**Decentralized Reputation Model based on Bayes' Theorem in Vehicular Networks**

**Intro:**

* This article presents a decentralized reputation model, where the activity of each node (i.e., vehicle) is observable for adjacent nodes.
* The proposed model enables nodes to detect malicious vehicles and avoids interacting with them.
* Authors proposed to use the Bayesian filter to measure the trust scores of vehicles accurately. Different from conventional trust models, the authors studied the concept of classification and misclassification.
* They then analyzed the accuracy of their Bayesian filter by computing the factors of Node Recall and Node Precision. The extensive simulations have shown that the proposed filter can assign an accurate trust score to nodes under various network conditions and misbehavior rates.

This paper presents a robust decentralized reputation model based on Bayes’ theorem to filter out malicious vehicles in vehicular networks. During the monitoring process, each node observes the behavior of its neighbors, using Watchdog checking.

In the model, authors considered three types of vehicular messages (i.e., periodic messages, urgent event messages, and traffic messages). They calculated the probability of malicious behavior using the Bayesian theorem. In addition, they explored the accuracy of their Bayesian filter by computing the factors of Node Recall and Node Precision. Authors also used the Total Cost Ratio (TCR) to observe the performance of the proposed filter; higher 𝑇𝐶𝑅 values indicate better detection performance.

**Related work and my views on those:**

1.

In [5], the authors proposed a novel trust evaluation and management (TEAM) framework that offers different levels of trust values for different vehicle types. TEAM includes various factors, like higher authority vehicles (e.g., ambulances), public transport vehicles (e.g., buses, taxis), professional vehicles, and ordinary vehicles. The main drawback of this approach is how to differentiate behaviors among different vehicles, which is not discussed adequately.

2.

In [6], Yang et al. proposed a trust model where the blockchain technology is used to store the trust values of vehicles. However, since the Roadside Units (RSUs) are used to calculate the trust values for every vehicle using specific methods, the model does not operate for a distributed scenario where RSUs do not exist in a vehicular environment.

3.

In [8], a detection model based on IDS in clustered VANETs has been proposed. The authors introduced a support vector machine (SVM) to classify specific nodes named Multi-Point Relay (MPR), as either cooperative or malicious. However, this model is not suitable for resource-constrained nodes due to the need to gather, propagate, store, and analyze the training data dispatched between vehicles.

4.

In [10], the authors proposed a system for detecting malicious behaviors by dropping suspicious packets. They categorize vehicle behaviors into two types: malicious and honest. This system is able to detect attacks that intentionally drop packets (e.g., Black hole and Gray hole). The authors did not present any strategies on how to prevent or isolate malicious nodes.

5.

In [11], the authors presented a trust evaluation model based on Reputation, Experience, and Knowledge, which is called (REK) in vehicular networks. The model assigns a score by calculating the trust of the vehicle based on three indicators PEK, then based on the score; they can recognize trusted vehicles. They use only data transmitted from trusted vehicles.

6.

The authors in [12] proposed a system for updating and querying the reputation of nodes. This system is based on a smart contract and an Interplanetary File System (IPFS). Their system is capable of identifying trustworthy nodes and recording the reputation of these nodes. They consider a pseudo-ID for each node after registration; however, a pseudo-ID does not always prevent the location tracking.

While explaining to Professor,

Look at the paper, for section-3, section-4. Section 5 is the conclusion where for future work, they said they will work on including a prediction function within the proposed reputation model. They said they will integrate a Markov process to predict each node’s behavior in the network.

I did not understand some of the equations they used but I understood all the graphs they produced.

**My views**

I understood Bayes theorem, conditional probability, and Total probability, but in the paper, they formulated many equations, I have doubts about many equations and have to get more clarity on how these equations which are developed step by step are going to help us in detecting malicious nodes. And also, why are some equations like that?

1.

Reputation, Experience, and Knowledge (REK)

We can think about including these parameters in calculating trust scores of vehicles in our model.

2.

3rd related work, where they introduced SVM can be checked and can get more insights.

3.

Can check this out the following papers. The following papers are referred in “Trust in VANET” paper which I presented ppt.

**Machine Learning-Based Trust Management:**

**Authors:** Oubabas et al. , Fan et al. , Zhang et al. , Shams et al.

**Proposals:**

Clustering algorithm with role assignment and trust update, fuzzy C-means clustering, deep reinforcement learning, and trust-aware intrusion detection using SVM.