ISSN 2225-9309 (Print)
2026. № 2 (36). С. 11–15

Молодежный
Вестник УГАТУ

http://journal.uust.ru

УДК 004.02

doi 10.54708/22259309_2026_23611

СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ ДЛЯ «ПОДКЛЮЧЕННОГО» АВТОМОБИЛЯ

Е. В. КУЗНЕЦОВА[1], А. Ю. СЕНЦОВА[2]

[1] katerinakuznet1@yandex.ru, [2] sentsova.alina@yandex.ru

ФГБОУ ВО «Уфимский университет науки и технологий» (УУНиТ)

Аннотация. Статья посвящена анализу систем обнаружения вторжений (IDS) в контексте V2X (Vehicle-to-everything) технологий, которые обеспечивают взаимодействие транспортных средств с дорожной инфраструктурой. В условиях растущих угроз кибербезопасности вопросы защиты данных и конфиденциальности пользователей становятся очень важными. Также рассматривается роль криптографической инфраструктуры на основе открытых ключей (PKI) в обеспечении информационной безопасности V2X-систем.

Ключевые слова: система обнаружения вторжений; V2X; атаки на транспортные системы.

ВВЕДЕНИЕ

Современные технологии взаимодействия транспортных средств с дорожной инфраструктурой формируют комплексные системы, где вопросы информационной безопасности становятся первостепенными для уменьшения дорожно-транспортных происшествий. Элементом защиты V2X систем выступает криптографическая инфраструктура на основе открытых ключей (PKI) [1]. Несмотря на архитектуру с чётким разграничением функций между центром регистрации (RA) и центром авторизации (AA), система все равно остаётся уязвимой к различным киберугрозам. Это обусловливает потребность в применении систем обнаружения вторжений (Intrusion Detection Systems, IDS), способных выявлять как известные, так и новые формы атак [2]. В статье осуществляется анализ IDS, ориентированных на применение в V2X-среде.

ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ (PKI) В V2X

Системы V2X работают по системе открытых ключей [3]. Функционирование системы PKI представлено на рис. 1.

На этапе производства каждому транспортному средству присваиваются уникальный цифровой идентификатор и первоначальный сертификат, информация о которых хранится в объекте регистрации (Registration Authority, RA). В процессе эксплуатации автомобиль осуществляет запрос на получение долгосрочного сертификата, который в дальнейшем используется для генерации псевдонимов через объект авторизации (Authorization Authority, AA). Сертификаты выдаются с разделением полномочий, что повышает безопасность системы: AA перед выдачей сертификата обязательно запрашивает подтверждение у RA, что обеспечивает дополнительный уровень защиты.

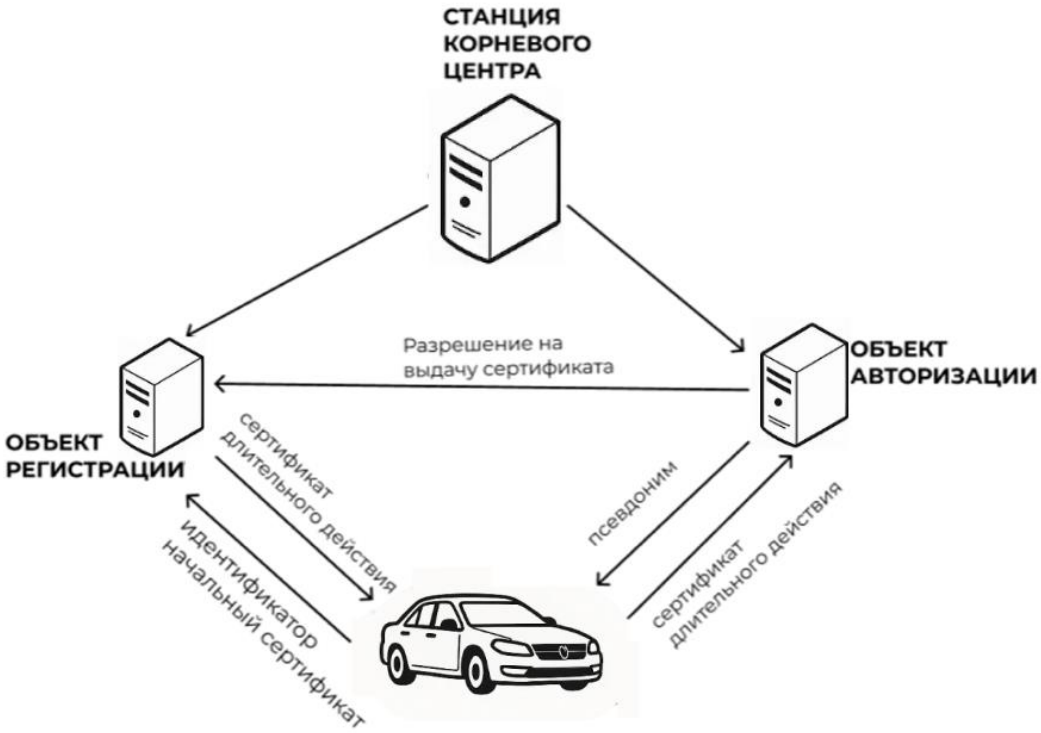

Рис. 1. Функционирование системы PKI

Особенности PKI-модели в V2X:

- RA располагает полной информацией о транспортном средстве, но не имеет доступа к содержанию его сертификатов;
- AA управляет сертификатами, не обладая сведениями об их владельцах, что предотвращает сопоставление с конкретным автомобилем.

Сертификаты обновляются с заданной периодичностью и предназначены для подтверждения подлинности передаваемых данных.

Несмотря на проработанную структуру, V2X-системы подвержены ряду угроз. Актуальные исследования указывают на следующие потенциальные атаки [4]:

1. Отказ в обслуживании (DoS). Целью атаки является выведение из строя системы связи путём перегрузки её фальшивыми запросами или сообщениями. В V2X злоумышленник может, например, непрерывно передавать большое количество сообщений в CAN-сеть (Controller Area Network) или по радиоканалу, что приводит к задержкам в передаче критически важных сообщений, таких как предупреждения о столкновении. В результате нарушается синхронизация между транспортными средствами, и увеличивается риск возникновения аварий.

2. Атака повторного воспроизведения (Replay). Повтор ранее записанных корректных сообщений с целью введения в заблуждение. В контексте V2X злоумышленник может перехватить сообщение о движении автомобиля и воспроизвести его позже, что создаёт иллюзию присутствия транспорта в месте, где его уже нет.

3. Спуфинг (Information Spoofing). Злоумышленник отправляет поддельные сообщения от имени другого транспортного средства или инфраструктурного объекта. В V2X это может выражаться в трансляции ложной информации о скорости, местоположении или направлении движения автомобиля. Например, атака может симулировать аварийную ситуацию впереди, вынуждая другие машины резко тормозить, создавая пробку.

4. Атака Сивиллы (Sybil). Злоумышленник создаёт множество псевдонимов (виртуальных идентификаторов транспортных средств), симулируя присутствие большого количества автомобилей. Это может повлиять на системы управления трафиком, изменяя маршруты других водителей или получая незаконное право приоритетного проезда (например, как у машин скорой помощи).

5. Message Falsification (фальсификация сообщений). Изменение содержимого передаваемого сообщения с целью искажения информации. Примером может быть подделка сообщения о зелёном сигнале светофора в системах V2I (Vehicle-to-Infrastructure), что может привести к тому, что машина пересечет перекресток на запрещающий сигнал светофора.

Все перечисленные атаки подчеркивают необходимость совершенствования механизмов защиты V2X-систем. В частности, внедрение систем обнаружения вторжений.

СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ И ИХ КЛАССИФИКАЦИЯ

Система обнаружения вторжений представляет собой специализированное программное обеспечение или аппаратное решение, основная задача которого – выявление несанкционированной и потенциально опасной активности [5].

Ключевая функциональная обязанность IDS сводится к своевременному выявлению фактов несанкционированного доступа злоумышленников к информационной инфраструктуре с последующей генерацией соответствующих предупреждений. Важно подчеркнуть, что данные системы выполняют исключительно мониторинговые и детектирующие функции, не обладая возможностями активного противодействия (такими как блокировка подозрительных операций).

В современной практике информационной безопасности выделяют два подхода к обнаружению вторжений: системы обнаружения вторжений на основе сигнатур, системы обнаружения вторжений на основе аномалий.

СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ НА ОСНОВЕ СИГНАТУР

Данный подход основан на принципе сравнения анализируемых данных с эталонными образцами известных атак (так называемыми сигнатурами). При обнаружении совпадения с шаблоном вредоносной активности система генерирует соответствующее оповещение. Основное преимущество данного метода заключается в высокой эффективности при выявлении атак, использующих уже изученные и документированные векторы проникновения. Однако ограничением такого подхода является неспособность распознавать новые, ранее неизвестные виды угроз.

В рамках исследования систем V2X в работах [6,–8] предложен специализированный алгоритм обнаружения вторжений для CAN-шин. Методология основана на комплексном анализе двух ключевых параметров:

1. Идентификаторов передаваемых сообщений
2. Характеристик их временного распределения.

Алгоритм функционирует таким образом: при превышении порогового значения числа сообщений определенного типа система генерирует предупреждение.

СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ НА ОСНОВЕ АНОМАЛИЙ

Этот подход предполагает постоянный мониторинг сетевой активности с последующим сопоставлением полученных данных с эталонной моделью нормального функционирования системы. Любые отклонения от установленного шаблона корректного поведения трактуются как потенциальная угроза. Главным достоинством данного метода является возможность выявления новых, ранее не встречавшихся типов атак.

В исследовании [9] предложен метод мониторинга полей сообщений CAN-шины.

Система:

1. Анализирует специальные метки в сообщениях.
2. Сравнивает их с эталонными значениями.
3. Обнаруживает атаки при несоответствии.

В ходе анализа литературы было установлено, что к основным проблемам системы обнаружения вторжений в V2X можно отнести:

1. Ложные срабатывания. В зависимости от ситуации ложные срабатывания даже сами по себе могут быть опасны: предупреждающий звук или мигающий свет фар может напугать или отвлечь водителя. А если ложные срабатывания происходят регулярно, то владелец транспортного средства может отключить IDS и вообще потерять её защиту [10].

2. Необходимость использования качественных наборов данных. Для эффективной работы системы обнаружения вторжений крайне важно иметь качественные наборы данных, на которых система обучается и тестируется. Качественные данные должны содержать разнообразные примеры

как нормального, так и аномального поведения, чтобы IDS могла правильно распознавать угрозы и минимизировать количество ложных срабатываний.

3. Необходимость точного определения аномального поведения.

4. Высокий уровень задержек. Задержки в обработке данных недопустимы в V2X, решения должны приниматься мгновенно (например, для предотвращения аварий).

5. Сложности в оценке эффективности. Тестирование и оценка IDS должны проводиться в условиях, максимально приближенных к реальным.

6. Интеллектуальные атаки. Злоумышленники могут использовать сложные методы, такие как генеративные атаки (GAN). В [11] разработали систему обнаружения вторжений для шины CAN, которая очень хорошо показала себя против стандартного набора атак – «отказ в обслуживании», атака самозванца. Однако когда авторы протестировали IDS против атак, созданных различными моделями машинного обучения, производительность оказалась очень низкой.

ЗАКЛЮЧЕНИЕ

Проведенный анализ систем обнаружения вторжений для V2X-сетей показал, что, несмотря на существующие решения на основе сигнатур и аномалий, остаются ряд нерешенных проблем. Ключевыми являются такие проблемы, как: ложные срабатывания, недостаточное количество качественных наборов данных для обучения, проблемы точного определения аномального поведения в условиях высокой динамики V2X-среды. Кроме того, усложнение методов атак, включая использование генеративных моделей, требует постоянного совершенствования защитных механизмов. Решение этих проблем видится в разработке гибридных систем, сочетающих преимущества обоих подходов разработки IDS, создании специализированных тестовых сред, максимально приближенных к реальным условиям, и внедрении адаптивных алгоритмов, устойчивых к интеллектуальным атакам.

СПИСОК ЛИТЕРАТУРЫ

1. **Qiu H., Qiu M., Lu R.** Secure V2X communication network based on intelligent PKI and edge computing //IEEE Network. – 2019. – Т. 34. – №. 2. – С. 172-178.

2. **Sedjelmaci, H., Senouci, S.-M., Ansari, N., Boualouache, A.** A trusted hybrid learning approach to secure edge computing // IEEE Consum. Electron. Mag. – (2021) – 11 (3). – Pp. 30–37.

3. **Haidar, F., Kaiser, A. and Lonc, B**. On the Performance Evaluation of Vehicular PKI Protocol for V2X Communications Security. 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), Toronto, ON, Canada – 2017.

4. **Petho, Z., Kazar, T. M., Szalay, Z. and Torok, A.** Quantifying Cyber Risks: The Impact of DoS Attacks on Vehicle Safety in V2X Networks // IEEE Transactions on Intelligent Transportation Systems. – Vol. 25. – No. 11. – Pp. 18591–18600, Nov.

5. **Глущенко М. В., Ширяев А. А., Глушенко С. А.** IDS/IPS-системы обнаружения и предотвращения вторжений //КОНЦЕПЦИЯ" ОБЩЕСТВА ЗНАНИЙ" в СОВРЕМЕННОЙ НАУКЕ: сборник статей по итогам Международной научно-практической конференции, Стерлитамак. – 2019. – Т. 18. – С. 115-117.

6. **Ajibuwa O., Hamdaoui B., Yavuz A. A**. AI/ML-Driven Intrusion and Misbehavior Detection in Networked Autonomous Systems: A Survey of Common Practices. – 2023

7. **Ling, C. and Feng, D.** An algorithm for detection of malicious messages on can buses // Proc. Nat. Conf. Inf. Technol. Comput. Sci. Paris, France: Atlantis Press. – 2012.

8. **Avatefipour**, **O.** Physical-fingerprinting of electronic control unit (ECU) based on machine learning algorithm for in-vehicle network communication protocol CAN-BUS' M.S. thesis, Dept. Comput. Eng., Univ. Michigan-Dearborn, Dearborn, MI, USA – 2017.

9. **Abbott-Mc Cune, S. and Shay, L. A.** Intrusion prevention system of automotive network CAN bus // Proc. IEEE Int. Carnahan Conf. Security Technol. (ICCST) – Oct. – 2016 – Pp. 1–8**.**

10. **Taylor, A., Japkowicz, N. and Leblanc**, **S.** Frequency-based anomaly detection for the automotive CAN bus // Proc. World Congr. Ind. Control Syst. Security (WCICSS. –, 2016 – Pp. 45–49.

11. **Aliyu, I., Engelenburg, S. V., Mu'azu, M. B. J., Kim, and Lim**, **C. G.** Statistical detection of adversarial examples in blockchain-based federated forest in-vehicle network intrusion detection systems» // IEEE Access. – 2022. – Vol. 10 – Pp. 2169–3536.

ОБ АВТОРАХ

КУЗНЕЦОВА Екатерина Васильевна, студентка каф. ВТиЗИ.

СЕНЦОВА Алина Юрьевна, канд. тех. наук, доцент каф. ВТиЗИ.

METADATA

Title: Intrusion detection system for the connected car

Author: E. V. Kuznetsova[1], A. U. Sentsova[2]

Affiliation:

[1,2] Ufa University of Science and Technology (UUST), Russia.

Email: [1] katerinakuznet1@yandex.ru, [2] sentsova.alina@yandex.ru

Language: Russian.

Source: Molodezhnyj Vestnik UGATU (scientific journal of Ufa University of Science and Technology), no. 2 (36), pp. 11-16, 2026. ISSN 2225-9309 (Print).

Abstract: The paper is devoted to the analysis of intrusion detection systems (IDS) in the context of V2X (Vehicle-to-everything) technologies that ensure the interaction of vehicles with road infrastructure. In the context of growing cyber security threats, issues of data protection and user privacy are becoming critically important. The role of cryptographic infrastructure based on public keys (PKI) in ensuring information security of V2X systems is considered.

Key words: Intrusion detection system, V2X, attacks on transport systems.

About authors:

KUZNETSOVA Ekaterina Vasilevna, student, Dept. of COMPUTER ENGINEERING AND INFORMATION SECURITY (UUST).

SENTSOVA Alina Yurievna, docent, Dept. of COMPUTER ENGINEERING AND INFORMATION SECURITY (UUST)).