Об автоматной модели защищенных компьютерных систем

А. В. Галатенко

В работе строится вероятностная модель компьютерной системы, вводится понятие безопасности для нее и приводятся условия, при соблюдении которых система является безопасной.

Введение

В работе [1] компьютерная система рассматривается как конечный автомат, что позволило распространить некоторые факты из теории автоматов на эти системы. Отмечается, что дальнейшее обобщение таких систем осуществляется за счет рассмотрения вероятностных автоматов. Ниже приводятся результаты такого обобщения.

§1. Основные понятия и результаты

Пусть Σ — конечное множество, Σ^* — множество всех конечных слов над Σ, и ε — пустое слово.

Под вероятностным автоматом понимается тройка $\mathbb{A} = (S, \Sigma, \delta)$, где S и Σ суть конечные множества (состояния и входной алфавит, соответственно), а δ — функция, определенная на множестве $S \times \Sigma$ и принимающая в качестве значений вероятностные меры на множестве S (обозначим множество таких мер через μ).

Для множества B через $\mid B \mid$ обозначим мощность B. Пусть $\mid S \mid = n$. Тогда $\mu = \left\{ (p_1 \dots p_n) \mid p_i \geq 0, i = 1 \dots n, \sum\limits_{i=1}^{n} p_i = 1 \right\}$. Функция δ может быть определена как некоторое множество стохастических матриц (напомним, что матрица называется стохастической, если все ее элементы неотрицательны и сумма элементов в любой строке равна 1). Пусть $\mid \Sigma \mid = m$. Тогда $\delta = (M_1 \dots M_m)$, где $M_k = \left(p_{ij}^k\right)_{i,j=1}^n$. Величина p_{ij}^k имеет смысл вероятности перехода по команде номер k из состояния номер i

в состояние номер j. Функционирование вероятностного автомата представляет собой некоторый случайный процесс.

Пусть $\tilde{\mu} = (\mu_1 \dots \mu_n) \in \mu$ — вектор исходного распределения вероятностей (μ_i есть вероятность того, что до начала работы автомат находился в состоянии $s_i \in S$), а $\{M_1 \dots M_m\}$ — система матриц, определяющая функцию δ. Тогда поведением вероятностного автомата называется отображение $\tilde{\delta} : S \times \Sigma^* \to \mu$, задаваемое формулой $\tilde{\delta}(\tilde{\mu}, \alpha) = \tilde{\mu} \cdot M_{a(1)} \cdot \ldots \cdot M_{a(k)}$, где $\alpha = a(1) \dots a(k)$ — входное слово.

Функция $\tilde{\delta}$ имеет смысл вероятности попадания в какое-либо состояние при условии заданного начального распределения и поступившего на вход слова.

Перечислим допущения о компьютерной системе, моделируемой автоматом $\mathbb{A}$. Пусть в системе работают два пользователя: H и L. Пользователь H имеет право знать о системе все, а L — только часть информации. Под безопасностью для $\mathbb{A}$ содержательно понимаем ситуацию, когда пользователь L не замечает влияния H на $\mathbb{A}$. Формализуем это. Пусть $\Sigma = \Sigma_H \sqcup \Sigma_L$, то есть у каждого пользователя есть свой набор команд, не пересекающийся с набором другого пользователя. В каждый момент времени только один пользователь может вводить команды. Пусть состояние — вектор параметров, часть которых соответствует пользователю L, а оставшаяся часть — пользователю H. Исходя из описанной идеологии, формально определим понятие безопасности.

Определим безопасное начальное состояние. В силу того, что пользователю L "не положено" видеть результаты работы H, естественно потребовать, чтобы в начальный момент в системе не было информации о H, то есть все H-компоненты начального состояния были занулены. Такие начальные состояния мы будем называть безопасными.

Начальное распределение состояний называем безопасным, если с вероятностью, равной 1, $\mathbb{A}$ находится в первый момент в некотором безопасном начальном состоянии.

Введем на S отношение эквивалентности, полагая $s_i \sim s_j$, если они отличаются только на H-компонентах. Соответствующие классы эквивалентности индуцируют проектор $\pi : S \to S/\sim$. Пусть $[s]$ — класс эквивалентности s. Введем функцию $F : \Sigma^* \to \Sigma_L^*$, определяемую так: если $\omega = x_1 \dots x_N$, то $F(\omega) = F(x_1) \dots F(x_N), F(x_i) = x_i$ при $x_i \in \Sigma_L$, и $F(x_i) = \varepsilon$ при $x_i \in \Sigma_H$.

Заметим, что F действует на Σ_L^* как тождественное отображение.

Занумеруем состояния автомата $\mathbb{A}$ так, что сначала берутся состояния, соответствующие первому классу эквивалентности, затем — второму, и так далее. Тогда матрицы вида M_k могут считаться состоящими из блоков, соответствующих переходу из одного класса эквивалентности в другой.

Пусть $\mid S/\sim\mid = l$. Обозначим через μ_L множество вероятностных мер на $S/\sim$. Рассмотрим проектор $\tau : \mu \to \mu_L$, задаваемый так.

Если p_{i_j} соответствует состоянию из i-того класса эквивалентности, то полагаем $p_i^L = \sum\limits_{j=1}^{k_i} p_{i_j}$, и при $\tilde{\mu} \in \mu$ выполнено $\tau(\tilde{\mu}) = \left(p_1^L \dots p_l^L\right)$.

Пусть $M(l)$ — множество квадратных матриц размеров $l \times l$. Определим функцию $Agr : \Sigma_L^* \to M(l)$ следующим образом.

Пусть $\omega \in \Sigma_L^*$, $\omega = \omega(1)\dots\omega(k)$ и $M = M_{\omega(1)} \cdot \ldots \cdot M_{\omega(k)}$. В матрице M происходит объединение состояний, соответствующих одному классу эквивалентности так, что для каждого класса выбирается один представитель, и в качестве вероятности перехода из данного класса в другие берется суммарная вероятность попадания из выбранного состояния в состояния другого класса. Таким образом, от матрицы M размеров $n \times n$ переходим к матрице N размеров $l \times l$ и говорим, что $Agr(\omega) = N$. Вообще говоря, это определение не является корректным, так как оно существенно зависит от выбора представителя класса эквивалентных состояний, однако можно сформулировать условия, при которых функция Agr определена корректно. Содержательно Agr означает переход к процессу с агрегированными состояниями.

Определение безопасности системы. Система, задаваемая вероятностным автоматом $\mathbb{A} = (S, \Sigma, \delta)$ и безопасным начальным распределением $\tilde{\mu}$, называется безопасной, если выполнены следующие два условия: (1) отображение $\hat{\delta}$, такое что $\hat{\delta}(\tilde{\mu}, \omega_L) = \tau(\tilde{\mu}) \cdot Arg(\omega_L)$, корректно определено и действует в μ_L;

(2) следующая диаграмма коммутативна:

$$\begin{array}{ccc} S \times \Sigma^* & \xrightarrow{\tilde{\delta}} & \mu \\ \downarrow F & & \downarrow \tau \\ S \times \Sigma_L^* & \xrightarrow{\hat{\delta}} & \mu_L \end{array}$$

Заметим, что, во-первых, определение безопасности отвечает интуитивным представлениям о безопасности, описанным выше. Действительно, условие (1) означает, что пользователь L не может различить состояния, отличающиеся только на H-компонентах, а условие (2) - что пользователь H не может менять L-компоненты. Во-вторых, определение соответствует предложенной в [5] идеологии, запрещающей читать вверх и писать вниз.

Определение безопасности системы не предоставляет конструктивного способа проверки безопасности. Сформулируем и докажем достаточные условия безопасности системы.

Будем рассматривать только автоматы с безопасным начальным распределением.

Будем говорить, что матрица вида M_k обладает свойством стационарности, если сумма элементов каждого блока по строке постоянна независимо от выбора строки в блоке.

Матрица вида M_k обладает свойством диагональности, если все ее внедиагональные блоки состоят из нулей.

Теорема 1. Для выполнения условия (1) безопасности системы достаточно, чтобы матрицы M_k, соответствующие каждому элементу Σ_L, были стационарными.

Теорема 2. Для выполнения условие (2) безопасности системы достаточно, чтобы матрицы M_k, соответствующие каждому элементу Σ_H, обладали свойством диагональности.

Таким образом, от условий на словах произвольной длины мы перешли к условиям на матрицы перехода. Отметим, что полученные условия "почти необходимы". Если существует матрица, соответствующая некоторому элементу Σ_L, имеющая в некотором блоке пару достижимых состояний с разными суммами по строке, можно указать входное слово, на котором нарушится условие (1) безопасности. Далее, если существует матрица, соответствующая некоторому элементу Σ_H, имеющая в некотором внедиагональном блоке ненулевой элемент, соответствующий переходу из достижимого состояния, легко указать входное слово, на котором нарушится условие (2) безопасности. Оба утверждения почти очевидны, и мы опустим их доказательство.

§2. Вспомогательные утверждения

Имеет место следующее утверждение.

Лемма 1. Пусть A и B - матрицы, удовлетворяющие условию стационарности. Тогда матрица $C = A \cdot B$ также удовлетворяет условию стационарности.

Доказательство. Пусть в матрицах A и B имеется l блоков D_t, в каждом из которых k_t состояний. Без ограничения общности, рассмотрим левый верхний блок матрицы C. Достаточно показать, что для i и i', таких что $1 \leq i < i' \leq k_1$, выполнено $\sum\limits_{j=1}^{k_1} c_{ij} = \sum\limits_{j=1}^{k_1} c_{i'j}$. Действительно,

$$d = \sum_{j=1}^{k_1} (c_{ij} - ci'j) = \sum_{j=1}^{k_1} \left(\sum_{k=1}^{n} (a_{ik} \cdot b_{kj} - a_{i'k} \cdot b_{kj}) \right) =$$

$$= \sum_{j=1}^{k_1} \left(\sum_{k=1}^{n} b_{kj} \left(a_{ik} - a_{i'k} \right) \right) = \sum_{k=1}^{n} \left(\sum_{j=1}^{k_1} b_{kj} \left(a_{ik} - a_{i'k} \right) \right) =$$

$$= \sum_{k=1}^{n} (a_{ik} - a_{i'k}) \sum_{j=1}^{k_1} b_{kj} = \sum_{m=1}^{l} \sum_{k \in D_m} (a_{ik} - a_{i'k}) \sum_{j=1}^{k_1} b_{kj}.$$

В силу того, что сумма элементов блоков матрицы B по строке не зависит от выбора строки в блоке, внутреннюю и среднюю суммы последнего выражения можно поменять местами, что дает

$$d = \sum_{m=1}^{l} \sum_{j=1}^{k_1} b_{kj} \sum_{k \in D_m} (a_{ik} - a_{i'k}).$$

С учетом того, что внутренняя сумма здесь по условию леммы тождественно равна нулю, $d = 0$. Лемма доказана.

Лемма 2. Пусть матрица A удовлетворяет условию стационарности, матрица B удовлетворяет условию диагональности. Тогда матрица $C = A \cdot B$ имеет те же суммы по строке элементов в блоке, что и матрица A.

Доказательство. В силу того, что матрица B обладает свойством диагональности, очевидно, что блоки матрицы C получаются перемножением одного блока матрицы A на один блок матрицы B. Без ограничения общности рассмотрим левый верхний блок матрицы C. Пусть он имеет размер $k_1 \times k_1$. Покажем, что для i, таких что $1 \leq i \leq k_1$, выполнено $\sum\limits_{j=1}^{k_1} a_{ij} = \sum\limits_{j=1}^{k_1} c_{ij}$. Нетрудно убедиться, что

$$d = \sum_{j=1}^{k_1} (a_{ij} - c_{ij}) = \sum_{j=1}^{k_1} \left(a_{ij} - \sum_{l=1}^{k_1} a_{il} b_{lj} \right) = \sum_{j=1}^{k_1} a_{ij} - \sum_{j=1}^{k_1} \sum_{l=1}^{k_1} a_{il} b_{lj} =$$

$$= \sum_{j=1}^{k_1} a_{ij} - \sum_{l=1}^{k_1} \sum_{j=1}^{k_1} a_{il} b_{lj} = \sum_{j=1}^{k_1} a_{ij} - \sum_{l=1}^{k_1} a_{il} \sum_{j=1}^{k_1} b_{lj} = \sum_{j=1}^{k_1} a_{ij} - \sum_{l=1}^{k_1} a_{il} = 0.$$

Тем самым лемма 2 доказана.

§3. Доказательство теорем 1 и 2

Доказательство теоремы 1. Корректность определения $\hat{\delta}$ в (1) следует из корректности определения функции Agr. Корректность определения Agr следует из леммы 1.

Из леммы 1 и стохастичности матриц перехода следует, что матрица $Agr\,(\omega_L)$ — также стохастическая. Значит $\hat{\delta}$ на самом деле действует в μ_L. Теорема 1 доказана.

Доказательство теоремы 2. Переведем определение 1 на язык теории вероятностей. У нас определен агрегированный процесс на словах пользователя L. В силу того, что диаграмма коммутирует, агрегированный процесс должен быть определен на любых входных словах. В силу теоремы 1 и стохастичности матриц в условии теоремы 2, такой процесс корректно определен. Коммутативность диаграммы достигается тогда и только тогда, когда агрегированные процессы эквивалентны, то есть матрицы перехода на любое число шагов совпадают.

Дальнейшее доказательство проведем индукцией по длине входного слова. Базис индукции: перед началом работы системы диаграмма, очевидно, коммутативна.

Для того, чтобы совершить индуктивный переход, достаточно показать, что введение в любой момент времени любой команды пользователя H не нарушит коммутативности при условии, что коммутативность не была нарушена до этого. Итак, достаточно показать, что для любого $\omega \in \Sigma^*$, для которого выполнено $Agr\,(\omega) = Agr\,(F\,(\omega))$, и любого $\omega_H \in \Sigma_H$ справедливо соотношение $Agr\,(\omega) = Agr\,(\omega \cdot \omega_H)$. А это является очевидным следствием леммы 2. Теорема 2 доказана.

Библиография

[1]. Ira S. Moskowitz, Oliver L. Costich. "A Classical Automata Approach to Noninterference Type Problems" — Department of the Navy, Naval Research Laboraory, 1992.
[2]. Кудрявцев В.Б., Алешин С.В., Подколзин А.С. "Введение в теорию автоматов" — М.: Наука. 1985.
[3]. Бухараев Р.Г. "Вероятностные автоматы" — Казань, 1970.
[4]. Кострикин А.И. "Введение в алгебру" — М.: Физматлит, 1994.
[5]. John McLean. "Reasoning about security models" — "Proc. of the 1987 IEEE Computer Society Symposium on Research in Security and Privacy", pp 123-131, Oakland, CA, 1987.
[6]. Dorothy E. Denning. "A lattice model of secure information flow" — "Communications of the ACM", 19(5), pp 236-243, 1976.
[7]. Joseph A. Goguen, Jose Meseguer. "Unwinding and interference control" — "Proc. of the 1984 IEEE Computer Society Symposium on Computer Security and Privacy", pp 75-86, Oakland, CA, 1984.