УДК 004.056.5 + 004.021

Микова С. Ю., Оладько В. С.

ОЦЕНКА КАЧЕСТВА АЛГОРИТМА ОБНАРУЖЕНИЯ СЕТЕВЫХ АНОМАЛИЙ НА ОСНОВЕ ДИСКРЕТНОГО ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ С ПОМОЩЬЮ F-МЕРЫ

В работе рассматривается проблема оценки качества алгоритмов обнаружения сетевых аномалий. В качестве показателя качества используется гармоническая F-мера. Предложена методика исследования качества алгоритма. Приводится количественная оценка показателей полноты, точности F-меры. Проведены экспериментальные исследования качества алгоритма обнаружения сетевых аномалий на основе дискретного вейвлет-преобразования, показывающие зависимость качества алгоритма от размера скользящего окна.

Ключевые слова: *классификация, сетевая атака, точность, полнота*

Mikova S. Yu., Oladko V. S.

ASSESSMENT OF QUALITY OF NETWORK ANOMALIES DETECTION ALGORITHM BASED ON DISCRETE WAVELET TRANSFORMS USING THE F-MEASURE

The paper considers the problem of quality assessment algorithms detect network anomalies The quality of the algorithms proposed to estimate the harmonic F-measure. Method of research quality of the algorithm proposed. Quantitative assessment of the completeness, accuracy, F-measure is provided. Experimental study of the quality of network anomalies detection algorithm based on discrete wavelet transform, showing the dependence of the quality of the algorithm on the size of the sliding window.

Keywords: *classification, network attack, accuracy, completeness.*

Вторжение в систему злоумышленника может привести к утечке, искажению или недоступности данных, обрабатываемых в информационных системах организаций и в технологических сетях предприятия. Часто аномалия в сети – это один из признаков сетевой атаки злоумышленника [1]. Существует много алгоритмов обнаружения сетевых аномалий. Каждый из алгоритмов имеет свои особенности реализации, количество и тип анализируемых параметров сетевого трафика и/или сетевых пакетов. При этом в процессе обнаружения аномалий каждым из существующих алгоритмов решается за-

Таблица 1. Возможные результаты классификации аномалий

Класс A=anomaly		Принадлежность к классу A	
		ДА	НЕТ
Результат Классификации	Правильный	Truepositive (TP) *anomaly* ⟶ *anomaly*	Falsepositive (FP) *normal* ⟶ *anomaly* (Ошибка второго рода)
	Неправильный	Falsenegative (FN) *anomaly* ⟶ *normal* (Ошибка первого рода)	Truenegative (TN) *normal* ⟶ *normal*

Где TP - истино-положительное решение (правильно обнаруженные аномалии); FP - ложно-положительное решение (ошибки второго рода); FN - ложно-отрицательное решение (ошибки первого рода); TN - истино-отрицательное решение.

дача классификации. И от того, насколько точно и достоверно в результате классификации анализируемых данных будет принято решение о принадлежности их к аномалии или нет, будет напрямую зависеть качество алгоритма. Чем выше качество алгоритма обнаружения сетевых аномалий, тем более вероятно, что программное средство, реализующее данный алгоритм, способно выявить аномалию или возможную атаку в сети предприятия с минимальными пропусками или ложными срабатываниями. Следовательно, актуально решение задач, связанных с оценкой качества алгоритмов обнаружения сетевых аномалий.

Процедура оценки качества алгоритма обнаружения сетевых аномалий. Так как при обнаружении аномалии алгоритмов в первую очередь решается задача классификации, то авторами в данной работе в качестве основного критерия качества алгоритма предлагается использовать F-меру, которая представляет собой функцию от полноты и точности алгоритма. Под точностью, полнотой и F-мерой понимается следующее [2, 3]:

1) точность – это отношение правильно обнаруженных аномалий алгоритмом к сумме правильно обнаруженных аномалий алгоритмом и ошибок второго рода;

2) полнота – это отношение правильно обнаруженных аномалий алгоритмом к сумме правильно обнаруженных аномалий алгоритмом и ошибок первого рода;

3) F-мера – это удвоенное отношение произведения оценок полноты и точности к сумме оценок полноты и точности.

Таким образом, чем меньше будет ошибок первого и второго рода при обнаружении аномалий, тем более полным и точным будет алгоритм по их обнаружению [3]. Возможные результаты классификации аномалий алгоритмами обнаружения сетевых аномалий представлены в таблице 1.

Из определения полноты следует, что она вычисляется по следующей формуле 1:

$$Recall = \frac{TP}{TP + FN} \quad (1)$$

Из определения точности следует, что она вычисляется по следующей формуле 2:

$$Precision = \frac{TP}{TP + FP} \quad (2)$$

Из определения F-меры следует, что она вычисляется по следующей формуле 3:

$$F = 2\frac{Precision*Recall}{Precision + Recall} \quad (3)$$

В качестве объекта исследования авторами был выбран алгоритм обнаружения сетевых аномалий на основе дискретного вейвлет-преобразования (ДВП). Для оценки качества классификации алгоритмом был разработан программный комплекс, который в процессе функционирования позволяет собрать следующие данные, характеризующие алгоритм:

1) ошибки первого рода – FN;

2) ошибки второго рода – FP;

3) количество правильно идентифицированных аномалий – TP.

На основании собранных данных проводится оценка полноты и точности алгоритма, на основании которых затем вычисляется значение F-меры.

Методика оценки качества алгоритма с использованием в качестве инструментального средств разработанного программного комплекса может быть представлена в виде следующей последовательности шагов:

1) Установить необходимый минимальный размер окон в программе.

2) Для текущего размера окна сгенерировать модель трафика с заданным числом аномалий (N) и числом интервалов (M).

3) Обработать текущую модель с помощью алгоритма ДВП. Перенести значения N, TP, FN, FP в таблицу.

4) Повторить шаги 2–3 несколько раз для более точной вероятностной оценки.

5) Посчитать математическое ожидание для TP, FN, FP.

6) Посчитать точность и полноту по формулам (1) и (2) для текущего размера окна и текущего числа аномалий.

7) Повторить шаги 2–6 для других значений N при том же значении M. Для полноты и качества анализа желательно взять значения показательной функции от ряда чисел. Например, $N = 2^x$, где x = [1, 2, 3…9] при M = 2200.

8) Посчитать среднее для точности и полноты для текущего размера окна.

9) Увеличить размер окна и повторить шаги 1–8. В приведенном примере размеры окон принимались от 10 до 30 с шагом 5.

Экспериментальные исследования точности и полноты алгоритма дискретного вейвлет-преобразования. Входными данными при проведении экспериментов являются: размер окна 1 (W1), размер окна 2 (W2), число интервалов (I=2200) и количество поданных аномалий (A). Экспериментальные исследования состояли из пяти опытов для каждой выборки значений входных данных, приведенных в таблице 2.

Таблица 2. Значение выборок входных данных экспериментальных исследований

Параметры	Значение параметров									
№ выборки	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
W1	15	15	15	15	15	15	15	15	15	15
W2	10	10	10	10	10	10	10	10	10	10
A	1	2	4	8	16	32	64	128	256	512
№ выборки	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
W1	20	20	20	20	20	20	20	20	20	20
W2	15	15	15	15	15	15	15	15	15	15
A	1	2	4	8	16	32	64	128	256	512
№ выборки	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**
W1	25	25	25	25	25	25	25	25	25	25
W2	20	20	20	20	20	20	20	20	20	20
A	1	2	4	8	16	32	64	128	256	512

Затем на каждой выборке входных значений был проведён анализ сетевого трафика на предмет аномалий и для полученных результатов алгоритма вычислены значения полноты и точности по формулам 1, 2. Пример проведения анализа результатов работы алгоритма ДВП для входного параметра размер окна W= 10 представлен в таблице 3.

Таблица 3. Анализ результатов работы алгоритма ДВП для размера окон W1 = 15, W2 = 10

W1	15	15	15	15	15	15	15	15	15	15
W2	10	10	10	10	10	10	10	10	10	10
I	2200	2200	2200	2200	2200	2200	2200	2200	2200	2200
A	1	2	4	8	16	32	64	128	256	512
Опыт 1										
TP	1	1	2	5	10	20	26	6	4	0
FN	7	12	24	44	90	196	267	136	7	0
FP	0	1	2	3	6	12	38	122	152	512

Опыт 2										
TP	1	1	4	5	12	18	26	8	2	0
FN	12	18	32	52	104	159	274	95	5	0
FP	0	0	0	3	4	14	38	120	253	512
Опыт 3										
TP	1	1	2	4	6	18	22	10	2	0
FN	14	17	30	43	64	174	266	142	4	1
FP	0	1	2	4	10	14	42	118	254	512
Опыт 4										
TP	1	2	3	5	10	20	20	10	1	0
FN	3	14	31	49	101	182	270	139	6	0
FP	0	0	1	3	6	12	44	118	255	512
Опыт 5										
TP	0	0	2	6	15	19	25	8	0	1
FN	6	2	21	57	126	187	300	98	6	0
FP	1	2	2	2	1	13	39	120	256	512
Результирующая оценка алгоритма ДВП										
$TP_{средн.}$	0,8	1	2,6	5	10,6	19	23,8	8,4	1,8	0,2
$FN_{средн.}$	8,4	12,6	27,6	49	97	179,6	275,4	122	5,6	0,2
$FP_{средн.}$	0,2	0,8	1,4	3	5,4	13	40,2	119,6	234	512
Precision	0,8	0,55	0,65	0,62	0,66	0,593	0,37	0,065	0,007	0,00039
Recall	0,086	0,073	0,086	0,092	0,098	0,095	0,07	0,064	0,24	0,5

Далее по формуле 3 была рассчитана F-мера, зависящая от оценок полноты и точности для каждой выборки. Полученные значения F-меры представлены в таблице 4.

Таблица 4. Значения F-меры доя алгоритма ДВП

W1	15	15	15	15	15	15	15	15	15	15
W2	10	10	10	10	10	10	10	10	10	10
F	**0,156**	**0,129**	**0,152**	**0,161**	**0,171**	**0,164**	**0,131**	**0,065**	**0,148**	**0,00072**
W1	20	20	20	20	20	20	20	20	20	20
W2	15	15	15	15	15	15	15	15	15	15
F	**0,095**	**0,027**	**0,008**	**0,01**	**0,002**	**0,0014**	**0,0081**	**0,0056**	**0,0015**	**0,00075**
W1	25	25	25	25	25	25	25	25	25	25
W2	20	20	20	20	20	20	20	20	20	20
F	**0,073**	**0,022**	**0,004**	**0,007**	**0,001**	**0,005**	**0,007**	**0,003**	**0,0091**	**0,00077**

Для того чтобы более наглядно увидеть зависимость размера окна от F-меры, было рассчитано среднее значение F-меры для каждого размера окна. Результаты представлены в таблице 5 и на рисунке 1.

Таблица 5. Среднее значения F-меры для алгоритма ДВП

Размер окна	W1=15 W2=10	W1=20 W2=15	W1=25 W2=20
F	0,114	0,016	0,013

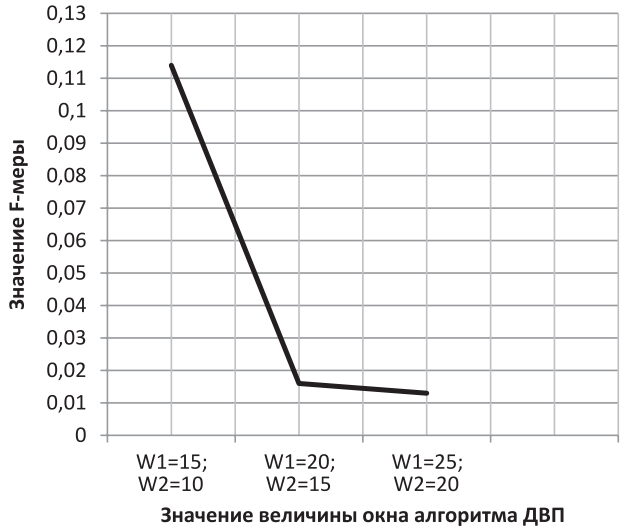

Рис.1. Зависимость F-меры от размера окна

Анализ полученных результатов исследования F-меры алгоритма дискретного вейвлет-преобразования показывает, что средние значения F-меры алгоритма напрямую зависят от такого входного параметра алгоритма, как размер окна. Чем меньше значение окна скользящего алгоритма, тем более высокое значение принимает F-мера, показывая лучшие значения (F=0,114) при величине окна W1=15;W2=10. Следовательно, можно сделать вывод, что для получения большего качества классификации алгоритмом необходимо при возможности минимизировать значение окон W1 и W2. А поскольку F-мера – это метрика, которая гармонически объединяет информацию о точности и полноте анализируемого алгоритма, то при использовании алгоритма ДВП для обнаружения сетевых аномалий необходимо еще в процессе обучения провести калибровку точности и полноты, варьируя значения окон W1 и W2, так как увеличение данных оценок влияет на увеличение качества классификации.

Примечания

1. Мельников Д. А., Петров В. Р., Радько А. Н., Бурый Д. С., Хрусталев С. А. Обнаружение уязвимостей информационно-технологических систем на основе анализа сетевого трафика//Безопасность информационных технологий. – 2013. - № 4. – С. 83–87.

2. Амелькин С. А. Оценка эффективности рекомендательных систем //Труды 14-й Всероссийской научной конференции «Электронные библиотеки: перспективные методы и технологии, электронные коллекции» — RCDL-2012, Переславль-Залесский, Россия, 15–18 октября 2012 г. – С. 288–291.

3. Микова С. Ю., Оладько В. С., Нестеренко М. А., Кузнецов И. А. Критерии оценки качества алгоритмов обнаружения сетевых аномалий // Международный научно-исследовательский журнал. – 2015. - № 4 (35) – С. 87–88.

Микова Софья Юрьевна, студент, кафедра «Информационная безопасность», ФГАОУ ВПО «Волгоградский государственный университет». E-mail: sofya_mikova@mail.ru

Mikova Sophia Yurievna student, Department of «Information Security», Volgograd State University. E-mail: sofya_mikova@mail.ru

Оладько Владлена Сергеевна, кандидат технических наук, доцент кафедры «Информационная безопасность», ФГАОУ ВПО «Волгоградский государственный университет», (8442) 46-03-68. E-mail: oladko.vs @yandex.ru

Oladko Vladlena Sergeevna, PhD (Engineering), Associate Professor of Information Security of «Information Security» department, Volgograd State University, (8442) 46-03-68. E-mail: oladko.vs@yandex.ru