А. А. Г р у ш о, Н. А. Г р у ш о, Е. Е. Т и м о н и н а (Москва, РГГУ).
О пропускной способности некоторых каналов передачи информации.

Рассмотрим модель скрытого канала, введенную Симмонсом [1]. Корреспондент A может использовать легальный канал для передачи скрытого сообщения корреспонденту B, а контролер U пытается выявить сам факт передачи скрытого сообщения. Мы предполагаем, что от A к B передается последовательность знаков в конечном алфавите, которая является допустимой с точки зрения некоторого языка L. Сделаем предположение, что любое слово конечной длины из языка L может быть правильным образом продолжено до бесконечного слова. Мы считаем, что U применяет только статистические методы выявления скрытой передачи, т.е. проверяет статистическую гипотезу о том, что передаваемое сообщение выбрано в соответствии с вероятностным распределением, характерным для легальных сообщений против гипотезы, что в передаваемой последовательности содержится скрытое сообщение. Допустим, что корреспондент B распознает сообщение статистическими методами. Тогда как для U, так и для B каждая альтернатива соответствует некоторому сообщению. Множество альтернатив соответствует множеству распределений вероятностей, которое описывает как методы скрытой передачи, так и сообщения в рамках конкретного метода передачи скрытого сообщения. Иначе говоря, перед корреспондентом B стоит задача распознавания конкретного сообщения в рамках заранее известного ему метода. Перед контролером U стоит задача об отклонении или принятии гипотезы, состоящей в том, что используется какой-то неизвестный ему метод скрытой передачи информации, в рамках которого передается какое-то из возможных скрытых сообщений. Окончательное решение контролер может принять при помощи критерия для произвольного n, где n — длина увиденного контролером начального участка передаваемой последовательности. При этом предполагается, что для каждого n у контролера есть статистический критерий для различения указанных гипотез. «Невидимость» скрытой передачи в данной модели соответствует отсутствию состоятельной последовательности статистических критериев.

В работе, представленной в данном сообщении, мы рассматриваем пропускную способность скрытого канала при условии, что контролер не может выявить скрытую передачу при любом n. Кроме того, у него не существует состоятельной последовательности критериев для различения указанных выше гипотез.

В работах [2], [3] доказаны необходимые и достаточные условия существования состоятельной последовательности статистических критериев в некоторых дискретных схемах. Задача рассматривается в рамках следующей модели.

Пусть $X = \{x_1, x_2, \ldots, x_n\}$ есть конечное множество, которое определяет последовательность конечных множеств $X, X^2, \ldots, X^n, \ldots$ На каждом из множеств этой последовательности заданы вероятностные меры

$$\{P_{0,n}(x_{i_1}, x_{i_2}, \ldots, x_{i_n}),\ (x_{i_1}, x_{i_2}, \ldots, x_{i_n}) \in X^n\}, \tag{1}$$

$$\{P_{1,\theta,n}(x_{i_1}, x_{i_2}, \ldots, x_{i_n}),\ (x_{i_1}, x_{i_2}, \ldots, x_{i_n}) \in X^n,\ \theta \in \Theta\}. \tag{2}$$

Обозначим X^∞ пространство бесконечных последовательностей $\{\alpha = (x_{i_1}, x_{i_2}, \ldots, x_{i_n}, \ldots),$ $x_{i_n} \in X,\ n = 1, 2, \ldots\}$. Пусть $(x_{i_1}, x_{i_2}, \ldots, x_{i_n}) \times X^\infty$ $(x_{i_n} \in X,\ n = 1, 2, \ldots)$ — элементарное цилиндрическое множество в X^∞, цилиндрическое множество I_n есть конечное объединение элементарных цилиндрических множеств, а $\mathcal{A}$ — минимальная σ-алгебра, порожденная всеми цилиндрическими множествами.

Пусть вероятностные меры, определяемые формулами (1) и (2), являются согласованными семействами конечномерных распределений [4]. Тогда $\{P_{0,n}(x_{i_1}, x_{i_2}, \ldots, x_{i_n})\}$ определяет единственную вероятностную меру P_0 на измеримом пространстве $\{X^\infty, \mathcal{A}\}$. Для каждого $\theta \in \Theta$ формулы (2) определяют единственную вероятностную меру $P_{1,\theta}$ на пространстве $\{X^\infty, \mathcal{A}\}$.

Сформулируем простую гипотезу H_0: P_0 против сложной альтернативы H_1: $\{P_{1,\theta}, \theta \in \Theta\}$. Рассмотрим такую последовательность критериев проверки H_0 против альтернативы H_1 с критическими множествами $S_1, S_2, \ldots$, что

$$\lim_{k\to\infty} P_0(S_k) = 0. \tag{3}$$

О п р е д е л е н и е 1. Последовательность критериев с критическими множествами $S_1, S_2, \ldots$ для проверки H_0 против альтернативы H_1 называется *состоятельной* [5], если выполняется условие (3) и $\lim_{k\to\infty} P_{1,\theta}(S_k) = 1$ для каждого $\theta \in \Theta$.

Критерий «невидимости» скрытой передачи может быть сформулирован в следующем виде.

Теорема. *Пусть для каждого такого $A \in \mathcal{A}$, что $P_0(A) = 1$, существует такое $\theta \in \Theta$, что $P_{1,\theta}(A) > 0$. Тогда не существует состоятельной последовательности критериев для проверки гипотезы H_0 против альтернативы H_1. Верно и обратное утверждение.*

Если Θ — конечное множество, то контролер U и корреспондент B находятся в одинаковых условиях при решении своих статистических задач. Поэтому, предположив, что B может получить сообщение, но контролер U «не видит» скрытый канал, мы приходим к условию, что Θ — бесконечное множество.

О п р е д е л е н и е 2. Множество альтернатив $\Theta_1 \subseteq \Theta$ называется *неотличимым для гипотезы H_0*, если выполняются условия: 1) Θ_1 — бесконечное множество; 2) любое бесконечное подмножество Θ_1 образует множество альтернатив, для которого отсутствует состоятельная последовательность критериев проверки H_0 против H_1.

Если в множестве параметров Θ можно выделить бесконечное подмножество альтернатив, для различения которых существует состоятельная последовательность критериев, то, используя эти альтернативы для скрытой передачи, корреспондент A создает возможность для контролера U раскрыть скрытую передачу. Несмотря на то, что для Θ не существует состоятельной последовательности критериев, контролер U получает возможность в некоторых случаях «увидеть» скрытую передачу.

Естественно, что «невидимый» для контролера скрытый канал определяется как некоторое множество альтернатив из Θ_1.

Все конечные последовательности языка L в проекциях меры P_0 на соответствующие пространства X^n и только они могут появляться с положительной вероятностью. Поэтому для любого n все «невидимые» для контролера скрытые сообщения являются допустимыми последовательностями языка L. В самом деле, пусть рассматриваемая длина сообщений равна n и множество допустимых последовательностей этой длины есть L_n. Если полученный контролером участок последовательности длины n не принадлежит L_n, то это значит, что U выявил наличие скрытой передачи. Принадлежность содержащей скрытое сообщение принятой последовательности к L_n означает, что U, работая только статистическими методами и не учитывая семантики и контекста, не имеет возможности выявить скрытую передачу на длине n. Максимум, что могут статистические методы, — это выявить принадлежность полученного слова или последовательности заданному языку. Большая или меньшая вероятность появления слова в языке не должны учитываться, если в дальнейшем не будет дополнительной информации, уточняющей действительную возможность использования этого сообщения в передаче. Но мы предположили, что такой информации нет. Если учитывать разные уровни вероятности сообщений в рассматриваемой ситуации, то получим увеличивающееся количество ложных решений, с которыми контролер без дополнительной информации не будет знать, что делать. В то же время, с увеличением n вероятности любых легальных последовательностей, как правило, становятся маленькими, а потребности легальной передачи разнообразными.

Поэтому без контекста много легальных, но маловероятных последовательностей могут рассматриваться контролером как нелегальные.

Из приведенных рассуждений следует, что носители всех скрываемых сообщений лежат в носителях мер $P_{0,n}$. Однако из этого не следует, что не существует состоятельной последовательности критериев для выявления скрытой передачи.

Рассмотрим проблему приема скрытого сообщения с позиций абонента B в модели Симмонса. Множество возможных скрытых сообщений при условии невидимости для контролера не может быть бесконечным. В противном случае у корреспондента B так же, как у контролера U, не будет существовать критерия для выявления и тем более для прочтения переданного сообщения. Это следует из того, что множество возможных сообщений для корреспондента B описывается распределениями, параметры которых принадлежат множеству Θ_1. Тогда можно считать, что существует конечный набор k альтернатив из Θ_1, соответствующих скрываемым сообщениям, т. е. существует минимальный набор последовательностей $\mu_1, \mu_2, \ldots, \mu_k$ из языка L, которые описывают все возможные сообщения длины n ($n > k$) для корреспондента B (можно рассматривать k групп последовательностей из языка). Таким образом, идентифицировав i-ю последовательность, B принимает решение о том, что ему передается сигнал № i. При этом B может допустить ошибку. Если легальное сообщение совпало с одним из передаваемых сигналов $\mu_1, \mu_2, \ldots, \mu_k$, то B считает это скрытой передачей, хотя на самом деле скрытой передачи не было. Отметим, что данная модель скрытого канала однозначно вытекает из предположения о «невидимости» скрытой передачи для контролера и полученных результатов об отсутствии состоятельных последовательностей критериев.

Из сказанного можно сделать следующий вывод. При условии, что контролер «не видит» скрытый канал, но получатель с вероятностью, стремящейся к 1, статистически распознает передаваемое срытое сообщение, число возможных скрываемых сообщений ограниченно. Скрытые каналы, в которых для передачи скрытого сообщения передаваемая последовательность изменяется настолько, чтобы можно было выявить вставку в исходной последовательности, либо не могут быть «невидимыми», либо преобразуют слова языка L. Тогда они попадают в рассматриваемый класс скрытых каналов.

Рассмотрим оценки пропускной способности, исходя из классических моделей. Для моделирования языка воспользуемся результатами Шеннона [6], в которых обосновывается следующая модель. Для каждого достаточно большого n число слов языка равно приблизительно e^{nH}, где H — энтропия текста. При этом вероятности всех слов приблизительно одинаковы и равны e^{-nH}. Если число передаваемых скрытых сообщений равно k, то B может ошибаться с вероятностью ke^{-nH} и правильно принять сообщение с вероятностью $1 - ke^{-nH}$. Если $ke^{-nH} \to \lambda > 0$ при $n \to \infty$, то B не может достоверно принять сообщение, что также было показано выше в более общей модели. Если $ke^{-nH} \to 0$, то скрытый канал асимптотически позволяет однозначно получать переданное сообщение. Поэтому пропускная способность канала (количество сообщений, которые можно передать) оценивается величиной $k = o\,(e^{nH})$, но при этом k может стремиться к бесконечности. Таким образом, модель Шеннона дает более грубую оценку пропускной способности скрытого канала по сравнению с той, которую мы получили из условия отсутствия состоятельной последовательности критериев.

Работа выполнена при поддержке РФФИ, проекты № 07–01–00484, № 07–07–00236.

СПИСОК ЛИТЕРАТУРЫ

1. *Simmons G. J.* The prisoner's problem and the subliminal channel. — In: Advances in Cryptology: Proceedings of Crypto'83. Ed. by D. Chaum. N. Y.: Plenum, 1984, p. 51–67.
2. *Грушо А. А.*, *Грушо Н. А.*, *Тимонина Е. Е.* Теоремы о несуществовании состоятельных последовательностей критериев в некоторых дискретных задачах. — Дискретн. матем., 2008, т. 20, № 2, с. 25–31.
3. *Грушо А. А.*, *Тимонина Е. Е.*, *Ченцов В. М.* Существование состоятельных последовательностей статистических критериев в дискретных статистических задачах при сложной нулевой гипотезе. — Информатика и ее примен., 2008, т. 2, в. 2, с. 64–66.
4. *Неве Ж.* Математические основы теории вероятностей. М.: Мир, 1969.
5. *Леман Э.* Проверка статистических гипотез. М.: Наука, 1964.
6. *Шеннон К.* Работы по теории информации и кибернетике. М.: ИЛ, 1963, 829 с.