ISSN 2658-5014 (Print)
2020. Т. 2, № 2 (4). С. 36–42
СИИТ
СИСТЕМНАЯ ИНЖЕНЕРИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
ISSN 2686-7044 (Online)
http://siit.ugatu.su

УДК 004.056

ВОПРОСЫ БЕЗОПАСНОСТИ СЕРВИСОВ В САМООРГАНИЗУЮЩИХСЯ СЕТЯХ ИНТЕЛЛЕКТУАЛЬНОЙ ТРАНСПОРТНОЙ СИСТЕМЫ VANET

Л. В. ЛЕГАШЕВ[1], Д. И. ПАРФЕНОВ[2], И. П. БОЛОДУРИНА[3], Ю. А. УШАКОВ[4]

[1] silentgir@gmail.com, [2]parfenovdi@mail.ru, [3]ipbolodurina@yandex.ru , [4]unpk@mail.ru

ФГБОУ ВО «Оренбургский государственный университет» (ОГУ)

Поступила в редакцию 16 октября 2020 г.

Аннотация. Разработка алгоритмов обеспечения сетевой безопасности в автомобильных самоорганизующихся сетях VANET с целью реализации интеллектуальной транспортной навигации, безусловно, имеет приоритетное значение. В работе проводится обзор существующих сетевых угроз VANET и криптографических алгоритмов аутентификации. Рассматриваются утилиты для работы с захваченным трафиком и популярные среды моделирования транспортных сетей. Формализуются основные элементы VANET, типы связей, уровни доверия, а также приводится схема взаимодействия юнитов VANET с точки зрения обнаружения сетевых угроз.

Ключевые слова: Автомобильные самоорганизующиеся сети; Интернет вещей; сетевые атаки; сетевая безопасность; симуляторы сетей; виртуализация сетевых функций.

ВВЕДЕНИЕ

Развитие парадигмы Интернета вещей (Internet of Things, IoT) приводит к появлению все большего количества умных мобильных устройств, передающих данные по беспроводным сетям. Одним из развивающихся направлений современных научных исследований являются самоорганизующиеся сети интеллектуальной транспортной системы (Vehicular ad hoc networks, VANETs), объединяющие «умные» транспортные устройства в единую сеть с целью обеспечения безопасности дорожного движения, ассистирования водителям, интеллектуальной навигации транспортных средств, распространения оповещений и предупреждений о ситуации на дорогах. Как и любые другие сетевые устройства, элементы системы VANET подвержены сетевым атакам различного рода, в связи с чем возникает потребность в разработке алгоритмов защиты информации в VANET.

ОБЗОР ИССЛЕДОВАНИЙ БЕЗОПАСНОСТИ В VANET

В рамках публикации [1] рассматриваются вопросы безопасности программно-конфигурируемых VANET сетей. Отмечая постоянный прогресс в технологиях VANET сетей, авторы выделяют основные сервисы: транспортные облачные вычисления, наблюдение, реклама на основе Интернета вещей, управление безопасности трафика и др. Акцентируется внимание на новых уязвимостях в отношении безопасности и конфиденциальности, которые возникают из-за сочетания VANET сетей и новых технологий, таких как программно-конфигурируемые сети, виртуализация сетевых функций и мобильные граничные вычисления.

Авторы статьи [2] исследуют VANET сети на предмет атак с ухудшением качества обслуживания (degradation-of-QoS attack), основная идея которых состоит в генерации фиктивных подключений и последующем исчерпании ресурсов придорожных юнитов RSU (roadside units). В качестве решения проблемы предлагается идея но-

Работа поддержана грантом РФФИ 20-57-53019 ГФЕН_а.

вого межуровневого протокола устойчивой к ретрансляции аутентификации на основе метода ограничения расстояний.

Метод на основе оптимизации муравьиной колонии используется в работе [3] для обнаружения наиболее оптимальных маршрутов передачи пакетов в VANET сетях, принимая во внимание особенности таких сетей – частые отключения, быстрая смена топологии сети и др. Представленное решение показывает эффективность для загруженной транспортной сети с большим количеством автомобилей.

Исследователи Y. Zheng, J. Luo и T. Zhong в статье [4] рассматривают вопросы безопасности сервисов на основе определения местоположения транспортного средства (location-based services, LBS). Авторы предлагают динамически регулируемый алгоритм анонимной группы соседних k транспортных средств и алгоритм защиты конфиденциальности местоположения на основе фиктивного местоположения транспорта в VANET сети. Как отмечается в публикации [5], большое количество избыточных или бесполезных сообщений LBS сервисов, распространяемых в VANET сетях, приводит к значительным накладным расходам на процесс аутентификации. Авторами предлагается упрощенный протокол LPPA аутентификации с сохранением конфиденциальности путем исключения дублирующих и бесполезных зашифрованных сообщений LBS сервисов перед выполнением аутентификации. В рамках статьи [6] также рассматриваются возможные пути решения проблемы раскрытия траектории движения транспортного средства с помощью LBS сервисов. Представленный механизм дифференциальной конфиденциальности на основе обучения с подкреплением случайным образом задает местоположение свободного транспортного средства с целью защиты семантической траектории транспортного средства.

Криптография на эллиптических кривых используется в работе [7] для обеспечения требований безопасности в роуминговых сервисах VANET сетей. Как отмечают авторы исследования, анонимность идентификатора каждого транспортного средства реализуется с помощью операции XOR, а отслеживаемость транспортного средства достигается посредством встраивания открытого ключа локального сервисного агента в псевдоним. В статье [8] оценивается влияние аутентификации с применением алгоритмов на эллиптических кривых в рамках плоскости управления многопереходной маршрутизацией (multihop routing) для реальной VANET сети. Авторы отмечают возможность существенного негативного влияния на службу маршрутизации тестируемой VANET сети при отсутствии высокопроизводительных вычислительных устройств.

Публикация [9] посвящена исследованию протоколов аутентификации между транспортным средством и инфраструктурой V2I (Vehicle-to-Infrastructure) и между двумя транспортными средствами V2V (Vehicle-to-Vehicle) для защиты информации от следующих сетевых атак: атака повторного воспроизведения, маскарадинг и «человек посередине». Для доказательства безопасности представленных протоколов обмена ключами используется криптографическая модель случайного оракула. В работе [10] описана схема аутентификации V2I на основе масштабируемых вычислений с поддержкой технологии блокчейна, которая обеспечивает быструю повторную аутентификацию транспортных средств посредством безопасной передачи прав собственности между инфраструктурами в сети VANET.

Авторы исследования [11] предлагают новый сетевой уровень VANET-Cloud с целью оптимального управления трафиком и повышения производительности VANET сети в условиях перегруженности. В работе используется механизм обмена данными для распространения предсказанных данных с использованием метода нечеткого агрегирования, сбор трафика осуществляется с помощью беспроводной сенсорной сети (connected sensor network, CSN).

Наши коллеги из Аньхойского университета активно занимаются изучением вопросов обеспечения безопасности и предотвращения сетевых атак в VANET. В первую очередь они фокусируют внимание на DDoS атаках, которые отлично распознаются существующими методами машинного обучения. В рамках работы [12] авторы предлагают новую схему анонимной аутентификации на основе идентификации для решения проблемы компрометации главного ключа и отзыва транспортного средства. В работе доказано, что безопасность предложенной схемы аналогична предположению о сложности дискретного логарифма над эллиптическими кривыми. В публикации [13] представлен новый подход к протоколу согласования группового ключа (Group Key Agreement, GKA), позволяющего группе участников установить открытый ключ сеанса для безопасного канала связи в рамках небезопасной сети VANET. Предложенная схема основана на алгоритме хаотических отображений в форме полиномов Чебышева. Статья [14] описывает безопасную схему взаимной аутентификации двух транспортных средств внутри сети VANET с сохранением конфиденциальности для

решения проблем, связанных с огромными вычислительными и коммуникационными издержками. Большинство программ мониторинга и тестирования сети используют библиотеку Pcap для захвата сетевых пакетов и возможности их последующей обработки. Существует множество утилит для работы с файлами в формате pcap с целью выделения ключевых особенностей трафика и подготовки датасета в .csv формате. Программа CICFlowmeter-V4.0 [15] представляет собой генератор сетевого трафика и анализатор для обнаружения атак в датасетах, как CICAAGM2017, CICIDS2017, CICAndMal2017 и CIC-DDoS2019. Утилита Wonka Flows Exporter [16] используется для экспорта pcap файлов с TCP-трафиком и последующим выводом в WEKA или CSV файл. Основные извлекаемые признаки: дельта между временем прибытия пакета; соотношение между переданными байтами/количеством пакетов; соотношение push-флаг/общее количество флагов. Утилита Pcap Features Extraction [17] имеет схожий функционал с предыдущей программой и позволяет выделять 26 признаков из pcap файла, включая время от первого пакета до последнего пакета в окне пакетов; среднюю дельту в окне пакетов; среднюю длину пакета; среднее значение пакета с небольшой полезной нагрузкой и др.

Для генерации аутентичного VANET трафика исследователи используют различные сетевые симуляторы. Наиболее известным является SUMO [18] – пакет моделирования автомобильного трафика с открытым исходным кодом, предназначенный для работы в больших сетях. Чаще всего симулятор дорожного трафика SUMO используется в связке со средой моделирования сетевого трафика OMNeT++ [19]. Особую популярность приобрел фреймворк Veins [20] для моделирования автомобильных самоорганизующихся сетей. В публикации [21] описан симулятор VENTOS на базе SUMO и OMNeT++. Представленное решение включает в себя возможности интеллектуального менеджмента трафика, совместное вождение и динамическое вождение. В работе [22] представлена среда моделирования VANET на базе системы дискретных событий MATLAB (DES) в наборе инструментов SimEvents.

ФОРМАЛИЗАЦИЯ ЭЛЕМЕНТОВ СИСТЕМЫ VANET

Наиболее критическим с точки зрения безопасности VANET является сетевое взаимодействие.

Представим ниже основные угрозы, возникающие в VANET:

1. Multiple-identity attack – вид сетевой атаки, при котором злоумышленник создает большое количество псевдонимных идентификаторов и использует их для получения информации с устройств в сети;

2. Impersonation Attack – вид сетевой атаки, при котором злоумышленник представляется доверенным узлом/устройством в сети;

3. Black hole attack – сетевая атака вида «отказ в обслуживании», при которой маршрутизатор вместо ретрансляции пакетов сбрасывает их;

4. Gray hole attack – вид сетевой атаки, при котором происходит выборочный сброс пакетов с целью повреждения передаваемой по сети информации;

5. Wormhole attack – вид сетевой атаки, при котором злоумышленник занимает стратегически выгодную позицию в сети и препятствует правильному выстраиванию маршрутов между узлами в процессе маршрутизации;

6. Alteration attack – вид сетевой атаки, при котором злоумышленник передает скомпрометированную информацию, изменяя маршрутизацию сообщений в сети.

7. Denial-of-Service and Distributed Denial-of-Service attacks – вид сетевых атак, забивающих канал связи, очереди на маршрутизаторах с целью исчерпания доступных сетевых ресурсов.

8. Radio Channel attack – вид сетевых атак на беспроводную сенсорную сеть, при которых бортовые устройства транспортных средств не смогут подключиться к остальным элементам VANET сети.

9. Reconnaissance attack – вид сетевой атаки, при которой происходит рекогносцировка сетевых устройств/топологии сети, перехват пакетов, сканирование портов, фишинг и т.д.

Большинство перечисленных выше сетевых атак по отношению к самоорганизующимся автомобильным сетям приводят к выводу из строя сети и невозможности нормального ее-функционирования.

Методы машинного обучения могут быть использованы при разработке модели обнаружения аномалий трафика в сети передачи данных VANET. Алгоритм обнаружения аномалий будет включать в себя следующие основные операции:

1. Выбор ключевых признаков на основе сырых данных – обработка pcap файлов и формирование датасета в формате CSV.

2. Подбор оптимальных гиперпараметров.

3. Обучение сети на известных датасетах, содержащих основные типы сетевых атак.

4. Тестирование обученной сети на реальном трафике VANET, который будет собран на основе одного из существующих симуляторов – оперативного обнаружения сетевой атаки, либо другой формы злонамеренной активности и принятия решения по блокировке, оповещению или ограничению каналов связи.

При разработке модели обнаружения аномалий трафика в VANET будет учитываться необходимость максимально снизить вычислительные издержки. Для построения такой модели необходимо формализовать функционирование автомобильной самоорганизующейся сети, а также построить классификатор сетевых угроз и задать функцию маркировки элементов VANET с точки зрения уровня доверия [1].

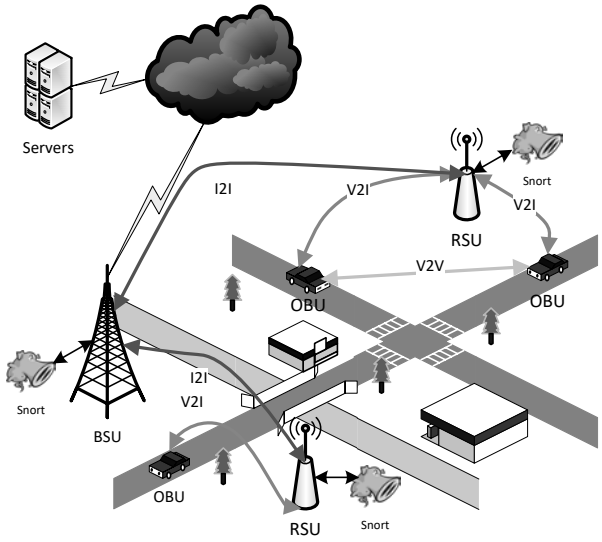

Рис. 1. Архитектура автомобильной самоорганизующейся сети

Формализуем основные элементы в сети VANET:

1. Бортовое устройство, OBU (Onboard Unit) – устройство, размещаемое на транспортном средстве и передающее данные о местоположении, скорости, ускорении, удерживанию дистанции, смене полос движения и обгонах транспортного средства;

2. Придорожное устройство, RSU (Roadside Unit) – функциональные узлы, размещаемые в определенных точках дорожного полотна для организации передачи информации о текущей ситуации в режиме реального времени;

3. Базовая станция, BSU (Base Station Unit) устройство для трансляции и сбора информации о транспортных средствах в режиме реального времени;

4. Анализатор трафика Snort – программное обеспечение, используемое для анализа сетевых пакетов.

5. Облако с развернутыми сервисами.

Также формализуем типы связей в сети VANET:

- Vehicle-to-Vehicle (V2V) – обмен данными осуществляется между легитимными транспортными средствами;
- Vehicle-to-Infrastructure (V2I) – обмен данными осуществляется между транспортным средством и инфраструктурным элементом (придорожным юнитом, базовой станцией и т.д.);
- Infrastructure-to-Infrastructure (I2I) – обмен данными осуществляется между инфраструктурными элементами; Формализуем элементы транспортной инфраструктуры системы VANET с точки зрения уровня доверия. Выделим три основных категории:
- Доверенные элементы (Trusted Units) (v_1) – сетевой трафик не был скомпрометирован или подменен, остальные юниты сети VANET могут доверять получаемым с транспортного средства данным;
- Недоверенные элементы (Untrusted Units) (v_2) – сетевой трафик был скомпрометирован или подменён в результате сетевой атаки, все входящие пакеты трафика, полученные с транспортного средства остальными юнитами сети VANET, маркируются зловредными, и пересылка прекращается;
- Частично доверенные элементы (Partially Trusted Units) (v_3) – известно, что часть передаваемых данных с транспортного средства была скомпрометирована или подменена (также, возможно, вышел из строя один или несколько датчиков бортового устройства), можно доверять оставшимся сетевым пакетам, получаемым с транспортного средства. Кроме того, устройство RSU или OBU может быть отнесено к данной категории, если через данный элемент проходят потоки трафика с недоверенных устройств без соответствующей реакции (блокировки трафика).

Схема взаимодействия юнитов системы VANET с точки зрения обнаружения сетевых угроз представлена на рис. 2.

Построим классификатор сетевых угроз в виде целевой функции $f(Z)\colon Z \to K$, присваивающей каждому потоку трафика z_i в анализируемой сети из множества всех сетевых потоков $Z = \{z_1, \dots, z_n\}$, где n – общее количество сетевых потоков, метку $k_j \in K$, соответствующую одному из видов атак, характерных для VANET.

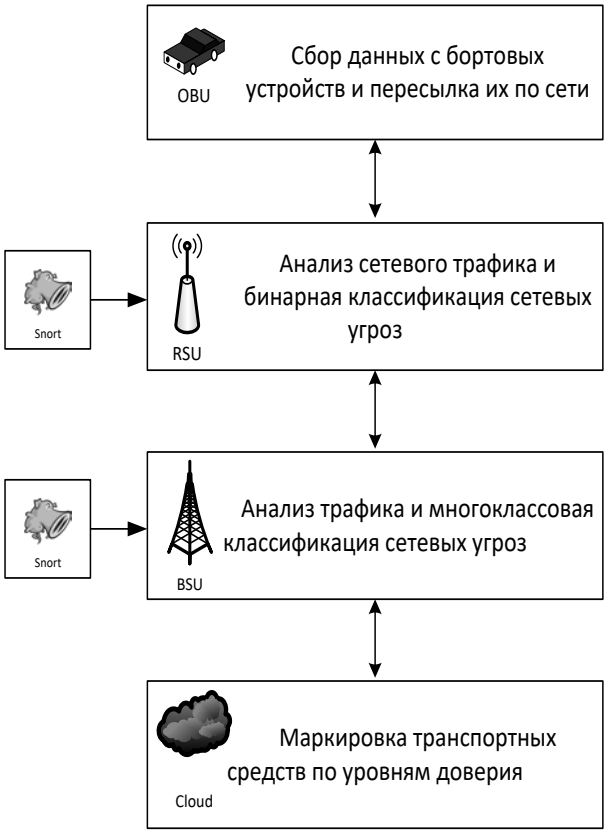

Рис. 2. Схема взаимодействия юнитов VANET с точки зрения обнаружения сетевых угроз.

На основе полученных данных определим метки классов, задействованных в анализируемых потоках транспортных средств в VANET, с точки зрения уровня доверия в виде следующей функции маркировки: $g(K): K \to V$, где $V = \{v_1, v_2, v_3\}$ – множество уровней доверия элементов системы VANET.

ЗАКЛЮЧЕНИЕ

В дальнейшем в рамках текущего исследования планируется разработать схему анализа потоков трафика и взаимодействия NFV (Network Functions Virtualization) сервисов системы безопасности; алгоритмы бинарной классификации трафика в плане наличия угроз; алгоритмы классификации по конкретным угрозам и конкретным сервисам; правила реагирования на инциденты безопасности транспортными средствами при обнаружении атак и расстановка уровня доверия к данным от соседних устройств на основе коллаборативной фильтрации.

Авторы выражают благодарность коллегам из Аньхойского университета, а также руководителю отдела информационной безопасности профессору Jie Cui за плодотворное научное сотрудничество.

СПИСОК ЛИТЕРАТУРЫ

1. **Jaballah W. B., Conti M., Lal C.** A survey on software-defined VANETs: benefits, challenges, and future directions // arXiv preprint arXiv:1904.04577. 2019. P. 1–17. [W. B. Jaballah, M. Conti, C. Lal, “A survey on software-defined VANETs: benefits, challenges, and future directions”, in *arXiv preprint arXiv:1904.04577,* 2019, pp .1-17.]

2. **Yang A.** et al. Deqos attack: Degrading quality of service in Vanets and its mitigation // IEEE Transactions on Vehicular Technology. 2019. – V. 68. – №. 5. – P. 4834–4845. [A. Yang “Deqos attack: Degrading quality of service in Vanets and its mitigation” in *IEEE Transactions on Vehicular Technology*. 2019, vol. 68, № 5, pp. 4834-4845.]

3. **Srivastava A., Prakash A., Tripathi R.** Quality-of-Service based Reliable Route Discovery using Ant Colony Optimization for VANET // 2019 IEEE Conference on Information and Communication Technology. – IEEE, 2019. – P. 1–6. [A. Srivastava, A. Prakash, R. Tripathi **“**Quality-of-Service based Reliable Route Discovery using Ant Colony Optimization for VANET” in *IEEE Conference on Information and Communication Technology*, 2019, pp. 1-6.]

4. **Zheng Y., Luo J., Zhong T.** Service recommendation middleware based on location privacy protection in VANET // IEEE Access. – 2020. – Vol. 8. – P. 12768–12783. [Y. Zheng, J. Luo, T. Zhong **“**Service recommendation middleware based on location privacy protection in VANET” in *IEEE Access*. 2020, vol. 8, pp. 12768-12783.]

5. **Zhou J.** et al. LPPA: Lightweight Privacy-Preserving Authentication From Efficient Multi-Key Secure Outsourced Computation for Location-Based Services in VANETs // IEEE Transactions on Information Forensics and Security. – 2019. – Vol. 15. P. 420–434. [J. Zhou **“**LPPA: Lightweight Privacy-Preserving Authentication From Efficient Multi-Key Secure Outsourced Computation for Location-Based Services in VANETs” in *IEEE Transactions on Information Forensics and Security*. 2019, vol. 15, pp. 420-434.]

6. **Wang W.** et al. Protecting Semantic Trajectory Privacy for VANET with Reinforcement Learning // ICC 2019-2019 IEEE International Conference on Communications (ICC). – IEEE, 2019. P. 1–5. [W. Wang “Protecting Semantic Trajectory Privacy for VANET with Reinforcement Learning” in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE, 2019, pp. 1-5.]

7. **Zhou Y.** et al. Conditional privacy-preserving authentication and key agreement scheme for roaming services in VANETs // Journal of Information Security and Applications. – 2019. – Vol. 47. – P. 295–301. [Y. Zhou “Conditional privacy-preserving authentication and key agreement scheme for roaming services in VANETs” in *Journal of Information Security and Applications*. 2019, vol. 47, pp. 295-301.]

8. **Cirne P.** et al. The impact of ECDSA in a VANET routing service: Insights from real data traces // Ad Hoc Networks. – 2019. – Vol. 90. – P. 101747. [P. Cirne **“**The impact of ECDSA in a VANET routing service: Insights from real data traces” in *Ad Hoc Networks*. 2019, vol. 90, pp. 101747.]

9. **Palaniswamy B.** et al. Continuous authentication for VANET // Vehicular Communications. – 2020. – P. 100255. [B. Palaniswamy “Continuous authentication for VANET” in *Vehicular Communications*. 2020, pp. 100255.]

10. **Wang C.** et al. B-TSCA: Blockchain assisted Trustworthiness Scalable Computation for V2I Authentication in VANETs // IEEE Transactions on Emerging Topics in Computing. – 2020. [C. Wang **"**B-TSCA: Blockchain assisted Trustworthiness Scalable Computation for V2I Authentication in VANETs" in *IEEE Transactions on Emerging Topics in Computing*. 2020.]

11. **Abdelatif S.** et al. VANET: A novel service for predicting and disseminating vehicle traffic information // International Journal of Communication Systems. – 2020. – Vol. 33. – № 6. – P. e4288. [S. Abdelatif "VANET: A novel service for predicting and disseminating vehicle traffic information" in *International Journal of Communication Systems*. 2020, vol. 33, № 6, pp. e4288.]

12. **Wang Y.** et al. Enhanced Security Identity-Based Privacy-Preserving Authentication Scheme Supporting Revocation for VANETs // IEEE Systems Journal. – 2020. [Y. Wang "Enhanced Security Identity-Based Privacy-Preserving Authentication Scheme Supporting Revocation for VANETs" in *IEEE Systems Journal*. 2020.]

13. **Cui J.** et al. Full Session Key Agreement Scheme Based on Chaotic Map in Vehicular Ad hoc Networks // IEEE Transactions on Vehicular Technology. – 2020. [J. Cui **"**Full Session Key Agreement Scheme Based on Chaotic Map in Vehicular Ad hoc Networks" in *IEEE Transactions on Vehicular Technology*. 2020.]

14. **Cui J.** et al. Secure mutual authentication with privacy preservation in vehicular ad hoc networks // Vehicular Communications. – 2020. – Vol. 21. – P. 100200. [J. Cui "Secure mutual authentication with privacy preservation in vehicular ad hoc networks" in *Vehicular Communications*. 2020, Vol. 21, pp. 100200.]

15. CICFlowMeter [Электронный ресурс] URL: https://github.com/CanadianInstituteForCybersecurity/CICFlowMeter (дата обращения 20.08.2020). [CICFlowMeter (2020, Aug. 20) [Online]. Available: https://github.com/CanadianInstituteForCybersecurity/CICFlowMeter]

16. flows_to_weka [Электронный ресурс] URL: https://github.com/fichtner/flows_to_weka (дата обращения 20.08.2020). [flows_to_weka (2020, Aug. 20) [Online]. Available: https://github.com/fichtner/flows_to_weka]

17. Pcap_Features_Extraction [Электронный ресурс] URL: https://github.com/lucadivit/Pcap_Features_Extraction (дата обращения 20.08.2020). [Pcap_Features_Extraction (2020, Aug. 20) [Online]. Available: https://github.com/lucadivit/Pcap_Features_Extraction]

18. Simulation of Urban Mobility [Электронный ресурс] URL: https://www.eclipse.org/sumo/ (дата обращения 20.08.2020). [Simulation of Urban Mobility (2020, Aug. 20) [Online]. Available: https://www.eclipse.org/sumo/]

19. OMNeT++ Discrete Event Simulator [Электронный ресурс] URL: https://omnetpp.org/ (дата обращения 20.08.2020). [OMNeT++ Discrete Event Simulator (2020, Aug. 20) [Online]. Available: https://omnetpp.org/]

20. Veins: The open source vehicular network simulation framework. [Электронный ресурс] URL: https://veins.car2x.org/ (дата обращения 20.08.2020). [Veins: The open source vehicular network simulation framework. (2020, Aug. 20) [Online]. Available: https://veins.car2x.org/]

21. **Amoozadeh M.** et al. VENTOS: Vehicular network open simulator with hardware-in-the-loop support // Procedia Computer Science. – 2019. – Vol. 151. – P. 61–68. [M. Amoozadeh **"**VENTOS: Vehicular network open simulator with hardware-in-the-loop support" in *Procedia Computer Science*. 2019, vol. 151, pp. 61-68.]

22. **Wang L., Iida R., Wyglinski A. M.** Vehicular network simulation environment via discrete event system modeling // IEEE Access. – 2019. – Vol. 7. – P. 87246–87264. [L. Wang, R. Iida, A. M. Wyglinski **"**Vehicular network simulation environment via discrete event system modeling" in *IEEE Access*. 2019, vol. 7, pp. 87246-87264.]

ОБ АВТОРАХ

ЛЕГАШЕВ Леонид Вячеславович, начальник отдела дист. техн. К-т техн. наук по мат. и прог. обеспеч. (УГАТУ, 2019) Иссл. в обл. облачных вычислений, эволюционных алгоритмов оптимизации.

ПАРФЕНОВ Денис Игоревич, доцент каф прикладной математики. К-т техн. наук по сист. и сетям (ПГУТИ, 2014) Иссл. в обл. математического моделирования, архитектуры высоконагруженных вычислительных систем.

БОЛОДУРИНА Ирина Павловна, заведующий каф. прикладной математики. Д-р техн. наук по упр. в соц. и эк. сист. (ЮУрГУ, 2004) Иссл. в обл. теории оптимального управления, математического моделирования.

УШАКОВ Юрий Александрович, доцент каф геометрии и компьютерных наук. К-т техн. наук по тел.ком. сист. и комп. сетям (ПГУТИ, 2009) Иссл. в обл. программно-конфигурируемых сетей, телекоммуникаций.

METADATA

Title: Issues of security of services in vehicular adhoc networks of intelligent transportation system.

Authors: L. V. Legashev [1], D. I. Parfenov[2], I. P. Bolodurina [3], Yu. A. Ushakov[4]

Affiliation:

Orenburg State University (OSU), Russia.

Email:[1]silentgir@gmail.com,[2]parfenovdi@mail.ru, [3]ipbolodurina@yandex.ru, [4]unpk@mail.ru.

Language: Russian.

Source: SIIT, no. 2 (4), pp. 36-42, 2020. ISSN 2686-7044 (Online), ISSN 2658-5014 (Print).

Abstract: The development of algorithms for ensuring network security in vehicular adhoc networks in order to implement intelligent transport navigation is certainly a priority. The paper reviews the existing VANET network threats and cryptographic authentication algorithms. Utilities for working with captured traffic and simulators for modeling transport networks are considered. The main elements of the VANET, the types of connections, the levels of trust of vehicles are formalized, and a diagram of the interaction of the units of the VANET from the point of view of detecting network threats is given.

Key words: Vehicular adhoc networks; Internet of Things; network attacks; network security; network simulators; network function virtualization.

About authors:

LEGASHEV, Leonid Vyacheslavovich, head of distance learning department. Cand. of Tech. Sci. (USATU, 2019).

PARFENOV, Denis Igorevich, associate professor of applied mathematics department. Cand. of Tech. Sci. (PSUTI, 2014).

BOLODURINA, Irina Pavlovna, head of applied mathematics department. Dr. of Tech. Sci. (SUSU, 2004).
USHAKOV, Yuri Alexandrovich, associate professor of geometry and computer science department. Cand. of Tech. Sci. (PSUTI, 2009).