DOI: 10.25728/tas.2019.50.5.5

ИСПОЛЬЗОВАНИЕ ОТНОШЕНИЙ В АВТОМАТАХ СПЕЦИАЛЬНОГО ВИДА ДЛЯ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПОНЕНТОВ БОЛЬШИХ СИСТЕМ

Максимовский А.Ю.
(*Институт проблем управления РАН, Москва*)
almxmwxy@mail.ru,

Доклад посвящен поиску путей развития предложенных в [8-9] методов и средств осуществления мониторинга информационной безопасности представимых в виде конечных автоматов компонентов сложных и активных систем, а также и сетей, посредством которых осуществляется взаимодействие этих компонентов. Данное проблематика является логичным дополнением подходов, предложенных в работах [4-7], применительно к системам, относящимся к критической информационной инфраструктуре Российской Федерации. Построен класс регистра сдвига, позволяющих повысить эффективность методов мониторинга, предложенных в [8], а также определены возможные направления дальнейших работ с использованием более общих по сравнению с известных алгебраических объектов

Ключевые слова: мониторинг информационной безопасности, конечный автомат, регистр сдвига, диаметр графа.

1. Введение

Одной из базовых проблем управления функционированием системами, относящимся к критической информационной инфраструктуре Российской Федерации (далее – КИИ РФ) является обеспечение их информационной безопасности (далее – ИБ) в

условиях активно предпринимаемых попыток воздействия на указанные системы с целью снижения эффективности их использования вплоть до полного или частичного вывода из строя. В такой ситуации наиболее эффективным инструментом обеспечения ИБ таких систем является мониторинг ИБ их компонентов и сетей, посредством которых осуществляется взаимодействие этих компонентов. Применительно к системам, относящимся к КИИ РФ, в работах [4-7] предложены подходы к построению параметрических моделей оценки уровня ИБ объектов КИИ и рискового потенциала. В качестве одного из критериев для мониторинга ИБ сетевых объектов, входящих в сложные системы, могут использоваться запреты их выходных последовательностей (см., [1-3,12]). В работах [8-9] предложены механизмы построения и использования экспериментов с автоматами, а также отношений специального вида для автоматных моделей компонентов сложных систем и ассоциированных с ними комбинаторных объектов (определяемых на графах или мультиграфах соответствующих автоматов -, в рассматриваемом случае, регистров сдвига или их обобщений), обладающих необходимыми свойствами для целей мониторинга ИБ сетевых объектов. В данном докладе обсуждаются пути развития результатов работ [8-9].

В работе [8] было предложено для проведения мониторинга безопасности сетевых объектов использовать свойство недоступности (l-недоступности) k-грамм выходных последовательностей сетевых объектов. Описан класс недвоичных регистров сдвига, для диаметров мультиграфов которых удалось получить нижние оценки эффективности и трудоемкости реализации методов мониторинга безопасности с использованием l-недоступности биграмм выходных последовательностей.

2. Недвоичные регистры сдвига

В данном разделе мы опишем подход к построению класса недвоичных регистров сдвига, которые позволяют гарантировать верхние оценки диаметров мультиграфов, и тем самым найти законченное решение рассматриваемой задачи.

В [8] рассматривался следующий класс регистров сдвига, Пусть $\rho(g)$ – регистр длины k над конечным множеством Ω_n, $|\Omega_n| = n$ с входным алфавитом X, выходным алфавитом Y и функцией обратной связи:

$$g(s_1, \dots, s_k, x) = z(s_1, \dots, s_k)H_x,$$

где функция z: $\Omega_n^k \to \Omega_n$ биективна по первой переменной, H_x – подстановка множества Ω_n, и множество $H_X = \{H_x, x \in X\}$ транзитивно на Ω_n. При этом $|H_X| = n$. В качестве функции выходов рассматривается проекция состояния регистра на его первую координату (или произвольное инъективное отображение множества Ω_n^k на алфавит Y).

Обозначим $\Gamma_{\rho(g)}^{[m]}$ орграф, вершинами которого являются кортежи, состоящие из m попарно различных состояний регистра сдвига $\rho(g)$, из вершины $(s_1, s_2, \dots, s_m)$ в вершину $(t_1, t_2, \dots, t_m)$ заходит дуга, если найдется входной символ $x \in X$ со свойством для каждого $j \in \{1, m\}$ и $s_j = (s_{1,j}, \dots, s_{k,j})$, $t_j = (s_{2,j}, \dots, s_{k,j}, z(s_{1,j}, \dots, s_{k,j})H_x)$. Пусть $\partial(\Gamma_{\rho(g)}^{[m]})$ - диаметр $\Gamma_{\rho(g)}^{[m]}$.

В [8] описан класс функций обратной связи регистра $\rho(g)$, для которых справедливо неравенство:

$$\partial(\Gamma_{\rho(g)}^{[2]}) \geq k^2 + k - 1.$$

Однако такая величина параметра недоступности применительно к конкретным ситуациям может оказаться слишком большой, что побуждает искать пути и условия его уменьшения.

3. Построение регистра сдвига с гарантированными верхними оценками диаметра мультиграфа биграмм состояний

Объектом нашего исследования будет регистр сдвига $C(\varphi, \hat{F})$ длины k над конечным множеством Ω_n $|\Omega_n| = n$ с входным алфавитом X, выходным алфавитом Y и функцией переходов:

$$(s_1, \dots, s_k)\rho(\varphi)F_x = (s_2, \dots, s_k, \varphi(s_1, \dots, s_k)F_x),$$

где функция φ: $\Omega_n^k \to \Omega_n$ биективна по всем своим существенным переменным, включая переменные с номерами 1 и k, F_x – подстановка из множества $\hat{F}$, дважды транзитивного на множестве Ω_n, так что $|X| \geq n(n-1)$. Аналогично графу $\Gamma_{\rho(g)}^{[m]}$ можно определить $\Gamma_C^{[m]}$.

Для изучения свойств $\Gamma_C^{[m]}$ используем новую редакцию понятия «соотношение связанности», введенного в [9], но ориентированную на $C(\varphi, \hat{F})$. Будем говорить, что регистр сдвига $C(\varphi, \hat{F})$ имеет «структурную связь» (СС) K типа $\varepsilon(K) \in \{0,1\}$, порядка $n(K) = l \epsilon \mathbb{N}$, с конфигурацией $\nu(K) = \{\nu_1, \dots, \nu_l\}$, шаблоном $\kappa(K) = (\kappa_{\nu_1}, \dots, \kappa_{\nu_l})$, где $\kappa_{\nu_i} \in \{0,1\}$, $\nu_i \in \mathbb{N}$?, $i = 1, \dots, l$, если для любых $i \in \mathbb{N}$ $F_{x_j} \in \hat{F}$, $j = 1, \dots \nu_l - k + 1$, любых $a_{i-k+\nu_l+1}, \dots, a_{i+\nu_l} \in \Omega_n$, $b_{i-k+\nu_l+1}, \dots, b_{i+\nu_l} \in \Omega_n$, удовлетворяющих условию: $\delta\left(a_{i+\nu_t}, b_{i+\nu_t}\right) = \kappa_{\nu_t}$, $t = 1, \dots, l$, имеет место равенство $\delta(a_i, b_i) = \varepsilon(K)$. Здесь обозначено:

$$\delta(a,b) = \begin{cases} 1, a \neq b \\ 0, a = b \end{cases}$$

$$(a_i, \dots, a_{i+k-1}) = (a_{i-k+\nu_l+1}, \dots, a_{i+\nu_l})(\rho(\varphi)F_{x_1} \dots \rho(\varphi)F_{x_{\nu_l-k+1}})^{-1}$$

$$(b_i, \dots, b_{i+k-1}) = (b_{i-k+\nu_l+1}, \dots, b_{i+\nu_l})(\rho(\varphi)F_{x_1} \dots \rho(\varphi)F_{x_{\nu_l-k+1}})^{-1}$$

Любой регистр $C(\varphi, \hat{F})$ имеет СС K_0, у которой: $\varepsilon(K_0) = 1$, $n(K_0) = k, \nu(K_0) = \{1, \dots, k\}, \kappa(K_0) = (0, \dots 0,1)$.

СС K' назовем следствием (СС) K, если $\nu(K) \subset \nu(K') = \{\nu_1', \dots, \nu_{l'}'\}$, $\kappa_{\nu_j} = \kappa_{\nu_j}'$, $\kappa(K') = (\kappa_{\nu_1'}', \dots, \kappa_{\nu_{l'}'}')$, $\varepsilon(K) = \varepsilon(K')$. Будем говорить, что СС K получена применением СС K_1 к СС K_2, если СС K является следствием СС K_2, причем $\nu(K_2) \backslash \nu(K) = \{\nu_j\}$, $\kappa_{\nu_j} = \varepsilon(K_1)$, и для $l = n(K_1)$ найдутся $\nu_{i_1}, \dots, \nu_{i_l}$, для которых $\nu(K_1) = \{\nu_{i_1} - \nu_j, \dots, \nu_{i_l} - \nu_j\}$, $\kappa(K_1) = (\kappa_{u_1}, \dots, \kappa_{u_l})$, $u_t = \nu_{i_t} - \nu_j$, $t = 1, \dots, l$. Назовем СС K производной от структурных связей $K_1, \dots, K_s$, если путем применения к СС K структурных связей $K_{i_1}, \dots, K_{i_j}$, $i_t \in \{1, \dots, s\}$, $t = 1, \dots, j$, мы получим СС, являющуюся следствием хотя бы одной из СС $K_1, \dots, K_s$.

Структурную связь, которая не является ни следствием, ни производной от других СС, назовем минимальной (МСС).

Сформулируем основные результаты об оценках диаметра $\partial(\Gamma_C^{[2]})$ графа $\Gamma_C^{[2]}$.

Теорема 1.

1. Если функция φ биективна по переменным с номерами $m_1 = 1 < m_2 < \cdots < m_t = k, t < k$, $\zeta_\varphi = \max\limits_{1<j<t}(m_j - m_{j-1})$, и не зависит от остальных переменных, тогда

$$\partial\left(\Gamma_C^{[2]}\right) \leq 6k - m_{t-1} - 1 + k\left\lfloor\frac{\zeta_\varphi - k + m_2 - 1}{t-1}\right\rfloor.$$

2. Если функция φ биективна по всем своим переменным, и регистр сдвига $C(\varphi, \hat{F})$ не имеет МСС $\hat{K}$ типа $\varepsilon(\hat{K}) = 0$ с конфигурацией $\nu(\hat{K}) = \{k, \dots, k + n(\hat{K}) - 1\}$, тогда

$$\partial\left(\Gamma_C^{[2]}\right) \leq 4k.$$

3. Если функция φ биективна по всем своим переменным, и конфигурация $\nu(\breve{K})$ МСС $\breve{K}$ регистра сдвига $C(\varphi, \hat{F})$, $\varepsilon(\breve{K}) = 0$, имеет вид $\nu(\breve{K}) = \{k, \dots, k + n(\breve{K}) - 1\}$, тогда

$$\partial\left(\Gamma_C^{[2]}\right) \leq 3k + k\left\lfloor\frac{k-1}{n(\breve{K})-1}\right\rfloor.$$

Приведем достаточные условия, при которых диаметр $\partial(\Gamma_C^{[2]})$ графа $\Gamma_C^{[2]}$ конечен, или ,что равносильно, группа $G(C) = G\big(C(\varphi, \hat{F})\big)$ регистра сдвига $C\big(\varphi, \hat{F}\big)$ дважды транзитивна.

Теорема 2.

Пусть функция φ биективна по переменной с номером j, и существует такое $\alpha \in \Omega_n$, что для любой $(k-1)$-граммы $(a_1, \dots, a_{k-1}) \in \Omega_n^{k-1}$ не пусто множество

$$C_i^{(a_1,\dots,a_{k-1})} = \{c | c \in \Omega_n, \varphi(a_1, \dots, a_{i-1}, c, a_i, \dots, a_{k-1}) \neq \varphi(\alpha, \dots, \alpha)\}.$$

Тогда группа $G(C)$ дважды транзитивна в каждом из следующих случаев:

1. $n \geq 4, j = k$ или $i = k, \left|C_k^{(a_1,\dots,a_{k-1})}\right| \geq 3$ для любой $(a_1, \dots, a_{k-1}) \in \Omega_n^{k-1}$.

2. $n \geq 5, j < i < k, k - i + 1$ и $k - j + 1$ взаимно просты, и при этом $\left|C_k^{(a_1,\dots,a_{k-1})}\right| \geq 3$ для любой $(a_1, \dots, a_{k-1}) \in \Omega_n^{k-1}$.

3. $n \geq 5,\ i < j < k,\ k - i + 1$ и $k - j + 1$ взаимно просты, и при этом $\left|C_k^{(a_1,\dots,a_{k-1})}\right| \geq 4$ для любой $(a_1, \dots, a_{k-1}) \in \Omega_n^{k-1}$.

4. Заключение

Результат теоремы 1 позволяет сделать ряд выводов о свойствах функции φ и предложений по оптимизации выбора как самой функции, так и автоматов, применяемых в качестве моделей элементов сложных систем, для разработке и апробации методов и средств мониторинга информационной безопасности :

1) если функция φ биективна по переменным с номерами 1, 2, $k - 1, k$, то $\partial\left(\Gamma_C^{[2]}\right) \leq 5k$, что указывает на то, что для достижения приемлемых значений величины $\partial(\Gamma_C^{[2]})$ нет необходимости увеличивать число существенных переменных функции φ;

2) если функции φ является особой в смысле определения, данного в работе [8], то мы оказываемся условиях третьего пункта теоремы для регистра сдвига $C(\varphi, \hat{F})$, который имеет МСС $\breve{K}$ с конфигурацией $\nu(\breve{K}) = \{k, \dots, k + 1\}$, и потому справедливо неравенство:

$$k^2 + k - 1 \leq \partial\left(\Gamma_C^{[2]}\right) \leq k(k + 2),;$$

что показывает достаточную точность оценки из теоремы 1;

3) увеличение мощности входного алфавита регистра сдвига позволило расширить класс преобразований, применяемых в функции перехода регистра сдвига и, в том числе, за счет этого уменьшить величину $\partial(\Gamma_C^{[2]})$ по сравнению с ее аналогом из [8];

4) в работе [9] на примере регистров сдвига с переносом предложены пути повышения эффективности методов мониторинга информационной безопасности за счет использования более общих алгебраических конструкций при синтезе автоматов, применяемых в целях моделирования и последующей реализации методов и средств мониторинга информационной безопасности;

5) с учетом результатов работы [9] представляет интерес исследование систем образующих симметрической группы подстановок, построенных на базе редуцированных регистров сдвига (см. [10,11]), с целью построения автоматов, имеющих небольшие диаметры мультиграфов k −грамм состояний и соответствующих выходных последовательностей.

Литература

1. БАБАШ А. В. *Запреты автоматов и двоичных функций* // Труды по дискр. матем., 2006, том 9, С.7–20
2. БАБАШ А. В. *Запреты автоматов* // Матем. заметки, 2012, том 91, выпуск 5, С. 667–673
3. ГРУШО А.А., ГРУШО Н.А., ТИМОНИНА Е.Е. *Включение новых запретов в случайные последовательности* // Информ. и ее примен., 8:4 (2014), С. 46-52
4. КАЛАШНИКОВ А.О., АНИКИНА Е.В. *Метод эффективного распределения сканеров для мониторинга информационной безопасности узлов гетерогенной сети* / // Информация и безопасность. - 2018. Т.21, вып.4. С. 455-464
5. КАЛАШНИКОВ А.О., АНИКИНА Е.В. *Модель управления информационной безопасностью критической информационной инфраструктуры на основе выявления аномальных состояний (Часть 1)* / // Информация и безопасность. – 2018. – Том 21. – № 2(4). – С. 145-154.
6. КАЛАШНИКОВ А.О., АНИКИНА Е.В. *Модель управления информационной безопасностью критической информационной инфраструктуры на основе выявления аномальных состояний (Часть 2)* / // Информация и безопасность. – 2018. – Том 21. – № 2(4). – С. 155-164.
7. КАЛАШНИКОВ А.О., САКРУТИНА Е.А. *Модель оценки безопасности критической информационной инфраструктуры на основе метода вейвлет-анализа* / // Информация и безопасность. – 2017. – Том 20. – № 4(4). – С. 478-491
8. КАЛАШНИКОВ А.О., МАКСИМОВСКИЙ А.Ю. *Использование специальных соотношений в автоматах для*

мониторинга информационной безопасности сетевых объектов // Информация и безопасность. – 2019. – Том 22. – № 1(1). – С. 30-37

9. МАКСИМОВСКИЙ А.Ю. *О двух классах автоматов над конечным кольцами, построенных на основе изоморфизма регистра сдвига с переносом, и их применении для защиты информации.* // Вопросы кибербезопасности. – 2019. – № 1(29). – С. 69-76
10. МАКСИМОВСКИЙ А.Ю. *О групповых свойствах подстановок, определенных на смежных классах конечной абелевой группы составного порядка по ее подгруппам*. Математические вопросы криптографии. 2016, Т.7, № 1, с. 83-92.
11. МАКСИМОВСКИЙ А.Ю., МЕЛЬНИКОВ С.Ю. *Спектральные и комбинаторные свойства редуцированных графов Де Брейна.*// Вопросы кибербезопасности. 2018. № 4, С. 70-76
12. СУМАРОКОВ С. Н. *Запреты двоичных функций и обратимость для одного класса кодирующих устройств* // Обозрение прикл. и пром. мат. - 1994. - Т.1 – Вып. 1, С. 33-55.