058.
16. Kuang, Fangjun, WeihongXu and Siyang Zhang, 2014 ,“A novel hybrid KPCA and SVM with GA model for intrusion detection,” Applied Soft Computing,Vol.18,pp.178-184.
17. Li, Wenchao, et al., 2014 ,“A new intrusion detection system based on KNN classification algorithm in wireless sensor network,” Journal of Electrical and Computer Engineering.
18. Li, Longjie, et al., 2018, “Towards Effective Network Intrusion Detection: A Hybrid Model Integrating Gini Index and GBDT with PSO,” Journal of Sensors.
19. MR Gauthama Raman, et al., 2017, “A hypergraph and arithmetic residue-based probabilistic neural network for classification in intrusion detection systems,” NeuralNetworks, Vol. 92, pp.89-97.
20. Mustafa Amir Faisal, et al., 2015, “Data-Stream-Based Intrusion Detection System for Advanced Metering Infrastructure in Smart Grid: A Feasibility Study,” IEEE Systems journal,Vol.9,No.1,pp.31-44.
21. Nathan Keegan, et al., 2016, “A survey of cloud-based network intrusion detection analysis,” Human-centric Computing and Information Sciences, Vol.6, No.1, pp.19.
22. Sandeep Kumar Singh, et al., 2018 ,“Joint-Transformation-Based Detection of False Data Injection Attacks in Smart Grid,” IEEE Transactions on Industrial Informatics, Vol. 14, No.1, pp. 89-97.
23. Shah Khalid Khan, NirajanShiwakoti, Peter Stasinopoulos, 2022, “A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles”.
24. Shengyi Pan, Thomas Morris and UttamAdhikari, 2015, “Developing a hybrid intrusion detection system using data mining for power systems,” IEEE Transactions on SmartGrid,Vol.6,No.6,pp.3104-3113.
25. Soo-YeonJi, et al., 2016, “A multi-level intrusion detection method for abnormal network behaviors,” Journal of Network and Computer Applications, Vol. 62, pp. 9- 17.
26. Syed Ali Raza Shah and BijuIssac, 2018, “Performance comparison of intrusion detection systems and application of machine learning to Snort system,” Future Generation Computer Systems, Vol. 80, pp.157-170.