Обеспечение безопасности интеллектуальных транспортных средств в инфраструктуре умного города

А.В. Скатков, А.А. Брюховецкий, Д.В. Моисеев, Д.Ю. Воронин

Севастопольский государственный университет

Аннотация. В настоящее время одним из распространенных подходов к развитию городской инфраструктуры является концепция «Умного города», охватывающая подавляющее большинство сфер человеческой жизнедеятельности: здравоохранение, безопасность, транспорт, жилищно-коммунальное хозяйство, образование и туризм. Развитие транспортной инфраструктуры умного города тесным образом связана с развитием технологий интеллектуальных транспортных средств. Работа посвящена анализу современного состояния и перспектив направления обеспечения безопасности интеллектуальных транспортных средств в инфраструктуре умного города. С целью разрешения указанных проблем возникает необходимость разработки адаптивных систем интеллектуальной поддержки принятия решений по обнаружению уязвимостей интерфейсов беспилотных транспортных средств. Применение предлагаемых в работе подходов позволит обеспечить гарантированный уровень ИТ-сервисов, позволяющих эффективно решать научные задачи обнаружения уязвимостей интерфейсов беспилотных транспортных средств.

Ключевые слова: беспилотное транспортное средство, умный город**,** электронный блок управления, сетевая шина управления, уязвимости интерфейсов.

Ensuring the safety of intelligent vehicles in the smart city infrastructure

A.V. Skatkov, A.A. Bryukhovetsky D.V. Moiseev, D.Y. Voronin

Sevastopol State University

Abstract. Currently, one of the common approaches to the development of urban infrastructure is the concept of “Smart City”, covering the vast majority of spheres of human life: health, safety, transport, housing and communal services, education and tourism. The development of the transport infrastructure of the Smart City is closely related to the development of intelligent vehicle technologies. The work is devoted to the analysis of the current state and future prospects of the safety ensuring for

intelligent vehicles in the smart city infrastructure. In order to solve these problems, it becomes necessary to develop adaptive intelligent decision support systems for detecting vulnerabilities in unmanned vehicle interfaces. The application of the approaches proposed in this work will provide a guaranteed level of IT services that will effectively solve the scientific problems of detecting vulnerabilities in unmanned vehicle interfaces.

Keywords: unmanned vehicle, smart city, electronic control unit, network control bus, vulnerabilities of interfaces.

Введение

В последнее десятилетие наблюдается быстрое развитие беспилотных транспортных средств (БТС), в том числе автомобильных систем, в самых разных аспектах. В нынешнем году Севастопольский государственный университет примет участие в создании высокотехнологичного производства компонентов гибкой модульной сенсорно-коммуникационной платформы для бортовых систем воздушного судна в рамках направления Аэронет. Исполнителем проекта станет Балтийский государственный технический университет «Военмех» имени Дмитрия Фёдоровича Устинова. Заказчик – ЗАО «Абрис» – ведущий производитель авиационной сенсорики.

Сложность современных транспортных систем в сочетании с резким увеличением использования электронных компонентов и беспроводных технологий изменила традиционную концепцию безопасности в автомобильной промышленности. Более того, растущий интерес к развитию специальных транспортных сетей (VANET) и интеллектуальных транспортных систем (ITS) привел к появлению новых проблем безопасности и уязвимостей [1]. Тем не менее, давно установленные политики компьютерной безопасности не соблюдаются отраслевыми стандартами для автомобильной отрасли и автомобильной связи из-за аппаратных ограничений и различий в конфигурации сети [2].

В настоящее время реализация атаки на транспортные средства происходит главным посредством обмена информацией по беспроводной связи, которая оказывается уязвимой к различным злонамеренным атакам. Следовательно, обеспечение секретности информации, конфиденциальности данных, обмена данными, включая входные и выходные данные, а также защиту электронных блоков управления (ECU) внутри транспортных систем, являются одними из наиболее важных вопросов безопасности и конфиденциальности для интеллектуальных транспортных средств [3].

Обеспечение кибербезопасности в БТС является одной из наиболее серьезных проблем, которая ставит под угрозу, в первую очередь, безопасность пассажиров. Кибербезопасность в интеллектуальных транспортных средствах включает в себя безопасность в автомобиле и безопасность межтранспортной связи. Безопасность электронных блоков управления (ECU) и сетевая шина управления (CAN) являются наиболее важными элементами беспилотного

транспортного средства, особенно в условиях развития 4G LTE и 5G коммуникационных технологий дистанционного управления для протокола V2X. В настоящее время защитным мерам безопасности на транспортных средствах и при взаимодействии между транспортными средствами не уделяется достаточного внимания, поэтому разработка методов обеспечения безопасности БТС является актуальной задачей, представляющей научный и практический интерес.

1. Архитектура системы умного транспортного средства

Серийное производство интеллектуальных транспортных средств высокого уровня (ICV) является активной темой исследований в автомобильной промышленности. Многие интеллектуальные функции вождения установлены на легковых автомобилях, такие как помощь в поддержании полосы движения (LKA), предупреждение о выходе из полосы движения (LDW) и другие системы помощи. Конечно, интеллектуальный автомобиль высокого уровня должен быть в состоянии выполнить все эти функции. Тем не менее, невозможно просто объединить все эти интеллектуальные системы помощи, просто сложив их вместе, так как традиционная электрическая / электронная архитектура (EEA) не была разработана для поддержки стольких интеллектуальных функций. В частности, требуемые возможности сбора и обработки данных выходят за рамки традиционных EEA. EEA следующего поколения нуждается в фундаментальном совершенствовании трех компонент умного города: общей инфраструктуре, сети связи между транспортными средствами и между беспилотными транспортными средствами и базовыми станциями, а также между БТС и диспетчерским центром.

Топология общей архитектуры является фундаментом для повышения производительности EEA. Основная задача проектирования топологии – обеспечить передачу потока данных в сети в соответствии с потребностями каждого узла. Как показано на рис. 1, традиционная схема EEA основана на контроллере локальной сети (CAN).

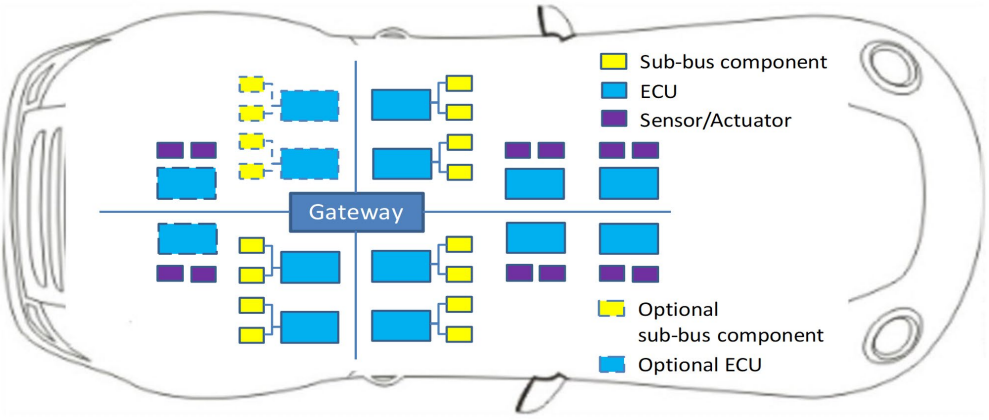

Рис. 1. Архитектура E / E на основе контроллера локальной сети (CAN).

В топологии CAN каждый узел в сети должен разделять пропускную способность между собой. Пропускная способность подобна узкому месту (бутылочному горлышку), которое ограничивает возможности обработки данных каждого блока управления двигателем в автомобиле (электронный блок управления) ECU в сети. Основной проблемой традиционного EEA является нехватка места для блока с высокой вычислительной мощностью, что необходимо для интеллектуального вождения.

В интеллектуальных транспортных средствах ICV процессоры должны выполнять более сотен миллионов инструкций для реализации интеллектуальных алгоритмов, включая обработку данных с датчиков и методы глубокого обучения. Поэтому необходима мощная вычислительная платформа с улучшенным аппаратным и программным обеспечением. Считается, что и GPU, и FPGA в ближайшем будущем получат широкое применение в автомобильной промышленности. Графический процессор специализируется на широкомасштабных параллельных вычислениях, и, таким образом, он успешно применяется в обработке изображений [8], что делает его идеальным в транспортных средствах с автономным управлением для сложных вычислительных систем, таких как система обнаружения препятствий и система предотвращения столкновений. Другой вариант – программируемые пользователем вентильные матрицы (FPGA), которые подходят для параллельных вычислений и потребляют меньше энергии.

Для достижения полного контроля как за состоянием автомобиля, окружающей средой, а также за пределами визуального диапазона, интеллектуальное транспортное средство должно быть оснащено множеством датчиков. На рисунке 2 показаны некоторые известные датчики, [10], которые используются в БТС.

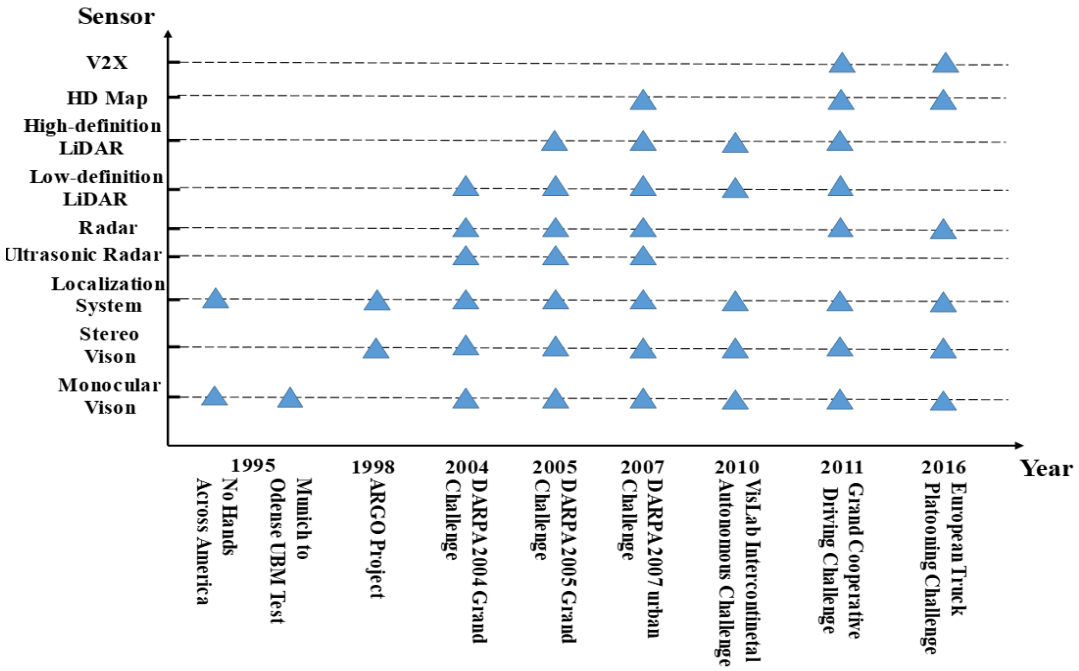

Рис. 2. Основные датчики, используемые в БТС

В последнее время большую популярность приобретают датчики для ICV высокого уровня: LiDAR, Radar, которые используются в умных камерах.

• LiDAR означает «обнаружение света» и «дальний свет», позволяет автомобилям с автоматическим управлением наблюдать за внешней средой. Фактически, это достигается использованием лазерных световых импульсов. Высокое разрешение LiDAR обеспечивает 360-градусное поле зрения с более чем 16 лазерными каналами. Что касается механизмов вращения, LiDAR можно разделить на три основные категории: механический LiDAR, полужесткий LiDAR и жесткий LiDAR.

• Радар миллиметрового диапазона способен «видеть» сквозь непрозрачные материалы, такие как дымка, пыль, снег и туман. Другими словами, основным преимуществом радара миллиметрового диапазона является его способность обрабатывать объекты малых размеров во всепогодных условиях и на больших расстояниях. Однако низкое горизонтальное разрешение и низкая боковая точность обнаружения является наиболее значимыми ограничения радаров [11]. Из-за этих недостатков необходимо совместное использование радаров миллиметрового диапазона с другими датчиками с целью повышения точности системы восприятия объекта. Одним из решений является использование радаров миллиметрового диапазона и монокулярной камеры.

• Интеллектуальные визуальные датчики: монокулярная визуальная система и система стереозрения являются основными интеллектуальными визуальными датчиками в интеллектуальных транспортных средствах. Они используются для того, чтобы достичь семантической сегментации визуальных сцен, обнаружения цели и ее слежения, масштабирования [10].

2 Требования безопасности и идентификация атак

Динамическая природа VANET и взаимодействие БТС в реальном времени говорят о том, что атаки могут быть эффективными и часто иметь пагубные последствия. В последние годы был обнаружен широкий спектр атак на интеллектуальные системы транспортных средств. На самом деле, кибербезопасность становится все более серьезной проблемой для многих правительств и корпораций во всем мире. Поскольку предполагается, что VANET сети будут работать, по крайней мере частично, на существующей архитектуре, число типов атак, с которыми сталкиваются VANET сети, постоянно расширяется.

Успешное, безопасное и надежное использование интеллектуальных автомобильных систем зависит от проектирования и разработки системы безопасности. Поэтому автомобильные системы должны соблюдать строгие требования к безопасности. Идентификация соответствующих требований безопасности на ранних стадиях концептуального проектирования и разработки играет ключевую роль в обеспечении того, чтобы транспортные средства и пассажиры всегда оставались в безопасности.

В литературе аутентификация, целостность, конфиденциальность и доступность являются одними из наиболее важных предпосылок, которые должна обеспечивать система безопасности. В этой работе обсуждаются эти четыре категории как ключевые требования для успешной и безопасной интеграции различных систем.

1) **Аутентификация** является одним из ключевых требований безопасности любых систем связи. Фактически, это требование для проверки личности участников связи, защиты конфиденциальной информации и критических данных путем предотвращения любого несанкционированного доступа [12]. Аутентификация в автомобильных системах является важным атрибутом, который необходимо тщательно рассмотреть на ранних этапах проектирования и внедрения системы. Это означает, что данные / информация могут быть доступны только авторизованным пользователям. По сути, только предполагаемые стороны должны иметь доступ к сообщению и извлекать его оригинальное содержание. Для выполнения требования аутентификации важно, чтобы управление ключами и их распределение были эффективными и точными.

2) **Целостность** системы связи относится к достоверности данных между отправителем и получателем. Основным требованием целостности в системе связи является то, что полученные данные являются точными и не изменяются злонамеренно [12]. В автомобильных сетях важно иметь возможность проверить, что сообщение не было повреждено во время передачи такими факторами ухудшения, как шум и замирание, а также целенаправленно злоумышленником. Для достижения этой цели должны быть реализованы коды обнаружения и исправления ошибок.

3) **Конфиденциальность.** В режимах связи совместно используемая информация между транспортными средствами посредством протоколов V2V и V2I, где БТС используют различные методы для обмена данными (например, информацией об их географическом местоположении), может использоваться злонамеренно для отслеживания пользователей [13]. Следовательно, конфиденциальность является еще одной серьезной проблемой в интеллектуальных системах транспортных средств, и конфиденциальная информация должна быть защищена в интеллектуальных БТС.

4) **Доступность** в автомобильных сетях имеет большое значение, так как получение необходимой информации всеми транспортными средствами должно быть обеспечено в режиме реального времени. Сети VANET очень динамичны и сеть должна отвечать на запросы в режиме реального времени. Непрерывную доступность трудно достичь в нормальных условиях эксплуатации, и это становится еще сложнее, если учесть, что обновления и исправления также должны будут использоваться в некоторых случаях. Поэтому вопросы доступности контента и снижения стоимости доставки информационных пакетов в канале связи приобретают особую важность. Когда в одной части сети происходит сбой или временное отключение, важно, чтобы работа сети продолжалась, и чтобы транспортные средства не зависели от каких-либо проблем. Важно, чтобы услуги были доступны в любое время. Следовательно, необходимая избыточность для этой цели должна быть реализована должным образом [14-16].

3. Методы обеспечения безопасности БТС

В этой работе представлены типы атак на компоненты БТС (Таблица 1) и существующие средства защиты, которые используются в настоящее время для борьбы с атаками на сетевую безопасность, а также обсуждаются достоинства и недостатки этих средств. Здесь рассматриваются методы защиты против атак заданных типов, базирующиеся на сигнатурном анализе (Signature-based Detection), выявления аномалий (Anomaly-based Detection) и обнаружения вредоносных атак (Malware Detection) [12-13].

Таблица 1. Идентифицированные атаки на БТС и методы защиты от них

	Cryptography	Network Security	Software Vulnerability Detection	Malware Detection
DoS	✓	✓	✓	
DDoS	✓	✓		
Black-hole	✓	✓		
Replay	✓			

Sybil	✓	✓		
Impersonation	✓	✓		
Malware	✓		✓	✓
Falsified Information	✓	✓		
Timing	✓			

Интеллектуальные транспортные средства требуют взаимодействия по каналам связи с другими транспортными средствами и датчиками. Эти коммуникации осуществляются между локальной сетью контроллеров (CAN) и электронными блоками управления (ECU). CAN и ECU являются важными целями для злоумышленников. Например, автомобили могут подключаться к проводным устройствам с помощью USB, CD, беспроводных сетей, таких как 3G, 4G, WiFi и смартфонов, и все это превращает автомобиль в открытую систему. Поэтому очень важно предложить подходящие контрмеры, чтобы уменьшить риски безопасности в интеллектуальном автомобиле. Системы обнаружения вторжений (IDS) являются наиболее действенной контрмерой и наиболее надежным подходом обеспечения защиты автомобильных сетей или традиционных компьютерных сетей.

1) **Обнаружение на основе сигнатур.** Этот метод сначала сохраняет различные существующие сигнатуры известных атак в базе данных для поиска и сравнения. Затем он обнаруживает атаку вторжения, сравнивая поступающие образцы (сигнатуры вторжений) с образцами базы данных Интернета известных атак.

2) **Обнаружение на основе аномалий.** Обнаружения на основе аномалий предполагает описание, обучение, тестирование и настройку параметров системы на данных, которые характеризуют нормальное поведение системы. В режиме контроля оценивается отклонение значений параметров от значений, которые соответствуют нормальному состоянию.

Недостатками методов обнаружения на основе аномалий являются: 1) в ряде случаев имеется большой процент ложных срабатываний, 2) обычно трудно подготовить правильные метрики для составления исходного описания. Тем не менее, ожидается, что данные методы могут помочь улучшить производительность и достоверность моделей в будущем.

4. Результаты исследования

С появлением и развитием Интернета вещей и Интернета транспортных средств самой большой проблемой для интеллектуальных транспортных средств в будущем является безопасность. Сравнивая предложенные направления для будущих решений в области безопасности, становится очевидным, что они обычно бывают легкими, быстрыми или

интеллектуальными. Следовательно, они обеспечивают подходящую среду для разработки более гибких и сложных средств защиты с высокой производительностью, отвечающих требованиям безопасности в транспортных средствах.

Наиболее актуальными проблемами, требующими своего разрешения уже сегодня, на наш взгляд, являются: повышение уровня достоверности классификации информационных состояний контролируемых объектов, распознавание уязвимостей на ранних стадиях обнаружения, снижение числа ложных тревог, принятие решений в условиях нестационарной среды и проведения объективной оценки состояния контролируемого источника уязвимостей. Указанные проблемы при оценке информационных ситуаций контролируемых событий во многом обусловлены изменяющимся состоянием сети, отсутствием периодической модификации правил классификации, сложностью реконфигурации системы при введении нового объекта наблюдения и др. Для разрешения указанных проблем, перспективными, на наш взгляд, являются следующие направления обнаружения уязвимостей интерфейсов БТС, базирующиеся на:

- адаптивной интеллектуальной обработке данных (нечеткие системы, экспертные системы, гибридные нейросетевые методы, методы искусственных иммунных систем, вероятностные модели). Данное направление характеризуется достаточно высокой достоверностью обнаружения уязвимостей, а так же возможностью обнаружения неизвестных ранее типов уязвимостей. К недостаткам этих методов следует отнести: потребность в высоких вычислительных мощностях, сравнительно длительное время обнаружения.
- классических методах статистического анализа данных, позволяющих за сравнительно небольшой временной промежуток с заданным уровнем достоверности определить наличие уязвимости, в том числе ранее неизвестного типа или вида. Недостаток: трудно обнаруживаются уязвимости, которые приводят к незначительным, медленным изменениям системных показателей сети.

Применение предлагаемых подходов позволит обеспечить гарантированный уровень ИТ-сервисов, позволяющих эффективно решать научные задачи обнаружения уязвимостей интерфейсов беспилотных транспортных средств.

Работа выполнена при частичной поддержке Российского фонда фундаментальных исследований (гранты № 19-29-06015/19, 19-29-06023/19), а также Правительства Севастополя в рамках научного проекта РФФИ № 20-47-920006.

Литература

1. Зегжда П.Д. Систематизация киберфизических систем и оценка их безопасности / П.Д. Зегжда, М.А. Полтавцева, Д.С. Лаврова // Проблемы информационной безопасности. Компьютерные системы. 2017. № 2 − С. 127-138.
2. Cheah M., Shaikh S. A., Bryans J., and Wooderson P. Building An automotive security assurance case using systematic security evaluations// Computers & Security. vol. 77. 2018. pp. 360–379.
3. Добрынин Д. А. Беспилотные транспортные средства, современное состояние и перспективы//Четырнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2014 (24–27 сентября 2014 г., г. Казань): тр. конф.: в 3 т. -Т. 3. М.: Физматлитгиз, 2014 − с. 265–274.
4. Haas W. and Langjahr P. Cross-domain vehicle control units in modern e/e architectures// 16. Internationales Stuttgarter Symposium. Springer. 2016 − pp. 1619–1627.
5. Hartwich F. et al. Can with flexible data-rate// Proc. iCC. Citeseer. 2012 − pp. 1–9.
6. Consortium F. Flexray communications system protocol specification// Version . 2010. vol. 3.0.1, no. 1– pp.1–341.
7. Obst M., Hobert L., and Reisdorf P. Multi-sensor data fusion for checking plausibility of V2V communications by vision-based multipleobject tracking// Vehicular Networking Conference (VNC), IEEE, 2014 – pp. 143–150.
8. Lindholm E., Nickolls J., Oberman S. Nvidia tesla: A unified graphics and computing architecture// IEEE micro. 2008. vol. 28. no. 2.
9. Guettier C., Bradai B., Hochart F. Standardization of generic architecture for autonomous driving: A reality check// Energy Consumption and Autonomous Driving.Springer. 2016 – pp. 57–68.
10. Johnson D. G. Development of a high resolution mmw radar employing an antenna with combined frequency and mechanical scanning// Radar Conference, RADAR’08. IEEE, 2008 – pp. 1–5.
11. Wang X., Xu L., Sun H., Xin J. Bionic vision inspired on-road obstacle detection and tracking using radar and visual information// Intelligent Transportation Systems (ITSC), 2014, 17th International Conference on. IEEE, 2014 – pp. 39–44.
12. Stavrou E. and Pitsillides A. A survey on secure multipath routing protocols in WSNS// Computer Networks. 2010.vol. 54, no. 13 – pp. 2215–2238.
13. Safi K., Luo S., Wei C., et al. Cloud-based security and privacy-aware information dissemination over ubiquitous vanets// Computer Standards & Interfaces. 2018. vol. 56 – pp. 107–115.
14. Клименко И.С. Обзор беспроводных транспортных сетей Vanet // Современные инновации/ 2018. № 5(27) – с.16-19.

15. Кучерявый Е.А., Винель А.В., Ярцев С.В. Особенности развития и текущие проблемы автомобильных беспроводных сетей VANET // Электросвязь. 2009. № 1 – С. 24-28.
16. Silva F. A., Boukerche A., Silva T. R. Geo-localized content availability in Vanets Ad Hoc Networks. 2016. vol. 36 – pp. 425–434.

References

1. Zegzhda P.D. Systematization of cyberphysical systems and assessment of their safety // P.D. Zegzhda, M.A. Poltavtseva D.S. Lavrova // Problemy informacionnoj bezopasnosti. Komp'yuternye sistemy. 2017. № 2 − pp. 127-138.
2. Cheah M., Shaikh S. A., Bryans J., and Wooderson P. Building An automotive security assurance case using systematic security evaluations// Computers & Security. vol. 77. 2018. pp. 360–379.
3. Dobrynin D.A. Unmanned vehicles, current status and prospects // CHetyrnadcataya nacional'naya konferenciya po iskusstvennomu intellektu s mezhdunarodnym uchastiem KII-2014 (September 24–27, 2014, Kazan) – T.3. M.: Fizmatlitgiz, 2014 − pp. 265–274.
4. Haas W. and Langjahr P. Cross-domain vehicle control units in modern e/e architectures// 16. Internationales Stuttgarter Symposium. Springer. 2016 − pp. 1619–1627.
5. Hartwich F. et al. Can with flexible data-rate// Proc. iCC. Citeseer. 2012 − pp. 1–9.
6. Consortium F. Flexray communications system protocol specification// Version . 2010. vol. 3.0.1, no. 1– pp.1–341.
7. Obst M., Hobert L., and Reisdorf P. Multi-sensor data fusion for checking plausibility of V2V communications by vision-based multipleobject tracking// Vehicular Networking Conference (VNC), IEEE, 2014 – pp. 143–150.
8. Lindholm E., Nickolls J., Oberman S. Nvidia tesla: A unified graphics and computing architecture// IEEE micro. 2008. vol. 28. no. 2.
9. Guettier C., Bradai B., Hochart F. Standardization of generic architecture for autonomous driving: A reality check// Energy Consumption and Autonomous Driving.Springer. 2016 – pp. 57–68.
10. Johnson D. G. Development of a high resolution mmw radar employing an antenna with combined frequency and mechanical scanning// Radar Conference, RADAR’08. IEEE, 2008 – pp. 1–5.
11. Wang X., Xu L., Sun H., Xin J. Bionic vision inspired on-road obstacle detection and tracking using radar and visual information// Intelligent Transportation Systems (ITSC), 2014, 17th International Conference on. IEEE, 2014 – pp. 39–44.
12. Stavrou E. and Pitsillides A. A survey on secure multipath routing protocols in WSNS// Computer Networks. 2010.vol. 54, no. 13 – pp. 2215–2238.

13. Safi K., Luo S., Wei C., et al. Cloud-based security and privacy-aware information dissemination over ubiquitous vanets// Computer Standards & Interfaces. 2018. vol. 56 – pp. 107–115.
14. Klimenko I.S. Overview of Vanet Wireless Transport Networks // Sovremennye innovacii / 2018. No. 5 (27) - p.16-19.
15. Kucheryavy E.A., Vinel A.V., Yartsev S.V. Features of development and current problems of car wireless networks VANET // Elektrosvyaz'. 2009. № 1 – pp. 24-28.
16. Silva F. A., Boukerche A., Silva T. R. Geo-localized content availability in Vanets Ad Hoc Networks. 2016. vol. 36 – pp. 425–434.