Максимовский А.Ю.

Экстремальные оценки параметров класса автоматов, используемых для мониторинга информационной безопасности сложных систем

Аннотация: Для осуществления мониторинга информационной безопасности представимых в виде конечных автоматов компонентов сложных систем, а также сетей, посредством которых осуществляется взаимодействие этих компонентов, в качестве критериев могут эффективно применяться особенности внешнего поведения автоматных моделей указанных объектов. Доклад посвящен оптимизации свойств автоматов, обладающих рядом особенностей внешнего поведения, к которым относятся отношения специального вида для автоматных моделей компонентов сложных систем и ассоциированные с ними комбинаторных объектов (определяемых на графах или мультиграфах состояний соответствующих автоматов). В качестве автоматных моделей рассматривались регистры сдвига и их обобщения, обладающие необходимыми свойствами для целей осуществления мониторинга информационной безопасности компонентов сложных систем. Построен класс регистров сдвига, позволяющих повысить эффективность ранее предложенных методов мониторинга, а также указан ряд свойств рассматриваемых регистров сдвига, существенных для реализации рассматриваемого класса методов мониторинга информационной мониторинга информационной безопасности.

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

Введение

Одним из эффективных инструментов обеспечения контроля за функционированием сложных систем является мониторинг информационной безопасности (далее – ИБ) их компонентов и сетей, посредством которых осуществляется взаимодействие этих компонентов. Развивая приведенные в работе [1] идеи

использования запретов выходных последовательностей для мониторинга ИБ, в работах [2-3] 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 рассмотренных случаях, регистров сдвига или их обобщений), обладающих необходимыми свойствами для целей мониторинга ИБ сетевых объектов. Данное направление является логичным дополнением подходов, предложенных в работах [4-6] для систем, входящих в критическую информационной инфраструктуру (КИИ) Российской Федерации. В данном докладе приведены результаты исследований мультиграфов класса автоматов, который является обобщением конструкции регистра сдвига над кольцом вычетов целых чисел составного порядка (см. [7]), и, как оказалось, обладает экстремальными для регистров сдвига значениями диаметра мультиграфа – грамм состояний по сравнению с полученными [1]. Полученный результат позволяет не только повысить эффективность метода мониторинга, предложенного в [1], но и оценить предельные значения его эффективности для данного класса автоматных моделей компонентов сложных систем и сетей, входящих в КИИ Российской Федерации.

Основные определения и обозначения

Редуцированным регистром сдвига над кольцом вычетов $\mathbb{Z}_N$, $N = nm$, следуя терминологии работ [2,7], назовем автомат $R = R_{n,m}(F) = (X, \mathbb{Z}_N, Y, \varphi, \psi)$, у которого функция переходов определена равенством: $\varphi(rm + s, x) = sn + rf_s(x)$, где $r \in \Omega_n = \{0,1 \dots, n-1\}, s \in \Omega_m$, $f_j(x)$ – подстановка множества Ω_n, $j = 0, \dots m-1$, $F = \{(f_0(x), \dots, f_{m-1}(x)), x \in X\}$, функция выходов ψ – произвольное инъективное отображение множества состояний автомата $R_{n,m}(F)$ в множество Y, $|Y| > 1$.

Обозначим $\Gamma_R^{[t]}$ орграф, вершинами которого являются кортежи, состоящие из t попарно различных состояний автомата R, при этом из вершины $(p_1, p_2, \dots, p_t)$ в вершину $(q_1, q_2, \dots, q_t)$ заходит дуга, если найдется входной символ $x \in X$ со свойством:

для каждого $j \in \{1, t\}$ и $p_j \in \mathbb{Z}_N$, $q_j = \varphi(p_j, x)$. Пусть $\partial(\Gamma_R^{[t]})$ - диаметр $\Gamma_R^{[t]}$.

Обозначим: $\gamma_k = \left[\frac{n^k}{nm}\right]$, $\Omega_n + jn = \{jn, jn+1 \dots, jn+n-1\}$, и $S(M)$ – симметрическую группу подстановок множества M.

Основные результаты

Теорема 1. Если множество $F = \{(f_0(x), \dots, f_{m-1}(x)), x \in X\}$ совпадает с прямым произведением $S(\Omega_n) \times S(\Omega_n + n) \times \dots \times S(\Omega_n + n(m-1))$, то справедливы утверждения:

а) $\partial\left(\Gamma_R^{[t]}\right) = k$ тогда и только тогда, когда $2 \le t \le \gamma_k$;

б) $\partial\left(\Gamma_R^{[t]}\right) = k+1$ тогда и только тогда, когда выполнено одно из двух условий:

б.1) $t \in \{\gamma_k, \dots, \left]\frac{\gamma_{k+1}}{\gamma_k+1}\right[\}$, $m \nmid n$, $\left]\frac{\gamma_{k+1}}{\gamma_k+1}\right[< n$,

б.2) $t \in \{\gamma_k + 1, \dots, \gamma_{k+1}\}$, $k \ge 3$, $m | n^{k-1}$, или $\left]\frac{\gamma_{k+1}}{\gamma_k+1}\right[= n$.

Теорема 2. Если множество $F = \{(f_0(x), \dots, f_{m-1}(x)), x \in X\}$ совпадает с прямым произведением групп $S(\Omega_n) \times S(\Omega_n + n) \times \dots \times S(\Omega_n + n(m-1))$, то диаметр $\partial\left(\Gamma_R^{[N]}\right)$ равен 3, если $n \ge m$, $m | n$, или $\left]\frac{\gamma_3}{\gamma_2+1}\right[= n$, и больше 3 в противном случае.

Заключение

Результаты, представленные в докладе, позволяют сделать следующие выводы:

1) увеличение мощности входного алфавита специальных классов регистров сдвига позволяет минимизировать (в отдельных случаях, существенно – ср., например, с [1]) значение диаметра мультиграфа – грамм состояний автоматной модели объекта и тем самым повысить надежность мониторинга ИБ объектов, моделируемых с использованием определенных классов регистров сдвига и их обобщений;

2) полученные результаты являются экстремальными для данного класса автоматов, потому что, во-первых, максимизирован до предела размер входного алфавита рассматриваемого автомата, и, во-вторых, максимизирован размер – грамм (см. теорему 2).

3) в целях оптимизации предложенного в докладе подхода к построению и использованию редуцированных регистров сдвига представляется исследовать поведение параметра $\partial\left(\Gamma_R^{[t]}\right)$, в случае, когда F является прямым произведением l −транзитивных множеств подстановок, а также рассмотреть другие классы автоматов, определенных на смежных классах конечной абелевой группы составного порядка по ее подгруппам (см. [7]).

Литература:

1. *Грушо А.А.* Включение новых запретов в случайные последовательности [Текст] /А.А.Грушо, Н.А. Грушо, Е.Е. Тимонина // Информ. и ее примен. – 2014. – № 8:4. – С. 46-52.
2. *Калашников А.О.* Использование специальных соотношений в автоматах для мониторинга информационной безопасности сетевых объектов [Текст] / Калашников А.О., Максимовский А.Ю.// Информация и безопасность. – 2019. – Том 22. – № 1(1). – С. 30-37.
3. *Максимовский А.Ю.* О двух классах автоматов над конечным кольцами, построенных на основе изоморфизма регистра сдвига с переносом, и их применении для защиты информации. [Текст] / А.Ю. Максимовский // Вопросы кибербезопасности. – 2019. – № 1(29). – С. 69-76.
4. *Калашников А.О.* Модель оценки безопасности критической информационной инфраструктуры на основе метода вейвлет-анализа [Текст] / А.О. Калашников, Е.А. Сакрутина // Информация и безопасность. – 2017. – Том 20. – № 4(4). – С. 478-491.
5. *Калашников А.О.* Модель управления информационной безопасностью критической информационной инфраструктуры на основе выявления аномальных состояний (Часть 1) [Текст]/ А.О. Калашников, Е.В. Аникина // Информация и безопасность. – 2018. – Том 21. – № 2(4). – С. 145-154.
6. *Калашников А.О.* Метод эффективного распределения сканеров для мониторинга информационной безопасности узлов гетерогенной сети (Часть 1) [Текст] /А.О. Калашников, Е.В. Аникина// Информация и безопасность. – 2018. – Т.21, вып.4. – С. 455-464.
7. *Максимовский А.Ю.* О групповых свойствах подстановок, определенных на смежных классах конечной абелевой группы составного порядка по ее подгруппам [Текст]/ А.Ю. Максимовский

// Математические вопросы криптографии. – 2016, Т.7, № 1 – С. 83-92.