Detection and prevention from different attacks in VANET: A Survey

Arun Singh Kaurav¹, Sushama Rani Dutta²

¹Research Scholar, ²Assistant Professor, Department of Computer Science & Engineering, KL Deemed to be University, Hyderabad, India
E-mail: aru.esoft678@gmail.com, sushamadutta@klh.edu.in

Abstract. Routing attacks will have distressing effects over the network and bequest a significant challenge once planning strong security mechanisms for vehicular communication. In this paper, we examine the effect and malicious activities of a number of the foremost common attacks and also mention some security schemes against some major attacks in VANET. The attacker's aim is only to modify the actual route or provides the false data about the route to the sender and also some attackers are only flooding unwanted packets to consume resources in available network. Various routing approaches are also mentioned in the paper because the routing of data is very important to deliver the traffic information to leading vehicles. It's advised that a number of the ways that to approach this made field of analysis issues in VANET might be to fastidiously design new secure routing protocols in which attacks are often rendered meaningless and because of the inherent constraints found in the network, there's a desire for light-weight and sturdy security mechanisms.

Keywords—VANET, Attack, Security, RSU, Nodes, Routing

1. Introduction

The wireless communication is the revolution in communication in between sender and receiver. The wireless network consists of towers, exchange offices, servers and mobile users [1]. The numbers of users are connected to tower/s and then the signals that are goes miles away [1,2]. The satellites also have very important role in communication [3]. In near living conditions associated with the location, the natural sensing process closes the sensor nodes and converts them into an electrical signal. Sensor’s signal contains some properties about substance situated and events occurring within the vicinity of the mobile nodes. Wireless Mesh Network (WMN) is a very secure network since it links all the nodes within each other's range [4]. The main in WMN is extra overhead for establish link with all in the range nodes. In some applications involving unattended operations [2][4], an outsized range of those non-reusable sensors is often networked. A WSN includes many sensing nodes. These sensors are able to interact flexibly with each other or with the external base station (BS) [4].

In the area of wireless communication, VANET has been the important research area in wireless connection. The parent field of ad-hoc network is known as VANET. Attacks can also easily influence the open network and security restrictions must be established and stopped from attacking the network [4]. VANET is a part of MANET which without relying on the opposite
infrastructure, organizes its own communication system [5]. The primary common application of MANET is a limited amount of knowledge exchange between various computers in the military due to its easy and basic communication mechanism. In distant and seldom hostile areas, it incorporates, by hand and gloves, space-dispersed autonomous small devices monitoring environmental or physical conditions. In recent advancements, development of micro-level and less costly sensors is feasible economically and technically. Before going into VANET, it is necessary to discuss its background related to the wireless communication i.e., shown in figure 1.

![Classification of Wireless Network](image)

Along with certain improvements, VANET is analogous to MANET. VANET consists of handheld nodes, side-of-road units [6]. Remote nodes are devices embedded in automobiles called on-board data sharing networks between Road Side Systems. RSUs are fixed installed devices that links between the MN and the servers or the Internet for connectivity purposes. There are many services provided by VANET, but most notably, road safety services are distributed over the Internet to reduce road fatalities by data sharing.

Many applications are used by VANET to create contact between vehicles. It is possible to relay information about congested areas from one car to another vehicle, warning drivers of collisions or potential traffic jams. Drivers are told that they are heading to a place where an accident or traffic jams are occurring. When this information taken as an input for the system of vehicle navigation to escape a crowded area, the system often produces alternate routes. Real-time travel information regarding vehicle is obtained and analysed by the RSU [7]. First the RSU produces traffic information that includes data like average pace of the vehicle, vehicle density, and traffic jam incidents. Finally, it is transmitted to relatively distant vehicles by the RSU. After the traffic information is obtained, the vehicles evaluate it with road condition data.

2. Types of communication in VANET

Communication modes are of two types, which are differentiated as follows:

The first is vehicle to RSU or vehicle to Infrastructure (V-I) and second one is vehicle to vehicle (V-V) communication. In vehicle to infrastructure communication the road unit is needed for transmutation. The node or vehicle interacts with the RSU and collects information from the network. The V-RSU communication is more superior because it enhances the possibility reliable communication. The main target is to increase vehicle safety. Suppose, any vehicle detects an abnormal situation or condition, it can also inform other vehicles[8].
In vehicle-to-vehicle communication, as shown in figure 3, vehicles communicate between each another. While for Vehicle-to-RSU communication, vehicles form an Ad-Hoc network, called VANET mentioned in figure 2. VANET is a distinct kind of Mobile Ad-Hoc Network (MANET) instead of nodes which has vehicles. VANET is a self-organizing and both centralized and decentralized network composed of high-speed moving vehicle [7]. In vehicle-to-vehicle communication chances of malicious actions is more compared to Vehicle to RSU communication. The message or information is more accurate in V-RSU communication. The vehicles that are using the highway have no need to ensure traffic status because high mobility speed is there. It is also possible to gain traffic information at that time of also down the speed of vehicle/s. The communication is only in between the vehicles mentioned in figure 3.
Many applications are used by VANET to create contact between vehicles. Information on congested roads may be conveyed from one car to another vehicle, warning drivers about crashes or possible traffic delays. Drivers are advised they are going to a location where there is an accident or traffic congestion. The method also generates alternative routes as this information is used as an input for the system of vehicle navigation to avoid a crowded area. The real-time movement data of a vehicle is obtained and processed by the RSU [9]. First the RSU produces traffic information that involves data such as vehicle average speed, vehicle number, and traffic jam incidents. Finally, it is communicated by the RSU to comparatively distant cars. After receiving the traffic information, the cars evaluate it along with the road condition data.

3. Network Model

In VANET [10], network artefacts can be separated into three groups. These groups include servers for application and authorization, facilities on the road side, and nodes/vehicles.

3.1. Application and Authorization Servers

These are powerful workstations, responsible respectively for managing and providing service data. The authority knows all the keys and is accountable for maintenance planning. For cars, device servers provide operation details. The government or foreign operators will fund them. We assume there are powerful processing capabilities for authorization and application servers. So, here we ignored computation time.

3.2. Road Side Infrastructure

Road Infrastructure consists of power supplies located near roads and responsible for the collection and dissemination of data. Through wired networks, RSUs are connected to power and communicate via radio with vehicles.

3.3. Nodes/ Vehicles

Nodes or Vehicles are moves in the road and communication with the RSU or also their information exchange information is received by RSU in network. Every vehicle is presumed to be fitted with a differential GPS receiver with a meter-order accuracy and an on-board computer (OBU) [11] responsible for all communication and computing tasks.

4. VANET Mobility Factor

Movement of vehicles are connected with cars, railways, bicycles, motorcycles and everything on the roads that moves with the wheels [12] [13]. For cars in the VANET, many factors influence their mobility, for example:

4.1. A. Street Construction

The highways, directions, traffic signals and signs on road determine traffic. Intersections and one or more roads, one-way or two-way, often affect it. In the simulation, intersections result in slower speeds, high knot density, and require to assign a probability value to predict each vehicle's rotation direction. Overtaking is banned on single-lane roads and speed is restricted and reliant on potential cars, whereas overtaking is permitted on multi-lane roads and driving is considered easier and safer.

4.2. Block Size

One of the small areas surrounded by streets can be considered. The size helps to assess intersections and how much the car decelerates and slows. Furthermore, streets with less intersections allow cars with more intersections to drive to higher speeds than city blocks. Vehicles are needed for slowing down more often and more accurate agility details will be considered.
4.3. Motion Control Mechanism
As mentioned in the first paragraph, streets differ in their designation. Traffic lights and stop signs are the major signs that consist predetermined location and help make any proposed mobility model more realistic [10]. They will summon the tail and slow down.

4.4. Interdependent Vehicle Traffic
Movement of vehicles effect the surrounding vehicles. Vehicle will be slow down, accelerate, change lanes, or even stop.

4.5. Average Speed
The higher the vehicle speed, the faster it will change position or location. In addition, speed limits affect the average vehicle speed. This can lead to changes in the connection to the network or network topology [11].

5. Routing Protocols in VANET
Routing protocols may be divided into several types based on their characteristics [14, 15]. Most popular method for differentiating VANET routing protocols depends on obtain and preserve routing information. Routing protocols are classed as follows:

5.1. Proactive Protocols
They monitor the networks topology all the times and the routes will be evaluated for all destinations continuously. Routes are stored by performing interchange of routing tables periodically in network, like the wired network. An advantage of this protocol is that routes must be decided and maintained in the buffer so whenever routing takes place these routes are used immediately so that the overall delay in the system must be reduced. To get the information of route and making a session is not very time consuming. This protocol has a disadvantage that whenever the topology changes, it reacts to those changes, though traffic is not affected, and results in the unwanted use of the bandwidth even there is not transfer of data. The protocols of this type are Optimized link state routing protocol and Destination sequenced distance vector routing protocol.

5.2. Reactive Routing
This protocol, often known as on demand routing protocols, only perform route determination on demand. In data transfer, reactive protocols select a route only at the start of a connection. It is done by launching the discovery of route by flooding it with packet known as route requests packets. once the route is created, the details are kept in the database of routing until the destination is unable to reach or the route expires. Because routing information is not updated on a regular basis, routing overhead is decreased dramatically during topology changes. The delay experienced during route finding is one of these systems’ drawbacks. These protocols, however, must be particularly efficient for highly mobile networks. AODV i.e., Ad hoc On-demand Distance Vector routing protocol and DSR i.e., Dynamic Source Routing (DSR) are two routing methods that fall under this category.

5.3. Hybrid Protocols
The benefits of both proactive and reactive routing systems are combined in hybrid routing strategies. On-demand routing offers less routing costs than traditional routing, however it suffers from routing latency. Table-driven routing guarantees great quality in static topologies but cannot be used to mobile networks. Combining the best features of both, a few hybrids routing protocols have been devised, in which routing is launched with certain proactive routes and subsequently satisfies demand from other nodes via reactive floods. Hybrid protocols make use of hierarchical network designs. In a dynamic network, typical routing protocols of this category include Zone Routing Protocol (ZRP).
6. **Types of attacks in MANET**

   It defines the intrusion as an action which tries to harm the main components of the security system [4]
   1) The integrity
   2) Availability of a resource
   3) Confidentiality
In the same work, the intruder therefore was defined as a private or group of people who take the action in the intrusion. The plainness of the many routing protocols for wireless sensor networks makes them a simple target for the attacks [16] [17]. The routing attacks are classified into the subsequent categories are:

   **6.1. Modified, or Replayed Routing Information**
   While sending the info, the data in transition could also be spoofed, altered, destroyed or resent. Due to short range communication of the nodes i.e., sensor nodes, an attacker having very huge power of the communication and the processing range can attack sensors parallelly and changes the sent information.

   **6.2. Selective Forwarding**
   In this reasonably attack the suspicious node may decline to forward every message it gets, acting as region or it could forward some messages to the incorrect receiver and simply drop others

   **6.3. Sinkhole Attack**
   The attacker aims to draw in all traffic. In case of a flooding-based protocol the compromised node may hear requests for routes, and then reply to the requesting node with messages restraining a bogus route with the shortest way to requested destination.

   **6.4. Sybil Attack**
   The malicious node will present itself as the multiple nodes. The attack of this kind aims to decrease the use and decrease the effectiveness of algorithms used. It is often performed against dispersed storage, routing, aggregation of data, correct resource allocation, voting and mischief detection [11].

   **6.5. Wormhole Attack**
   In this attack [12] the node that is malicious, tunnels messages from the one side of network on link, that normally not exists, to another side of network. The only sort of that kind of attack is to convince the nodes that they're neighbors. The attacks of this kind can be utilized with the select forwarding and eavesdropping

7. **Literature Survey**
   The contribution of various researchers in field of VANET security is discussed in this section. These previous works are providing the idea of novel security scheme in VANET. Also found the research gad in recent work i.e. mention it in table 1.
The framework, in particular, is based on the Dirichlet distribution, foundation for platoon service requests and platoon management. Computation. Furthermore, vehicle communications serve as the communications safeguard manner. The private key cryptography specially designed to defend VANET in a unique vehicle architecture of the security is called hybrid key cryptography, communications protection in ad hoc vehicle networks. The method is based on IWD (intelligent water droplets), and the confidence model is applied. In dynamic moving networks, where nodes move at fast rates and the network architecture is unstable, IWD offers the following advantages: it is employed in systems that can adapt to shifts and have a highly crucial high processing speed. Trust is the most important aspect in establishing a trusted vehicle environment that promotes safety in car networks.

This research developed a Swarm-based technique for detecting routing attacks on VANET networks. The method is based on IWD (intelligent water droplets), and the confidence model is applied. In dynamic moving networks, where nodes move at fast rates and the network architecture is unstable, IWD offers the following advantages: it is employed in systems that can adapt to shifts and have a highly crucial high processing speed. Trust is the most important aspect in establishing a trusted vehicle environment that promotes safety in car networks.

This research focuses on hybrid device to device message authentication (HDMA) technique for the 5G-supported VANETs is suggested, which employs a unique group signature-based technique for the mutual authentication between V2V communication. In addition, to decrease the calculation overhead of the modular exponentiation process, an already calculated lookup database is used.

In this research a hybrid architecture, consisting of automobiles, boulevard side units (RSUs), a server, and a trust authority (TA), is described, allowing for feedback storage and integrity ranking computation. Furthermore, vehicle communications serve as the foundation for platoon service requests and platoon management. The framework, in particular, is based on the Dirichlet distribution, which ensures great accuracy and dynamics.

Table 1 Related Work Overview

| S.No. | Reference | Worked Done | Drawbacks |
|-------|-----------|-------------|-----------|
| 1     | [18]      | This research highlights key flaws for the protocols suggested for V-to-I and V-to-V communication and suggests an alternative protocol suite. Authentication of driver, key exchanges, data exchange, change of offline password, protocols for vehicle complain are part of our suite. V-to-I protocol for key exchange allows handoff capabilities to provide ongoing authentication when cars move from one RSU area to other. | In different groups, how they decide the direction of vehicles because no direction information not transfer with traffic request packets. Performance measure in average speed of vehicles but actually vehicles speed is random. |
| 2     | [19]      | In this research focus is on hybrid device to device message authentication (HDMA) technique for the 5G-supported VANETs is suggested, which employs a unique group signature-based technique for the mutual authentication between V2V communication. In addition, to decrease the calculation overhead of the modular exponentiation process, an already calculated lookup database is used. | Storage or computation overhead for revocation is high. In city scenario security is important but on highways guidelines available. |
| 3     | [20]      | This research developed a Swarm-based technique for detecting routing attacks on VANET networks. The method is based on IWD (intelligent water droplets), and the confidence model is applied. In dynamic moving networks, where nodes move at fast rates and the network architecture is unstable, IWD offers the following advantages: it is employed in systems that can adapt to shifts and have a highly crucial high processing speed. Trust is the most important aspect in establishing a trusted vehicle environment that promotes safety in car networks. | Trust based scheme is based on bandwidth and delay. But due to high packet dropping delay and bandwidth shows satisfactory values. How to reach to malicious node is not mentioned. The attacker identification is not possible because trust is calculated at receiver end and here the receiver is attacker. |
| 4     | [21]      | This method outlines the suggested safety method for vehicle communications protection in ad hoc vehicle networks. The architecture of the security is called hybrid key cryptography, specially designed to defend VANET in a unique vehicle communications safeguard manner. The private key cryptography public key cryptography used to encode and decode facts distinguishes this security method. For security, AES and RSA are employed. | Both techniques are old and enhance overhead in dynamic network. Never identified dropping but performance of key exchange secure communication. The detection of attacker and prevention are not elaborated. |
| 5     | [22]      | The author focuses largely on the hole formation assault in this research, in which malevolent or attacker drivers inside the network scatter the links by lowering or increasing their own speed to generate holes. The Stable Routing Protocol (RRP) protect messages from hole formation attacks between the source and destination. To protect against the vulnerability created by the VANET malicious drivers, RRP comprises of an attacker node or normal node security module and a recovery module. | From attacker nodes, loss is not mentioned and also number of attacker nodes which are flood the wrong information in traffic. The overhead of control also is not calculated which consist the request packets from attacker and reply information of packet. |
| 6     | [23]      | The initial purpose of this research is to prevent erroneous information management concerns and the incompatible aims of protection and traceability. They suggest identity-based batch substantiation (IBV) techniques to provide anonymous verification, message integrity, anonymity, and traceability. The suggested IBV system may be utilized for both V2I and V2V communications. Second, the IBV system can handle our specified problems, such as forging, anti-traceability assaults, and loss of identity privacy. | The vehicles in network are always accelerating with random velocity but here the performance is evaluated in different fixed speed scenarios. The signature generation scheme is enhancing the overhead in communication then the better is to follow the accurate accepting message guidelines or standard communication guidelines. |
| 7     | [24]      | In this research a hybrid architecture, consisting of automobiles, boulevard side units (RSUs), a server, and a trust authority (TA), is described, allowing for feedback storage and integrity ranking computation. Furthermore, vehicle communications serve as the foundation for platoon service requests and platoon management. The framework, in particular, is based on the Dirichlet distribution, which ensures great accuracy and dynamics. | Volume of traffic information packets is dropped because of presence of attacker or other issues. Then how to differentiate the attacker drop or other drop measurement. The dependency on platoon head vehicles is more. That means at initial level, if the platoon is fail then the further security will also not sure effectively work against attacks. |
8. Optimal Route Selection in VANET

The optimized routing algorithm or route section in Vehicular ad-hoc network (VANET) is a critical issue, but some researchers have proposed some concepts of optimal routing [25][26]. There may fields in VANET on which they already authors doing hard work but without routing, it is challenging to transfer the traffic information to the far vehicles. So, optimal routing approaches also depends on the specific stream in the research field. This paper focuses on the authentication techniques in VANET, so optimal routing provides better performance but the security approach role is essential. The same is with other streams like congestion, location tracking and resource sharing.

9. Conclusion and Future work

In VANET, mobile nodes are equipped by the wireless technology and acting as computing nodes will move on roads. Network is self-organizing and provides better communication and coordination in vehicles by already maintained interaction among vehicles (V - V) and among vehicles (V - RSU). The vehicles are easily misguided by malicious vehicles because they only flood the incomplete data to leading vehicles. The procedure of VANET communication is completely different from MANET. In our paper, the focus is to how possible to deliver the complete traffic information in VANET. The overview is required to observe that what is needed to make the vehicle's communication more effective in a dynamic environment. The attacks and its role are completely different but the aim is only one i.e., to lost all valuable traffic information. The RSU is able to find the misbehaviour. Previous work promotes the new idea of modelling the security algorithm for secures vehicle communication. In previous work, the different security schemes were used against the attacker and almost all are very effective to prevent the network from attacks in VANET. IOT devices with Machine learning model can bring very big change in the VANET in future to make the process faster and more effective [27,28,29]. In the futuristic approaches, possible Artificial Intelligence and Machine learning techniques also may play a vital role in this work and for detecting the abnormal node based on the type of data sent with the packet [30,31,32]. More security features can be applied for accurate detection of attacks using some method [33]. The security schemes also have some drawbacks because it not possible to prove security effectiveness in all criteria. The classification of routing is discussed to know about the routing protocols techniques. The routing techniques performance measurement depends on the load in the network. The various researchers' contribution is useful for detection and secure communication.

References

[1] John R. Vacca, "Guide to Wireless Network Security," Springer, 2006.
[2] Jean Walrand, P. Varaiya, "High Performance Communication Networks," Science Direct, Second Edition, 2000.
[3] www.wisdomjobs.com/e-university/wireless-communication-tutorial-2262/wireless-communication-satellite-26541.html
[4] Pradeep Kumar Singh, Bharat K. Bhargava, Marcin Paprzycki· Narottam Chand Kaushal, Wei-Chiang Hong," Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's," Advances in Intelligent Systems and Computing 1132, Springer, 2020.
[5] Gaurav Soni, Mahendra Kumar Jhariya, Kamlesh Chandravanshi Deepak Tomar, "A Multipath Location based Hybrid DMR Protocol in MANET," 3rd International Conference on Emerging Technologies in Computer Engineering: Machine Learning and Internet of Things (ICETCE-2020), 07-08 February 2020.
[6] Sabih ur Rehman, M. Arif Khan, Tanveer A. Zia, Lihong Zheng, “Vehicular Ad-Hoc Networks (VANETs) – An Overview and Challenges”, ResearchGate, Journal of Wireless Networking and Communications, pp 29 – 38, 2013.
[7] G. Guett, C. Bryce, "Using TPMs to Secure Vehicular Ad-Hoc Networks (VANETs)", IFIP International Federation for Information Processing 2008 pp.106-116, WISTP 2008, LNCS 5019.

[8] G. Guett, C. Bryce, "Using TPMs to Secure Vehicular Ad-Hoc Networks (VANETs)", IFIP International Federation for Information Processing 2008 pp.106-116, WISTP 2008, LNCS 5019.

[9] B. Rakesh Kumar and Mayank Dave " A Review of Various VANET Data Dissemination Protocols", International Journal of u- and e- Service, Science and Technology Vol. 5, No. 3, pp. 27-24 September, 2012.

[10] Y. Hao, Y. Cheng, C. Zhou, and W. Song, “A Distributed Key Management Framework with Cooperative Message Authentication in VANETs", IEEE Journal on Selected Areas of Communication, Vol. 29, No. 3, pp. 616–629, March 2011.

[11] G. Li, L. Boukhatem, and J. Wu, “Adaptive Quality-of-Service-based Routing for Vehicular Ad hoc Networks with Ant Colony Optimization,” IEEE Transaction on Vehicular Technology, vol. 66, no. 4, pp. 3249–3264, 2017.

[12] A. Mahajan, N. Potnis, K. Gopalan and A.-I. A. Wang, "Urban Mobility Models for VANETs," in Proc. of 2nd Workshop on Next Generation Wireless Networks, 2006.

[13] D. S. Gaikwad and M. Zaveri, "A Novel mobility model for realistic behavior in Vehicular Ad Hoc Networks," in 11th IEEE International Conference on Computer and Information Technology, Cyprus, 2011.

[14] Kayhan Zrar Ghafoor and Marwan Aziz Mohammed, "Routing Protocols in Vehicular Ad hoc Networks: Survey and Research Challenges", Network Protocols and Algorithms, Vol. 5, No. 4, pp. 39-83, 2013.

[15] Tarik Taleb, Elssan Sakhaee, Abbas Jamalipour, Kazuo Hashimoto, Nei Kato, and Yoshiaki Nemoto, "A Stable Routing Protocol to Support ITS Services in VANET Networks", IEEE Transactions On Vehicular Technology, Vol. 56, No. 6, pp. 3337-3347, November 2007.

[16] Muhammad Sameer Sheikh and Jun Liang "A Comprehensive Survey on VANET Security Services," in Traffic Management System, Wireless Communications and Mobile Computing, Volume 2019, Hindawi, Article ID 2423915, 2019.

[17] Gaurav Soni, Kamlesh Chandravanshi, Mahendra Ku. Jhariya, Arjun Rajput, "An IPS Approach to Secure V-RSU Communication from Blackhole and Wormhole Attacks in VANET," Contemporary Issues in Communication, Cloud and Big Data Analytics Proceedings of CCB, Springer 2020

[18] Basker Palaniswamy, Seyit Camtepeb Ernest Fooa, Leonie Simpsona, Mir Ali Rezazadeh Baeza, Josef Pieprzykb, "Continuous authentication for VANET, " Vehicular Communications, Elsevier, 2020.

[19] Peng Wang, Chien-Ming Chen, Senior Member, Saru Kumari, “HDMA: Hybrid D2D Message Authentication Scheme for 5G-Enabled VANETs," IEEE Transactions On Intelligent Transportation Systems, 2020.

[20] Vasilii Krundyshev, Maxim Kalinin, Peter Zegzhda "Artificial swarm algorithm for VANET protection against routing attacks", IEEE Industrial Cyber-Physical Systems (ICPS), 2018.

[21] Hao Hu, Rongxing Lu, Zonghua Zhang and Jun Shao," REPLACE: A Reliable Trust-Based Platoon Service Recommendation Scheme in VANET," Transactions on Vehicular Technology, pp.1-11, 2016.

[22] Thanmayee Karimirreddy, Ahmad Ghulam A Bakshi, "A Hybrid Security Framework for the Vehicular Communications in VANET", IEEE WiSPNET Conference, 2016.

[23] Sourav Kumar Bhoi, Rajendra Prasad Nayak, Debasis Dash and Jyoti Prakash Rout, "RRP: A Robust Routing Protocol for Vehicular Ad Hoc Network against Hole Generation Attack ", International conference on Communication and Signal Processing, pp. 1175-1179 April 3-5, 2013, India.
[24] Shiang-Feng Tzeng, Shi-Jinn Horng, Tianrui Li, Xian Wang, Po-Hsian Huang, and Muhammad Khurram Khan Enhancing Security and Privacy for Identity-Based Batch Verification Scheme in VANETs IEEE Transactions on Vehicular Technology, Vol. 66, No. 4, April 2017.

[25] Tony Santhosh Gnanasekar, Dhandapani Samiappan "Optimal Routing in VANET using Improved Meta-heuristic Approach: A Variant of Jaya, IET Communication Journal, First published: 03 September 2020.

[26] Sumendra Yogarayan, Siti Fatimah, Abdul Razak Afizan Azman, Kirbana Jai Raman, "A Review of Routing Protocols for Vehicular Ad-Hoc Networks (VANETs),” IEEE 8th International Conference on Information and Communication Technology (ICoICT), 2020.

[27] Dutta, Sushama Rani, et al. "IoT in Autism Detection in Its Early Stages." Internet of Things: Enabling Technologies, Security and Social Implications. Springer, Singapore, 2021. 47-58.

[28] Dutta, Sushama Rani, Sujoy Datta, and Monideepa Roy. "Using cogency and machine learning for autism detection from a preliminary symptom." 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE, 2019.

[29] Dutta, Sushama Rani, et al. "A Machine Learning-Based Method for Autism Diagnosis Assistance in Children." 2017 International Conference on Information Technology (ICIT). IEEE, 2017.

[30] Giri, Soumyajit, Sushama Rani, et al. "A real time epidemic alert generation system for rural areas using WBANs and kiosks." 2017 International Conference on Information Technology (ICIT). IEEE, 2017.

[31] Dutta, Sushama Rani, and Monideepa Roy. "EDOT: Context-aware tracking of similar data patterns of patients for faster diagnoses.” 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT). IEEE, 2017.

[32] Dutta, Sushama Rani, and Monideepa Roy. "Providing context-aware healthcare services using circular geofencing technique." 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom). IEEE, 2016.

[33] Dutta, Sushama Rani, et al." Handling Scarcity of Data in Autism Identification using Binary Imputation Method” International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-1, May 2019