Применение графов атак для моделирования нарушений движения автотранспортных средств в конвое

Р. Р. Фаткиева
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
rikki2@yandex.ru

***Аннотация*. В работе проводится исследование алгоритмов движения беспилотных автотранспортных средств. Описана математическая модель функционирования системы управления. Выполнен анализ информационных угроз при движении автотранспортных средств в конвое. Построены графы информационных атак. На примере моделирования угроз нарушения передачи и обработки информации показаны возможные нарушения функционирования. Предложены мероприятия по их нейтрализации.**

Ключевые слова: беспилотный автомобиль; Pure Pursuit Controller; алгоритм прямого преследования; сетевые атаки

I. Введение

В современном мире транспорт является одним из объектов критической информационной инфраструктуры. Связано это с увеличением количества электронных компонентов входящих в его состав и возможностью подключения к системам связи (V2X). Такой подход позволяет автоматизировать управление автотранспортными средствами (АТС), однако влечет за собой увеличение количества атак на его инфраструктуру. Существующие модели и методы обеспечения безопасности не всегда в полном объеме справляются с идентификацией и подавлением атаки [1–10]. В работе [2, 6–10] показано, что движение в конвое особенно уязвимо для атак типа «отказ в обслуживании», поэтому в [2] для смягчения последствий предложено использовать многоуровневые карты планирования по гистограмме векторного поля с оценкой поведенческих схем движения. В работах [3–5] рассмотрена модель угроз, предложенная для оценки эффективности и безопасности движения в конвое, однако выявлен не весь набор возможных атак. В работах [6–10] рассмотрены основные атаки на сети передачи данных о движении, однако предложенные средства защиты предполагают значительные затраты вычислительных ресурсов. При этом в исследованиях недостаточное внимание уделяется влиянию угроз на изменение характеристик движения АТС, что делает данные исследования актуальными.

II. Модель движения автотранспортных средств в конвое

Основные методы отслеживания траектории делятся на две категории: методы на основе геометрической трассировки и методы прогнозирования на основе моделей. Рассматриваемый в данной работе метод Pure Pursuit [11] относится к методу на основе геометрической трассировки. Алгоритм принимает заднюю ось транспортного средства в качестве точки касания, а продольный корпус транспортного средства - в качестве касательной. Управляя углом поворота переднего колеса, транспортное средство может перемещаться по дуге, проходящей через точку цели, согласно следующей модели:

Шаг 1. Сбор АТС в конвой:

1.1 Определение множества АТС, входящих в конвой, с назначением порядковых номеров движения в конвое: $M = \{m_1, m_2, \dots, m_i, \dots, m_n\}$, где m_i – АТС, $i = \overline{1,N}$. При этом осуществляется выделение головного центра управления, т.е. первого ведущего АТС конвоя.

1.2 Выстраивание АТС в колонну и установление соответствующих начальных координат движения:

$$A_0 = \{A_{m_1}\left(x_{0_{m_1}}, y_{0_{m_1}}\right), \dots, A_{m_j}\left(x_{0_{m_j}}, y_{0_{m_i}}\right), \dots,$$

$A_{m_n}\left(x_{0_{m_N}}, y_{0_{m_N}}\right)\}$, где A_0 – множество начальных координат АТС в конвое, A_{m_n} – начальная точка движения -ого АТС в конвое, $x_{0_{m_n}}$ – абсцисса начальной точки n-ого АТС в конвое, $y_{0_{m_n}}$ – ордината начальной точки n-ого АТС в конвое, n – количество АТС в конвое.

Шаг 2. Определение маршрута.

2.1 Установление соответствующих конечных координат движения для конвоя:

$$A_d = \{A_{m_1}\left(x_{d_{m_1}}, y_{\mathrm{d}_{m_1}}\right), \dots, A_{m_j}\left(x_{\mathrm{d}_{m_i}}, y_{\mathrm{d}_{m_i}}\right), \dots,$$

$A_{m_N}\left(x_{d_{m_N}}, y_{d_{m_N}}\right)\}$, где A_{d} – множество конечных координат АТС в конвое, A_{m_n} – конечная точка движения -ого АТС в конвое, $x_{d_{m_n}}$ – абсцисса конечной точки n-ого АТС в конвое, $y_{\mathrm{d}_{m_n}}$ – ордината конечной точки n-ого АТС в конвое, n – количество АТС в конвое.

2.2 Определение множества маршрутов от текущего местоположения машины до назначенных конечных координат движения в конвое: $D_{\mathrm{M}} = \{D_1, D_2, \dots, D_{\mathrm{i}}, .., D_{\mathrm{l}}\}$, где D_{l} – множество маршрутов движения -ого АТС от начальной точки до конечной точке для конвоя.

2.3 Применение алгоритма поиска оптимального маршрута из множества всех маршрутов:

$$\mathrm{S}_D = \min(D_l)$$

Шаг 3. Формирование множества информационных и управляющих сообщений:

3.1 Формирование множества информационных сообщений: $C = \{C_1, C_2, \dots, C_j \ \dots, C_K\}$, $j = \overline{1,K}$ позволяющих осуществлять управление при движении в конвое (например, подача сигнала о начале сбора автотранспортных средств в конвой).

3.2 Рассылка информационных сообщений для АТС конвоя с маршрутом C_{S_D}.

Шаг 4. Движение конвоя.

4.1 Вход АТС в конвой. Выполняется проверка принадлежности элемента множества АТС, который выполняет задачу входа в конвой, к множеству M — АТС, которые входят в конвой в настоящий момент.

4.2 Выполнение проверки условия, что выбрано ведущее АТС -$m_1 \neq \{\emptyset\}$. С помощью множества информационных сообщений С производится проверка выполнения условия, что при движении ведущего АТС выполняется движение остальных АТС в конвое: Если $\vartheta_{M_1} \neq 0$, то $\vartheta_{M_n} \neq 0, n = \overline{2,n}$, где ϑ_{M_1} – ведущее АТС.

Далее осуществляется выполнение проверки условия, что все АТС в конвое движутся с соблюдением дистанции и прохождением верного маршрута.

4.3 Движение конвоя.

4.4 Перестроение элементов конвоя осуществляется за счет операций вхождения и выхода АТС.

- для операции вхождения выполняется проверка принадлежности элемента множества m' – АТС, который выполняет задачу входа в конвой к множеству M – АТС, которые входят в конвой на текущий момент времени. Если данный элемент не принадлежит множеству М, то выполняется операция объединения множеств, так что Если $m' \notin M = 0$, то $M' = m' \cup M = \{m_1, m_2, m_{\text{i}}, \dots, m_n, m'\}$
- для операции выхода выполняется проверка принадлежности элемента множества m_i— АТС, который выполняет задачу выхода из конвоя, множеству M – АТС, которые имеются в конвой: Если $m_i \in M$, то $M' = M \backslash m_i = \{m_1, m_2, \dots, m_{i-1}, m_{i+1}, \dots, m_n\}$

4.5 Управление движением конвоя. Для этого на заданные промежутки времени формируются информационные сообщения из п. 3.1 с запросом о состоянии АТС, и на основании ответов осуществляется выполнение проверки условий передвижения конвоя. Например, что при движении ведущего АТС выполняется движение остальных АТС с соблюдением дистанции и прохождением верного маршрута. Если пороговые значение характеристик движения не выходит за штатные режимы функционирования, то движение продолжается. В противном случае формируется управляющее сообщение (например, остановка конвоя, возврат АТС в конвой, на заданную траекторию и т. п).

Шаг 5. Расформирование конвоя.

III. Модель угроз безопасности системы управления движением автотранспортных средств в конвое

Для построения множества управляющих сообщений, сформированных на шаге 3.1, необходимо определить множество угроз безопасности при движении АТС в конвое [12]: $U = \{U_1, U_2, \dots U_r\}$, где U_r – элемент множества угроз. Это позволяет перейти к определению множества элементов АТС, функционирование которых нарушено при нанесении ущерба: $Z_R = \{Z_{1_r}, Z_{2_r}, \dots, Z_{w_r}\}$, где Z_{w_r} – элемент АТС после реализации r-ой угрозы и осуществить поиск возможных мероприятий по устранению угроз $E_R = \{E_{1_r}, E_{2_r}, \dots, E_{q_r}\}$, где E_{q_r} – мероприятие, направленное на предупреждение, выявление и/или исключение угроз безопасности.

IV. Моделирование нарушения траектории движения автотранспортных средств под воздействием атак

Моделирование нарушения траектории движения АТС под воздействием атак осуществлялось с использованием программного обеспечения MATLAB Simulink, в условиях длины моделируемого АТС равным 4 метра (стандартная длина легкового АТС), обзорного расстояние между АТС в 5 метров и времени моделирования в 16 секунд. Рассмотрено поведение модели под воздействием атак троянскими вредоносными программами, Сивиллы и DDos. Графы атак представлены на рис. 1–3 соответственно.

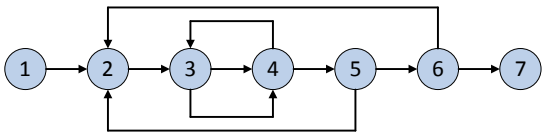

Рис. 1. Граф атаки троянской программой, где: 1 – принятие злоумышленником решения о применении атаки вредоносным ПО; 2 – разработка ПО для атаки; 3 – загрузка ПО на АТС (через USB-устройства; через сетевое соединение); 4 – ПО загружено; 5 – запуск ПО; 6 – изменение параметров исходной управляющей программы АТС; 7 – нарушение траектории движения после запуска ПО

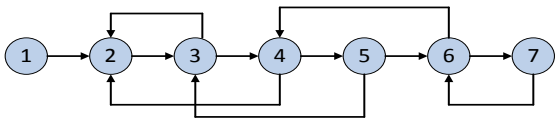

Рис. 2. Граф атаки Сивиллы, где: 1 – принятие злоумышленником решения о выполнении атаки Сивиллы; 2 – поиск и получение информации о структуре, сетевых адресах датчика геолокации впереди идущего и ведомого АТС; 3 – сообщение датчику геолокации об использовании сетевого адреса приемника ведомого АТС; 4 – сообщение приемнику ведомого АТС об использовании сетевого адреса датчика геолокации ведущего АТС; 5 – перехват отправления информации ведомого АТС; 6 – отправление ложных данных о местоположении ведущего АТС; 7 – нарушение траектории движения АТС.

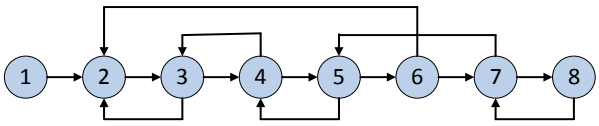

Рис. 3. Граф DDos атаки, где: 1 – принятие злоумышленником решения о выполнении DDoS атаки; 2 – поиск и получение информации о структуре, сетевых адресах АТС; 3 – подключение удаленного доступа к датчику геолокации на ведущем АТС; 4 –

захват контроля над датчиком; 5 – перехват управляющей информации ведущего АТС; 6 – подмена доверенного хоста на ложный сервер; 7 – отправление большого количества ложных данных о местоположении ведущего АТС; 8 – формирование отказа в обслуживании.

Передвижение ведущего АТС на маршруте отражено в модели кривой из красных точек, а следующего за ним транспортного средства — кривой из белых точек (рис. 4). *Атака троянскими вредоносными программами* позволяет злоумышленнику не только несанкционированно проникнуть в систему управления АТС, но и выполнить на устройстве вредоносный код, который может изменить данные в исполняемом файле и вызвать сбой в его работе с блокировкой доступа к определенным данным. При моделировании атаки происходит изменение траектории движения (рис. 4). Данная атака может также нарушить передачу данных о местонахождении ведущего АТС, изменить информацию о его координатах, вследствие чего происходит нарушение движения ведомых АТС (которые зацикливаясь возвращаются в одну точку, рис. 4).

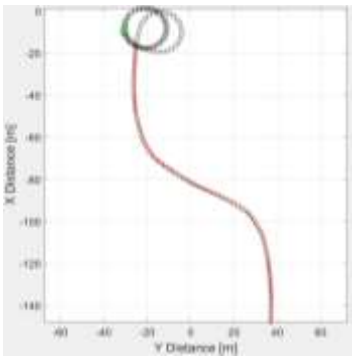

Рис. 4. Траектория движения АТС в условиях атаки троянским ПО

Еще одним объектом в исполняемом коде, который может подвергнуться атаке злоумышленника, является значение обзорного расстояния для ведомого АТС. Увеличение данного параметра приведет к тому, что ведомое АТС передвигается по более плавной траектории, при этом «срезая» углы вдоль маршрута (рис. 5).

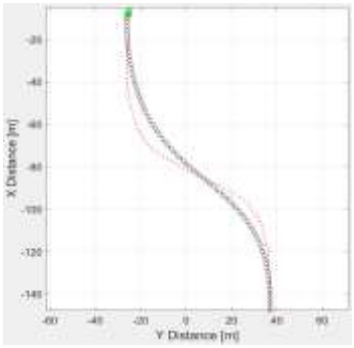

Рис. 5. Траектория движения АТС при увеличении значения обзорного расстояния

Если же данному параметру присвоить значение меньше, чем при штатном режиме функционирования, то это может привести к некорректной работе в отслеживании и преследовании ведущего АТС. Тогда в траектории появятся колебания, вызывающие нестабильное поведение ведущего АТС (рис. 6).

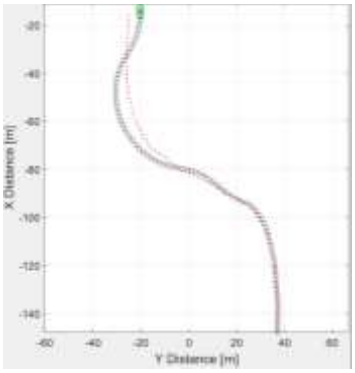

Рис. 6. Траектория движения АТС на уменьшение значения обзорного расстояния

При несанкционированном изменении параметра начального угла отклонения для ведомого АТС траектория движения изначально будет выглядеть некорректной, но со временем вернется в норму (рис. 7).

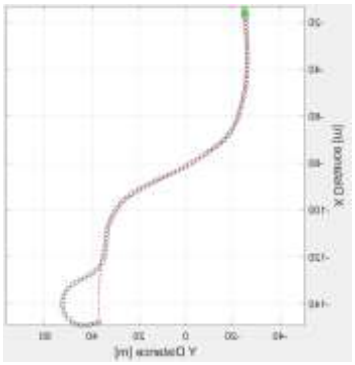

Рис. 7. Траектория движения АТС при атаке на значение начального угла движения

Атака Сивиллы (спуфинг) может использоваться как фальсификация данных о координатах местонахождения для ведущего АТС. В этом случае злоумышленник воздействует на датчики, с подменой сведений о геолокации для ведущего АТС (рис. 8).

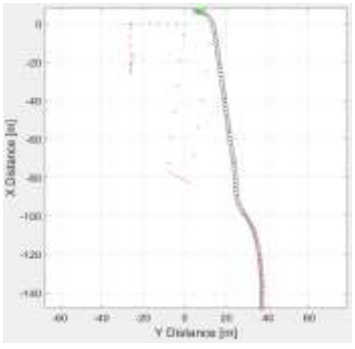

Рис. 8. Траектория движения АТС при условиях атаки Сивиллы

DDoS атака – разновидность атаки на канал передачи данных, по которому передаются сведения о местоположении ведущего АТС. С помощью нее злоумышленник сможет перегрузить пропускную способность канала связи с системой геолокации, например, заполнив его паразитным трафиком: пустыми запросами и пакетами. Результат моделирования движения АТС под воздействием DDos атаки аналогичен результату, представленному на рис. 4.

Моделирование поведение АТС под воздействием атак (рис. 5–8), дает возможность сформировать множество элементов, на которые осуществляется воздействие, что позволяет идентифицировать атаку (табл. 1) и в дальнейшем сформировать комплекс воздействий для борьбы с ними.

ТАБЛИЦА I. ИДЕНТИФИКАЦИЯ АТАК

Атака	Элементы воздействия	Вид нарушения
DDoS	Координаты ведущего АТС	Движение вокруг точки или по окружности
Спуфинг	Координаты ведущего АТС	Значительное нарушение траектории движения
Троянская вредоносная программа	Увеличение обзорного расстояния	Сглаживание углов траектории движения
	Уменьшение обзорного расстояния	Колебания относительно траектории движения
	Угол начального отклонения	АТС вначале передвигается в противоположном направлении от маршрута
	Координаты ведущего АТС	Движение вокруг точки или по окружности

Например, в рамках выбранной системы моделирования можно выполнить следующие мероприятия по обнаружению и предотвращению атак:

Ввод системы проверки координат. С помощью добавления в исполняемый код программы управления движением, цикла, сравнивающего координаты, по которым происходит движение ведущего АТС с координатами маршрута. Это позволяет реализовать отслеживание корректности траектории движения. При несовпадении данных координат на определенном шаге будет появляться сообщение об ошибке и выполняться восстановление корректных данных путем обновления переменной массива, элементами которого являются запланированные координаты ведущего АТС. Введение данной функциональности позволяет избежать атаку Сивиллы на датчик геолокации впереди идущего АТС.

Ограничение времени ожидания отклика от ведущего АТС, т. е. время на ожидание изменений координат от ведущего АТС. Если через заданный промежуток времени от ведущего АТС не поступают данные об изменениях координат, или поток данных не поступает вовсе, то следует передать сигнал ведомому АТС о необходимости остановке. Введение такого мероприятия в систему управления позволяет предупредить атаку на зацикливания движения около одной точки, в случае ее возникновение даст возможность АТС остановиться через заданное время.

Если ведомое АТС начинает «вилять» относительно траектории движения ведущего АТС, целесообразно сформировать набор сообщений с рекомендацией о перезагрузки ПО. В этом случае, после перезапуска система вернется к изначальным нормальным условиям, тем самым движение АТС вернется к штатному режиму движения. Такие же действия следует предпринять, если ведомое АТС начало движение в сторону отличную от направления движения ведущего АТС. Применение данного подхода позволит, во-первых, детектировать факт несанкционированного вторжения нарушителем в систему и изменения в ней данных. Во-вторых, предоставит возможность своевременно оперативно предпринять меры по нейтрализации атак, которые направлены на увеличение или уменьшение значения обзорного расстояния. Применение перезапуска алгоритма функционирования АТС при условии атаки на значение обзорного расстояния, приводит к восстановлению системы и возвращению к нормальным условиям управления.

V. ЗАКЛЮЧЕНИЕ

Применение графов атак позволяет вывить основные характеристики движения, динамическое изменение которого дает возможность определить отклонения пороговых значений и идентифицировать атаку. К дальнейшему направлению исследования целесообразно отнести расширение пространства рассмотренных атаки и алгоритмов движения АТС.

СПИСОК ЛИТЕРАТУРЫ

[1] Абдулов А.В., Абдулова Е.А. Аспекты безопасного функционирования беспилотных транспортных средств в среде умного города / А. В. Абдулов, Е. А. Абдулова // Моделирование, оптимизация и информационные технологии. 2020. Т. 8, № 3(30). DOI 10.26102/2310-6018/2020.30.3.010.

[2] Cheung C., Rawashdeh S., Mohammadi A. Jam Mitigation for Autonomous Convoys via Behavior-Based Robotics. // Appl. Sci. 2022, 12, 9863. https://doi.org/10.3390/app12199863

[3] Vorobiev V., Fatkieva R., Evnevich E. Security Assessment of Robotic System with Inter-Machine Interaction // 2018 International Russian Automation Conference (RusAutoCon), Sochi, Russia, 2018, pp. 1-7. doi: 10.1109/RUSAUTOCON.2018.8501753.

[4] Hodge Cabell, Konrad Hauck, Shivam Gupta, Jesse Bennett. Vehicle Cybersecurity Threats and Mitigation Approaches. Golden, CO: National Renewable Energy Laboratory.2019. NREL/TP-5400-74247. https://www.nrel.gov/docs/fy19osti/74247.pdf

[5] Qayyum A., Usama M., Qadir J., Al-Fuqaha A.. Securing Connected & Autonomous Vehicles: Challenges Posed by Adversarial Machine Learning and the Way Forward // IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 998-1026, Secondquarter 2020, doi: 10.1109/COMST.2020.2975048.

[6] Trkulja N, Starobinski D, Berry R. A. Denial-of-Service Attacks on C-V2X Networks //Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2021 25 February 2021, Virtual ISBN 1-891562-68-1 https://dx.doi.org/10.14722/autosec.2021.23006.

[7] M. N.-E. Saulaiman, M. Kozlovszky and Á. Csilling, "A Survey on Vulnerabilities and Classification of Cyber-Attacks on 5G-V2X, // 2021 IEEE 21st International Symposium on Computational Intelligence and Informatics (CINTI), Budapest, Hungary, 2021, pp. 000235-000240, doi: 10.1109/CINTI53070.2021.9668440.

[8] Hasan M., Mohan S., Shimizu T. and Lu H., "Securing Vehicle-to-Everything (V2X) Communication Platforms," in IEEE Transactions on Intelligent Vehicles, vol. 5, no. 4, pp. 693-713, Dec. 2020, doi: 10.1109/TIV.2020.2987430.

[9] Brocklehurst C., Radenkovic M.,Resistance to Cybersecurity Attacks in a Novel Network for Autonomous Vehicles. J. Sens. Actuator Netw. 2022, 11, 35. https://doi.org/10.3390/jsan11030035.

[10] Cyber-attacks on autonomous vehicles. https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/14462/KAZOLEAS_MTE2010.pdf?sequence=1&isAllowed=y

[11] Implementation of the Pure Pursuit Path 'hcking Algorithm. https://www.ri.cmu.edu/pub_files/pub3/coulter_r_craig_1992_1/coulter_r_craig_1992_1.pdf

[12] Банк данных угроз безопасности информации. https://bdu.fstec.ru/threat-section