Webology (ISSN: 1735-188X)
Volume 17, Number 2, 2020

Challenges And Issues In VANET-Based Surveillance Systems: A Comprehensive Review

Dr. Sanjiv Kumar Shukla

Department of Computer Science & Engineering,
Rungta College of Engineering and Technology,
Bhilai, C.G, India.

ABSTRACT :

VANET (Vehicular Ad-Hoc Network) is an subset of MANETs Mobile Ad-Hoc Network with several addition of content that helps in routing, identification and mapping of objects, also helps in controlling latency in networks and in tackling of delays. VANETs established there network on the availability of on road vehicle and some infrastructure along the road that provides support, for example base stations. Road-side supporting infrastructure and Vehicles are essential for continuing communications facility, even when there are not enough vehicles presently unavailable on the roads for an effective communication. VANETs plays an important role in providing safety and non-safety applications to a wider range of road users. Even though there are some challenges for VANET, like in creating an effective communication between fast moving objects, therefore the major issues for safety and non-safety applications in VANETs are message routing. Issues in designing a reliable and robust message dissemination technique is mainly because of QoS requirements of safety systems. This paper mainly researched through various methods and some literature conducted ideas to develop a model for dissemination of messages at a reliable and efficient manner and also to develop an routing technique to tackle these routing problems.

Keywords: VANET, QoS, MANET, Routing Protocol and Dissemination of Data.

A. INTRODUCTION

In this section of paper we presents an overview of the whole work done in the corresponding sections, such as VANETs basic ideas and is introduced as an integral part of Intelligent transportation systems, previous researches, challenges and problems. Also discussion is made for the proposed approach and containing work scope with future work and plans. In today's digital world, Intelligent Transportation Systems (ITS) play an important role in facilitating the lives of citizens in every aspect. ITS aims to provide better traffic flow by reducing traffic congestion and controlling adverse events. ITS provides comprehensive and powerful services in ensuring traffic safety and security, reducing traffic accidents and improving traffic flow, providing in car entertainment services. The automotive industry recognizes the need for tools connected with IT systems; for example, communication between vehicles improves traffic safety and makes traffic situations less complex. This can be done to meet the needs that cannot be made by the sensors and to detail the condition of the vehicle. Traffic irregularities, driving behavior and driving behavior can be detected and shared with nearby vehicles.

Vehicle Ad Hoc Network (VANET) was introduced to share this information and improve the communication quality of vehicles. The purpose of smart transportation is to ensure safety and improve traffic flow. VANET is directional MANET type based on registration, routing units (RSUs) and resident units (OBUs). OBU is a radio installed in each vehicle and acting as a communication device with each vehicle, while RSU is a network device installed on the road. The RSU is used to communicate with the infrastructure and is equipped for Dedicated Short Range Communications (DSRC). VANETs fall into two categories: Vehicle-To-Vehicle (V2V) and Vehicle-To-Infrastructure (V2I) . VANET's main function is to create a good communication system; Basically, nodes need special resources to get information, communicate with neighbors and then make decisions. Recently, VANET has been attracting great attention in wireless and mobile communication technology. It is one of the most powerful options for using Intelligent Transportation Systems (ITS). VANETs and MANETs are very different from each other in term of high node traffic, network architecture, and unreliable channels, as well as deadlines, reduced reliability, driving conditions, and network fragmentation. The special features of VANETs such as mobility and flexability make them more vulnerable to internal or external cyber attacks. These attacks cause problems in the creation of secure VANETs in terms of security, privacy and reliability. In recent years, key control strategies have received a lot of attention due to their properties and reliability in ensuring safety in air use. This concept can be used in VANET to build cloud systems based on RSUs such as edge routers and smart lighting.

VANETs face many security issues, including issues with authentication and privacy. Besides, unreliable tools increase many security and communication problems in VANET. In VANETs, all communications is in an open environment, making VANETs more vulnerable to attack. Thus, an attacker can modify, capture, inject and delete messages in VANET. For example, an attacker could gain access to traffic Information and used this information for directing vehicles on the road. Attackers having access to messages and spreading false information on the road, causing accidents, traffic accidents, Accidents including massive dangers, etc. To use VANET effectively in wireless communication, security and privacy issues must be appropriately addressed by introducing sophisticated methods to deal with various threats and attacks. Many studies on authentication and privacy for VANET systems have been proposed to solve these problems. There are many ways to use a public key system (PKI) to identify an agent, which consists of a digital signature from a certificate authority (CA) and the public key of the agent.

B. QUALITY OF SERVICE (QOS) BAS

QoS helps improve network performance and makes it easier and accurate to coordinate information exchange across the network and improve network performance. The concept of QoS provides customers with network latency, latency differential, capacity, packet loss (loss rate), etc. A network arrangement or guarantee to provide a variety of special priority services, including IETF RFC 2386 defines QoS as certain connection criteria that a network must meet for packet flow from destination to destination.

A network's ability to provide exceptional QoS depends on the network's characteristics, which reveal key elements of the network.These attributes include contact delay, transmission, phase error, and transmission error rate. It provides hardware features, processing speed, and storage capacity in a node. In addition to the physical characteristics of the system and the communication relationship, QoS control algorithms operating at different levels often lead to QoS in the network. Unfortunately, MANET's features have poor support for QoS.

The actual transmit power with small error and weak fault is the time difference. Nodes can also be used to connect to other wireless devices on MANET. Every technology must have a MAC layer to support QoS. The QoS model around the MAC framework is also easily compatible with many core wireless technologies. Supporting a variety of services in a diverse community can be a task. The poor nature of the communication quality in MANET makes it difficult to guarantee the system. To use VANETs effectively in wireless communications, security and privacy issues need to be properly addressed by introducing sophisticated techniques to deal with a variety of threats and attacks.
Many studies on authentication and privacy of VANET systems have been proposed to solve these problems.

C. LITERATURE REVIEW:

The development of routing protocols in VANET is based on various models and methods. Some of them are considered well-known models in the literature for many applications. We present some of them here. Many researchers have developed formal methods for VANETs based on meta-heuristic optimization methods. Some researchers have used multi-objective optimization for this purpose and improved existing methods to make them suitable for VANETs.

In [1]'s work, Firefly was used to perform multi-objective optimization as an enhancement to VANET OLSR. More specifically, the framework has three levels: 1- creating scenarios to create network routes and traffic, 2- weighted reward formulation, and 3- optimization of protocol without using decision no on messages retention time, connect refresh time events and welcome messages etc. But the evaluation includes the number of unchecked solutions, excessive volume, light coverage, etc. has not yet developed the MOO assessment to measure The literature includes many meta-heuristics for optimizing VANET networks at multiple layers. In the context of using metaheuristics to optimize MAC layer in VANET [2], MOO framework is proposed to optimize MAC and physical layer. The framework is designed to optimize three metrics: throughput, packet loss, and latency. The solution is to include multiple parameters in the two layers of the system. For optimization, the framework is evaluated according to the non-dominant sequencing genetic algorithm NSGA-II. The work of [3] demonstrates the use of a genetic whale optimization algorithm to help select the central channel for transmission. The protocol is called Modified Cognitive Tree Routing Protocol MCTRP.

This process can be classified as Active Channel in VANET. Another area where metaheuristic optimization is used in VANET is to manage data transmission and prevent broadcast storms. In [4]'s study, the authors focus on improving connection security and longevity and reducing the number of problems in the selection process. The optimization is designed as an objective function consisting of two statements. Next, the method uses discrete particle swarm optimization. Complexity analysis proves the applicability of this method in practical use. Some researchers have proposed a meta-heuristic-based optimization method to optimize performance in VANETs.

An improved QoS-constrained multicast routing (ISFLABMR) based on the competitive frog algorithm [5] has been proposed. The goal is to find the best subtree for the message. This subtree is the optimal multicast tree, having a choice of multicast trees between sources and sources. The power function is designed to improve various QoS parameters, especially jitter, latency and bandwidth, to reduce the transmission cost of multicast routing. Also, some articles, such as the study of [6], wherea common intelligence is recommended to attack the challenge, focus on meta-heuristic methods based on VANET security. The literature on VANET routing protocols includes many techniques based on metaheuristics. [7]'s study proposes a method to select routes based on health benefits using genetics. Find ways to use anger, then choose the best way based on genetics. After showing that the method outperforms other methods,the authors show that the computation of the algorithm is slow and the combination with heuristics can improve the performance of the algorithm.

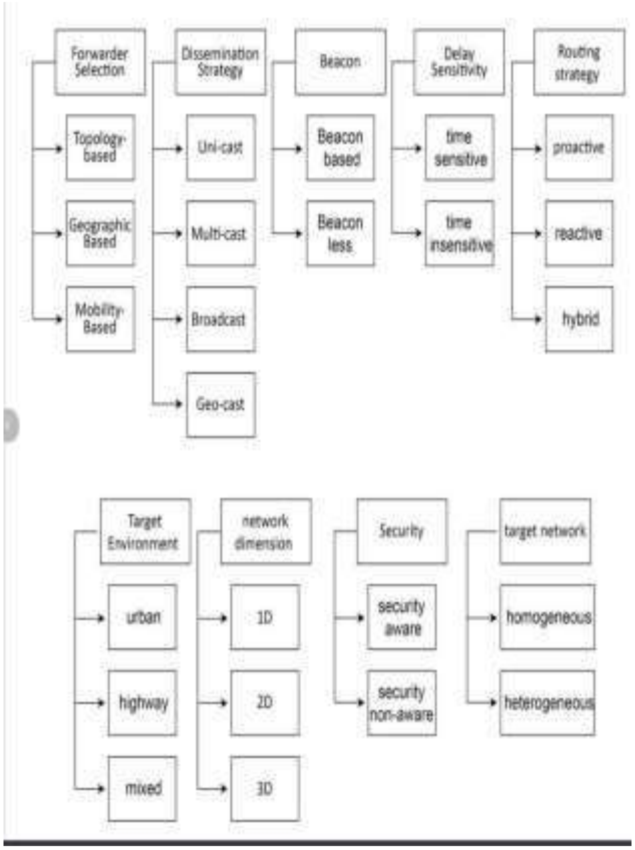
This focus on the speed of genetic algorithms has also beennoted by other authors, for example [8], in their work genetic algorithms are used in both serial and parallel fashion, and they show the superiority of similar models when using multi-core architectures. Other researchers have developed quality control measures. These measurements, like the work of [9], include information about signal strength, path loss, transmission, and frequency, and propose an algorithm based on genetic improvement in addition to new measurements. This method uses a no-selection method using k-means clustering. The authors also mentioned real-time concerns and see this as future research. It has been found in the literature that many meta-heuristic-based routing focuses on the problem of multicast routing and its impact on network congestion.

An example is the study of [10], which used a micro artificial bee colony for multicast routing. This algorithm isfor implementing VANETs that improve QoS while increasing network lifetime and reducing the cost of latency. The algorithmic solution proposes a bitwise encoding of the path between the source and the source in the spanning tree. The algorithm also shows that the power model is suitable for power consumption. On the other hand, optimization only considers a small part of the population, which makes it more effective. A similar study for the development of meta-heuristic-based multicast routing is the work in [11]; where Firefly is developed using the Levely distribution and bit string encoding is recommended to look for the way to get the best price by reducing the number of Agents. . Power consumption andE2E delay use the same target function.

D. SOLUTION PROPOSED:

In 2014, Sharef et al. The routing features and problems in VANETs are analyzed, which can be considered when designing routing protocols for VANETs. Engoulou et al. 2014 evaluated VANET security issues and issues and discussed their security and applications, but did not

include many aspects of VANET security. Recently, various simulation and experimental tools have been developed in the research paper by Qu et al. 2015. and in 2016 Azees et al. Concerns regarding the privacy and security of VANETs have been noted. Hasrooney et al. By presenting the real security architecture with VANET routing protocol, VANET security, challenges, causes and solutions are discussed; this intensive assessment is limited to 2017. Lu et al. A survey was conducted in 2018 where they discussed architecture, security, privacy and trust management at VANETs. They also talk less about privacy and security at VANETs and less about network simulators and cluster simulators. Sharma and Kaul explore intrusion prevention devices (IDS) and security mechanisms such as VANETs and VANET clouds to resolve security issues in connected vehicles. This research discusses the challenges of IDS implementation in VANETs. Boualouache et al.
Published a survey on VANET's pseudonymization policy. This research discusses and compares these ideas with some related systems and identifies unresolved issues. Ali et al. Authentication and privacy for VANETs are explored



by classifying and discussing their models, requirements and attacks, and describing operational vulnerabilities.

1. Communication reliability: To improve communication reliability, several techniques have

been proposed, including routing protocols that can adapt to the dynamic topology of the network and mitigate the effects of interference and packet loss. For example, the proactive routing protocol (DSDV) can provide reliable communication by maintaining a consistent routing table, while the reactive protocol (AODV) can establish communication routes on demand.

2. Network congestion: To mitigate network congestion, several techniques have been proposed, such as the use of multi-channel communication, which allows multiple channels to be used simultaneously to reduce interference and increase network capacity. Other techniques include dynamic bandwidth allocation and load balancing to optimize the use of network resources.

3. Privacy: To protect privacy, the system can use techniques such as anonymous communication, which can ensure that the identity of the sender and receiver is not revealed. Other techniques include data encryption and pseudonymization, which can protect personal data and prevent unauthorized access.

4. Security: To ensure security, the system can use techniques such as digital signatures, which can authenticate the origin of messages and prevent data tampering. Other techniques include intrusion detection systems, which can detect and prevent attacks, and access control mechanisms, which can limit access to sensitive information.

E. CONCLUSIONS AND DIRECTION FOR FUTURE RESEARCH:

In conclusion, the research has highlighted the significant challenges faced in VANET-based street surveillance systems. These challenges include limited communication range, high mobility of vehicles, channel congestion, and privacy concerns. The limited communication range of VANETs makes it difficult to establish reliable communication between surveillance nodes, especially in urban environments with tall buildings and other obstructions. The high mobility of vehicles also poses a challenge as the topology of the network keeps changing, making it difficult to maintain a stable and reliable connection. Furthermore, the issue of channel congestion arises when a large number of surveillance nodes try to communicate simultaneously, causing interference and reducing the quality of service. Privacy concerns are also a significant challenge as the system may be vulnerable to attacks that could compromise the confidentiality and integrity of the data being transmitted.

In addressing these challenges, future research can explore the use of more advanced communication technologies such as 5G and beyond, and the implementation of more robust security mechanisms to ensure data privacy and integrity. The integration of AI and machine learning algorithms can also help to optimize the performance of VANET-based street surveillance systems by reducing congestion and improving communication reliability.

Overall, while VANET-based street surveillance systems have the potential to revolutionize urban security, it is important to address the challenges highlighted in this research to ensure that the systems are reliable, secure, and effective

F. ACKNOWLEDGEMENT:

The author would like to thanks Associate Professor Soumalya Ghosh for his overall supervision for the research Paper and for their valuable feedback and comments on the research.

G. REFERENCES:

[1]U. Mohanakrishnan and B. Ramakrishnan, "MCTRP: An Energy Efficient Tree Routing Protocol for Vehicular Ad Hoc Network Using Genetic Whale Optimization Algorithm," Wireless Personal Communications, vol. 110,no. 1, pp. 185-206, 2020.

[2] Q. Yang, et al., "ACAR: Adaptive Connectivity Aware Routing for Vehicular Ad Hoc Networks in City Scenarios," Mobile Networks and Applications, vol. 15, no. 1, pp. 36-60, 2010.

[3] M. Eusuff, et al., "Shuffled frog-leaping algorithm: A memetic meta-heuristic for discrete optimization," Engineering Optimization, vol. 38, no. 2, pp. 129-154, 2006.

[4] V. Krundyshev, et al., "Artificial swarm algorithm for VANET protection against routing attacks," Proc. - 2018 IEEE Industrial Cyber-Physical Systems (ICPS 2018), pp. 795-800, 2018.

[5] G. Zhang, et al., "Genetic Algorithm Based QoS Perception Routing Protocol for VANETs," Wireless Communications and Mobile Computing, vol. 2018, pp. 1-11, 2018.

[6] H. Bello-Salau, et al., "An optimized routingalgorithm for vehicle ad-hoc networks," Engineering Science and Technology, an International Journal, vol. 22, no. 3, pp. 754-766, 2019.

[7] X. Zhang, et al., "A micro-artificial bee colony based multi-cast routing in vehicular ad hoc networks," Ad Hoc Networks, vol. 58, pp. 213-221, 2017.

[8] M. Elhoseny, "Intelligent firefly-based algorithm with Levy distribution (FF-L) for multi-cast routing in vehicular communications," Expert Systems with Applications, vol. 140, 2020.

[9] J. J. Mulcahy, et al., "Autonomic computing and VANET," SoutheastCon, pp. 1-7, 2015.

[10] F. Arena and G. Pau, “An Overview of Vehicular Communications,” Future Internet, vol. 11, no. 2, pp. 27-38, 2019.

[11] F. Li and Y. Wang, “Routing in vehicular ad hocnetworks: A survey,” IEEE Vehicular technology magazine, vol. 2, no. 2, pp. 12-22, 200