ABSTRACT

With the rise in the number of devices in the Internet of Things (IoT), the number of malicious devices will also drastically increase. Smart cities' decisions are based on data being collected by IoT devices in real-time, of which a connected-vehicle system is included. Behaviors such as malicious data injection can significantly impact connected vehicles. To aid in combating this threat, monitoring smart city and connected vehicle's sensor data will allow for construction of a behavioral model. Implementing machine learning will aid in constructing a standard behavior such that any device that begins to malfunction or behave maliciously can be detected and mitigated in real-time. This behavioral analysis will be further applied to supplement trust management approaches such that a more accurate value can be associated with the device's perceived trustworthiness without the need to rely on a majority consensus.