Traffic Accident Prediction Techniques in Vehicular Ad-hoc Network: A Survey

Features:

The paper includes the brief discussion on Vehicular Ad-Hoc Network and signifies the summarized work done in this field.

Discuss on VANET and the approaches that considered as Communications (V2V & V2I) and applications (safety applications & non-safety applications).

Analysis of previous work done for prediction of accident applying Machine Learning.

Provides Machine Learning approaches which include SVM, KNN, CNN and Deep learning and Fuzzy Logic approaches.

Observation of using fuzzy logic with benefits and need of In-Depth study.

Methods:

The paper generalizes the outline of various methods used for implementation of traffic accident prediction model.

Uses of method in Machine Learning that gather the contribution, methods, simulations, accuracy of prediction and limitations of previous studies.

Apply for method in Fuzzy logic that gathers the technique, architecture model, challenges and advantages of previous studies.

Limitations:

The survey is qualitative but not quantitative measurement.

Lack of concepts, works-activity, and specific technical tools, simulator tools are not providing.

Usability:

The study can help identify the best approach and develop better technique in VANET.

Provides the best techniques and approach of predicting accidents.

Serve as a basic and informative lesson for more papers.

A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy

Features:

Review on the basic knowledge of VANETs and main security services with their threats and attacks.

Discuss on the anonymous authentication schemes, three types of trust models and the significant properties of models are to establish efficient trust management in VANETs.

Provides requirement of VANET evaluate on aspects of performance and security, integrated simulation platforms with the idea of bidirectional coupling.

Provides elaborate idea of trust model, simulator tools, trust management, security service and location-based privacy in VANET.

Methods:

The paper generalizes the outline of several processes of security, privacy and trust in VANETs.

Avoids the existing survey on well-researched security topics.

Focus on the new techniques for protecting privacy and trust models, fills in the gaps, and reports recent developments in VANETs.

Limitations:

No real life implementation or experiment of trust model and simulator tool has shown.

Specific details process of Simulator tools but no description of technical details.

Should focus on privacy preservation and trust management technique more precisely.

Usability:

The paper has a proper overview of VANET and the survey of trust, privacy and security in VANETs for better assume.

Provides a comprehensive analysis on various trust management models in VANETs.

The classifications of security attacks, privacy-preserving authentication, trust models, simulator tools can help identify threats and develop better approach.

Serve as an informative study for privacy preservation and trust management technique in VANETs.

**VEHICLE TO EVERYTHING (V2X) COMMUNICATION PROTOCOL BY USING VEHICULAR AD-HOC NETWORK**

Vehicular Ad-hoc networks is a huge thought from the investigation organize and the vehicle business to improve the organizations of cooperate intelligent transportation system. The potential results of vehicle-to vehicle, vehicle-to-structure, vehicle to cloud, vehicle to house, vehicle to network, vehicle to pedestrian correspondence showing and PC entertainment will be shown.

It improves road safety, traffic efficiency, and comfortability of vehicles.

**Features:**

Provide the definition about vehicle-to vehicle, vehicle-to-structure, vehicle to cloud, vehicle to house, vehicle to network, vehicle to pedestrian correspondence.

Improve road safety, traffic efficiency, and comfortability of vehicles.

Maps can be utilized for street arrangement plans through VEINS Technology

Connected vehicles (CVs) and non-connected vehicles (non-CVs), and filtering algorithm are used to distinguish between them using Basic Safety Message (BSM) packages.

Multiple sensors like (BSM packages, inductive loop, video, and magnetometer) are fused to accurately identify CVs and non-CVs vehicles.

**Method:**

1.Use different type of simulator like SUMO, Network Simulator, VANET Simulator those can consume the high rate of traffic, decrease road accident frequently.

They Approach Cellular-based C-V2X technology is superior to WLAN based in terms of communication range, performance, and reliability

Use hardware-on top of its simulation (HILS) technique can capture roadway sensor information from four different sources DSRC broadcast messages, inductive circles, video detectors, and wireless magnetometers.

The paper initially raises different kind of factor & build-up different approach.

**Usability:**

This study help to detect every moment real-time situation strictly for this if any kind of problem occurs in traffic it is fix fast.

Emergency traffic like medical vehicle or others emergency transport don’t have to wait a long time in road.

Decrease sudden accident on road-side area through this traffic.

Each & every part of the road will be properly under control.

**Limitation:**

Identification of CVs and Non-CVs term they should find out that is their particular vehicle is registered or not under VANET Server.

This paper can’t implement whole theme as they explain.

No central control is here.

VANET Routing Protocols: Review, Implementation and Analysis

Features:

The paper provides the overview of routing protocol of VANET includes classification and methodology.

Discuss the classification of routing protocol like Geo-based routing, Cluster Based Routing Protocols, Topology Based Routing Protocols and so on.

Presents the challenge of good quality video streaming and studies the related routing protocol.

Finds the suitable protocol which is AODV by OPENET implementation comparing with DSR protocol.

Methods:

Literature review on related studies of routing protocol and video streaming issue in VANET.

Finds the best approachable protocols after analyzing existing related papers.

Implements by OPENET, shows the simulation result and gives the better result AODV which is perform well than DSR.

Limitations:

The paper discuss only about routing protocols but no discussion about privacy and security of VANET.

Lack of real-world examples and implementation.

For more comprehensive scenario the routing protocols implementation cannot be explained.

Usability:

The paper has a proper overview of routing protocol and its methodology in VANET effective for beginners.

Provides better result of routing protocol in video streaming in VANET.

Simulation of routing protocol like ADOV and DSR in simple and complex scenario.

**Features:**

Protect the vehicular network from malicious nodes and fake messages

Every vehicle as a transmitter to communicate with each vehicle Properly Through OBU (On Board Unit).

Communicate with the infrastructure and contain the network devices for dedicated short-range communication (DSRC) through RSU (Road Side Unit).

Can communicate with the neighbor vehicle easily by sensors, cameras, GPS.

The transferred messages are not injected or altered by the attackers through VANET security.

**Method:**

This survey paper generalized/follow different different wireless communication frequency channel for Control full VANET system properly

2.In this paper they want to apply wave layout & use five main domains such as (availability, confidentiality, authenticity, data integrity, and nonrepudiation) for VANET security requirement.

Privacy-Preserving Authentication they basically Categories authentic schemes to provide a complete structure how VANET application attribute will be design.

4.Provide various type of VANET simulator like:( mobility simulator and network simulators)

**Usability:**

This survey paper uses really some of great method which can ensure VANET security.

VANET security challenge address properly.

We can gather knowledge about multivariant attack, for defend future attack

This paper provides many types of security related approach, for this if any organization who work with VANET they follow this all approach for secure their VANET Properly.

**Limitation:**

1.No Real life implement actually occur in this paper they just give idea of VANET security.

2.Lack of VANET Emergency support roadway-Both.