«Современные материалы и технические решения», Лондон, 20-27 октября 2013 г.

Технические науки

ХАОС И КРИПТОГРАФИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫХ СЕТЯХ

Тен Т.Л., Когай Г.Д., Мухамеджанова Б.О.

Карагандинский экономический университет, Караганда;
Карагандинский государственный технический университет, Караганда, e-mail: tentl@mail.ru

Существует несколько признаков, при которых наблюдается хаотическое поведение системы [1]. В частности, необходимыми условиями являются два классических свойства – топологическая транзитивность и чувствительность к начальным условиям.

Динамическая система $\langle X, f \rangle$ называется хаотической, если выполняются условия:

1. Функция $f: X \to X$ топологически транзитивна на некотором метрическом множестве $X \subset R^d$, если для любых открытых множеств $U, V \subset X$ существует $n \geq 0$, такое что

$$f^n(U) \cap V \neq 0 .$$

2. Функция f чувствительна к начальным условиям, если существует $\delta > 0, n \geq 0$, такое что для любого $x \in X$ и его окрестности H_x есть $y \in H_x$ для которого

$$\left| f^n(x) - f^n(y) \right| > \delta .$$

Другими словами, динамическая система называется хаотической, если все ее траектории ограничены, но быстро расходятся в каждой точке фазового пространства.

Криптосистемы по своим требованиям похожи на хаотические системы: топологическая транзитивность необходима, с одной стороны, для сохранения состояния криптосистемы в тех пределах, которые допускает носитель информации, а, с другой стороны, для «покрытия» всего пространства состояний шифротекста. Чувствительность к начальным условиям соответствует чувствительности криптосистемы к открытому тексту или семени псевдослучайного генератора.

Таким образом, и в теории хаоса, и в криптографии системы защиты в распределенных сетях наблюдается небольшое изменение начальных условий, которое приводит к существенным изменениям во всей траектории.

В определении хаотической системы было введено понятие чувствительности к начальным условиям. Показатель Ляпунова $\lambda(x_0)$, определяемый для каждой точки $x_0 \in X$, является мерой чувствительности, то есть характеризует скорость экспоненциального разбегания траекторий, находящихся в окрестности x_0. Для одномерной системы

$$\left| f^n(x_0 + \varepsilon) - f_n(x_0) \right| = \varepsilon \cdot e^{n\lambda(x_0)},$$

где ε – небольшое отклонение от начального состояния x_0, и n – число итераций (дискретное время). В общем случае λ зависит от начальных условий x_0, поэтому определяют усредненное значение. Для систем, сохраняющих меру, λ остается постоянным для всех траекторий. Практически, показатель Ляпунова можно вычислить как предел (формула (1) или (2))

$$\lambda(x_0) = \lim_{n \to \infty} \lim_{\varepsilon \to \infty} \frac{1}{n} \log \left| \frac{f^n(x_0 + \varepsilon) - f^n(x_0)}{\varepsilon} \right| \quad (1)$$

или

$$\lambda(x_0) = \lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} \log \left| f'(x_k) \right| = \lim_{n \to \infty} \frac{1}{n} \log \prod_{k=1}^{n} \left| f'(x_k) \right| \quad (2)$$

Для каждого k производная $f'(x_k)$ показывает, как быстро изменяется функция f по отношению к возрастанию аргумента с x_k до x_{k+1}. Предел равен среднему значению логарифма производной после n итераций и показывает скорость расхождения траекторий в течение дискретного времени n. Положительное значение показателя ($\lambda > 0$) есть индикатор хаотического поведения системы.

Для d-мерной системы мы имеем набор $\lambda = \{\lambda_1, ..., \lambda_d\}$ и более сложное поведение, которое качественно не отличается от одномерного случая.

Для учета разрешения (точности) наблюдения, более полезной информацией оказывается энтропия Колмогорова-Синая h_{KS}. С позиции криптографии, показатель Ляпунова является мерой криптографической эффективности системы. Чем больше λ, тем меньше итераций требуется для достижения заданной степени распыления или смешивания информации.

Традиционные криптосистемы (схемы шифрования, псевдослучайные генераторы) можно рассматривать как динамические системы, осуществляющие преобразования информации (таблица).

Взаимосвязь между объектами изучения в теории хаоса и криптографии

Теория хаоса	Криптография
Хаотическая система	Псевдохаотическая система
– нелинейное преобразование	– нелинейное преобразование
– бесконечное число состояний	– конечное число состояний
– бесконечное число итераций	– конечное число итераций
Начальное состояние	Открытый текст
Заключительное состояние	Шифротекст
Начальные условия и параметры	Ключ
Асимптотическая независимость начального и конечного состояний	Запутывание
Чувствительность к начальным условиям и параметрам, смешивание	распыление

Можно предположить, что известные свойства хаотических систем (экспоненциальное расхождение траекторий, эргодичность, смешивание) окажутся полезными в криптографии (в частности, при разработке новых схем шифрования).

С точки зрения акцентов и объектов изучения, между криптографией и теорией хаоса существуют фундаментальные различия:

Криптография изучает эффект конечного числа итерационных преобразований ($n < \infty$), в то время как теория хаоса (непрерывного и дискретного) изучает асимптотическое поведение системы ($n \to \infty$).

Классические хаотические системы представлены некоторым объектом (множеством) фазового пространства, который часто имеет дробную раз мерность (то есть является фракталом). В криптографии используются все возможные комбинации независимых переменных (что делает систему максимально непредсказуемой) и работают с пространствами с целыми размерностями.

Важно, что в компьютерной криптографии рассматриваются системы с конечном числом состояний, а пространство состояний хаотической системы определено на бесконечном множестве непрерывных или дискретных значений.

Таким образом, последовательность состояний характеризуется равномерным законом распределения вероятности и не имеет корреляций (паттернов). Понятие абсолютной непредсказуемости эквивалентно истинной случайности. Так же, истинно случайная последовательность часто называется белым шумом. Источником белого шума может быть хаотическая система, с большим количеством степеней свободы (например, замкнутая система с идеальным газом).

Список литературы

1. Бейсембби М.А., Тен Т.Л., Когай Г.Д. Разработка криптографической системы и управление детерминированным хаосом: монография. – Караганда: КарГТУ, 2013. – 170 с.

«Управление производством. Учет, анализ, финансы», Лондон, 20-27 октября 2013 г.

Экономические науки

ОЦЕНКА ЭФФЕКТИВНОСТИ ЭКОНОМИЧЕСКОГО РАЗВИТИЯ ПРОИЗВОДСТВЕННЫХ ОРГАНИЗАЦИЙ

Акимов А.А.

ФГБОУ ВПО «Пензенский государственный университет», Пенза, e-mail: akiand@yandex.ru

Критерием эффективности функционирования производственных организаций является максимизация дохода, аккумулированного предприятиями этой сферы деятельности, по отношению к затратам, связанным с созданием добавленной стоимости. В качестве данного критерия может выступать темп роста рентабельности организаций данной сферы деятельности. Этот показатель характеризует динамику развития производственных организаций.

Другим показателем эффективности реализации стратегического плана экономического развития производственных организаций является темп роста инвестиций в основной капитал. Данный показатель характеризует инвестиционную привлекательность и динамику технического перевооружения производственных организаций. На основе указанных выше показателей проводится сравнительный анализ. В его рамках рассчитываются следующие целевые рейтинговые индексы:

ЦРИР – целевой рейтинговый индекс развития;

ЦРИ – целевой рейтинговый индекс инноваций;

ЦРР – целевой рейтинговый индекс рентабельности.