Project Proposal

Paper Title: TangleCV: A Distributed Ledger Technique for Secure

Message Sharing in Connected Vehicles

Group Members: Robert Elizondo, Robert Bonham, Rishita Elaganti, Kevin Garcia Lopez

Task 1 (10 points) Give a high-level overview (like a summary) of the key contributions of the paper that your team has picked?

Overview: < Summarized description of the paper>

This paper describes the TangleCV technique for validating the Basic Safety Messages (BSM) among connected vehicles in a decentralized, distributed way. This technique uses a modified version of the Tangle algorithm, both of which utilize a Directed Acyclic Graph (DAG) protocol rather than a linear blockchain. This paper describes the differences between Tangle and TangleCV, and argues that the TangleCV technique is superior because it meets the timing constrains of a connected vehicle network, secures the network against tampering attacks by providing ground truth through the vehicle's on-board sensors, and scales well to larger networks. It goes on to investigate two tip selection strategies: the Nearest Neighbor (NN) strategy, and the Random-in-Range (RIR) strategy. The paper provides simulation results indicating that the NN strategy is more efficient than RIR for tip selection, and overall argues that the TangleCV approach is more efficient than current PKI-based security mechanisms for connected vehicles.

Intellectual Merit: < Key Takeaways from the paper>

One of the key takeaways from this paper would be the general idea that a linear blockchain approach that Bitcoin is based on would be consider low transaction performance and a high computation cost. But after reading about the general idea behind it on page 4. It makes it clear that this approach will not work in a massive connective system, with its expensive PoW and the linear nature of the blockchain. Hence, making it inefficient in a large scalable system with ever changing connective vehicles, that are consistently sharing and receiving data while in use. To combat the ineffectiveness of linear-base blockchains. Several ideas have been proposed. One of them suggests the idea of using directed acyclic graph (DAG) based protocol that uses partially ordered logs of transaction to reach an agreement. An implementation of DAG is TangleCV. Whereas instead of using blocks, it instead uses ledgers to keep track of the transactions, where every incoming transaction needs to be validated by two transactions that came before the current one to be added into the ledges. By doing this we can increase the throughput of transactions and achieve parallels in insurance and validation.

Another takeaway is that the algorithm used for Tip Selection has a significant impact on the efficiency of the TangleCV algorithm. The paper provides simulation results indicating that the Nearest Neighbor (NN) approach is more efficient than the Random-in-Range (RIR) approach.

Task 2 & 3

Proposed Work and Methodology

Task 2: (5 pts) Describe which specific topic from the paper you are investigating in further detail over the next two months and why you picked that topic? Describe how it ties to the topics that we have covered in the class? Which application areas can the idea that you have chosen to be applied to?

The topic we have chosen to investigate further is TangleCV, we picked this topic because it focuses on implementing a secure distributed ledger system that takes priority in keeping information integrity and defending against spoofing attacks. This technology is currently applicable to the IOTA field, specifically connected vehicles. It is important to have this type of technology in place since we are moving into an era of autonomous and connected devices that rely on each other to operate successfully, with no room for error. This topic is related to some of the topics that we have covered in class, such as integrity in systems security and the TangleCV distributed ledger technique. TangleCV deals with integrity since it focuses on detecting and preventing erroneous or malicious data from causing malfunctioning in connected vehicles.

Task 3: (5 pts) As part of the final presentation, you will be required to demonstrate software for one idea presented in the paper or a new idea that you may have based on what you learned from the paper? For the project proposal phase, describe which idea you will be picking and how you plan on approaching this task?

For the software part of our project, we plan to develop a simulation of TangleCV showing vehicles joining the network and validating transactions, the tip selection algorithm, calculating cumulative weight of vehicles and how it is affected when vehicles produce erroneous data. The approach we will take to demonstrate TangleCV is implementing a directed acyclic graph to simulate the network of connected vehicles, where each node is a vehicle that issues and validates transactions, a tip is a newly created transaction that needs approval, and it is connected to the issuer and validator by edges. We plan to implement the tip selection algorithm by using the nearest neighbor algorithm. To calculate the cumulative weight of the nodes, we will assign a direct weight to each node and then use it to calculate the cumulative weights. To simulate erroneous data and validation, we plan to give the same data to most of the nodes and give one or two bogus data that does not align with the others so that they are not validated.