УДК 621.391 **DOI 10.52167/1609-1817-2025-136-1-108-120**

М.Н. Иманкул[1], Ж.Д. Манбетова[2], А.А. Ержан[3], А. Мухамеджанова[3]
[1]L.N. Gumilyov Eurasian National University, Астана, Казахстан
[2]Saken Seifullin University, Астана, Казахстан
[3]Energo University, Алматы, Казахстан
E-mail: a.mukhamejanova@aues.kz

ЭЛЕМЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АВТОМОБИЛЬНЫХ БЕСПРОВОДНЫХ СЕТЯХ

Аннотация. В перспективе нынешние подключенные и автоматизированные транспортные средства CAV (connected and automated vehicles, подключенные и автоматизированные транспортные средства) превратятся в автономные транспортные средства AV (Autonomous Vehicles). Из-за лазеек в автомобильных системах безопасности, таких как ненадежная связь, открытые каналы, небезопасные шинные системы и наличие интеллектуальных хакеров аппаратные и программные системы AV могут быть скомпрометированы. Хакеры могут захватить AV и подключенные транспортные средства через свои беспроводные сети (Wi-Fi, сотовые сети и т. д.). В данной статье рассмотрены отдельные исследования по безопасности CAV, так как расширение возможностей подключения транспортных средств увеличивает подверженность потенциальным уязвимостям и открывает возможности для кибератак. Отмечено влияние кибератак на CAV. Показано, что обеспечение функционирования CAV связано с безопасным и надежным применением CAV на практике. Отмечена атака BNT (Beacon Non-Transmission, непередача сигнала маяка), при которой вредоносный источник подавляет собственные периодические передачи данных, предназначенные для целевого приложения ITS (intelligent transportation system). Также было отмечено использование облачных технологий и методов искусственного интеллекта для защиты от интеллектуальных кибератак. Приведены характеристики некоторых наиболее распространенных угроз на автомобильные беспроводные сети. Показано, что уровень дорожно-транспортных происшествий можно существенно снизить с помощью технологии V2X, а технология 5G значительно улучшает связь V2X, обеспечивая более быструю, надежную и более высокую пропускную способность связи.

Ключевые слова. Автономные транспортные средства, подключенные транспортные средства, V2X, S-V2X, IEEE 802.11p, VANET, интеллектуальная транспортная система.

Введение.

Одним из направлений цифровой трансформации мирового автомобилестроения является бурное развитие рынка беспилотных (автономных) автомобилей: в 2017 г. произведено 330 тыс. единиц, а к 2035 г. ожидается выпуск уже 30,4 млн штук беспилотных автомобилей, и по прогнозам их доля в структуре общемировых продаж увеличится с 2 % (2017 г.) до 50 % к 2035 г. [1]. Набирающая обороты комбинация подключенных и программно-определяемых транспортных средств (ТС) открывает новые возможности для атак. Следующее поколение интеллектуальных и автономных транспортных средств требует улучшенных автомобильных служб, способных справляться со сверхнадежными ситуациями. В соответствии с общедоступной информацией о трендах автомобильной кибербезопасности в Upstream Security на начало 2022 г. имелась информация о более чем 900 событиях автомобильного взлома. Наблюдается рост

удаленных взломов (85% атак), которые включают атаки через Интернет и беспроводные сети. Остальные нападения носят физический характер и требуют доступа к транспортным средствам (ТС). Уязвимости в компонентах программного обеспечения (ПО) – CVE (Common Vulnerabilities and Exposures) – обычно обнаруживаются в электронных системах производителей оригинального оборудования OEM (original equipment manufacturer) или в цепочке поставок продукции OEM-производителя. Прогнозируется, что вскоре автомобильная кибербезопасность может стать элементом кибервойны между странами. Например, выведение из строя нескольких тысяч ТС в ключевых городах нанесет ущерб ТС страны.

Работа CAV серьезно пострадает, если соединение с ТС будет нарушено, что может привести к дополнительному повреждению ТС или непосредственно к авариям. Известно, что с помощью одной уязвимости можно атаковать много ТС, а повышенная степень автоматизации увеличивает зависимость от сенсорных технологий и снижает зависимость от водителя; расширенные возможности подключения увеличивают степень уязвимости ТС и увеличивают риск осуществления злоумышленником кибератаки [2].

CAV сочетают в себе технологии автономных ТС (AV) и подключенных ТС CV (connected vehicles) для обеспечения более быстрого, надежного и безопасного дорожного движения (ДД). CAV используют различные коммуникационные технологии для достижения автономного и совместного вождения, а также эффективно сочетают технологии автономных ТС на базе датчиков и подключенных ТС на основе связи. Производители автомобилей и их цепочки поставок добавляют оборудование и ПО для улучшения киберзащиты, однако параллельно хакеры-злоумышленники расширяют свои возможности, и появляется больше возможных вариантов для атак [3].

Материалы и методы.

Развитие AV-технологий позволяет устанавливать различные типы датчиков на ТС, которые помогают человеку управлять автомобилем, однако датчики (камеры, лидары, радары, GPS (Global Positioning System), датчики измерения давления в шинах TPMS (tire pressure measure sensors), инерциальные измерительные блоки IMU (inertial measurement units), датчики управления двигателем и т. д.) легко поддаются воздействию шума и вводятся в заблуждение вредоносными атаками, которые могут привести к опасности и несчастным случаям [4]. CV обеспечивают различные типы беспроводной связи в системах внутри ТС, следовательно, кибератаки могут быть осуществлены удаленно. CV включает в себя несколько специфических типов беспроводной связи для предоставления информации, необходимой для реализации приложений V2X **(**Vehicle-to-Everything, связь между ТС и различными объектами), таких как V2V (Vehicle-to-Vehicle), V2I (Vehicle-to-Infrastructure, связь между ТС и оборудованием инфраструктуры), V2N (Vehicle-to-Network, связь между ТС и сетью), V2P (Vehicle-to-Pedestrian, связь между ТС и пешеходом), т.д. ТС, оснащенные технологиями связи между транспортными средствами (V2V) и между транспортными средствами и инфраструктурой (V2I), могут участвовать в связи D2D (Device-to-Device), использующей близлежащие коммуникационные устройства**,** для повышения безопасности ДД, управления ДД и координации.

Технология V2X – метод, в котором используется современное оборудование, ПО, устройства и системы для улучшения связи между автомобилями, пешеходами, светофорами и другой дорожной инфраструктурой для обеспечения эффективной городской мобильности. Это также улучшает экономию топлива и снижает количество аварий и выбросов углекислого газа [5]. Сервисы V2X продолжают получать поддержку систем на базе 4G и 5G благодаря стандартизации 3GPP (3rd Generation Partnership Project). Благодаря связи V2X ТС могут быстро обнаруживать потенциально опасные и некомфортные дорожные условия и сообщать о них другим ТС, пешеходам на обочине

дороги и придорожным узлам для дальнейшего распространения информации, прежде всего, для повышения безопасности ДД.

AV включают в себя широкий спектр разнообразных технологий, связанных с электроникой, динамикой ТС, связью, контролем, датчиками и правильным знанием человеческих поведенческих инстинктов на дороге. Внедрение новаторских технологий, таких как IoT (Internet of Things), периферийный интеллект EI (Edge Intelligence), 5G и блокчейн в архитектуру AV раскроют потенциал эффективной и устойчивой транспортной системы [6]. Функции частично автономной системы, такие как предотвращение лобового столкновения, предупреждения о выходе из полосы движения и помощь при боковом обзоре могут предотвратить аварии и снизить количество травм и смертельных случаев на 33% [7].

Для беспилотных ТС существуют две беспроводные технологии, которые могут дополнять друг друга для удовлетворения важнейших требований двух сервисов V2X – C-V2X (Cellular Vehicle-to-Everything) и IEEE 802.11p (DSRC (dedicated short-range communications)/ITS-G5), которые работают в лицензированных и нелицензионных диапазонах. Большинство современных автомобилей оснащены портами Bluetooth или точками доступа Wi-Fi для подключения внешних устройств. Кибератакеры могут напрямую подключаться к ТС или взломать устройство, подключенное к точке доступа Wi-Fi. Как правило, радиус действия таких кибератак довольно мал, примерно десятки метров. Bluetooth можно использовать в V2P благодаря его энергосберегающим свойствам. ТС может быть скомпрометировано с помощью Bluetooth-соединения на расстоянии нескольких метров от ТС [8]. Wi-Fi удовлетворяет требованиям некоторых типов связи V2X благодаря преимуществам низкой стоимости и простоты развертывания. Однако все эти средства связи имеют свои собственные уязвимости и сталкиваются с проблемами безопасности.

Результаты и обсуждение.

Автомобильная связь, основанная на IEEE 802.11p (Wi-Fi), сталкивается с рядом проблем из-за некоторых устаревших функций, которые плохо подходят для автомобильной связи. Сегодня ТС оснащены рядом активных датчиков (радар, лидар, камеры), что вынуждает систему V2X обеспечивать дополнительные характеристики, включая большую дальность действия и надежность, особенно в сценариях, когда другие ТС и здания препятствуют системам обзора автомобиля. Ограниченный радиус действия 802.11p ограничивает полезность и общий набор приложений, которые он может обслуживать, что, безусловно, ставит под сомнение его способность обеспечивать безопасность.

Сотовые сети считаются потенциальным источником, который может гарантировать мобильность и бесперебойное соединение в V2V и V2I. Из-за больших зон покрытия и высокой скорости проникновения сотовых сетей некоторые исследователи использовали сотовые сети для проведения удаленных кибератак. В работе [9] авторы показали, что хакеры успешно взломали неизмененный Jeep Cherokee через сотовую сеть, а затем дистанционно управляли важнейшими функциями автомобиля, такими как отключение тормозов и рулевого управления и т.д. C-V2X (Cellular-V2X) является частью общего процесса 3GPP по переходу сотовых систем с технологий 4G на технологии 5G. Услуга C-V2X, основанная на многих существующих инфраструктурах сотовой связи, охватывает большие территории и обладает высокой степенью проникновения и низкой стоимостью, что потенциально позволяет удовлетворить требования высокой пропускной способности и QoS (quality of service)-чувствительных требований автомобильных приложений.

На рисунке 1 показаны кибератаки на CAV. ITS (Intelligent transport systems) – технология, в которой многочисленные ТС взаимодействуют друг с другом с использованием коммуникационной инфраструктуры для обмена критически важными данными. Бортовой блок OBU (on-board unit) ТС отвечает за обмен информацией между ТС в пути. После того, как OBU загрузит информацию в режиме реального времени (РВ) через беспроводную сеть, серверная платформа будет принимать решения и отдавать команды, информируя ведущего водителя ТС о дорожных условиях и помогая в управлении ТС. В частности, технология C-V2X преодолевает ограничения, связанные с интеллектом одного ТС, например, высокую стоимость модификации и множество слепых зон. Камеры, радары, датчики и придорожные устройства RSU (roadside units) развертываются вдоль улицы для сбора подробной информации об окружающих ТС, пешеходах и дорожных условиях, которые затем будут взаимодействовать с OBU для согласования информации. В экстренных или сложных ситуациях, например, при слиянии на перекрестке или риске столкновения в пределах прямой видимости, на бортовом компьютере появится предупреждение, помогающее ему принимать точные решения об автономном вождении. В то же время собранная информация будет передаваться на серверную часть через сеть 5G, обрабатываться и анализироваться облачной платформой, чтобы определить оптимальную скорость, расход топлива и маршрутизацию для максимальной эффективности.

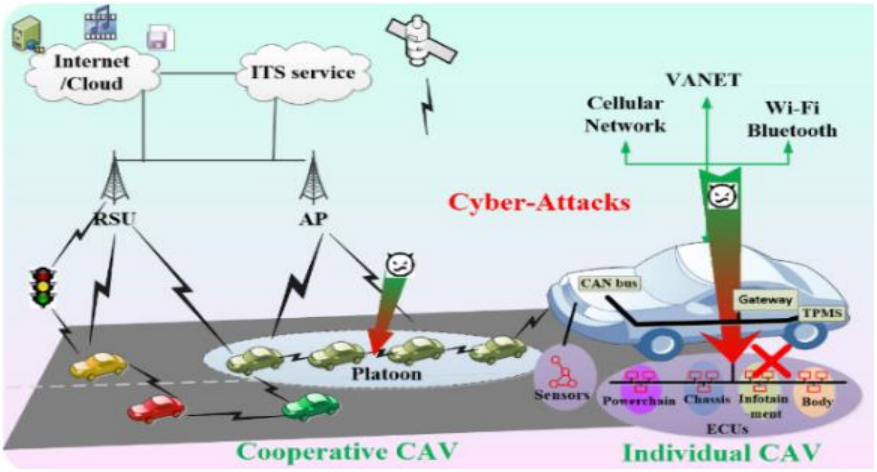

Рисунок 1 - Кибератаки на подключенные и автономные ТС [2]

В VANET (vehicular ad hoc network) безопасный обмен данными между ТС имеет решающее значение для обеспечения эффективности транспортировки, а также безопасности водителя /пассажира (рис. 1). Шина CAN (Controller Area Network, сеть контроллеров) работает как магистраль бортовой сети автомобиля, принимая множество управляющих сообщений и доставляя их в соответствующие ECU (Electronic Control Unit). Атаки на шину CAN включают в себя прослушивание и анализ трафика, глушение и DoS (denial-of-service), а также вредоносную модификацию или инъекцию. Подключаемость ТС увеличила шансы доступа к бортовой сети автомобиля, что подвергает шину CAN большему количеству типов атак. Например, атака может успешно получить доступ к шине CAN и отправить сообщения по шине удаленно с помощью сотовой связи.

ECU – это своего рода встроенная система в ТС, используемая для мониторинга состояния соответствующего компонента в режиме РВ и передачи параметров состояния в шинную систему. Тем временем ECU обрабатывает информацию, поступающую от системы шин, и берет на себя управление операциями, чтобы адаптировать поведение автомобиля. На практике многие ECU соединены друг с другом для выполнения

некоторых сложных функций управления [10], следовательно, атака на один ECU потенциально может повлиять на широкие функциональные возможности управления автомобилем.

VANET – частный случай системы ITS, где мобильные станции – это ТС, а стационарные станции – инфраструктура беспроводной сети, в частности RSU. В последние годы в VANET была применена групповая подпись для защиты анонимности ТС помимо аутентификации. C-V2X и VANET обладают разными функциями и соответственно сталкиваются с разными проблемами безопасности: C-V2X потенциально поддерживает прямую связь V2V, а для повышения безопасности и эффективности сети необходима прямая защищенная связь без предварительной настройки сети ключей. Напротив, VANET изначально поддерживает V2V и V2I, но требует эффективной аутентификации с сохранением конфиденциальности и управлением ключами в групповой подписи для обеспечения безопасной и эффективной связи между несколькими ТС. Поскольку VANET задействует RSU или другую инфраструктуру в своих развертываниях, то необходимо тщательно учитывать безопасность и злоупотребление мощностью RSU или инфраструктуры. Более того, поскольку автомобильное соединение значительно увеличивается, VANET производит постоянно растущий объем данных, что создает серьезные проблемы для эффективной, надежной и безопасной передачи и обработки данных в VANET [10].

Основные векторы атак, которые хакеры используют для автомобильных эксплойтов, выглядят так [3]:

– атаки на облачные серверы (угрозы безопасности любого автомобильного сервера);

– метод входа без ключа, используемый хакерами для кражи и взлома ТС;

– атаки на электронные блоки управления ECU;

– с ростом числа датчиков в современных системах помощи водителю и будущих автономных ТС за этой категорией стоит следить.

5G сделает V2X проще, быстрее и надежнее. Основное различие между платформами 5G и V2X состоят в следующем [11]:

– 5G, как и любая радиомобильная служба, использует инфраструктуру, в которой ландшафт разделен на отдельные ячейки, широко перекрывающиеся и управляемые соответствующими антенными системами (базовыми станциями).

– V2X, как и любой беспроводной сервис, имеет более гибкую структуру, в которой небольшие системы антенных устройств, служащие «горячими точками» («hotspots»), обеспечивают соединение с максимальной эффективностью за счет использования сильной стратегии сотрудничества.

Отметим, что преимущество C-V2X в том, что он основан на технологии, изначально предназначенной для высокоскоростных мобильных приложений, которая была усовершенствована специально для использования в автомобилях, уделяя особое внимание недостаткам, наблюдавшимся в 802.11p в течение нескольких лет исследований. DSRC, будучи устаревшей технологией, может с трудом успевать за меняющимися требованиями к подключению и технологическими требованиями современных систем ITS (intelligent transportation system) [12]. ITS включает в себя интегрированный набор приложений, работающих поверх сетевой структуры, установленной между ТС, общающимися на дороге. Приложения ITS основаны на применении передовых методов обработки информации на данных, собранных с бортовых датчиков (например, датчика давления в шинах, GPS и т. д.) и других устройств мониторинга состояния. Данные периодически передаются между соседними ТС, а также центральным блоком по беспроводному каналу, использующему различные технологии связи. ТС поддерживают связь через OBU, представляющее собой защищенные от несанкционированного доступа

(НСД) устройства и хранят криптографические ключи для обеспечения безопасной связи между ТС. Пользователи ТС подписываются на различные услуги ITS, которые в основном подразделяются на три типа: безопасность, удобство или эффективность дорожного движения и коммерция [13].

C-V2X предлагает более гибкое и масштабируемое решение, которое может преодолеть проблемы нехватки спектра, с которыми сталкивается DSRC. Ключевыми моментами для C-V2X была необходимость поддержки новых автомобильных приложений с интенсивным использованием данных и низкой задержкой для повышения безопасности и автономного вождения, наряду с существенными усовершенствованиями в области беспроводной связи [14]. Преимущества, предлагаемые технологией C-V2X: повышение безопасности, повышение эффективности ДД и снижение воздействия на окружающую среду [12]. Отметим, что по оценкам, автомобили ответственны примерно за 30% выбросов углекислого газа. Для достижения полной автономии управления транспортным средством, ТС должно превосходить человеческое восприятие, принятие решений и интеллект, что может быть достигнуто с помощью более сильных алгоритмов искусственного интеллекта (ИИ) и машинного обучения в сочетании с эффективной связью между ТС и всем (V2X) [15]. V2X как дополнительная технология, обеспечивающая 360-градусную осведомленность об окружающей среде для ТС, будет поддерживаться появлением коммуникационных технологий 5G и 6G, которые направлены на обеспечение сверхнадежной передачи со сверхнизкой задержкой для бесперебойной автомобильной связи. V2X становится одним из популярных способов снижения затрат, связанных с огромными вычислительными потребностями в автономных передовых вычислительных системах, как показано на рисунке 2.

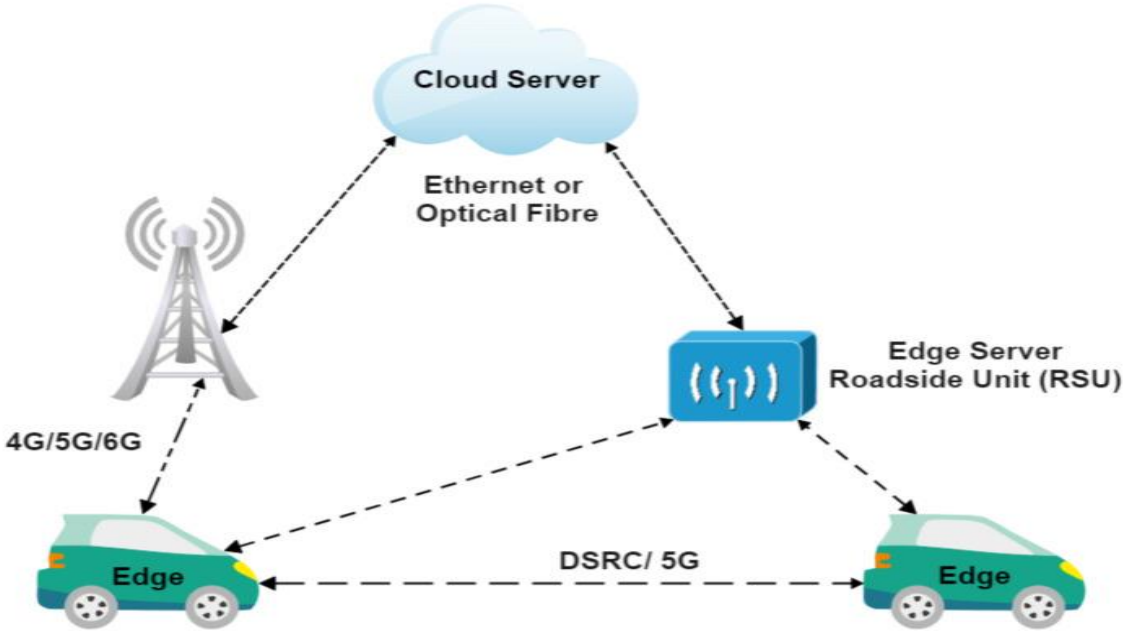

Рисунок 2 - Автономная передовая вычислительная система [16].

Большое внимание уделяется исследованиям V2V и V2I, поскольку они способствуют обмену информацией между транспортными средствами и переносу вычислений на придорожные устройства RSU (road side units). В V2V, даже если два автомобиля не подключены по беспроводной сети, другие автомобили будут передавать сообщение между ними. 3GPP и Qualcomm подготовили дорожную карту для услуг V2X на базе 5G. Исследование 5GAA (5G Automotive Association) показывает, что доставка ITS

через сотовые сети по сравнению с RSU значительно дешевле. Развитие сети 5G наделяет Интернет транспортных средств IoV (Internet of Vehicles) значительными преимуществами, что обеспечивает повышенную безопасность, надежность, эффективность транспортировки, низкую задержку и более широкое покрытие сети, доступное для IoV. IoV включает в себя инфраструктуру и подключенные ТС, которые предлагают пассажирам доступ к мультимедийному контенту, социальным платформам и потоковым сервисам. Кроме того, для повышения качества вождения осуществляется своевременный и мгновенный обмен информацией о безопасности и ДД [17]. Рассмотрим кратко характеристики некоторых наиболее распространенных угроз на автомобильные беспроводные сети:

– Routing: Blackhole (черная дыра), Greyhole (серая дыра), Wormhole (червоточина), Tunnelling (туннелирование) – атаки по маршрутизации – НСД к конфиденциальной информации, нарушение маршрута следования данных. Например, червоточина – вредоносное перенаправление пакетов в беспроводных сетях. Методами борьбы с данными атаками служат: цифровая подпись ПО и датчиков; криптографический сертификат, симметричная криптография, MAC (Media Access Control, контроль доступа к среде) и односторонний хэш в протоколе маршрутизации.

1. Sybil (Сибилла) – атака на аутентификацию – разрушение репутации сети путем клонирования ложных идентификаторов.

2. Node impersonation (олицетворение узла) – подмена идентификации участника ДД.

3. Man, in the middle (человек посередине) – перехват и модификация сообщений между автомобилями и точками доступа.

4. GPS-spoofing / Hidden vehicle (position faking) (скрытое транспортное средство (имитация местоположения)) – подмена координат местоположения узла (используя GPS-симулятор, злоумышленник генерирует сигнал, превосходящий мощностью реальный сигнал спутника, а ТС считывают более сильный, ложный сигнал, который транслирует автомобилю неверное местоположение, принимаемое за истинное).

5. Traffic analysis (анализ трафика) – определение топологии сети, маршрутизации (перехват и анализ различного рода служебных и информационных пакетов, которые могут содержать в себе местоположение, идентификационные данные, маршрут и т.д.).

6. Key and/or certificate replication (репликация ключа и/или сертификата) – неавторизованная идентификация в системе (использование дубликатов ключей, сертификатов или их комбинации для неавторизованной идентификации пользователя в системе).

7. DoS – атаки на доступность – отказ в обслуживании (доведение VANET до отказа или увеличение задержки в сети, что сделает невозможным или затруднит получение информации легитимными пользователями). Здесь отметим, что информация в автомобильных беспроводных сетях очень быстро устаревает, следовательно, даже небольшие задержки могут свести работу отдельного сегмента к нулю, так как в момент получения информации дорожная ситуация уже будет совершенно иной.

8. Tracking (отслеживание) – НСД к идентификационной информации об узле (отслеживание местоположения ТС в течение промежутка времени для получения детальной информации об узле).

9. Message tampering / suppression / fabrication (подделка /подавление /фальсификация сообщений) – атаки на передаваемые сообщения [18].

Message tampering (подделка сообщений) – угроза направлена на нарушение целостности передаваемых сообщений: злоумышленник модифицирует сообщения OBU-OBU и OBU-RSU, при этом фальсификации могут быть подвержены, как запрос приложения, так и ответ на запрос.

Атака Message Suppression (подавление сообщений) направлена на нарушение конфиденциальности передаваемых сообщений: злоумышленник осуществляет выборку пакетов и транслирует их в сеть, доступ к которой имеют посторонние пользователи, не участвующие в валидном обмене этих пакетов; пакеты, в частности, могут содержать информацию, относящуюся к безопасности узла.

Атака Message Fabrication (изготовление сообщений) направлена на нарушение целостности и конфиденциальности передаваемых сообщений: злоумышленник транслирует в сеть ложные сообщения; подобным образом злоумышленник может получить право приоритетного проезда, неавторизованный доступ к системным ресурсам и конфиденциальным данным (пароли, логины других узлов).

Практически все приведенные угрозы характерны для любой беспроводной сети. К специфическим угрозам именно для VANET относятся GPS-spoofing / Position faking [19]. Из этого следует, что VANET - инфокоммуникационная система, которая наследует далеко не все уязвимости ее составных частей (например, беспроводной сети), но приобретает принципиально новые.

Физические атаки на датчики включают использование яркого света для ослепления камер и создание помех с помощью ультразвука или радиоволн, чтобы отвлечь другие датчики от правильного восприятия препятствий. Такие ситуации могут даже привести к несчастным случаям со смертельным исходом. Если какой-либо отказ датчика останется незамеченным, неизбежно произойдут катастрофические и фатальные аварии. Например, датчики GNSS (Global Navigation Satellite System), точно сообщающие глобальную оценку положения, имеют слишком низкую скорость обновления, чтобы соответствовать требованиям PB и склоны к кибератакам, преднамеренному глушению и спуфингу (подмене). В последнее время, благодаря развитию технологии ИИ, возможности восприятия датчиков могут быть улучшены, чтобы повысить скорость обнаружения и снизить частоту ошибок [20]. Типичным примером является то, что точность обнаружения камер можно повысить с помощью методов нейронных сетей [21]. Таким образом, развитие технологий ИИ в некоторой степени может сделать датчики более устойчивыми к вредоносным атакам.

Злоумышленник может даже перехватывать сообщения внутри и между транспортными средствами связи (V2V и V2I) и серьезно угрожать безопасности и конфиденциальности владельцев и других AV. Кибератаки могут привести к проблемам с функциональной безопасностью и могут легко привести к краже конфиденциальности и/или личных данных, даже ценой чьей-то жизни, если злоумышленник преднамеренно меняет направление и получает полный контроль над действиями AV [22].

В предотвращение конфликтов и обеспечение доступности и надежности связи вносит вклад и инфраструктура (RSU, облака). Инфраструктура будет играть решающую роль в распределении каналов, кэшировании, загрузке контента, агрегации/распространении данных, автоматическом режиме, местоположении, маршрутизации и безопасности автомобильной связи в будущем [23]. Если инфраструктура будет скомпрометирована кибератаками, то это может нанести масштабный ущерб. Между тем, инфраструктура может иметь другую архитектуру, помимо включения существующих устройств, например кооперативную архитектуру, виртуальную архитектуру и т. д., что также делает ее уязвимой для многих кибератак. Поэтому защита инфраструктуры от кибератак станет серьезной проблемой.

В случае CAV на способность обнаружения могут влиять злонамеренные атаки посредством спуфинга (например, поддельные сигналы GPS) с целью создания мошенничества или ненадежных данных. Кроме того, злоумышленники могут задержать сбор и передачу данных с помощью DoS-атак, чтобы отключить чувствительные к задержке приложения и, таким образом, поставить под угрозу безопасность ТС. Локально

каждое транспортное средство и RSU/BS (base station) оснащаются дополнительными вычислительными блоками и хранилищем для обработки некоторых данных/информации для удовлетворения требований чувствительных ко времени приложений. Неизбежно, что многие сообщения собираются ТС из одного и того же региона, что указывает на большое дублирование и избыточность в сообщениях. Благодаря использованию облака эти сообщения могут быть объединены и сокращены посредством анализа релевантности данных, прежде чем они будут повторно переданы в регион или определенное количество ТС. Путем передачи компактных, но полезных сообщений можно улучшить полезность каналов связи, а кибератаки типа DoS/спуфинг, можно предотвратить.

Новым типом атаки в ITS служит атака без передачи маяка BNT (Beacon Non-Transmission), при которой злоумышленник является не промежуточным ТС, а, скорее, исходным транспортным средством. При атаке BNT транспортное средство подавляет передачу своих собственных периодических пакетов маяков, чтобы избавиться от автоматических протоколов обнаружения неправильного поведения при вождении, работающих в ITS, или организовать атаку типа DoS, чтобы нанести ущерб функциям управления трафиком ITS [24].

Для обнаружения неисправности или присутствия хакеров может быть установлено различное ПО с частыми обновлениями ПО и изменением архитектуры безопасности. Правительства США, Китая, Евросоюза и Сингапура приняли новое законодательство для устранения рисков конфиденциальности и кибербезопасности, а также приняли стратегию, ориентированную на контроль. Растущие потребности в автономном вождении привели к слиянию машинного обучения и граничных вычислений, что привело к появлению граничного интеллекта, который позволяет AV точно определять свое окружение, разгружая данные на более мощный пограничный сервер, расположенный на базовой станции. Поскольку AV не постоянно запускают приложения с интенсивными вычислениями, можно использовать систему граничных вычислений с малой задержкой для эффективного управления транспортными ресурсами. Многие аспекты безопасности можно обеспечить с помощью решений на основе технологий 5G и блокчейн, внедрив контрмеры для устранения подавляющего спектра атак и их глушения, а также сбоя канала связи или неэтичного контроля. Блокчейн стал лучшим решением для обеспечения защиты AV благодаря прозрачности данных, неизменности и децентрализованному подходу.

Заключение.

Потребители находятся в центре экосистемы ТС, и они должны знать о проблемах безопасности. В автомобильных сетях возникают проблемы с безопасностью и конфиденциальностью из-за информации, предоставляемой ТС. Злоумышленники могут изменить передаваемое ТС сообщение. Используемые коммуникации V2X включают в себя многочисленные системы, которые взаимодействуют на разных уровнях и направлены на охват различных факторов, влияющих на вождение. ТС становятся более совершенными и эволюционируют в сторону интеллектуальных и автономных ТС, поэтому требования к V2X становятся все более жесткими. Технология C-V2X позволяет ТС связываться друг с другом, с пешеходами и с окружающей инфраструктурой с помощью сотовой сети. C-V2X предназначен для повышения безопасности ДД, уменьшения заторов на дорогах и повышения эффективности транспортной системы. Однако современные автомобильные сетевые технологии (IEEE 802.11p, C-V2X) не могут удовлетворить требования к автономным ТС следующего поколения, которым требуется сверхнадежная связь для критически важных приложений и приложений безопасности. Сегодня ТС производителей Tesla и Toyota полагаются на датчики для непрерывного определения своего окружения, в первую очередь путем идентификации и

классификации информации (восприятия) с последующим воздействием на нее посредством автономного управления ТС при условии доступности покрытия сети, низкой задержки и высокой скорости соединения. Дальнейшая эволюция беспилотных ТС (AV), являющихся неотъемлемой частью наземного транспорта, зависит от многих факторов из-за чрезвычайно строгих требований к безопасности, защищенности и надежности. Сложность инфраструктуры AV делает ее уязвимой для атак на безопасность и конфиденциальность, которые могут поставить под угрозу жизнь пассажиров. В перспективе широко распространятся AV, поэтому необходимо подготовиться к вызовам безопасности, связанным с ТС, автомобильными сетями. С появлением технологии 5G и AV безопасность ДД станет более безопасной с меньшим количеством человеческих ошибок, но пока интеграция 5G и AV все еще находится на начальной стадии [25]. С увеличением количества беспроводных подключений ТС, таких как Bluetooth, VANET и сотовые сети, потенциальные уязвимости ТС становятся все более уязвимыми, и кибератаки могут осуществляться с целью использования уязвимостей и воздействия на производительность и работу CAV. Безопасность CAV должна быть тщательно продумана и построена до того, как CAV будет полностью разработан и развернут на практике**.** Для использования на практике полностью автономных ТС, восприятие и работа ТС должны быть хорошо защищены, что является главным требованием для приложений CAV. С развитием IoV некоторые мощные меры обнаружения и защиты могут быть реализованы в облаке, которое обладает огромными объемами информации и мощными ресурсами для защиты CAV от некоторых типов интеллектуальных атак. Основная техническая задача, которую необходимо решить при обнаружении новых атак типа BNT, – точно и эффективно отличить потерю пакетов маяков из-за ошибки канала и умышленное подавление маяков транспортным средством злоумышленника BNT. Внедрение блокчейна в интегрированные периферийные вычисления на базе 5G в автомобильных сетях дает некоторые преимущества, поэтому появляется необходимость интеграции блокчейна в автомобильные сети на базе 5G для обеспечения безопасности, защиты конфиденциальности и кэширования контента.

ЛИТЕРАТУРА

[1] Технологии в автомобилестроении//Tadviser [Электронный ресурс] URL: https://www.tadviser.ru/index.php/ Статья: Технологии_в_автомобилестроении (дата обращения 15.12.2023).

[2] Zhendong Wang et al. Security Issues and Solutions for Connected and Autonomous Vehicles in a Sustainable City: A Survey // Sustainability. - 2022, 14, 12409. https://doi.org/10.3390/su141912409.

[3] Egil Juliussen. Automotive Cybersecurity: More Than In-Vehicle and Cloud. [Электронный ресурс] URL: https://www.eetimes.eu/automotive-cybersecurity-more-than-in-vehicle-and-cloud/ (дата обращения 15.12.2023).

[4] Parkinson S., Ward P., Wilson K., Miller J. Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges // IEEE Trans. Intell. Transp. Syst. - 2017, - 18, 2898–2915.

[5] https://www.thebrainyinsights.com/report/vehicle-to-everything-v2x-market-13502. 2023. (не открывается ссылка)

[6] Biswas A, Wang HC. Autonomous Vehicles Enabled by the Integration of IoT, Edge Intelligence, 5G, and Blockchain // Sensors (Basel). – 2023, - 23(4):1963. DOI: 10.3390/s23041963.

[7] Anderson J.M. et al. Autonomous Vehicle Technology: A Guide for Policymakers. Rand Corporation; Santa Monica, CA, USA: 2014.

[8] Checkoway, S. et al. Comprehensive Experimental Analyses of Automotive Attack Surfaces. In Proceedings of the USENIX Security Symposium, San Francisco, CA, USA, 8–12 August 2011.

[9] Chris, V.; Charlie, M. Remote Exploitation of an Unaltered Passenger Vehicle. White Paper. 2015; p. 93. [Электронный ресурс] URL: https://illmatics.com/Remote%20Car%20Hacking.pdf.

[10] Cheng, N.; Lyu, F.; Chen, J.; Xu, W.; Zhou, H.; Zhang, S.; Shen, X. Big data driven vehicular networks. IEEE Netw. 2018, *32*, 160–167.

[11] https://www.wevolver.com/article/a-deep-dive-into-the-new-v2x-and-cellular-v2x-architectures-based-on-5g.

[12] Dhinesh Kumar R., Rammohan A. Revolutionizing Intelligent Transportation Systems with Cellular Vehicle-to-Everything (C-V2X) technology: Current trends, use cases, emerging technologies, standardization bodies, industry analytics and future directions // Vehicular Communications. - 2023. 100638. ISSN 2214-2096. https://doi.org/10.1016/j.vehcom.2023.100638.

[13] Bauza R. et al. Traffic congestion detection in large-scale scenarios using vehicle-to-vehicle communications // J. Netw. Comput. Appl. 2013.

[14] David Martín-Sacristán, Jose F. Monserrat. 5G New Radio Numerologies and their Impact on V2X Communications Josue Flores de Valgas. // Waves – 2018. ISSN 1889-8297

[15] Tong W., Hussain A., Bo W.X., Maharjan S. Artificial intelligence for vehicle-to-everything: A survey // IEEE Access. - 2019; 7:10823–10843. DOI: 10.1109/Access.2019.2891073.

[16] Liu S., Liu L., Tang J., Yu B., Wang Y., Shi W. Edge computing for autonomous driving: Opportunities and challenges // Proc. IEEE. 2019; 107:1697–1716. DOI: 10.1109/JPROC.2019.2915983.

[17] Anas Knari et al. Multi-Agent Deep Reinforcement Learning for content caching within the Internet of Vehicles // Ad Hoc Networks, - 152, - 2024. 103305. ISSN 1570-8705. https://doi.org/10.1016/j.adhoc.2023.103305.

[18] Bujnevich M.V., Stoljarova E.S., Horoshenko S.V., Shirjaev D.M., Vladyko A.G. Top-10 ugroz informacionnoj bezopasnosti VANET: analiticheskij obzor [Top 10 information security threats VANET: survey] (in Rus)

[19] Vinh H.L., Cavalli A.R. Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey // International Journal on AdHoc Networking Systems, - 2014, -4, №. 2, 1-20.

[20] Azarang A. Kehtarnavaz N. Image fusion in remote sensing by multi-objective deep learning // Int. J. Remote Sens. - 2020, - 41, 9507–9524.

[21] Zeng X., Wang Z., Hu Y. Enabling Efficient Deep Convolutional Neural Network-based Sensor Fusion for Autonomous Driving // arXiv 2022, arXiv:2202.11231.

[22] Kim S., Shrestha R. Automotive Cyber Security. Springer; Berlin/Heidelberg, Germany: 2020. Security and Privacy in Intelligent Autonomous Vehicles; 35–66.

[23] Silva, C.M.; Masini, B.M.; Ferrari, G.; Thibault, I. A survey on infrastructure-based vehicular networks // Mob. Inf. Syst. - 2017, 6123868.

[24] Fahiem Altaf, Kumar Prateek, Soumyadev Maity. Beacon Non-Transmission attack and its detection in intelligent transportation systems // Internet of Things, - 2022. 100602. ISSN 2542-6605. https://doi.org/10.1016/j.iot.2022.100602.

[25] Saqib Hakak, Thippa Reddy Gadekallu, et al. Autonomous Vehicles in 5G and Beyond: A Survey. https://doi.org/10.48550/arXiv.2207.10510.

Манат Иманкул, т.ғ.к., доцент, L.N. Gumilyov Eurasian National University, Астана, Қазақстан, mimankul57@gmail.com
Жанат Манбетова, PhD, Saken Seifullin University, Астана, Қазақстан, zh.manbetova@kazatu.kz
Асель Ержан, PhD, доцент, Energo University, Алматы, Қазақстан, a.erzhan@aues.kz
Альмира Мухамеджанова, PhD, Energo University, Алматы, Қазақстан, a.omarbekova@aues.kz

КӨЛІКТЕРДІҢ СЫМСЫЗ ЖЕЛІЛЕРІНДЕГІ АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЭЛЕМЕНТТЕРІ

Аңдатпа. Болашақта қазіргі қосылған және автоматтандырылған CAV көліктері (connected and automated vehicles, қосылған және автоматтандырылған көлік құралдары) автономды AV көліктеріне (Autonomous Vehicles) айналады. Сенімсіз байланыс, ашық арналар, қауіпті шина жүйелері және ақылды хакерлердің болуы сияқты автомобиль қауіпсіздігі жүйелеріндегі саңылауларға байланысты AV аппараттық және бағдарламалық қамтамасыз ету жүйелері бұзылуы мүмкін. Хакерлер сымсыз желілер (Wi-Fi, ұялы желілер және т.б.) арқылы AV және қосылған көліктерді тартып ала алады. Бұл мақалада CAV қауіпсіздігі бойынша жеке зерттеулер қарастырылған, өйткені көлік құралдарының байланысын кеңейту ықтимал осалдықтарға ұшырауды арттырады және кибершабуылдарға мүмкіндіктер ашады. Кибершабуылдардың CAV-ке әсері атап өтілді. CAV-тің жұмыс істеуін қамтамасыз ету CAV-ті іс жүзінде қауіпсіз және сенімді қолданумен байланысты екендігі көрсетілген. BNT (Beacon non-Transmission, маяк сигналының берілмеуі) шабуылы атап өтілді, онда зиянды көз мақсатты ITS (intelligent transportation system) қолданбасына арналған өзінің мерзімді деректерін басады. Интеллектуалды кибершабуылдардан қорғау үшін бұлтты технологиялар мен жасанды интеллект әдістерін қолдану да атап өтілді. Автомобиль сымсыз желілеріне кейбір кең таралған қауіптердің сипаттамалары келтірілген. V2X технологиясы арқылы жол-көлік оқиғаларының деңгейін айтарлықтай төмендетуге болатындығы көрсетілген, ал 5G технологиясы V2X байланысын айтарлықтай жақсартады, бұл жылдамырақ, сенімді және жоғары байланыс өткізу қабілеттілігін қамтамасыз етеді.

Түйінді сөздер. Автономды көлік құралдары, қосылған басқарылатын көлік құралдары, V2X, S-V2X, IEEE 802.11p, VANET, интеллектуалды көлік жүйесі.

Manat Imankul, candidate of technical sciences, docent, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, mimankul57@gmail.com
Zhanat Manbetova, PhD, Saken Seifullin University, Astana, Kazakhstan, zh.manbetova@kazatu.kz
Assel Yerzhan, PhD, docent, Energo University, Almaty, Kazakhstan, a.erzhan@aues.kz
Almira Mukhamejanova, PhD, Energo University, Almaty, Kazakhstan, a.omarbekova@aues.kz

ELEMENTS OF INFORMATION SECURITY IN VEHICLE WIRELESS NETWORKS

Abstract. In the future, the current connected and automated CAV vehicles (connected and automated vehicles) will turn into autonomous AV vehicles (Autonomous Vehicles). Due to loopholes in automotive security systems such as unreliable communications, open channels, unsafe bus systems and the presence of intelligent hackers, AV hardware and software systems

can be compromised. Hackers can hijack AV and connected vehicles through their wireless networks (Wi-Fi, cellular networks, etc.). This article examines selected studies on CAV security, as the expansion of vehicle connectivity increases exposure to potential vulnerabilities and opens up opportunities for cyber-attacks. The impact of cyber-attacks on the CAVs was noted. It is shown that ensuring the functioning of CAVs is associated with the safe and reliable application of CAVs in practice. A BNT (Beacon Non-Transmission) attack has been noted, in which a malicious source suppresses its own periodic data transfers intended for ITS (intelligent transportation system) target application. The use of cloud technologies and artificial intelligence methods to protect against intelligent cyber-attacks was also noted. The characteristics of some of the most common threats to car wireless networks are given. It is shown that the level of traffic accidents can be significantly reduced using V2X technology, and 5G technology significantly improves V2X communication, providing faster, more reliable, and higher communication bandwidth.

Keywords. Autonomous vehicles, connected vehicles, V2X, S-V2X, IEEE 802.11p, VANET, intelligent transportation system.

****

Редакцияға түсті / Поступила в редакцию / Received 29.02.2024
Жариялауға қабылданды / Принята к публикации / Accepted 27.01.2025