**Trustworthy Routing in VANET: A Q-learning Approach to Protect Against Black Hole and Gray Hole Attacks**

**Intro:**

In the paper, they proposed QL-TRT (Q-learning-based trustworthy routing technique) which is basically a reinforcement learning approach.

I have to learn about this RL, in some more depth!

The authors focused on Black hole and Gray Hole attacks. There is a subtle difference between Black hole and grey hole attacks. In black hole attacks, almost 100% of the packets are dropped, whereas in gray hole attacks some packets are dropped and some packets are sent. It is like 0% to 50% of the packets are dropped in grey hole attacks, which is even more difficult to detect compared to black hole attacks.

QL-TRT approach, which is formulated based on the Markov Decision Process, allows the vehicle to choose the best neighbor for routing and avoid malicious neighbors. To evaluate the trustworthiness and reliability of the links between pairs of vehicles, authors consider factors such as **packet forwarding ratios, energy consumption, and expected transmission time**. Q-learning is used to learn the trust value of links and select the most trusted route from source to destination. The evaluation results demonstrate the effectiveness of QL-TRT in detecting black hole and gray hole attacks, while ensuring the communication performance in VANETs.

Have to know in some extent about this Markov Decision Process.

As part of the black hole attack, the malicious node advertises that it has the shortest route to the destination. As a result, the source directs messages to the malicious vehicle, and the attacker drops all the messages instead of forwarding them. In contrast, a gray hole attack involves a malicious node intentionally dropping some packets, but not all. This can disrupt communication and make it difficult to detect an attacker that behaves normally most of the time.

This paper proposes a RL-based trustworthy and reliable routing algorithm as an alternative to the original ad-hoc on-demand distance vector (AODV) routing protocol that protects vehicular networks against black hole and gray hole attacks. The purpose of this work is to establish trustworthy routing in VANETs, while also improving quality of service (QoS). By calculating the trust level of links between vehicles and by employing Q-learning, a well-known RL algorithm, the proposed scheme can determine a trusted route from source to destination while avoiding attackers.

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

Researchers have proposed several solutions for improving security mechanisms in black hole attacks and secure routing with and without ML (Machine Learning) techniques in recent years.

I just presented some works here, there are some more in the paper.

**Non-ML methods**

**1.**

[5] proposed an algorithm based on an existing ad-hoc on-demand multi-path distance vector (AOMDV) routing scheme, based on clustering techniques. They designed an algorithm to reduce end-to-end latency and enhance reliability by removing unnecessary route request (RREQ) messages.

However, the proposed solution was not able to prevent and detect different types of network attacks.

**2.**

In [8], the authors discuss a method by which a malicious node can be detected by sending a forged RREQ that includes the address of an unreal destination node. Next, the other nodes will be notified in order to identify the malicious nodes, and they will remove the malicious node from their routing table. In fact [8] appears to increase network traffic by generating forged route requests.

Note this One more idea for detecting malicious nodes.

**3.**

[6] introduced a secure AODV routing algorithm which is a modified version of the original AODV routing protocol that is intended to detect black hole attacks. The source and destination nodes are verified using cryptography techniques, and the source node verifies the destination node before forwarding packets. While the suggested method provides robust performance, it remains susceptible to gray hole attacks.

This method involves cryptography.

One has to verify the next node, before forwarding a packet to it or not. And so, every node in the route has to be checked right. Then, just by checking the destination node, is it going to help? How?

**4.**

In [9], a trust based QoS routing algorithm was proposed to improve the security of MANETs in the presence of malicious nodes. The proposed algorithm, called TQR, monitors the behavior of each node in the network and only allows packets to be forwarded through trusted routes with low delay. If a malicious node is detected, it is isolated from the network to prevent packets from being forwarded through or from it.

The authors compared QL-TRT with both AODV and TQR. The proposed QL-TRT outperformed both AODV and TQR --> Refer Section 5, clearly visualized by building graphs by considering PDR (Packet Delivery Ratio) and End-to-End Delay.

**5.**

Hassan et al. [10] developed an intelligent detection scheme that precalculates thresholds for parameters. The authors consider four parameters including destination sequence numbers, hop count values, packet delivery ratios and end-to-end delay to detect the black hole attack in VANETs.

Note this idea, where the authors used thresholds for four parameters to detect black hole attack.

1. Destination Sequence number

2.Hop count values

3.Packet Delivery Ratios

4.End-To End delay

**ML- methods**

**1.**

[11] proposed a supervised learning approach to detect black hole attacks based on a neural networks (NN) algorithm, while [12] designed a method to protect against gray hole and rushing attacks. Both [11], [12] analyzed mobility vehicles behavior in the VANET in order to determine whether they are malicious or not.

**2.**

A multi-level ML-based intrusion detection method was proposed by [13] for the detection of gray hole and black hole attacks. In their approach, two binary classification models were used. In the first binary classifier, an NN was deployed at the roadside unit (RSU) to secure cluster heads, and in the second, a support vector machine (SVM) was used to detect malicious multi-point relays (MPR) locally.

**3.**

[14] presented a scheme for detecting and preventing black hole attacks in a VANET environment by combining statistical modeling and different supervised machine learning mechanisms, including SVM, Gradient Boosting, Gaussian Naive Bayes, K-NN, and Logistic Regression.

**It has been noted that these ML methods were focused on detecting attackers; however, the authors neglected the QoS of the network service. To address this issue, this paper proposes an innovative trusted routing technique based on Q-learning that considers network parameters to improve network performance and reduce end-to-end delays in VANETs, along with meeting the security-related goals.**

While explaining to Professor,

Look at the paper, for section-3, section-4 and section-5. Section-6 is conclusion where for future work, they said they will work on Deep RL algorithm.

I Understood all the equations they used and all the graphs they produced.

**My views**

These ML approaches looking to be promising, can go with these:

Can use

1. Trust values
2. Packet Forwarding Ratio (PFR)
3. Energy Consumption
4. Expected Transmission Time (ETT)
5. Betweenness approach from my previous idea—Refer to my Word document “Security attacks in VANETs and my proposed solutions”
6. I can even try to use Clustering techniques or KNN or other ML approaches instead of RL and can think about it for the same problem, in the same approach followed by authors. Or for a new attack.
7. The 2nd method in non-ML methods seems to be good!
8. In our new solution can we use PFR and ETT as evaluation metrics instead of PDR and end-to-end delay?