Разработка и исследование алгоритма обнаружения вторжения в систему управления беспилотным транспортным средством

В.А. Кондратьев[1], А.В. Кузнецов[1,2]

[1]*Самарский национальный исследовательский университет им. академика С.П. Королева, Московское шоссе 34а, Самара, Россия, 443086*
[2]*Институт систем обработки изображений РАН - филиал ФНИЦ «Кристаллография и фотоника» РАН, Молодогвардейская 151, Самара, Россия, 443001*

Аннотация

В настоящее время разработано несколько систем обнаружения вторжений (СОВ) или Intrusion Detection System (IDS) в англоязычных источниках, предназначенных для анализа работы бортовой сети автомобиля. Многие СОВ анализируют кадры с встроенных камер кругового обзора посредством шины CAN, чтобы обнаруживать среди них аномальные. В данной работе были созданы и проанализированы несколько СОВ и протестирована их эффективность на примере тестов, включающих в себя несколько различных типов атак на CAN шину беспилотного автомобиля.

Ключевые слова

Сверточная нейронная сеть, CAN, система обнаружения вторжений, беспилотное транспортное средство

1. Введение

Безопасность для транспортных средств имеет решающее значение. Современные автомобильные системы реализованы на базе широко известного протокола Controller Area Network (CAN), который используется для связи между электрическими подсистемами внутри транспортного средства (ТС), такими как рулевое колесо, тормоз и двигатель, каждая из которых контролируется посредством электронного блока управления (ЭБУ). ЭБУ собирает, а затем инкапсулирует данные в пакеты, помещая их в шину CAN. Для простоты и увеличения скорости передачи данных пакет CAN не содержит идентификационной информации отправителя или получателя. Отсутствие идентичности в пакетах CAN и создает возможность для злоумышленников внедрять поддельные сообщения.

CAN-шина обеспечивает двустороннюю связь между всеми электронными системами машины: по ней передаются команды ко всем модулям, а те посылают обратные сигналы, которые выполняют системы ТС [1]. Возможность вмешательства в сбалансированную систему с обратными связями через CAN-шину и представляет собой одну из главных уязвимостей современного автомобиля. Современные ТС подключаются к внешнему миру по нескольким каналам, что оставляет злоумышленникам возможность использовать разные направления для атаки. Уже были выявлены конкретные вторжения в ЭБУ пилотируемого транспортного средства, способные вызвать поломку ТС или дорожно-транспортное происшествие [2].

2. Системы обнаружения вторжений в ЭБУ

Для противодействия злоумышленникам были созданы системы обнаружения вторжений [3,4,5,6] (СОВ) в бортовую сеть автомобиля, но они, как правило, не учитывают информацию о дорожном контексте. Если опытный взломщик сможет получить доступ к управлению ЭБУ для внедрения поддельных кадров данных, и поскольку цифровая подпись блока управления будет

неизменной и легитимной, то СОВ будет работать неправильно. В результате такая модель атаки находится за пределами возможностей некоторых СОВ (пример Fingerprinting Electronic Control Units [7]).

Существует особенность, которая не учитывалась при разработке СОВ для защиты сети транспортных средств: все кадры, передаваемые по шине CAN, генерируются в соответствии с решениями, принятыми водителем ТС, и именно дорожный контекст способствует правильному принятию решения водителем. Но водители имеют высоко индивидуальный опыт и привычки и по-разному реагируют на один и тот же дорожный контекст, например, знак остановки или изгиб дороги. Из этого следует нецелесообразность проектирования СОВ с дорожным контекстом для пилотируемых человеком транспортных средств.

Ситуация с автономным автомобилем совершенно другая, так как в нем решения принимаются с помощью хорошо обученной модели самостоятельного вождения, которая и получает динамические данные о дорожном контексте с помощью нескольких датчиков. Ввиду этого дорожный контекст и соответствующие контролирующие сигналы, которые в конечном итоге приводят к кадрам данных, передаваемым по шине CAN, должны напоминать обычный и понятный шаблон. При вторжении в данные, передаваемые по CAN в условиях непрерывной дороги, нарушение этого шаблона может быть заметным. Это наблюдение и послужило основой для идеи создания СОВ, учитывающей дорожный контекст. В данной работе предлагается алгоритм обнаружения атак, учитывающий дорожный контекст, в основе которого лежит свёрточная нейронная сеть, соотносящая цифровое изображение с фронтальной камеры ТС и данных о повороте руля из ЭБУ и позволяющая выявлять аномалии, которые свидетельствуют о проведении атаки.

3. Заключение

В настоящее время CAN является неотъемлемой частью любого автомобиля. Но протокол CAN был создан без предположения о возможности злонамеренного вторжения в работу сети, и, поэтому, не дает даже теоретической возможности обнаружить вредоносные действия в CAN-шине. Созданный в данной работе прототип СОВ способен с приемлемой точностью определить злонамеренное вторжение в шину CAN и избежать последствий такой атаки. Однако достигнутая точность не позволяет использовать данную СОВ отдельно от других проверяющих значения с датчиков и использующихся в алгоритме вождения.

4. Литература

[1] Третьяков, С.А. CAN – локальная сеть контроллеров / С.А. Третьяков // Электроника. – 1998. – Т. 9, № 10.

[2] Как взламывают автомобили через CAN-шину [Электронный ресурс]. – Режим доступа: https://www.zr.ru/content/articles/912117-antivirus-dlya-avtomobilya (01.09.2020).

[3] Muter, M. Entropy-based anomaly detection for in-vehicle networks / M. Muter, N. Asaj // IEEE Intelligent Vehicles Symposium (IV). – 2011. – P. 1110-1115.

[4] Song, H.M. Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network / H.M. Song, H.R. Kim, H.K. Kim // Proceedings of the International Conference on Information Networking (ICOIN). – 2016. – P. 63-68.

[5] Wasicek, A. Context-aware intrusion detection in automotive control systems / A. Wasicek, M.D. Pese, A. Weimerskirch, Y. Burakova, K. Singh // Proceedings of the 5th Embedded Security in Cars Conference (ESCar 17). – 2017.

[6] Taylor, A. Anomaly detection in automobile control network data with long short-term memory networks / A. Taylor, S. Leblanc, N. Japkowicz // IEEE International Conference on Data Science and Advanced Analytics (DSAA). – 2016. – P. 130-139.

[7] Cho, K.T. Fingerprinting electronic control units for vehicle intrusion detection / K.T. Cho, K.G. Shin // Proceedings of the 25th USENIX Security Symposium. – 2016. – P. 911-927.