

УДК 681.327.8:519.81

ТЕОРЕТИКО-ИГРОВАЯ ОЦЕНКА СТОЙКОСТИ ШИФРА В СИСТЕМАХ ТЕЛЕКОММУНИКАЦИИ

Маригодов В.К., Хайков В.Л.

Севастопольский национальный технический университет

Студгородок г. Севастополь, Украина, 99053

Рассмотрена конфликтная ситуация взаимодействия шифровальщика передаваемой информации и лица, имеющего несанкционированный доступ к системе телекоммуникации. Определены оптимальные (минимаксные) стратегии игроков и цена игры.

Введение. Если обозначить X , K , Y – произвольные непустые конечные множества соответственно открытых текстов, ключей и шифрованных текстов, то шифр можно представить в виде тетрады

$$\langle X, K, Y, f \rangle, \quad (1)$$

где $f : X \times K \rightarrow Y$ – функция шифрования.

Уравнения зашифрования/расшифрования имеют вид [1]

$$\left. \begin{aligned} y &= f(x, z), \quad x \in X, \quad z \in Z, \\ x &= f^{-1}(y, z). \end{aligned} \right\} \quad (2)$$

Множества X , K , Y с заданными на них вероятностными распределениями рассматриваются как конечные вероятностные схемы. Тогда с учетом (2) можно записать через соответствующие энтропийные представления

$$\left. \begin{aligned} H(Y/X, K) &= 0, \\ H(X/Y, K) &= 0, \end{aligned} \right\} \quad (3)$$

т.е. неопределенность шифрованного текста при наличии открытого текста и ключа равна нулю. Неопределенность открытого текста при наличии шифрованного текста и ключа также равна нулю.

Пусть в конфликтной ситуации взаимодействия оператора системы телекоммуникации (шифровальщика) и лица, пытающегося подобрать ключ, функция $M(X, Y, K)$ определена на прямом произведении дискретных множеств [2]

$$X = \{x_1, \dots, x_n\}, \quad Y = \{y_1, \dots, y_m\}, \quad K = \{k_1, \dots, k_L\}.$$

Стратегия игрока I (оператора системы телекоммуникаций) является рандомизированной и заключается в вероятности выбора стойкости шифра $p = \{p_1, \dots, p_n\}$. Стратегия игрока II (лица, совершающего несанкционированный доступ к системе) $q = \{q_1, \dots, q_m\}$ – вероятность подбора ключа K . Пусть на эти рандомизированные стратегии наложены следующие информационные ограничения:

$$H_x(p) \geq H_1, \quad (4)$$

$$H_y(q) \geq H_2, \quad (5)$$

где обозначено

$$p_i = P(x_i), \quad q_j = P(y_j), \quad i = 1, \dots, n; \quad j = 1, \dots, m;$$

$$H_x(p) = -\sum_{i=1}^n p_i \ln p_i, \quad H_y(q) = -\sum_{j=1}^m q_j \ln q_j.$$

Таким образом, ограничения (3), (4) налагают условия фиксации на энтропии случайных величин $x \in X$ и $y \in Y$, соответствующие распределениям $p(x)$ и $q(y)$.

Условия существования цены игры и оптимальных стратегий игроков. Математическое ожидание выигрыша игрока I или проигрыша игрока II (обеспечение совершенной стойкости шифра) будет определяться как

$$E(p, q) = \sum_{i=1}^n \sum_{j=1}^m M(y_i, k_j) p_i q_j, \quad (6)$$

где y_i – выбор шифра; k_j – подбор нужного ключа к шифру; $M(y_i, k_j)$ – функция выигрыша.

Оптимальные (минимаксные) стратегии, если они существуют, должны удовлетворять условию [2]

$$E(p, q^*) \leq E(p^*, q^*) \leq E(p^*, q)$$

при любых p и q из (4) и (5). Здесь p^* , q^* – оптимальные стратегии.

При $H_1 = H_2 = 0$ игра имеет решение, так как ограничениям (4), (5) удовлетворяют любые распределения.

Если $H_1, H_2 \neq 0$, существование цены игры определяется из решения уравнения

$$\min_q E(p^*, q) = \max_p E(p, q^*).$$

Определение оптимальных стратегий и цены игры. Находим $\max_p E(p, q)$ при фиксированном q и ограничении (4). Эта задача адекватна поиску экстремума

$$\max_p [E(p, q) - \lambda H_x(p)] = \max_p \sum_{i=1}^n p_i \left[\sum_{j=1}^m M(y_i, k_j) q_j + \lambda \ln p_i \right], \quad (7)$$

где λ – множитель неопределенности Лагранжа.

Экстремальное распределение $p_{i \text{ extr}}$ из (7) получается в виде

$$p_{i \text{ extr}} = \frac{\exp \left[-\frac{1}{\lambda} \sum_{j=1}^m M(y_i, k_j) q_j \right]}{\sum_{i=1}^n \exp \left[-\frac{1}{\lambda} \sum_{j=1}^m M(y_i, k_j) q_j \right]}. \quad (8)$$

Множитель λ находится из ограничения (4) :

$$H_{x \text{ extr}}(p) = -\sum_{i=1}^n p_{i \text{ extr}} \ln p_{i \text{ extr}} = H_1.$$

После преобразования окончательно получаем

$$\lambda = 1 / \ln(H_1 / \sum_{i=1}^n \exp \alpha), \quad (9)$$

где $\alpha = \sum_{j=1}^m M(y_i, k_j) q_j$.

Экстремальное распределение получается равным

$$p_{i \text{ extr}} = \frac{\exp \left[-\alpha \ln \frac{H_1}{\sum_{i=1}^n \exp \alpha} \right]}{\sum_{i=1}^n \exp \left[-\alpha \ln \frac{H_1}{\sum_{i=1}^n \exp \alpha} \right]}. \quad (10)$$

Подставляя (10) в (7), находим

$$\max_p E(p, q) = \sum_{i=1}^n \alpha \left\{ \frac{\exp \left[-\alpha \ln \frac{H_1}{\sum_{i=1}^n \exp \alpha} \right]}{\sum_{i=1}^n \exp \left[-\alpha \ln \frac{H_1}{\sum_{i=1}^n \exp \alpha} \right]} \right\}. \quad (11)$$

Таким образом, экстремальное распределение является экспоненциальным. В работе [3] показано, что такое распределение обладает минимаксными свойствами при передаче информации по каналам с медленными общими замираниями.

Далее находим $\min_q E(p, q)$ при фиксированном p и ограничении (5), т.е.

$$\min_q [E(p, q) - \mu H_y(q)] = \min_q \sum_{j=1}^m q_j \left[\sum_{i=1}^n M(y_i, k_j) p_i + \mu \ln q_j \right], \quad (12)$$

где μ – множитель неопределенности Лагранжа.

Если обозначить $\sum_{i=1}^n M(y_i, k_j) p_i = \beta$, то по аналогии с предыдущими

вычислениями получаем

$$H_y(q) = - \sum_{j=1}^m q_j \ln q_j = H_2, \quad (13)$$

$$q_j \ln q_j = \exp\left(-\frac{\beta}{\mu}\right) \left/ \left(\sum_{j=1}^m \exp\left(-\frac{\beta}{\mu}\right) \right) \right|^{-1}, \quad (14)$$

$$\mu = \left(\ln \left(\frac{H_2}{\sum_{j=1}^m \exp \beta} \right) \right)^{-1}, \quad (15)$$

$$\min_q E(p, q) \sum_{j=1}^m \beta \left\{ \frac{\exp \left[-\beta \ln \frac{H_2}{\sum_{j=1}^m \exp \beta} \right]}{\sum_{j=1}^m \exp \left[-\beta \ln \frac{H_2}{\sum_{j=1}^m \exp \beta} \right]} \right\}. \quad (16)$$

Формулы (12)-(16) аналогичны выражениям (7)-(11) при определении $\max_p E(p, q)$.

Для существования цены игры V должно иметь место равенство

$$V = \min_q E(p^*, q) = \max_p E(p, q^*), \quad (17)$$

где p^*, q^* – оптимальные (минимаксные) стратегии игроков I и II.

Выполнение равенства (17) эквивалентно существованию и равенству верхней V_1 и нижней V_2 цены игры, т. е.

$$V = V_1 = \max_p \min_q E(p, q) = V_2 = \max_q \min_p E(p, q) . \quad (18)$$

Выражение (18) справедливо при следующих условиях:

$$\alpha = \beta \quad \text{или} \quad \sum_{j=1}^m M(y_i, k_j) q_j = \sum_{i=1}^n M(y_i, k_j) p_i ,$$

$$H_1 = H_2 \quad \text{или} \quad - \sum_{i=1}^n p_i \ln p_i = - \sum_{j=1}^m q_j \ln q_j .$$

Заключение. Таким образом, показано, что цена игры в рандомизированных стратегиях шифровальщика и лица, стремящегося к раскрытию ключа, существует. Оптимальные стратегии обоих игроков имеют экспоненциальные распределения, обладающие минимаксными свойствами. Для существования цены игры V и решения игры, состоящего в нахождении триады $\langle p^*, q^*, V \rangle$, необходимо принять одинаковость информационных ограничений ($H_1 = H_2$), а также вероятностей выбора игроками своих чистых стратегий. При этом следует отметить, что реализация теоретической стойкости шифра потребует у лица, совершившего несанкционированный доступ к системе телекоммуникации больших затрат времени даже при наличии самой совершенной вычислительной техники.

Библиографический список

1. Банкет В.Л. Защита информации в системах телекоммуникации Учеб. пособие / В.Л. Банкет, Н.В. Захарченко, А.В. Дырда; Под ред. В.Л.Банкета. — Одесса: Изд-во Укр. гос. акад. связи им. А.С. Попова, 1997. — 95 с.

2. Крапивин В.Ф. Теоретико-игровые методы синтеза сложных систем в конфликтных ситуациях/ В.Ф.Крапивин. — М.: Сов. радио, 1972. —

192 с.

3. Маригодов В.К. О минимаксном распределении вероятностей в каналах с медленными общими замираниями / В.К. Маригодов // Отбор и передача информации. — 1980. — Вып. 60. — С. 5–8.

Поступила в редакцию 31.08.2001 г.