УДК 004.56

МОДЕЛЬ ОБНАРУЖЕНИЯ АНОМАЛЬНЫХ ДАННЫХ НА ОСНОВЕ ИНФОРМАЦИОННОГО КРИТЕРИЯ

Брюховецкий А.А.

к.т.н., доцент

Севастопольский государственный университет

Севастополь, Россия

Аннотация

Рассматривается подход, связанный с разработкой методов обнаружения аномалий в потоках данных. Подход базируется на основе оценки статистического расстояния между распределениями вероятностей случайной величины. В качестве критерия оценки предлагается информационный критерий Дженсена-Шеннона, обеспечивающий симметричную версию дивергенции Кульбака-Лейблера. Обнаружение аномалий моделируется на примере изменения состояния ресурсов беспилотных транспортных средств под воздействием внешнего возмущения.

Ключевые слова: информационный критерий, компьютерная безопасность, обнаружение аномалий, статистическое расстояние.

ANOMALOUS DATA DETECTION MODEL BASED ON INFORMATION CRITERION

Bryukhovetskiy A.A.

Ph.D., associate professor

Sevastopol State University

Sevastopol, Russia

Abstract

An approach related to the development of methods for detecting anomalies in data streams is considered. The approach is based on an estimate of the statistical distance between the probability distributions of a random variable. As an evaluation criterion,

the Jensen-Shannon information criterion is proposed, which provides a symmetric version of the Kullback-Leibler divergence. Anomaly detection is modeled on the example of changes in the state of the resources of unmanned vehicles under the influence of external disturbances.
Keywords: information criterion, computer security, anomaly detection, statistical distance.

Разработка методов контроля информационного состояния ресурсов БТС сталкивается с новыми проблемами, вызванными увеличивающимися масштабами и сложностью транспортных сетей и, как следствие, возрастающими неоднородными потоками зашумленных данных с переменной интенсивностью в условиях дефицита априорной информации. Возникает необходимость решения задач в реальном масштабе времени с высокой достоверностью. При этом основные проблемы связаны с обработкой больших объемов данных, высокой динамикой объектов, нестационарным состоянием среды.

Автомобильные интерфейсы (CAN, LIN, FlexRay и MOST) уязвимы для различных атак кибербезопасности. Через порт бортовой диагностики (OBD) или порт USB злоумышленники могут остановить двигатель или воздействовать на тормозную систему транспортного средства и привести к аварии [1]. Атака «воспроизведения» и атака с использованием «имитации» на шину CAN описаны в [2]. Авторы [3] имитировали атаку «спуфинга (Sybil)» на шину FlexRay.

Каждый инцидент, который фиксируется в БТС, характеризуется точкой входа, которую злоумышленник использует для выполнения атаки. Открытые порты являются основным местом уязвимости, через которое проникают и распространяются вирусы. Под портом в сетевых технологиях подразумевается виртуальная «дверь», в которую можно получить доступ. Для устранения уязвимости выявляют подозрительные процессы, использующие порты [4].

Поэтому контроль над ними является первоочередной задачей для обеспечения безопасности.

Поскольку различные технологии используются в транспортных средствах, поэтому как для внутренней, так и для внешней связи с БТС имеется сравнительно много интерфейсов. В связи с тем, что сложность интерфейсных технологий варьируется в широких пределах, поэтому знание этих технологий является необходимым для оценки методов реализации атак и, следовательно, для определения выполнимости атак. Это особенно важно также для оценки возможного ущерба вследствие реализации атаки. В работах [5,6] представлены результаты моделирования процессов обнаружения аномальных данных с использованием рангового критерия Спирмена и непараметрического критерия Кульбака-Лейблера.

Предлагаемый метод обнаружения аномальных данных рассматривается на примере распознавания изменения информационных состояний ресурсов БТС, таких как, канал связи, процессор, память. К числу контролируемых признаков может относиться загрузка ресурса и скорость изменения загрузки ресурса. Значения этих характеристик могут использоваться при оценке состояния ресурса. Подход базируется на основе оценки статистического расстояния между распределениями вероятностей случайной величины за различные временные промежутки. В качестве критерия оценки предлагается информационный критерий Дженсена-Шеннона [7], обеспечивающий симметричную и нормализованную версию дивергенции Кульбака-Лейблера.

Введем обозначение $D_{KL}(P,Q)$ для вычисления расхождения (дивергенции) Кульбака-Лейблера между двумя распределениями Q и P. Тогда дивергенция определится как

$$D_{KL}(P,Q) = \sum_{i=0}^{n} Pi(x) * (\log (P_i(x) / Q_i(x)))$$

Следует отметить, что значение дивергенции KL не является симметричным:

$$D_{KL}(P,Q) \neq D_{KL}(Q,P)$$

Поэтому предлагается использовать дивергенцию Дженсена-Шеннона – D_{JS}, которая позволяет оценить расхождения между двумя вероятностными распределениями. В этом случае используется дивергенция для расчета нормализованной оценки, которая является симметричной. Это означает, что расхождение P от Q такое же, как Q от P, т.е.

$$D_{JS}(P,Q) = D_{JS}(Q,P)$$

Расхождение D_{JS} может быть определено следующим образом [7]:

$$D_{JS}(P,Q) = 1/2 * D_{KL}(P,M) + 1/2 * D_{KL}(Q,M)$$

где распределение M вычисляется как

$$M = 1/2 * (P + Q).$$

Дивергенция Дженсена — Шеннона ограничена значением единицы для двух распределений вероятности, если в дивергенции Кульбака — Лейблера используется логарифм по основанию два :

$$0 <= D_{JS}(P,Q) <= 1$$

Основное достоинство предлагаемого метода состоит в том, что он обеспечивает сглаженную и нормализованную версию дивергенции Кульбака с оценками от 0 (расхождение между распределениями отсутствует) до 1 (максимально отличающиеся распределения).

Дивергенция Дженсена — Шеннона распределения P относительно Q может быть оценена как:

$D_{JS}(P,Q) <= Z$ – отсутствие расхождения,

$D_{JS}(P,Q) > Z$ – наблюдение расхождения выборок,

где Z – предельное значение расстояния, зависящее от критичности контролируемого значения параметра объекта, которое задается экспертом. Тогда нулевая гипотеза H_0 имеет место при $D_{JS}(P,Q) <= Z$ – отсутствие расхождения. В противном случае принимается гипотеза H_1 – качественное изменение информационного состояния объекта.

С целью сравнения оценок расхождений между двумя вероятностными распределениями исследовалась модель обнаружения изменения состояния

ресурсов. В качестве информационной меры используется расстояние Дженсена — Шеннона. Определим понятие зоны оценки величины расхождения. Будем для определенности рассматривать следующие интервалы распознавания: $[0;Z_1)$, $[Z_1;Z_2)$, $[Z_2;1]$.

В зависимости от принадлежности текущего значения расстояния $JS(P,Q)=\sqrt{D_{JS}(P,Q)} \in Z_i \ (i=1,k)$ будем классифицировать следующие информационные состояния объекта на примере трех интервалов:

$0 <= JS(P,Q) < Z_1$ – отсутствие расхождения (нормальное состояние),

$Z_1 <= JS(P,Q) < Z_2$ – неустойчивая область (предкритическое состояние),

$Z_2 <= JS(P,Q) <= 1$ – наблюдение расхождения (критическое состояние).

На практике число интервалов распознавания Z_i задается экспертом и зависит от назначения объекта, его динамических свойств, требований к точности контроля, возможных рисков при контроле и т.д.

Задача оценки расхождения выборок решается по следующей алгоритмической схеме:

- Задаются входные данные: V – объём выборки, k – число интервалов гистограммы, cr – информационный критерий.
- Задаются области значений $[Z_{i-1};Z_i]$ – ширина зон распознавания критерия проверки информационных ситуаций: отсутствия расхождений / неустойчивой области расхождений / наличие расхождений.
- Генерируются выборки X объема V из генеральной совокупности с заданным законом распределения.
- Выполняется статистическая обработка данных и строятся гистограммы распределения значений контролируемого параметра для выборок P и Q .
- Вычисляется значение расстояния $JS(P,Q)$ и определяется его принадлежность заданным зонам распознавания.

В соответствии с поставленными задачами были проведены эксперименты, в ходе которых определялось влияние ряда значений параметров на изменения информационного состояния ресурсов: объемы выборок - V, число интервалов

гистограммы – k, ширина интервалов $[Z_{i-1};Z_i]$ оценки состояния ресурса. Ниже представлены результаты моделирования.

1. Исследование влияния объема выборок – V. Задано: зоны классификации состояния ресурсов $[Z_{i-1};Z_i]$ для трех состояний, отличающихся шириной интервалов. Число интервалов k=3. Сравнивались оценки расхождений для распределений P и Q для случаев, когда границы зон распознавания отличались незначительно (однородные) и существенно (неоднородные). Были заданы следующие границы зон распознавания:

- интервалы-1 {0; 0,50; 0,80 ; 1},
- интервалы-2 {0; 0,40; 0,60 ; 1},
- интервалы-3 {0; 0,30; 0,70 ; 1},
- интервалы-4 {0; 0,10; 0,50 ; 1},

Ширина интервалов-1,2,3 между собой отличается незначительно, а ширина интервалов – 4 существенно отличается от остальных. Каждый эксперимент повторялся 20 раз. На рис.1 представлены значения расстояния $JS(P,Q)$ при сравнений распределений выборок для различных значений интервалов: эксп 1-2, эксп 1-4 при V=30.

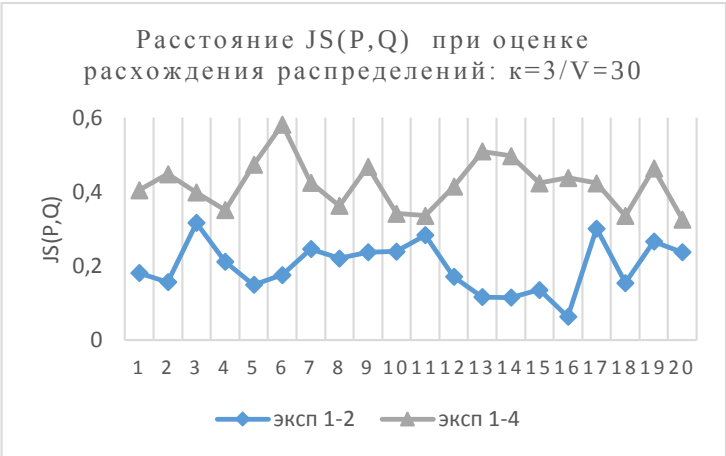

Рис.1 - Расстояние $JS(P,Q)$ при оценке расхождения делений : $k=3$ / V=30. Авторская разработка

В проведенных экспериментах при сравнении интервалов 1-2 – эксп1-2 максимальное расстояние составляло 0,32, а минимальное – 0,06, в то время как

в экспериментах 1-4 оно составляло, соответственно – 0,58 и 0,33. Аналогичные эксперименты проводились при оценке расхождений для выборок *V*=40, 60 и 100.

На рис.2 представлены значения расстояния *JS(P,Q)* при сравнении распределений выборок для различных интервалов: эксп1-2, эксп2-3, эксп 1-4 при *V*=100.

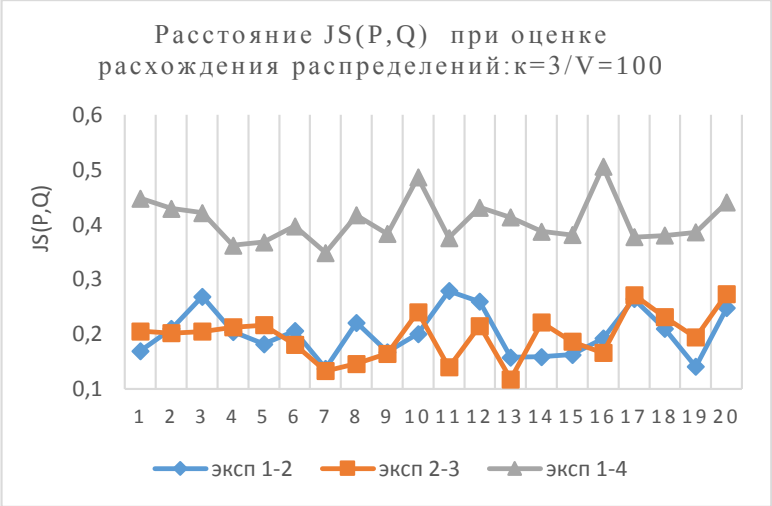

Рис.2 - Расстояние *JS(P,Q)* при оценке расхождения распределений эксп 1-2, эксп 2-3, эксп 1-4: k=3 / *V*=100. Авторская разработка

В экспериментах эксп1-2, эксп2-3 максимальное расстояние составляло 0,28, а минимальное – 0,12, в то время как для неоднородных выборок в экспериментах 1-4 оно составляло соответственно – 0,51 и 0,35. Таким образом при увеличении объема выборки мы наблюдаем увеличение расстояния между однородными и неоднородными распределениями за счет уменьшения значения СКО. При этом *max(JS(P,Q))*=0,28 для однородных распределений 1-2, 2-3 меньше, чем минимальное расстояние для неоднородных распределений 1-4: *min(JS(P,Q))=0,35*. Этот факт свидетельствует о повышении достоверности классификации состояний объектов и уменьшении числа ошибок 1-ого и 2-ого рода.

На рис.3 представлена зависимость величины среднеквадратического отклонения СКО расстояния *JS(P,Q)* между однородными 1-2, 2-3 и неоднородными 1-4 распределениями в зависимости от объема *V* при *k*=3. На

рисунке видно, что наблюдается тенденция уменьшения величины СКО от увеличения объема *V* во всех экспериментах. Результаты экспериментов являются подтверждением того, что при возрастании объемов *V* значение среднеквадратического отклонения (длина доверительного интервала для заданного уровня достоверности – α) уменьшается пропорционально корню квадратному из объема выборки – *V*.

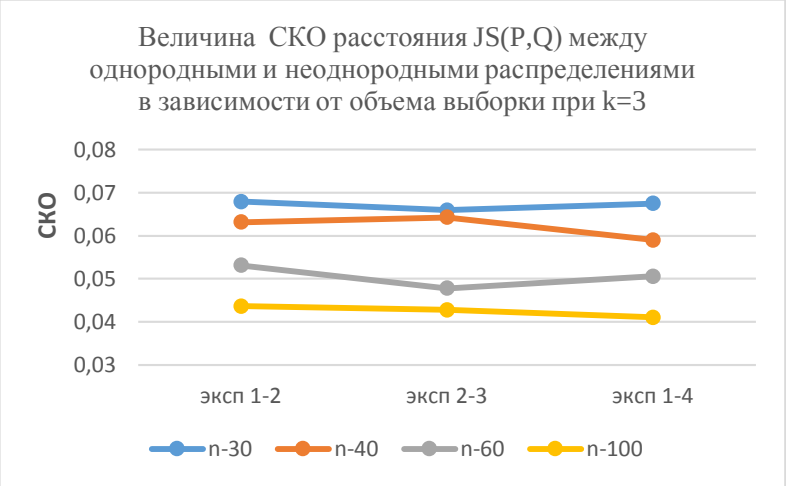

Рис.3 - Величина СКО расстояния *JS(P,Q)* между однородными и неоднородными распределениями в зависимости от объема выборки при *k*=3.

Авторская разработка

2. Исследование влияния объема выборок – *V* при измененном числе интервалов *k*=4. Задано: зоны классификации состояния ресурсов $[Z_{i-1};Z_i]$ для четырех состояний, отличающихся шириной интервалов. Число интервалов *k*=4. Были заданы следующие границы зон распознавания:

- интервалы-1 {0; 0,30;0,60; 0,90 ; 1},
- интервалы-2 {0; 0,20;0,40; 0,80 ; 1},
- интервалы-3 {0; 0,10;0,30; 0,50 ; 1}.

Эксперименты проводились по сценарию предыдущего. Первая пара выборок 1-2 незначительно отличается по ширине интервалов, в то время как вторая пара 1-3 – существенно. На рис.4 представлены значения расстояния *JS(P,Q)* при сравнении распределений выборок для различных значений интервалов: эксп1-2, эксп1-3 при объеме выборки *V*=100.

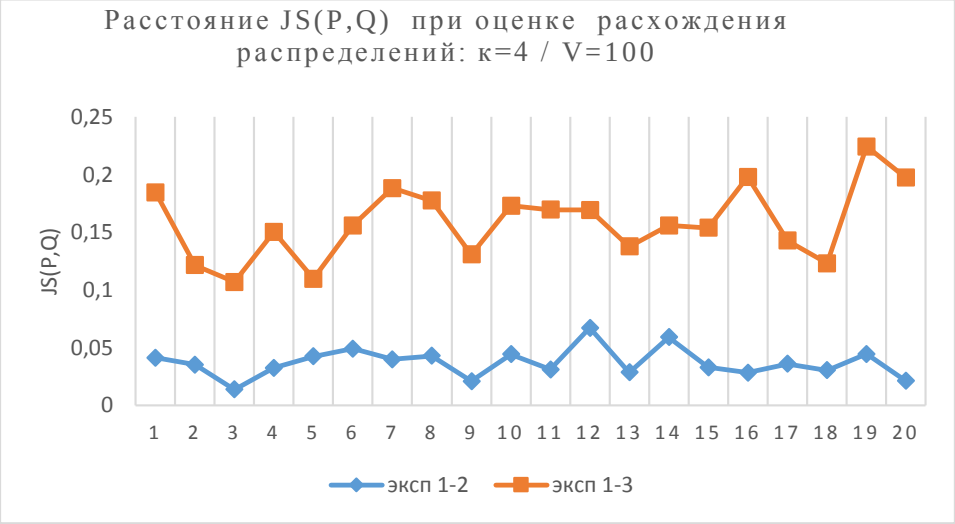

Рис.4 - Расстояние JS(P,Q) при оценке расхождения распределений эксп 1-2, эксп 1-3 *: k*=4 / *V*=100. Авторская разработка

В таблице 1 представлены значения расстояния *JS(P,Q)* для *k*=4 и *V*=30, 100. Следует констатировать, что разброс между максимальными и минимальными значениями расстояния *JS(P,Q)* при увеличении объема уменьшился: при сравнении однородных выборок он составил 0,05, а неоднородных – 0,12 при *V*=100 , а при *V*=30 соответственно составил 0,19 и 0,25.

Таблица 1. Значения расстояния *JS(P,Q)* для *k*=4 и *V*=30, 100

Объемы выборок	*V*=30		*V*=100	
	эксп 1-2	эксп 1-3	эксп 1-2	эксп 1-3
max	0,312898	0,571586	0,067323	0,224536
min	0,124797	0,324762	0,013745	0,106922
СРЗНАЧ	0,201451	0,429998	0,037132	0,158575
Δ	0,188101	0,246824	0,053578	0,117614

Эта тенденция наблюдается в других экспериментах при увеличении объема выборки. Аналогичные эксперименты проводились при оценке расхождений для выборок *V*=30, 40, 60 и 100 и числе интервалов *k*=5, 7 и других.

Выводы. Результаты, полученные при проведении экспериментов, позволяют заключить, что предложенная модель Дженсена — Шеннона обеспечивает статистическую устойчивость при оценке изменений состояния ресурсов БТС при увеличении объема выборок и числа интервалов. Оценки по выбору значений указанных величин приводятся в [8]. В проведенных экспериментах лучшие оценки были получены при *V=100, k=5*, худшие при *V=30, k*=3. При малой ширине зон распознавания $[Z_{i-1};Z_i]$ и малом объеме выборок встречались ситуации, когда отдельные интервалы гистограмм содержали нулевые значения.

Таким образом, полученные результаты исследования модели на основе информационной меры Дженсена-Шеннона подтверждают факты наличия возмущений при оценке изменения состояния объектов. Основными достоинствами предлагаемого метода являются: невысокая вычислительная трудоемкость, чувствительность к внешним воздействиям и к изменениям состояния ресурсов. Поэтому оценка изменения состояния ресурсов (неоднородности) за различные промежутки времени может использоваться для обнаружения внешних воздействий на БТС.

В планах будущих исследований предполагается выполнить эксперименты по аппроксимации значений гистограмм непрерывными функциями плотности распределения вероятностей и провести оценку ошибок 1-ого и 2-ого рода при распознавании состояния ресурсов.

Исследование выполнено при финансовой поддержке РФФИ в рамках научных проектов № 19-29-06015/20, № 19-29-06023/20, № 18-47-92007/20.

Библиографический список:

1. L. Pan, X. Zheng, H. Chen, et al .Cyber security attacks to modern vehicular systems// Journal of Information Security and Applications. 2017. vol. 36 – pp. 90–100.

2. M. Markovitz and A. Wool. Field classification, modeling and anomaly detection in unknown can bus networks// Vehicular Communications. 2017 vol. 9. – pp. 43–52.

3. D. K. Nilsson, U. E. Larson, F. Picasso, et al. A first simulation of attacks in the automotive network communications protocol flexray// Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems CISIS'08.Springer. 2009 – pp. 84–91.

4. Top 20 and 200 most scanned ports in the cybersecurity industry// SecurityTrails blog, may 07 2019 securitytrails team, https://securitytrails.com/blog/top-scanned-ports

5. А.А. Брюховецкий, А.В. Скатков, Ю.Е. Шишкин. Моделирование процессов обнаружения аномалий в сложноструктурированных данных мониторинга // Системы контроля окружающей среды,2017, №9 (29). – с.45-49.

6. Скатков А.В., Брюховецкий А.А., Моисеев Д.В. Мера Кульбака в задачах динамической кластеризации наблюдений состояния окружающей среды // Системы контроля окружающей среды. № 3 (37). 2019 – С. 35–38.

7. Frank Nielsen and Richard Nock. Total Jensen divergences: definition, properties and clustering// In 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pages 2016–2020.

8. Ю.Н. Орлов. Оптимальное разбиение гистограммы для оценивания выборочной плотности функции распределения нестационарного временного ряда // Препринты ИПМ им. М.В.Келдыша, 2013, № 14. – 26 с. URL: http://library.keldysh.ru/preprint.asp?id=2013-14

Оригинальность 88%