**Security Attacks in VANETS and my proposed solutions**

For Sybil attacks, many solutions have been proposed, so I haven’t touched that now.

For now, I focused on:

1. Social Attack

2. DOS Attack

3. Message Falsification/Alteration Attack

4. Message Delay and/or Suppression

(Packet Drop Attack (or) Black Hole Attack (or) Block Hole Attack)

**1. Social Attack:**

1.

We can use sentiment analysis, which is a subfield of natural language processing, to find the emotions (positive or negative or neutral) of the message. NLP uses ML algorithms.

Natural Language Processing is a subfield of machine learning that makes it possible for computers to understand, analyze, manipulate, and generate human language. We encounter NLP machine learning in our everyday lives, from spam detection to autocorrect, to our digital assistant (“Hey, Siri?”).

How is NLP used in sentiment analysis?

In sentiment analysis, natural language processing is essential. NLP uses computational methods to interpret and comprehend human language. It includes several operations, including sentiment analysis, named entity recognition, part-of-speech tagging, and tokenization.

What is Sentiment Analysis?

Sentiment analysis (or opinion mining) is a natural language processing technique used to determine whether data is positive, negative, or neutral.

Eg: Sentiment analysis is often performed on textual data to help businesses monitor brand and product sentiment in customer feedback and understand customer needs.

**2. DOS Attack:**

1.

Definitely, channel switching is one of the solutions. Switch the frequency range of communication.

2.

In the VANET, for a location say, put X as the maximum bandwidth available (make/assume X is large enough).

Now, use X/k

Where k=2,3, 4... (k >1 Initially, depends on the maximum possible bandwidth of the channel or system)

K is a positive integer considerably little bigger (say 4 initially, if our original channel bandwidth is large).

Initially & if we feel that the bandwidth is compromised due to DOS attack, and almost exhausted, then immediately increase bandwidth to X/k-1, as an immediate step.

Since, we already detected that there is some kind of DOS attack (which might be true in most of the cases, until and unless there are really many vehicles in the location and the bandwidth is compromised genuinely without any attack or any malicious presence).

Try to detect the malicious node (In case of a normal DOS attack from say, only one attacker) & remove that node from the system or avoid that node, decrease its trust value, or report this activity to the system.

In the case of a DDOS attack from many attackers and say only a few messages are delivered from each attacker, then it is difficult to detect whether the current exhaustion of bandwidth is due to DOS attack?

So, have to think about this case!

**3. Message Falsification/Alteration Attack:**

1.

Like analogical to the checksum method, which we use in networking, similar type of approach can be used.

So, whenever a node/vehicle sends a message, there is something attached to it, which validates it.

So, when the message reaches the destination, at that time, this validation takes place and if any differences are there in the message content, then we can detect that there is a message falsification or alternate alteration attack and can just ignore that message.

2.

Using Encryptions:

1. Symmetric Encryption – using MAC
2. Asymmetric Encryption – Digital signature, usage of both public and private keys.
3. Quantum Encryption – QKD and QED

**4. Message Delay and/or Suppression Attack:**

Watchdog Mechanism-----> You mentioned in previous discussion.

Watches the network and detects if there are any such nodes, which are dropping the packets (or) holding the packets for more time to cause a delay in the delivery of the message to the destination node.

Now, we have to think about the tunneling problem, where Dr.Paranjothi said, a node instead of dropping or holding for a long time just creates a tunnel such that the message may revolve around the nodes involved in the tunnel.

a.

I think trust mechanisms can be used in detecting such malicious nodes.

b.

If we can able to track the path of a message from the sender node to till it reaches its destination, then if there is any cycle (or like atleast one node is seen twice in the path), then we can say that there is some malicious node and even we can be able to find that malicious node ( where the cycle starts and ends say ).

After finding that malicious node, just remove it from the network (or) decrease its trust value to an incredibly low value.

c.

In the “Trust in VANETs ...” paper, under game theory-based approach, there is on term “Betweenness”

which records the frequency with which a particular node is selected as a relay or as an intermediate node during the shortest path calculation.

Betweenness measures the importance of a node among its neighbors.

So, for every node, once we calculate this betweenness at regular intervals, we need to see the ratio between this

Betweenness of a node V : Number of successful message deliveries to the destination node where V is present in the path.

So, if the ratio = 1, then we can assign high trust value to the node V.

If the ratio > 1, then we can assign low trust value to the node V.

If the trust value of V < Threshold, then it can be identified as a false node.