7. Kleinrock L. *Queuing theory*. Ed by V.I. Neimona. Transl. From English. Moscow: Mashinostroeinie, 1979, 432 p. (In Russ.)
8. Do T.V., Chakka R., Sztrik J. Spectral expansion solution methodology for QBD-M processes and applications in future internet engineering. *Studies in Computational Intelligence*, 2016, vol. 479, pp. 131–142. DOI: 10.1007/978-3-319-00293-4-11
9. Ma X.A. et al. Spectral method for two-dimensional ocean acoustic propagation. *Journal of Marine Science and Engineering*, 2021, no. 9, pp. 1–19. DOI: https://doi.org/ 10.3390/jmse9080892
10. Aliev T.I. *Fundamentals of discrete system modeling*. Saint Petesburgs: SPbGU ITMO, 2009, 363 p. (In Russ.)
11. Aliev T.I. Approximation of probability distributions in queueing models. *Nauchno-tekhnicheskij vestnik informacionnyh tekhnologij, mekhaniki i optiki*, 2013, vol. 84, no. 2, pp. 88–93. (In Russ.)
12. Myskja A. An improved heuristic approximation for the GI/GI/1 queue with bursty arrivals. *Teletraffic and datatraffic in a Period of Change: ITC-13*. Elsevier Science Publishers, 1991. pp. 683–688.
13. Whitt W. Approximating a point process by a renewal process: two basic methods. *Operation Research*, 1982, vol. 30, no. 1, pp. 125–147.
14. Gromoll H.C., Terwilliger B., Zwart B. Heavy traffic limit for a tandem queue with identical service times. *Queueing Systems*, 2018, vol. 89, no. 3, pp. 213–241.
15. Jacobovic R., Kella O. Asymptotic independence of regenerative processes with a special dependence structure. *Queueing Systems*, 2019, vol. 93, pp. 139–152. DOI: 10.1007/s11134-019-09606-1
16. Wang L., Kulkarni V. Fluid and diffusion models for a system of taxis and customers with delayed matching. *Queueing Systems*, 2020, vol. 96, pp. 101–131. DOI: 10.1007/s11134-020-09659-7
17. Legros B. M/G/1 queue with event-dependent arrival rates. *Queueing Systems*, 2018, vol. 89, no. 3, pp. 269–301.
18. Tarasov V.N., Bahareva N.F. Simulation model of a QS with hyperexponential distribution in the GPSS WORLD environment. *Infokommunikacionnye tekhnologii*, 2022, vol. 20, no. 4, pp. 7–13. (In Russ.)

Received 20.03.2024

СЕТИ СВЯЗИ И МУЛЬТИСЕРВИСНЫЕ УСЛУГИ

УДК 004.852

ВЫЯВЛЕНИЕ АНОМАЛИЙ ТРАФИКА В БОРТОВОЙ СЕТИ АВТОМОБИЛЯ С ПОМОЩЬЮ РЕКУРРЕНТНОЙ LSTM НЕЙРОСЕТИ

Трошин А.В.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: a.v.troshin77@yandex.ru

В современных автомобилях высокого уровня применяется множество электронных блоков контроля и управления, повышающих удобство вождения и собирающих большие объемы информации о работе различных узлов. В значительной части такого автотранспорта для обмена сообщениями между электронными блоками применяется сеть контроллеров - надежное и простое решение, которое, однако, не обеспечивает никаких средств защиты передаваемых данных. Проблема уязвимости сети контроллеров все более обостряется по мере того, как возрастает обмен данными между автомобилями, дорожной инфраструктурой и Интернетом. Трафик атак на сеть контроллеров можно рассматривать как аномальный по отношению к легитимным сообщениям, что позволяет использовать для их обнаружения различного рода методы обнаружения аномалий. В данной работе рассматривается способ выявления аномалий трафика на базе рекуррентной нейросети с ячейками долгой краткосрочной памяти, спроектированной по архитектуре энкодер-декодер.

Ключевые слова: *сеть контроллеров, обнаружение аномалий, обучение без учителя, кибербезопасность, рекуррентная нейросеть*

Введение

Современный автотранспорт оснащается все большим количеством электронных датчиков и систем, обеспечивающих комфортное и безопасное вождение. Со временем данные системы станут настолько совершенными, что позволят добиться частичной или полной автономности управления.

Работа электронных систем автомобиля невозможна без надежного обмена данными, различают два вида интерфейсов связи: внутренние и внешние. Внутренние интерфейсы (in-vehicle) обеспечивают обмен данными между электронным блоками самого автомобиля, тогда как внешние интерфейсы служат для обмена данными с другим транспортном (V2V, Vehicle-to-Vehicle) или окружающей инфраструктурой (V2I, Vehicle-to-Infrastructure). Помимо этого, на значительной части автомобилей работают приложения, обменивающиеся данными со всемирной сетью Интернет. Поскольку для вождения необходимо тесное взаимодействие всех систем автомобиля, то в результате внутренние интерфейсы не являются больше полностью изолированными от внешних сетей и могут стать целью проведения сетевых атак [1–5].

Одним из стандартных решений для построения внутренних интерфейсов автомобилей является сеть контроллеров (CAN, Controller Area Network). CAN обеспечивает простой и надежный способ обмена данными между электронными блоками управления (ECU, Electronic Control Unit) (рисунок 1).

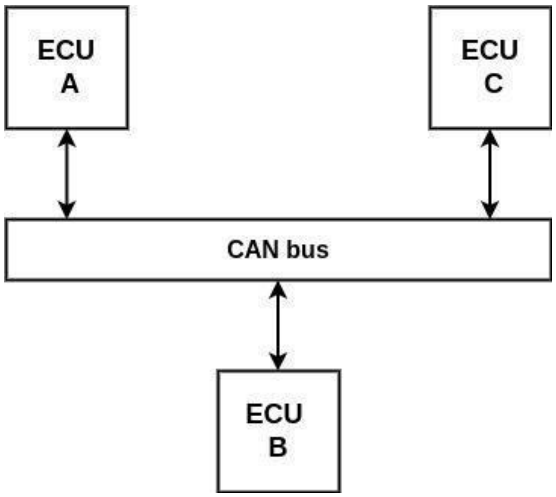

Рисунок 1. Блок-схема CAN

Все электронные блоки напрямую подключены к шине (CAN bus), данные по которой передаются в виде коротких кадров. Кадры рассылаются широковещательно всем блокам одновременно, для предотвращения коллизий блоки проверяют занятость шины перед передачей. Разрешение коллизий производится путем побитового арбитража: при одновременной передаче блоки последовательно сравнивают каждый бит, и если они совпадают, то продолжают передачу; при несовпадении бит передачу продолжает блок, передающий логический ноль. Получение кадров без ошибок каждым блоком должно быть подтверждено путем отправки слота подтверждения, неверно принятые кадры направляются повторно [2; 5].

Стандартом CAN 2.0 определено четыре типа кадров:

- кадр данных (data frame);
- кадр удаленного запроса (remote frame);
- кадр перегрузки (overload frame);
- кадр ошибки (error frame).

Кадр данных используется для передачи данных между блоками. Кадр удаленного запроса применяется для запроса данных у определенного блока. Кадр перегрузки нужен для задержки передачи следующего кадра, чтобы текущий кадр успел быть обработан. Кадр ошибки служит для отправки сообщения об ошибки передачи текущего кадра.

Основная информация в кадрах передается в следующих полях:

- идентификация (ID);
- код длины данных (DLC);
- полезные данные (Payload).

Поле идентификации (ID, IDentification) служит для идентификации, передаваемого сообщения, а также задания его приоритета – чем больше логических нулей оно содержит, тем выше будет приоритет сообщения в случае арбитража.

Код длины данных (DLC, Data Length Code) содержит количество передаваемых байт данных. Полезные данные могут иметь длину от 0 до 8 байт.

Полезные данные (Payload) передаются в поле, размер которого задается DLC.

Как видно из описания стандартный вариант CAN не имеет никаких механизмов защиты от подделки кадров, что делает данную сеть легкой целью для проведения различного рода сетевых атак. Например, скомпрометированный ECU может наводнить шину CAN поддельными сообщениями с наивысшим приоритетом 0x0000, что может привести к блокированию передачи кадров другими блоками. В свою очередь нарушения в работе CAN могут привести к очень серьезным последствиям в виде автомобильных аварий [2].

Поддельные кадры на шине CAN можно рассматривать как аномалии, имеющие определенные отличия от параметров нормального трафика, например, в значениях полей ID и DLC, которые не встречаются в обычных кадрах.

Для выявления аномалий сетевого трафика могут применяться следующие методы [11]:

– на базе сигнатур;
– статистические методы;
– методы машинного обучения.

В основе методов на базе сигнатур лежат правила, которые позволяют произвести проверку трафика на аномальность, например, на запрещенные значения полей кадров. Данные методы достаточно эффективны, однако требуют тщательной разработки и проверки правил, и не позволяют оперативно реагировать на появление новых видов сетевых атак.

В статистических методах аномалии рассматриваются как редкие события, сильно отклоняющиеся от усредненных параметров сетевого трафика. Данные методы позволяют обойтись без создания большого набора правил проверки, однако для их реализации необходимо определение точной стохастической модели сетевого трафика, что часто сложно реализовать на практике.

В основе методов машинного обучения для выявления аномалий лежат алгоритмы, которые позволяют получать критерии определения аномалий непосредственно из данных. Большинство методов машинного обучения относят к методам обучения с учителем (supervised learning) [7], так как они обучаются на заранее размеченных данных, разделенных на нормальные и аномальные экземпляры. Такие методы отличает высокая точность выявления аномалий, однако их недостатком является необходимость подготовки больших объемов размеченных данных для обучения, что является достаточно сложным и дорогостоящим процессом. Помимо этого, в случае появления новых видов сетевых атак, необходимо переобучение алгоритмов на данных, включающих этих атаки.

В методах обучения без учителя (unsupervised learning) алгоритмы самостоятельно структурируют неразмеченные данные, что значительно упрощает их практическое использование, кроме того, отсутствует необходимость в их переобучении [7]. К недостаткам методов обучения без учителя можно отнести их меньшую точность выявления аномалий.

На данный момент имеется несколько практических исследований по выявлению аномалий, связанных с атаками на CAN сети автомобилей [1–5]. В абсолютном большинстве из них для выявления аномалий применяются модели машинного обучения с учителем, основанные на искусственных нейросетях. Как было уже сказано, несмотря на высокую точность таких методов, они не позволяют оперативно реагировать на новые виды сетевых угроз.

В данной работе предлагается для выявления аномалий CAN использовать рекуррентную LSTM-нейросеть, построенную по архитектуре энкодер-декодер, в режиме обучения без учителя. Это позволит ее использовать для выявления как известных, так и ранее не применявшихся сетевых атак.

Архитектура рекуррентной нейросети

Простая рекуррентная нейронная сеть (RNN, Recurrent Neural Network) состоит из трех слоев нейронов: входного, скрытого и выходного, рисунок 2 [7]. В отличии от других типов нейросетей текущее состояние на выходах RNN зависит не только от сигналов на входе, но и от предыдущих состояний.

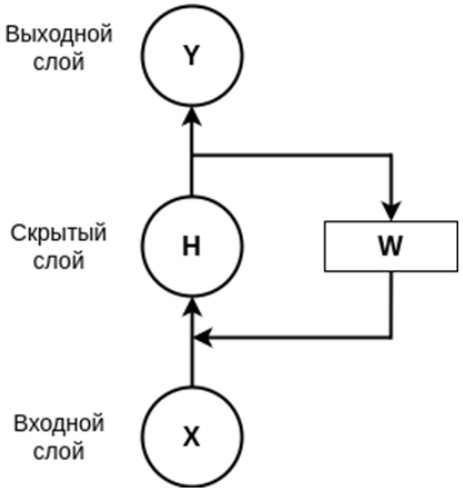

Рисунок 2. Вид простой RNN

Скрытый слой нейронов RNN в момент t определяется как:

$$\mathbf{H}_t = g(\mathbf{W}\mathbf{H}_{t-1} + \mathbf{U}\mathbf{x}_t + \mathbf{b})H ,$$

где **W** и **U** – матрицы весов для скрытого слоя и входного слоя, соответственно; **x** – вектор входных нейронов; **b** – вектор смещений данного слоя; g – функция активации нейронов.

Преимуществом RNN в сравнении с другими типами нейросетей является учет временных зависимостей сигнала на входе от предыдущих состояний, главный недостаток – исчезновение градиента со временем, что не позволяет RNN обучать длительным взаимосвязям. Для устранения данного недостатка были разработаны RNN с элементами долгой краткосрочной памяти (LSTM, Long Short-Term Memory), которые могут учитывать хронологические взаимосвязи входного сигнала на длительных промежутках, однако LSTM требуют значительно больших вычислительных ресурсов для обучения [7].

Поскольку сетевые атаки на CAN приводят к нарушению нормального порядка передачи кадров

во времени, то для их выявления предлагается использовать LSTM-нейросеть по архитектуре энкодер-декодер (рисунок 3) [6; 8; 9].

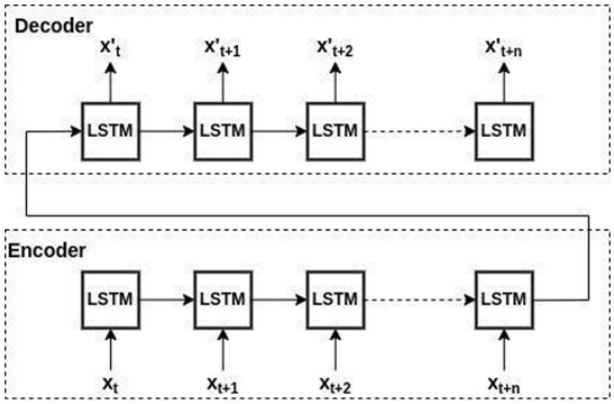

Рисунок 3. Сеть LSTM с архитектурой энкодер-декодер

Энкодер представляет собой цепочку LSTM-ячеек, на вход которых подается исходная временная последовательность длиной *n*: **Xt** = {x_t, x_{t+1}, x_{t+2}, …, x_{t+n}}, где x_t – вектор из *m*-параметров в момент времени *t*. Целью энкодера является обучение наиболее характерным свойствам временной последовательности, которые запоминаются LSTM-ячейками. На выходе энкодера формируется выходной вектор из m-параметров, *n*-копий которого поступают на вход декодера.

Декодер представляет цепочку LSTM-ячеек, на выходах которых формируется последовательность $\mathbf{X'_t}$, которая является реконструкцией входной последовательности, таким образом, задачей LSTM-декодера является воссоздание исходной последовательности по главным свойствам, выявленным декодером.

В процессе обучения делается предположение о том, что аномальные экземпляры встречаются в тренировочных данных намного реже нормальных. В результате нейросеть обучается реконструированию нормальных данных по их наиболее характерным свойствам.

В режиме выявления аномалий входная последовательность оценивается на аномалию путем определения среднеквадратической ошибки реконструкции последовательности в момент времени t:

$$RMSE_t = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(x_{t+i} - x'_{t+i}\right)^2} \ ,$$

где *n* – размерность данных; x_{t+i} – вектор исходных параметров; x_{t+1}' – вектор реконструированных параметров.

Затем определяется усредненное значение RMSE для всех параметров, которое сравнивается с пороговым значением φ. При превышении данного порога вся последовательность относится к аномалиям.

Качество выявления аномалий тем или иным методом оценивается с помощью таких параметров как точность и чувствительность [7; 11]. Точность (precision) определяется как отношение числа правильно отнесенных экземпляров к аномалиям, TP (True Positive) к общему числу экземпляров, отнесенных как правильно к аномалиям, так и неправильно FP (False Positive):

$$P = \frac{TP}{TP + FP} \ .$$

Чувствительность (recall) определяется как отношение числа правильно отнесенных случаев к аномалиям к общему числу аномалий в данных как выявленных, так и не выявленных FN (False Negative):

$$R = \frac{TP}{TP + FN} \ .$$

Следует отметить, что точность и чувствительность по-разному зависят от установленного порогового значения: с ростом порога точность выявления аномалий увеличивается, а чувствительность падает, поскольку растет число не выявленных аномалий.

Зависимость точности от чувствительности для разных пороговых значений представляется в виде кривой (precision recall curve), которая в идеальном случае имеет постоянный характер.

В связи с этим для общей оценки пригодности метода к выявлению аномалий используется усредненная оценка точности (average precision) по разным пороговым значениям:

$$AP = \sum_i \left(R_i - R_{i-1}\right) P_i \ ,$$

где P_i и R_i – точность и чувствительность для порогового значения φ_i.

Использованные данные

Для оценки выявления аномалий рекуррентной нейросетью рассматриваемой архитектуры были использованы данные, подготовленные для соревнований по кибербезопасности [10]. Данные были собраны на автомобиле Hyundai Avante, в стационарном и движущемся состояниях, и представлены как нормальным трафиком, так и несколькими сетевыми атаками: флудинг, спуфинг, повтор и фазинг [1].

Целью флудинга (flooding) является перегрузка шины CAN кадрами с наименьшим идентификатором (0x000), чтобы затруднить передачу нормального трафика.

При спуфинге (spoofing) атакующий отправляет на шине CAN поддельные кадры с целью нарушения работы отдельных функций автомобиля.

Атака повтора (replay) заключается в захвате и повторной отправке по шине нормальных кадров, что может приводить к неверному срабатыванию ряда систем автомобиля.

Во время фазинга (fuzzing) атакующий отправляет по шине кадры со случайно сгенерированными полями, что может вызывать нарушения во время вождения. Данный вид атаки наиболее прост в осуществлении, так как не требует никаких знаний у атакующего о функционировании CAN данной модели или предварительного захвата и анализа трафика.

В набор данных включены такие параметры трафика как отметка времени захвата кадра, поля идентификации, длины и полезной нагрузки, а также класс трафика (нормальный или аномальный) и подкласс (тип атаки).

Результаты и выводы

Для моделирования весь собранных с шины CAN трафик был разбит на последовательности, состоящие из двух, следующих друг за другом кадров. Если в последовательность входит хотя бы один аномальный кадр, то вся она расценивается как аномальная.

Полученные таким образом данные были разделены на три части: для обучения (75%), тестирования (15%) и валидации (10%).

Для реализации рекуррентной LSTM-нейросети рассматриваемой архитектуры, был использован пакет TensorFlow, слои энкодера и декодера состоят из 32 LSTM-ячеек.

Оценка точности модели по выявлению аномалий проводилась при помощи функций пакета Scikit-Learn. Программным код, рассматриваемой модели, в формате Jupyter Notebook представлен в репозитории [12].

Рисунок 4. Результаты выявление аномалий трафика в сети стоящего автомобиля

Полученные результаты выявления аномалий для стоящего автомобиля представлены на рисунке 4.

Результаты для движущегося автомобиля приведены на рисунке 5.

Рисунок 5. Результаты выявления выявления аномалий трафика в сети движущегося автомобиля

Использование рассматриваемой рекуррентной нейросети позволяет достигнуть 94-95% точности выявления аномалий трафика сети CAN автомобиля, что является весьма высоким результатом для методов машинного обучения без учителя. Несмотря на то, что предлагаемый способ проигрывает в точности методам обучения с учителем, которые демонстрируют на базе нейросетей точность на уровне 99%, он не требует сложной и затратной подготовки данных для обучения. Тем не менее, следует отметить, что выявления аномалий трафика автомобиля требует очень высокой точности, так как неверное распознавание аномалий может привести к возникновению аварийнх ситуаций во время движения. Поэтому предлагаемый способ может применяться для выявления аномалий трафика автотранспорта в связке с другими методами для гарантии общей безопасности их использования.

Литература

1. Car hacking and defense competition on in-vehicle network / H. Kang [et al.] // Third International Workshop on Automotive and Autonomous Vehicle Security. 2021. URL: https://dx.doi.org/10.14722/autosec.2021.23035 (дата обращения: 20.11.2023).
2. CAN-ADF: The controller area network attack detection framework / S. Tariq [et al.] // Computers & Security. 2020. Vol. 94. P. 101857. DOI: 10.1016/ j.cose.2020.101857
3. An intelligent secured framework for cyberattack detection in electric vehicles' CAN bus using machine learning / O. Avatefipour [et al.] // IEEE Access. 2019. Vol. 7. P. 127580–127592.

DOI: 10.1109/ACCESS.2019.2937576
4. Song H.M., Woo J., Kim H.K. In-vehicle network intrusion detection using deep convolutional neural networks // Vehicular Communications. 2020. Vol. 21. URL: https://doi.org/10.1016/j.vehcom.2019.100198 (дата обращения: 10.12.2023).
5. Anomaly detection for in-vehicle network using CNN-LSTM with attention mechanism / H. Sun [et al.] // IEEE Transactions on Vehicular Technology. 2021. Vol. 70, no. 10. P. 10880–10893. DOI: 10.1109/TVT.2021.3106940
6. LSTM-Autoencoder-based anomaly detection for indoor air quality time-series data / Y. Wei [et al.] // IEEE Sensors Journal. 2023. Vol. 23, no. 4. P. 3787–3800. DOI: 10.1109/JSEN.2022.3230361
7. Goodfellow I., Bengio Y., Courville A. Deep Learning. Cambridge, Massachusetts: MIT Press, 2016. 800 p.
8. Ergen T., Mirza A.H., Kozat S.S. Unsupervised and Semi-supervised Anomaly Detection with LSTM Neural Networks. 2017. URL: https://doi.org/10.48550/arXiv.1710.09207 (дата обращения: 20.11.2023).
9. Reconstruction-based LSTM-Autoencoder for Anomaly-based DDoS Attack Detection over Multivariate Time-Series Data / Y. Wei [et al.] // 2023. URL: https://arxiv.org/abs/2305.09475 (дата обращения: 20.11.2023).
10. Car-Hacking: Attack & Defense Challenge 2020 Dataset. URL: https://ieee-dataport.org/open-access/car-hacking-attack-defense-challenge-2020-dataset (дата обращения: 25.11.2023).
11. Трошин А.В. Обнаружение аномалий трафика сети с помощью методов понижения размерности // Инфокоммуникационные технологии. 2022. Т. 20, № 4 (80). С. 34–43. DOI: 10.18469/ikt.2022.20.4.05
12. Troshin A. Car hacking detection by LSTM neural network. URL: https://github.com/av-troshin77/car_hacking (дата обращения: 25.11.2023).

Получено 15.04.2024

Трошин Александр Викторович, к.т.н., доцент кафедры сетей и систем связи Поволжского государственного университета телекоммуникаций и информатики. 443010, Российская Федерация, г. Самара, ул. Л. Толстого, 23. Тел. +7 846 339-11-26. E-mail: a.v.troshin77@yandex.ru

TRAFFIC ANOMALY DETECTION IN VEHICLE BUS BY RECURRENT LSTM NEURAL NETWORK

Troshin A.V.
Povolzhskiy State University of Telecommunications and Informatics, Samara, Russian Federation
E-mail: a.v.troshin77@yandex.ru

Modern high-end cars have many electronic control units for driving assistance that combine huge amounts of data about the functioning of car components. A significant part of these vehicles use a controller area network for communication between electronic units. Controller area network is a simple and reliable network protocol that due to its simplicity lacks any security mechanisms for data transmission. The problem of controller area network vulnerability is worsening as constantly growing amounts of data between cars, road infrastructure and the Internet. The traffic of attacks on controller area networks can be treated as abnormal that allows using anomaly detection methods for their recognition. In this work we propose the recurrent long short-term memory encoder-decoder neural network for controller area network attacks detection.

Keywords: *controller area network, anomaly detection, long short-term memory, unsupervised learning, network attacks, cybersecurity*

DOI: 10.18469/ikt.2023.21.4.02

Troshin Alexander Victotovich, Povolzhskiy State University of Telecommunications and Informatics, 23, L. Tolstoy Street, Samara, 443010, Russian Federation; Assistant Professor of Networks and Systems of Telecommunication Department, PhD in Technical Science. Tel. +7 846 339-11-26. E-mail: a.v.troshin77@yandex.ru

References

1. Kang H. et al. Car hacking and defense competition on in-vehicle Network. *Third International*

Workshop on Automotive and Autonomous Vehicle Security, 2021. URL: https://dx.doi.org/10.14722/autosec.2021.23035 (accessed: 20.11.2023).
2. Tariq S. et al. CAN-ADF: The controller area network attack detection framework. *Computers & Security*, 2020, vol. 94, pp. 101857. DOI: 10.1016/ j.cose.2020.101857
3. Avatefipour O. et al. An intelligent secured framework for cyberattack detection in electric vehicles' CAN bus using machine learning. *IEEE Access*, 2019, vol. 7, pp. 127580–127592. DOI: 10.1109/ACCESS.2019.2937576
4. Song H.M., Woo J., Kim H.K. In-vehicle network intrusion detection using deep convolutional neural networks. *Vehicular Communications*, 2020, vol. 21. URL: https://doi.org/10.1016/j.vehcom.2019.100198 (accessed: 10.12.2023).
5. Sun H. et al. Anomaly detection for in-vehicle network using CNN-LSTM with attention mechanism. *IEEE Transactions on Vehicular Technology*, 2021, vol. 70, no. 10, pp. 10880–10893. DOI: 10.1109/TVT.2021.3106940
6. Wei Y. et al. LSTM-Autoencoder-based anomaly detection for indoor air quality time-series data. *IEEE Sensors Journal*, 2023, vol. 23, no. 4, pp. 3787–3800. DOI: 10.1109/JSEN.2022.3230361
7. Goodfellow I., Bengio Y., Courville A. *Deep Learning*. Cambridge, Massachusetts: MIT Press, 2016. 800 p.
8. Ergen T., Mirza A.H., Kozat S.S. Unsupervised and Semi-supervised Anomaly Detection with LSTM Neural Networks, 2017. URL: https://doi.org/10.48550/arXiv.1710.09207 (accessed: 20.11.2023).
9. Wei Y. et al. Reconstruction-based LSTM-Autoencoder for Anomaly-based DDoS Attack Detection over Multivariate Time-Series Data, 2023. URL: https://arxiv.org/abs/2305.09475 (accessed: 20.11.2023).
10. Car-Hacking: Attack & Defense Challenge 2020 Dataset. URL: https:// ieee-dataport.org /open-access/car-hacking-attack-defense-challenge-2020-dataset (accessed: 25.11.2023).
11. Troshin A.V. Network traffic anomaly detection by dimensionality reduction methods. *Infokommunikacionnye tehnologii*, 2022, vol. 20, no. 4, pp. 34–43. DOI: 10.18469/ikt.2022.20.4.05 (In Russ.)
12. Troshin A. Car Hacking Detection by LSTM Neural Network. URL: https://github.com/av-troshin77/car_hacking (accessed: 25.11.23).

Received 15.04.2024

УДК 621.391: 621 39

СРАВНЕНИЕ ГИПЕРЭКСПОНЕНЦИАЛЬНЫХ И ГРУППОВЫХ ПУАССОНОВСКИХ МОДЕЛЕЙ ТРАФИКА МУЛЬТИСЕРВИСНЫХ СЕТЕЙ СВЯЗИ

Лихтциндер Б.Я.[1], Привалов А.Ю.[2]
[1] Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
[2] Самарский национальный исследовательский университет имени С.П.Королева, Самара, РФ
E-mail: b.lihtcinder@psuti.ru, privalov1967@gmail.com

Целью работы было проведение сравнения гиперэкспоненциальных и групповых пуассоновских потоков заявок в качестве моделей пачечного трафика мультисервисных сетей связи. Рассматриваются различные модели трафика для задачи приближения средней очереди, создаваемой видеотрафиком современных мультисервисных сетей. Рассмотрены пуассоновский и гиперэкспоненциальный потоки, как ординарные, так и групповые. Показано, что для задачи приближения очереди видеотрафика подходят групповые потоки обоих типов. Групповые пуассоновские потоки позволяют получить весьма простые аналитические зависимости средних значений очередей от коэффициента загрузки систем массового обслуживания и поэтому являются наиболее предпочтительными. Показана неадекватность применения ординарных гиперэкспоненциальных моделей для аппроксимации пачечных потоков заявок, поскольку, при малых значениях коэффициента загрузки, зависимости средних значений очередей для гиперэкспоненциальных потоков практически близки к нулю, в то время, как указанные зависимости для пачечных потоков имеют весьма значительный угол наклона. Сделанные выводы подтверждаются результатами имитационного моделирования.

Ключевые слова: *видеотрафик, пуассоновский поток, гиперэкспоненциальный поток, групповые потоки*