СИСТЕМА АУТЕНТИФИКАЦИИ ДЛЯ СЕТИ ТРАНСПОРТНЫХ СРЕДСТВ

Азарко И.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Борискевич А.А. – д.т.н., профессор

Система аутентификации для сети транспортных средств основана на использовании технологии автомобильных беспроводных сетей VANET (Vehicular Ad-hoc Networks).

В VANET существует два типа связи:

– От автомобиля к автомобилю (V2V);

– Связь между транспортным средством и инфраструктурой (V2I).

Главной особенностью таких сетей является повышение эффективности безопасности дорожного движения за счет:

– Навигации;

– Информировании об ограничениях скорости;

– Предупреждение об аварийных ситуациях на дороге.

Данные таких сетей приводят к некоторым неточностям и проблемам безопасности движения транспорта, когда дело доходит до качества предобработки данных:

– Передача данных происходит только по длине маршрута, исключая требования безопасности;

– Отсутствие проверки состояния нового узла при условиях отсутствия сервера аутентификации;

– Невозможность разделения инфраструктуры.

В работе предлагается использовать алгоритм аутентификации процесса взаимоотношений участников системы аутентификации для сети транспортных средств. Алгоритм аутентификации процесса взаимоотношений участников системы аутентификации для сети транспортных средств на рисунке 1.

Рисунок 1 – Алгоритм аутентификации процесса взаимоотношений участников системы аутентификации для сети транспортных средств

Согласно рисунку 1 алгоритм аутентификации состоит из шести этапов: инициализация системы, аутентификация системы, генерация рейтинга сообщений, расчёт смещения значения доверия, выбор майнера и генерация блока, распределенный консенсус. Первый этап предлагаемого решения начинается с инициализации системы. Этот этап отвечает за проверку подлинности узлов и выдачу сертификата для них, когда узлы перемещаются в сеть. Последующим этапом является проверка подлинности системы, который действует как уровень

безопасности для аутентификации узлов, прежде чем узлы смогут начать связь друг с другом в сети. Далее, генерация рейтинга сообщений связана с предоставлением рейтинга на сообщения, отправленные узлами связи для обеспечения их надежности. После этого четвертый этап - расчет смещения значения доверия, который требуется для расчета надежности каждого узла в сети. После этого система проводит выборы майнера и блокирует генерацию, которая реализует технологию цепочки блоков для эффективного отслеживания узлов в системе. Последний этап алгоритма заключается в распределении консенсуса, который действует как бухгалтерская книга, которая распространяется по сети.

В ходе работы для программной реализации были выбраны Python и MATLAB, которые в свою очередь определили надежность данного алгоритма в сравнении с эталонным. Это связано с тем, что Python и MATLAB хорошо подходят для научного и математического программирования. Параметры для разных классификаторов были определены экспериментально.

Список использованных источников:

1. Zeadally, S.; Hunt, R.; Chen, Y.S.; Irwin, A.; Hassan, A. Vehicular ad hoc networks (VANETS): Status, results, and challenges. Telecommun. Syst. 2012, pp.217–241