5. Tarasov V.N., Gorelov G.A., Ushakov Y.A. Vosstanovlenie momentnyh harakteristik raspredeleniya intervalov vremeni mezhdu paketami vhodyaschego trafika [Restoring moment distribution characteristics interval between packets of incoming traffic]. *Informacionnye technologii*, 2014, no. 2, pp. 40–44. (In Russian).
6. Tarasov V.N. *Veroyatnostnoe komp'yuternoe modelirovanie slozhnyh sistem* [Probabilistic Computer Modeling of Complex Systems]. Samara: SNC RAN Publ., 2002, 194 p. (In Russian).
7. 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*, 1991, pp. 683–688.
8. Whitt W. Approximating a point process by a renewal process: two basic methods. *Operation Research*, 1982, vol. 30, no. 1, pp. 125–147.
9. Aliev T.I. *Osnovy modelirovaniya diskretnyh system* [Fundamentals of Modeling Discrete Systems]. SPb.: SPbGU ITMO, 2009, 363 p. (In Russian).
10. Aliev T.I. Approksimaciya veroyatnostnyh raspredelenij v modelyah massovogo obsluzhivaniya [Approximation of probability distributions in queuing models]. *Nauchno-tekhnicheskij vestnik informacionnyh tekhnologij, mekhaniki i optiki*, 2013, no. 2 (84), pp. 88–93. (In Russian).
11. RFC 3393 IP Packet Delay Variation Metric for IP Performance Metrics (IPPM). URL: https://tools.ietf.org/html/rfc3393 (accessed: 26.02.2016).
12. Tarasov V.N., Bahareva N.F. Obobshchennaya dvumepnaya diffuzionnaya model' massovogo obsluzhivaniya tipa GI/G/1 [Generalized two-dimensional diffusion queuing model type GI/G/1]. *Telekommunikacii*, 2009, no. 7, pp. 2–8. (In Russian).
13. Tarasov V.N., Malakhov S.V., Kartashevskiy I.V. Teoreticheskoe i eksperimental'noe issledovanie zaderzhki v programmno-konfiguriruemyh setyah [Theoretical and experimental study of delay in software-configured networks]. *Infokommunikacionnye technologii*, 2015, no. 4, pp. 409–413. (In Russian).

Received 16.01.2020

НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 681.3

АДАПТИВНЫЙ МЕТОД ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ ИНТЕРФЕЙСОВ БЕСПИЛОТНЫХ ТРАНСПОРТНЫХ СРЕДСТВ В ИНФРАСТРУКТУРЕ УМНОГО ГОРОДА

Скатков А.В., Брюховецкий А.А., Моисеев Д.В., Шевченко В.И.
Севастопольский государственный университет, Севастополь, РФ
E-mail: dmitriymoiseev@mail.ru

Предлагается метод обнаружения уязвимостей интерфейсов беспилотных транспортных средств на основе анализа состояния трафика в каналах связи беспилотных транспортных систем. Подход базируется на методах непараметрической статистики для оценки информационных состояний контролируемых объектов, к которым относятся такие ресурсы беспилотных транспортных систем, как: канал связи, процессор, память, источник питания и др. Для каждого из этих ресурсов предлагается оценивать изменение таких характеристик, как степень загрузки ресурса и скорость его изменения. Распознавание состояния сетевого трафика осуществляется в условиях дефицита априорной информации о свойствах источника вторжений и стохастической природы распознаваемых событий. Для повышения уровня достоверности обнаружения уязвимостей в модели производится адаптивная динамическая настройка правил принятия решений по классификации информационного состояния трафика беспилотных транспортных средств.

Ключевые слова: *беспилотное транспортное средство, адаптивная модель, обнаружение уязвимостей, классификация информационных состояний, оценочная матрица*

Введение

В последнее десятилетие наблюдается быстрое развитие беспилотных транспортных систем (БТС) в самых разных аспектах. Сложность современных транспортных систем в сочетании с резким увеличением использования электронных устройств 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. При этом возникают задачи по созданию информационных технологий, обеспечивающих безопасность объектов критической информационной инфраструктуры «умный город». Применительно к БТС как к киберфизическому объекту в инфраструктуре «умного города» можно выделить три зоны уязвимости:

– системы управления движением: хранилища данных и динамические потоки данных и команд, передаваемые по каналам связи и обрабатываемые в автоматизированных системах;

– техническая инфраструктура: технологии, системное программное обеспечение, устройства, с помощью которых осуществляется реализация основных действий по управлению БТС;

– информационное взаимодействие субъектов «умного города» с использованием информации, получаемой от БТС (передаваемой БТС) и обрабатываемой посредством технической инфраструктуры.

Разработке моделей механизмов защиты в информационно-вычислительных сетях и исследованию их эффективности посвящены [1–5]. Особое место занимает проблема обеспечения безопасности критических инфраструктур [6], к которым относится система «умный город», представляющая собой масштабную киберфизическую систему, координирующую взаимодействия между разнородными физическими устройствами и вычислительными системами в реальном масштабе времени. Разнородность приложений и беспроводных коммуникаций существенно усложняет обеспечение безопасности таких систем.

Поэтому разработка методов, обеспечивающих безопасность информационного взаимодействия БТС с другими субъектами «умного города» посредством программных интерфейсов, представляет собой актуальную задачу.

В статье рассматривается подход, базирующийся на основе методов непараметрической статистики для оценки информационных состояний контролируемых объектов, к которым относятся ресурсы БТС: канал связи, процессор, память, источник питания. Для каждого из этих ресурсов предлагается оценивать изменение таких характеристик, как степень загрузки ресурса и скорость его изменения.

Модель обнаружения уязвимостей

Будем оценивать степень внешнего информационного воздействия на БТС по изменению информационного состояния, например сетевого трафика БТС. При достаточно общей постановке задачи речь идет о необходимости сравнения двух выборок результатов наблюдений над состоянием объекта с целью выявления значимости его качественного изменения. Совокупность наблюдений представляет собой набор измерений состояния объекта – множество выборок:

$$X = \{X_1, X_2, \ldots, X_n\},$$

где $X_i = \{x_1, x_2, \ldots, x_V\}$, x_i – значение измеряемого параметра объекта; n – число выборок; V – объем каждой выборки.

Вопрос заключается в том, можно считать наблюдаемые в двух из n выборках между X_p и X_q различия на основе оценки информационной меры Кульбака существенными, значимыми или различия между ними следует отнести на счет случайного рассеивания значений исследуемого признака. Последнее предположение представляет нулевую гипотезу H_0 об отсутствии существенного различия между двумя информационными состояниями ресурса [6]. Расстояние Кульбака распределения X_p относительно X_q может быть оценено как

$D(X_p \parallel X_q) <= Q$ – отсутствие J-эффекта;

$D(X_p \parallel X_q) > Q$ – наблюдение J-эффекта,

где Q – предельное значение расстояния, зависящее от критичности контролируемого ресурса. Тогда нулевая гипотеза H_0 имеет место при $D(X_p \parallel X_q) <= Q$ – отсутствие J-эффекта. В этом случае состояние ресурса принимается за стабильное, в противном случае принимается гипотеза H_1 – имеет место качественное изменение информационного состояния ресурса.

Введем понятие зоны распознавания J-эффекта. Будем для определенности рассматривать следующие границы зон распознавания: Q_1, Q_2, Q_3. Тогда зоны определяются следующими интервалами:

$$[0; Q_1), [Q_1; Q_2), [Q_2; Q_3].$$

В зависимости от принадлежности текущего значения расстояния $D_{pq} \in Q_i$ (i = 1, m) будем

классифицировать следующие информационные состояния ресурса:

$0 <= D_{pq} < Q_1$ – стабильное, устойчивое;

$Q_1 <= D_{pq} < Q_2$ – неустойчивое;

$Q_2 <= D_{pq} < Q_3$ – предкритическое.

В общем случае число зон распознавания Q_i определяется экспертом и зависит от критичности ресурса, динамики его состояния, требований к качеству контроля его характеристик, затрат на выполнение контроля и возможных потерь при контроле. Чем больше значение D_{pq}, тем более динамичный объект, то есть его состояние во времени (значение контролируемого параметра) подвержено б*о*льшим изменениям. Поэтому если ресурс критического назначения и ставится задача контролировать незначительные изменения его состояния, то необходимо использовать:

– высокую частоту f съема значений контролируемого параметра;

– малый интервал зон распознавания ΔQ;

– большое число зон распознавания m;

– большой объем выборки V;

– большое число интервалов гистограммы g.

Соблюдение указанных требований обеспечивает:

– высокую достоверность определения информационного состояния ресурса;

– снижение величины ошибок первого и второго рода;

– минимальный возможный ущерб от потери информации.

В то же время обеспечение высокой достоверности контроля в сочетании с минимальным ущербом приведет к увеличению времени контроля и затрат при контроле. Как следствие, последние две характеристики могут оказаться препятствием для проведения контроля в реальном масштабе времени. Возникает противоречие, когда улучшение одних характеристик контроля вызывает ухудшение других.

Общей рекомендацией для оценки обнаружения *J*-эффекта является следующее. В зависимости от назначения системы эксперт (ЛПР) вправе задавать значение p – уровня достоверности, и соответствующие ему значения f – частоты измерения, и Q – предельного значения расстояния, зависящие от критичности ресурса, для которых, с одной стороны, будет обеспечена высокая достоверность значений характеристик объектов, с другой – достигается допустимое число ошибок первого и второго рода, а значит, будут снижены риски при принятии ошибочных решений.

Выбор параметров системы контроля производится таким образом, чтобы обеспечить мини-

	V_1	…	V_k	…	V_v
$Q_1 f_1$	L_{11}^1		L_{11}^k		L_{ij}^v
$Q_1 f_2$					
…	…	…	…	….	…
$Q_1 f_t$					
…	…	…	…	…	…
$Q_i f_j$			L_{ij}^k		
…	…	…	…	…	…
$Q_m f_1$					
…	…	…	…	…	…
$Q_m f_t$	L_{m1}^m				L_{mt}^m

Рисунок 1. Структура оценочной матрицы потерь

мальные потери при оценке состояния ресурса, которые могут возникнуть из-за несвоевременного принятия решения. Потери зависят от пороговых значений расстояния Кульбака Q_i, частоты измерений f_j, объема выборки V_k. Чем выше частота и чем меньше диапазон пороговых значений ΔQ, тем оперативнее будет приниматься решение о текущем состоянии ресурса. Чем больше объем выборки, тем точнее будет вычислено значение потерь.

Одним из возможных подходов к структурированию информации и использованию ее в целях адаптации параметров системы контроля к текущему информационному состоянию ресурса и среды является применение оценочной матрицы. Оценочная матрица позволяет выбрать наиболее оптимальные значения контролируемых параметров с точки зрения обеспечения принятых критериев, задаваемых экспертом.

Будем рассматривать потери L, связанные с оценкой информационного состояния ресурса, на элементах множества декартова произведения $\{Q \times f \times V\}$. Структура оценочной матрицы изображена на рисунке 1. Ее элементами являются значения потерь L_{ij}^k, а входами – пороговые значения расстояния Кульбака Q_i, (i = 1, m); частота измерения контрольных параметров ресурса f_j, (j = 1, t) и значения V_k объемов выборок (k = 1, l).

Каждая зона распознавания $[Q_{i-1}; Q_i]$ содержит значения потерь для множества частот f_j (j = 1, t). Будем полагать, что в пределах отдельной зоны распознавания значение контролируемого параметра изменяется монотонно во времени, то есть является не убывающим или не возрастающим для любых двух моментов времени, в которые производятся измерения.

Введем обозначения для заданных Q_i, f_j, V_k: $f_{i,j,\min}^k$ – значение частоты для интервала, обес-

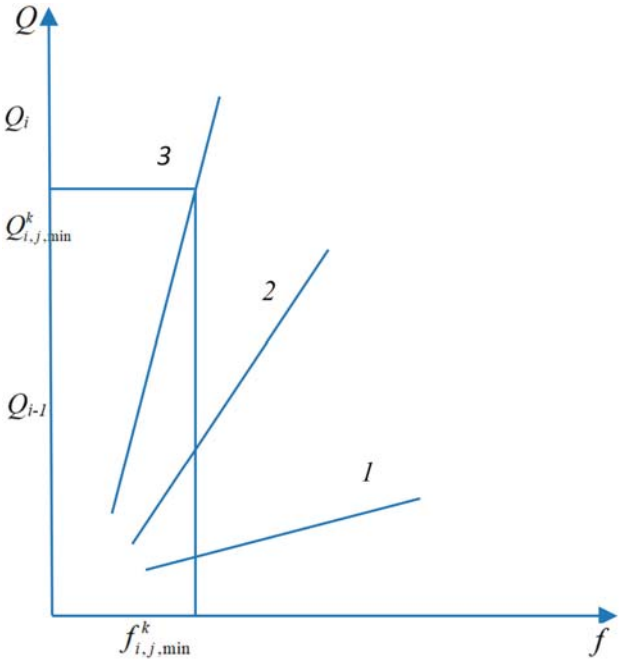

Рисунок 2. Пример иллюстрации скорости изменения $\Delta Q / \Delta f$ состояния ресурса в пределах зоны $[Q_{i-1}; Q_i]$: *1* – скорость незначительна; *2* – скорость превышает допустимый порог; *3* – скорость изменения высокая

печивающее минимум потерь L_{ij}^k; $Q_{i,j,\min}^k$ – значение порогового расстояния Кульбака, обеспечивающее минимум потерь L_{ij}^k; L_{ij}^k – текущие потери при оценке расстояния Кульбака между выборками X_p и X_q.

Указанные значения определяются в режиме обучения и настройки. Значение потерь предлагается вычислять с помощью модифицированной функции Тагучи [8]:

$$L_{ij}^k(p,q) = \\ = \alpha\left(\frac{f_{p,q} - f_{i,j,\min}^k}{f_{i,j,\min}^k}\right)^2 + \beta\left(\frac{D_{p,q} - Q_{i,j,\min}^k}{Q_{i,j,\min}^k}\right), \quad (1)$$

где $f_{p,q}$, $D_{p,q}$ – текущие значения частоты и информационной меры Кульбака.

Будем полагать, что для каждой зоны распознавания $[Q_{i-1}; Q_i]$ задается множество значений частот $f_{i,j,\min}^k$ и расстояний $Q_{i,j,\min}^k$, для которых обеспечивается минимум потерь. Это позволит в пределах отдельной зоны распознавать скорость изменения состояния ресурса:

– устойчивое состояние, при котором скорость изменения незначительна;

– неустойчивое (переходное) состояние, когда скорость изменения превышает минимально допустимый порог;

– предкритическое состояние, в котором скорость изменения высокая, вследствие чего возможна критическая ситуация.

На рисунке 2 представлена графическая иллюстрация скорости изменения состояния ресурса $\Delta Q / \Delta f$.

Предлагаемый подход позволит выбирать оптимальные значения частоты контроля и объема выборки, обеспечивающие минимум потерь. Каждому виду потерь сопоставляется коэффициент α или β, причем $\alpha + \beta = 1$. Имеется возможность исследовать дуальный принцип управления, при котором управляющие воздействия носят двойственный характер [9]. С одной стороны, они призваны управлять объектом, с другой – служат для изучения его функциональных (структурных) свойств и закономерностей поведения для формирования последующих управляющих воздействий. Следовательно, структура управляющих воздействий должна меняться в соответствии с изменениями параметров системы объекта управления. Дуальное управление применяется в таких ситуациях, когда необходимо повысить интенсивность накопления информации о заранее неизвестных динамических свойствах объекта.

Каждое из слагаемых выражения (1) позволяет оценивать значимость значений параметров при оценке информационных потерь. Варьируя значениями коэффициентов α и β, мы можем детально изучать влияние $f_{p,q}$, $D_{p,q}$ на величину потерь в зависимости от величины интервала ΔQ зоны распознавания и скорости изменения состояния ресурса.

Заключение

Предлагаемая адаптивная модель обнаружения возможных уязвимостей интерфейсов в БТС на основе методов непараметрической статистики может являться основой для IT-технологий обеспечения компьютерной безопасности в условиях адаптации при быстром изменении состояния сетевого трафика в каналах связи БТС – диспетчерский центр – базовая станция. Использование адаптивной модели системы принятия решений позволяет повысить уровень правдоподобия распознавания событий, минимизировать число ложных тревог, а также обеспечить высокую реактивность системы, что особенно важно для этапов раннего обнаружения.

Работа выполнена при частичной поддержке РФФИ, гранты № 19-29-06015/19 и 19-29-06023/19.

Литература

1. Patsakis C., Dellios K., Bouroche M. Towards a distributed secure in-vehicle communication architecture for modern vehicles // Computers & Security. 2014. Vol. 40. P. 60–74.

2. Vanet security challenges and solutions: A survey / H. Hasrouny [et al.] // Vehicular Communications. 2017. Vol. 7. P. 7–20.
3. Building an automotive security assurance case using systematic security evaluations / M. Cheah [et al.] // Computers & Security. 2018. Vol. 77. P. 360–379.
4. Зегжда П.Д., Полтавцева М.А., Лаврова Д.С. Систематизация киберфизических систем и оценка их безопасности // Проблемы информационной безопасности. Компьютерные системы. 2017. № 2. С. 127–138.
5. Онтологии и безопасность автономных (беспилотных) автомобилей / О.Н. Покусаев [и др.] // International Journal of Open Information Technologies. 2019. Vol. 7. № 2.
6. Интеллектуальная система мониторинга для решения крупномасштабных научных задач в облачных вычислительных средах / А.В. Скатков [и др.] // Информационно-управляющие системы. 2017. № 2 (87). С. 19–25.
7. Skatkov A., Brykhovetskiy A., Moiseev D. Detecting changes simulation of the technological objects' information states // MATEC Web of Conferences. 2018. Vol. 224. P. 02072.
8. Кампанелла Дж. Экономика качества. Основные принципы и их применение / пер. с англ. М.: РИА Стандарты и качество, 2005. 232 с.
9. Скурихин В.И., Забродский В.А., Копейченко Ю.В. Проектирование систем адаптивного управления производством. Харьков: Высшая школа, 1984. 384 с.

Получено 15.01.2020

Скатков Александр Владимирович, д.т.н., профессор кафедры информационных технологий и компьютерных систем (ИТКС) Севастопольского государственного университета (СевГУ). 299053, Российская Федерация, г. Севастополь, ул. Университетская, 33. Тел. +7 978 784-08-84. E-mail: vm1945@mail.ru

Брюховецкий Алексей Алексеевич, к.т.н., доцент, заведующий кафедрой ИТКС СевГУ. 299053, Российская Федерация, г. Севастополь, ул. Университетская, 33. Тел. +7 978 811-62-46. E-mail: a.alexir@mail.ru

Моисеев Дмитрий Владимирович, д.т.н., профессор кафедры ИТКС СевГУ. 299053, Российская Федерация, г. Севастополь, ул. Университетская, 33. Тел. +7 978 709-29-96. E-mail: dmitriymoiseev@mail.ru

Шевченко Виктория Игоревна, к.т.н., доцент кафедры ИТКС СевГУ. 299053, Российская Федерация, г. Севастополь, ул. Университетская, 33. Тел. +7 978 767-71-73. E-mail: shevchenko-vika@mail.ru

AN ADAPTIVE MODEL FOR DETECTING THE VULNERABILITIES OF UNMANNED VEHICLES INTERFACE IN SMART CITY INFRASTRUCTURE

Skatkov A.V., Bryukhovetskiy A.A., Moiseev D.V., Shevchenko V.I.
Sevastopol State University, Sevastopol, Russian Federation
E-mail: dmitriymoiseev@mail.ru

A method of detection vulnerabilities in unmanned vehicle interfaces based on an analysis of a traffic condition in communication channels of unmanned transport systems is proposed. The approach is based on non-parametric statistics methods for assessing the information states of controlled objects, which include such unmanned vehicles resources as: communication channel, processor, memory, power supply, etc. For each of these resources, it is proposed to evaluate the change in such characteristics as the degree of load resource and its rate of change. Recognition of the state of network traffic is carried out in conditions of a lack of a priori information about the properties of the intrusion source and the stochastic nature of the recognized events. To increase the reliability level of vulnerability detection in the model, adaptive dynamic tuning of decision-making rules for classifying the information state of the traffic of unmanned vehicles is carried out.

Keywords: *unmanned vehicle, adaptive model, vulnerability detection, classification of information states, assessment matrix*

DOI: 10.18469/ikt.2020.18.1.07

Skatkov Alexander Vladimirovich, Sevastopol State University, 33, Universetetskaya Street, Sevastopol, 299053, Russian Federation; Professor, Doctor of Technical Science, Professor of information technology and computer systems. Tel. +7 978 784-08-84. E-mail: vm1945@mail.ru

Bryukhovetskiy Alexey Alexeevich, Sevastopol State University, 33, Universetetskaya Street, Sevastopol, 299053, Russian Federation; Associate Professor, PhD in Technical Science, Head of information technology and computer systems. Tel. +7 978 811-62-46. E-mail: a.alexir@mail.ru

Moiseev Dmitriy Vladimirovich, Sevastopol State University, 33, Universetetskaya Street, Sevastopol, 299053, Russian Federation; Associate Professor, Doctor of Technical Science, Professor of information technology and computer systems. Tel. +7 978 709-29-96. E-mail: dmitriymoiseev@mail.ru

Shevchenko Viktoriya Igorevna, Sevastopol State University, 33, Universetetskaya Street, Sevastopol, 299053, Russian Federation; Associate Professor, PhD in Technical Science, Associate Professor of information technology and computer systems. Tel. +7 978 767-71-73. E-mail: shevchenko-vika@mail.ru

References

1. Patsakis C., Dellios K., Bouroche M. Towards a distributed secure in-vehicle communication architecture for modern vehicles. *Computers & Security*, 2014, vol. 40, pp. 60–74.
2. Hasrouny H. et al. Vanet security challenges and solutions: A survey. *Vehicular Communications*, 2017, vol. 7, pp. 7–20.
3. Cheah M. et al. Building an automotive security assurance case using systematic security evaluations. *Computers & Security*, 2018, vol. 77, pp. 360–379.
4. Zegzhda P.D., Poltavceva M.A., Lavrova D.S. Sistematizaciya kiberfizicheskih sistem i ocenka ih bezopasnosti [Systematization of cyberphysical systems and assessment of their security]. *Problemy informacionnoj bezopasnosti. Komp'yuternye sistemy*, 2017, no. 2, pp. 127–138. (In Russian).
5. Pokusaev O.N. et al. Ontologii i bezopasnost' avtonomnyh (bespilotnyh) avtomobilej [The ontology of security and Autonomous (unmanned) vehicles]. *International Journal of Open Information Technologies*, 2019, vol. 7, no. 2. (In Russian).
6. Skatkov A.V. et al. Intellektual'naya sistema monitoringa dlya resheniya krupnomasshtabnyh nauchnyh zadach v oblachnyh vychislitel'nyh sredah [Intelligent monitoring system for solving large-scale scientific problems in cloud computing environments]. *Informacionno-upravlyayushchie sistemy*, 2017, no. 2 (87), pp. 19–25. (In Russian).
7. Skatkov A., Brykhovetskiy A., Moiseev D. Detecting changes simulation of the technological objects' information states. *MATEC Web of Conferences*, 2018, vol. 224, p. 02072.
8. Campanella J. *Ekonomika kachestva. Osnovnye principy i ih primenenie / per. s angl.* [The Economy of Quality. Basic Principles and their Application. Trans. from English]. Moscow: RIA Standarty i kachestvo, 2005, 232 p. (In Russian).
9. Skurihin V.I., Zabrodskij V.A., Kopejchenko Yu.V. *Proektirovanie sistem adaptivnogo upravleniya proizvodstvom* [Design of Adaptive Production Management Systems]. Kharkiv: Vysshaya shkola, 1984, 384 p. (In Russian).

Received 15.01.2020