тически значимым и имеющим потенциал по применению в актуальных задачах, требующих надёжного сокрытия алгоритмов.

Выводы

Предложен новый механизм обфускации на основе искусственных нейронных сетей и доказано его соответствие требованиям функционального обфускатора неразличимости. Отмечены его основные свойства, перспективы дальнейших исследований и практического применения.

ЛИТЕРАТУРА

1. *Venkatesh S. and Ertaul L.* Novel obfuscation algorithms for software security // Proc. Intern. Conf. SERP'05. 2005. V. 1. P. 209–215.
2. *Варновский Н. П., Захаров В. А., Кузюрин Н. Н.* Математические проблемы обфускации // Математика и безопасность информационных технологий. Материалы конф. в МГУ 28–29 октября 2004 г. М.: МЦНМО, 2005. С. 65–91.
3. *Barak B., Goldreich O., Impagliazzo R., et al.* On the (im)possibility of obfuscating programs // Crypto'01. LNCS. 2001. V. 2139. P. 1–18.
4. *Goldwasser S. and Guy N. R.* On best-possible obfuscation // J. Cryptology. 2007. No. 27. P. 480–505.
5. *Garg S., Gentry C., Halevi S., et al.* Candidate indistinguishability obfuscation and functional encryption for all circuits // Proc. 54th IEEE Ann. Symp. FOCS'13. October 26–29, 2013. P. 40–49.
6. *Albrecht M. R., Cocis C., Laguillaumie F. and Langlois A.* Implementing candidate graded encoding schemes from ideal lattices // ASIACRYPT 2015. LNCS. 2015. V. 9453. P. 752–775.
7. *Ma H., Ma X., Liu W., et al.* Control flow obfuscation using neural network to fight concolic testing // 10th Intern. ICST Conf., SecureComm 2014, Beijing, China, September 24–26, 2014. Part I. P. 287–304.
8. *Yan Wang* Obfuscation with Turing Machine. A Thesis in Information Sciences and Technology. Pennsylvania State University, 2017. 42 p.
9. *Хайкин С.* Нейронные сети: полный курс. 2-е изд. М.: Вильямс, 2008.
10. *Алексеев Д. В.* Приближение функций нескольких переменных нейронными сетями // Фундаментальная и прикладная математика. 2009. Т. 15б. № 3. С. 9–21.
11. *Hecht-Nielsen R.* Kolmogorov's mapping neural network existence theorem // IEEE First Ann. Int. Conf. Neural Networks. San Diego, 1987. V. 3. P. 11–13.

УДК 519.21 DOI 10.17223/2226308X/12/47

ОЦЕНКА ВЕРОЯТНОСТИ УСПЕШНОЙ АТАКИ НАРУШИТЕЛЯ В БЛОКЧЕЙН-СЕТИ

И. В. Семибратов, В. М. Фомичев

Рассмотрена вероятностная модель, определяющая начала активных периодов функционирования злоумышленника и майнера как случайные величины, распределённые по биномиальному закону. Получены оценки вероятностей успешной атаки злоумышленника (создания ложного блока данных) при различных исходных условиях. Результаты вычислений подтвердили естественные предположения, что вероятность успешной атаки злоумышленника убывает как с ростом положительной разности длительностей сеансов майнера и злоумышленника, так и с ростом числа активных майнеров, и возрастает с ростом в положительном

диапазоне разницы между ожидаемым временем начала сеанса майнера и временем начала сеанса злоумышленника.

Ключевые слова: *блокчейн, майнер, механизм консенсуса, хеш-функция, биномиальное распределение вероятностей.*

Введение

Технология блокчейн (БЧ) направлена на создание в децентрализованной системе цепей, состоящих из блоков достоверных данных. Последующие блоки цепи возникают после подтверждения аутентичности предыдущих блоков в результате поиска входного слова x хэш-функции по её значению. Центральный вопрос успешности технологии БЧ состоит в необходимости достичь консенсуса пользователей информационной системы в вопросе добавления блоков в цепь при отсутствии взаимного доверия. Один из базовых тезисов в части безопасности состоит в том, что число злоумышленников, стремящихся создавать блоки ложных данных, должно быть меньше числа майнеров — добропорядочных пользователей, участвующих в создании новых блоков данных.

Представлена вероятностная модель креативной деятельности одного злоумышленника и m майнеров в течение временного периода (суток), $m \geqslant 1$. В рамках модели при различных параметрах оценена вероятность $P_{1,m}$ успешной атаки злоумышленника (создания блока ложных данных).

1. Оценка вероятности успешной атаки злоумышленника

Длительность временных отрезков измеряется в условных единицах (у.е.), где за 1 у.е. принят 10-минутный отрезок, который в настоящее время считается достаточным для того, чтобы некоторые майнеры отыскали слово x. Разделим временную ось на периоды длины $t = 144$ у.е., что соответствует одним суткам. Положим, что за период длины t каждый участник отрабатывает отрезок времени (сеанс), где длительность сеанса злоумышленника равна θ и майнера — τ, $0 < \theta, \tau \leqslant t/2$. При $m \geqslant 1$ положим $r = \tau - \theta \geqslant 0$, иначе злоумышленник гарантированно совершает успешную атаку.

Пусть начало сеанса совпадает с началом одного из отрезков, то есть с одним из моментов времени $0, 1, \ldots, t - t_0$, где $t_0 = \theta$ для злоумышленника и $t_0 = \tau$ для майнера. Тогда конец сеанса совпадает с одним из моментов времени $t_0, t_0 + 1, \ldots, t$. В данных условиях $t - \theta$ и $t - \tau$ суть суммарные длительности отрезков времени, когда пассивны (то есть не участвуют в действиях по развитию БЧ) злоумышленник и майнер соответственно.

Пусть вычислительные мощности всех участников равны. Атаку злоумышленника в период длины t признаем успешной, если найдётся отрезок, когда злоумышленник активен, а майнер пассивен.

Обозначим $\xi_{\text{з}}$ и $\xi_{\text{м}}$ случайные моменты начала сеанса злоумышленника и майнера соответственно. Рассчитаем вероятность успешной атаки злоумышленника в предположении, что данные величины распределены по биномиальному закону [1] на сегментах $[a_{\text{з}} - \theta/2, a_{\text{з}} + \theta/2]$ и $[a_{\text{м}} - \tau/2, a_{\text{м}} + \tau/2]$ со средними значениями $a_{\text{з}}$ и $a_{\text{м}}$ соответственно:

$$b_i = \mathsf{P}[\xi_{\text{з}} = a_{\text{з}} \pm i] = 2^{-\theta} \mathrm{C}_{\theta}^{\theta/2-i}, \ i = 0, 1, \ldots, \theta/2; \tag{1}$$

$$a_i = \mathsf{P}[\xi_{\text{м}} = a_{\text{м}} \pm i] = 2^{-\tau} \mathrm{C}_{\tau}^{\tau/2-i}, \ i = 0, 1, \ldots, \tau/2. \tag{2}$$

Функции вероятности для биномиального распределения случайных величин $\xi_{\text{з}}$ и $\xi_{\text{м}}$ симметричны относительно точек $a_{\text{з}}$ и $a_{\text{м}}$ соответственно. Злоумышленник и майнеры выбирают начало сеанса случайно и независимо друг от друга с вероятностью, заданной формулами (1) и (2).

Рассмотрим некоторые случаи с одним злоумышленником и с различным числом майнеров при $t = 144$. При фиксированных τ и θ обозначим $P_m(\tau, \theta)$ вероятность успешной атаки злоумышленника, которому противодействуют m майнеров, $m \geqslant 1$; $p_i = \mathsf{P}[\xi_{\text{м}} > i]$, $q_i = \mathsf{P}[\xi_{\text{м}} < i]$, $a_{\text{м}} - \tau/2 \leqslant i \leqslant a_{\text{м}} + \tau/2$. Из (2) следует:

$$p_i = \sum_{j=i+1}^{a_{\text{м}}+\tau/2} a_j = 2^{-\tau} \sum_{j=i+1}^{\tau} \mathrm{C}_\tau^j, \quad q_i = \sum_{j=a_{\text{м}}-\tau/2}^{i-1} a_j = 2^{-\tau} \sum_{j=0}^{i-1} \mathrm{C}_\tau^j = 1 - p_i - \mathrm{C}_\tau^i, \ i = 1, \ldots, \tau.$$

По формуле полной вероятности из (1) и (2) получаем

$$P_{1,m}(\tau, \theta) = \sum_{i=a_{\text{з}}-\theta/2}^{a_{\text{з}}-\theta/2+r} b_i p_i^m + \sum_{i=a_{\text{з}}-\theta/2+r+1}^{a_{\text{з}}+\theta/2-\tau} b_i (q_{i-r} + p_i)^m + \sum_{i=a_{\text{з}}+\theta/2-\tau+1}^{a_{\text{з}}+\theta/2} b_i q_{i-r}^m.$$

Данное равенство можно записать иначе:

$$P_{1,m}(\tau, \theta) = \sum_{i=a_{\text{з}}-\theta/2}^{a_{\text{з}}+\theta/2} b_i (q_{i-r} + p_i)^m. \tag{3}$$

Здесь $q_i = 0$ при $i \leqslant a_{\text{м}} - \tau/2$ и $p_i = 0$ при $i \geqslant a_{\text{м}} + \tau/2$.

По формуле (3) посчитаны вероятности $P_{1,m}(\tau, \theta)$ при параметрах $(a_{\text{з}}, a_{\text{м}}) \in \in \{(36, 36); (36, 40); (36, 44); (36, 48)\}$. Результаты даны в табл. 1–3.

Таблица 1

Значения вероятностей $P_{1,1}(\tau, \theta)$

(τ, θ)	$a_{\text{з}} = a_{\text{м}} = 36$	$a_{\text{з}} = 36, a_{\text{м}} = 40$	$a_{\text{з}} = 36, a_{\text{м}} = 44$	$a_{\text{з}} = 36, a_{\text{м}} = 48$
(72,4)	0,4544	0,7889	0,9577	0,9960
(72,8)	0,4555	0,7830	0,9535	0,9952
(72,12)	0,4566	0,7774	0,9494	0,9942
(72,16)	0,4576	0,7721	0,9454	0,9931
(72,20)	0,4585	0,7671	0,9413	0,9920
(72,24)	0,4594	0,7624	0,9373	0,9908
(72,28)	0,4602	0,7579	0,9334	0,9895
(72,32)	0,4610	0,7537	0,9295	0,9882
(72,36)	0,4617	0,7496	0,9257	0,9868
(72,40)	0,4624	0,7457	0,9220	0,9853
(72,44)	0,4630	0,7420	0,9183	0,9839
(72,48)	0,4637	0,7385	0,9147	0,9823
(72,52)	0,4643	0,7351	0,9111	0,9808
(72,56)	0,4665	0,7320	0,9077	0,9792
(72,60)	0,4799	0,7307	0,9044	0,9776
(72,64)	0,5382	0,7416	0,9031	0,9761
(72,68)	0,6898	0,7981	0,9148	0,9768
(72,72)	0,9336	0,9468	0,9726	0,9910

Таблица 2

Значения вероятностей $P_{1,4}(\tau, \theta)$

(τ, θ)	$a_з = a_м = 36$	$a_з = 36, a_м = 40$	$a_з = 36, a_м = 44$	$a_з = 36, a_м = 48$
(72,4)	0,0532	0,4037	0,8436	0,9843
(72,8)	0,0637	0,4072	0,8324	0,9809
(72,12)	0,0737	0,4104	0,8220	0,9773
(72,16)	0,0832	0,4133	0,8124	0,9734
(72,20)	0,0922	0,4159	0,8036	0,9694
(72,24)	0,1006	0,4183	0,7954	0,9653
(72,28)	0,1086	0,4205	0,7878	0,9610
(72,32)	0,1161	0,4226	0,7807	0,9568
(72,36)	0,1233	0,4245	0,7741	0,9525
(72,40)	0,1301	0,4262	0,7679	0,9482
(72,44)	0,1365	0,4279	0,7621	0,9439
(72,48)	0,1427	0,4294	0,7566	0,9336
(72,52)	0,1485	0,4309	0,7515	0,9354
(72,56)	0,1541	0,4322	0,7467	0,9313
(72,60)	0,1599	0,4337	0,7421	0,9272
(72,64)	0,1749	0,4387	0,7390	0,9233
(72,68)	0,2760	0,4860	0,7528	0,9237
(72,72)	0,7634	0,8087	0,8993	0,9660

Таблица 3

Значения вероятностей $P_{1,16}(\tau, \theta)$

(τ, θ)	$a_з = a_м = 36$	$a_з = 36, a_м = 40$	$a_з = 36, a_м = 44$	$a_з = 36, a_м = 48$
(72,4)	0,0001	0,0438	0,5283	0,9395
(72,8)	0,0004	0,0608	0,5231	0,9281
(72,12)	0,0011	0,0764	0,5195	0,9167
(72,16)	0,0023	0,0906	0,5168	0,9056
(72,20)	0,0041	0,1035	0,5148	0,8950
(72,24)	0,0062	0,1153	0,5132	0,8849
(72,28)	0,0088	0,1262	0,5119	0,8754
(72,32)	0,0117	0,1362	0,5109	0,8664
(72,36)	0,0148	0,1454	0,5100	0,8579
(72,40)	0,0182	0,1540	0,5093	0,8499
(72,44)	0,0216	0,1620	0,5086	0,8423
(72,48)	0,0252	0,1695	0,5081	0,8352
(72,52)	0,0289	0,1765	0,5076	0,8284
(72,56)	0,0326	0,1830	0,5072	0,8220
(72,60)	0,0364	0,1892	0,5068	0,8160
(72,64)	0,0405	0,1954	0,5068	0,8104
(72,68)	0,0538	0,2100	0,5153	0,8092
(72,72)	0,3686	0,4735	0,7007	0,8889

Выводы

Судя по табл. 1–3, вероятность успешной атаки злоумышленника убывает с ростом r; убывает с ростом числа активных майнеров; возрастает с ростом $a_м - a_з$ в положительном диапазоне.

ЛИТЕРАТУРА

1. *Чистяков В. П.* Курс теории вероятностей. 5-е изд. М.: Агар, 2000. 256 с.