$$R = G_1 \cap G_2 \cap \ldots \cap G_g = \left\{ \frac{\min\limits_{i=1,g} \mu_{G_i}(R_1)}{R_1}, \frac{\min\limits_{i=1,g} \mu_{G_i}(R_2)}{R_2}, \ldots, \frac{\min\limits_{i=1,g} \mu_{G_i}(R_k)}{R_k} \right\}. \quad (2)$$

В полученном нечетком множестве R наилучшим вариантом будет считаться тот, у которого наибольшая степень принадлежности, т. е. $R_o = \arg\max(\mu_{R_o}(R_1), \mu_{R_o}(R_2), \ldots, \mu_{R_o}(R_k))$.

Для учёта разной важности степеней принадлежности в нечётком множестве R будем использовать для G_i коэффициенты относительной важности критериев α_i ($\alpha_1 + \alpha_2 + \ldots + \alpha_g = 1$). Тогда

$$\mu_{R_0}(R_j) = \min_{i=1,g}(\mu_{G_i}(R_j))^{\alpha_i}, \quad j = 1,k \cdot \quad (3)$$

Показатель степени α_i в формуле (3) разбавляет (операция DIL) нечеткое множество в соответствии с мерой важности критерия. Для получения этих коэффициентов предлагается использовать тот же метод парных сравнений по шкале Т. Саати.

В работе для практического применения описанного метода предлагается использовать разработанные табличные модели, реализованные в среде EXCEL. Описываются основные аналитические выражения для обработки экспертных оценок, расчета коэффициентов принадлежности и коэффициентов важности критериев на примере выбора наилучшей распределённой системы управления сортировочной горкой (из 4 структур по 7 критериям).

Мирошник М.А. (УкрГУЖТ),
Крылова В.А. (НТУ «ХПИ»)

УДК 004.056.5

ПРИМЕНЕНИЕ КЛЕТОЧНЫХ АВТОМАТОВ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ ЗАЩИТЫ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

Непрерывное развитие вычислительных средств и сетевых технологий постоянно оказывает влияние на развитие способов противоборства. Происходит непрекращающееся проникновение геоинформационных систем, автоматизированных систем управления, различных интеллектуальных и экспертных систем поддержки принятия решений в процессы управления.

Работа таких систем требует эффективного выполнения функций автоматизированного сбора, накопления и обработки разнородной информации о состоянии окружающей обстановки. С увеличением объема поступающей информации, ужесточением требований к ее полноте и оперативности сбора в целях увеличения скорости и качества управления возникает необходимость поиска новых средств ее сбора.

Решением данной проблемы могут стать беспроводные сенсорные сети WSN. Беспроводная сенсорная сеть представляет собой пространственно распределенную самоорганизующуюся систему автономных миниатюрных датчиков (сенсоров или узлов), способных измерять определенные физические параметры окружающей среды, а затем совместно передавать накопленную информацию, ретранслируя ее от узла к узлу через образованную самими датчиками беспроводную сеть в единую точку сбора. Такие сенсорные сети позволяют контролировать измеряемые параметры окружающей среды на значительных пространствах, а также считывать показания всей сети, подключившись к ее произвольному узлу.

Гибкая архитектура, снижение затрат при развертывании выделяют беспроводные сенсорные сети среди других систем сбора информации, особенно когда речь идет о большом количестве соединенных между собой устройств. При этом сеть должна быть устойчива к выходу из строя части узлов. Кроме того, она должна быть способна восполнять потери и расширяться за счет расположения впоследствии новых сенсорных узлов.

В связи с невозможностью ограничить доступ к физической среде беспроводной связи, а также из-за децентрализованного характера сенсорных сетей проблема обеспечения в них информационной безопасности стоит особенно остро. Информационный обмен в сетевой среде вынуждает к широкому использованию криптографических средств защиты информации. Ограниченные вычислительные и энергетические ресурсы сенсорных узлов, с одной стороны, и потребность в непрерывном шифровании регистрируемой и передаваемой сенсорами информации — с другой, требуют поиска новых криптографических методов защиты передаваемой информации.

В основе существующих криптосистем лежат последовательные вычислительные алгоритмы. Применение технологий распараллеливания таких алгоритмов не позволяет значительно повысить эффективность процесса генерации последовательностей с позиций затрат и производительности, так как рост потребностей опережает линейный рост возможностей кремниевых технологий. Усилия исследователей все более сосредоточиваются на поиске новых вычислительных моделей, реализующих изначально параллельные способы решения триединой задачи: криптозащиты,

имитозащиты и защиты данных от случайных сбоев при преобразовании и передаче.

В качестве такой вычислительной модели может выступать клеточный автомат (КЛА) — бесконечная сеть одинаковых автоматов Мура, расположенных в точках пространства с целочисленными координатами, связанных одинаковым образом друг с другом и изменяющих состояние в зависимости от состояний соседей и своего собственного. Динамика состояний однородной пространственно распределенной дискретной системы с локальным взаимодействием элементов может представлять разнообразные варианты поведения (устойчивые конфигурации, циклы, хаос), в том числе не имеющие прямого аналога среди аттракторов непрерывных динамических систем. Такая система в силу однородности и локальности преобразований устойчива к сбоям отдельных элементов.

Алгоритмическая неразрешимость прямой задачи - синтеза функции глобальных (для всех элементарных автоматов) переходов КЛА по локальной функции и обратной задачи - определения структуры и параметров КЛА по множеству его состояний- позволяет использовать такую модель в качестве криптосистемы.

Криптосистемы на клеточных автоматах могут быть как симметричными, так и асимметричными. В случае симметричных криптосистем ключом может служить, например, начальное состояние клеточного автомата, осуществляющего генерацию псевдослучайной последовательности состояний и преобразование открытого текста на основе только локальных правил перехода. Для реализации асимметричных криптосистем могут использоваться обратимые клеточные автоматы. В этом случае в качестве открытого ключа может выступать, например, локальная функция переходов. Для двумерных КЛА отыскание функции, инверсной к заданной локальной функции переходов, относится к числу алгоритмически неразрешимых задач. Поэтому важным направлением исследования является поиск универсальных обратимых КЛА.

Проблему универсальности КЛА можно рассматривать в двух аспектах. В рамках первого универсальность сводится к представлению одних КЛА в других. Клеточный автомат является универсальным, если он моделирует поведение любого другого КЛА той же размерности.

Другой подход к универсальности восходит к универсальной вычислимости. Клеточный автомат является универсальным, если он моделирует универсальную машину Тьюринга. Представляет интерес поиск КЛА с минимальными значениями параметров. Следует отметить, что в общем виде проблема распознавания представимости КЛА также относится к числу алгоритмически неразрешимых.

Кравченко М.В., Лисечко В.П.
(Український державний університет залізничного транспорт, м. Харків)

ДОСЛІДЖЕННЯ МЕТОДІВ НАВЧАННЯ СИСТЕМ УПРАВЛІННЯ МЕРЕЖАМИ КОГНІТИВНОГО РАДІО

Метою роботи є дослідження методів навчання системами управління мережами когнітивного радіо. Це завдання стає все актуальнішим і виходить на передній план, розв'язання якого дало б можливість суттєво підвищити основні характеристики протоколу IEEE 802.22.

В даний час попит на послуги безпроводових телекомунікаційних мереж широкосмугового доступу не забезпечений повною мірою, особливо у приміських і сільських місцевостях, бо постачальники цих послуг найчастіше орієнтовані на густонаселені райони і великі міста. Виходячи з цього, можна стверджувати, що розробка і реалізація безпроводових мережевих рішень регіонального масштабу є актуальною і перспективною.

Стрімкий розвиток безпроводових систем, таких як: системи стільникового та супутникового радіозв'язку, LTE, безпроводові технології Wi-Fi і WiMAX, виявило серйозну проблему. Практично весь частотний діапазон до теперішнього часу розподілений і ліцензований, проте використовується недостатньо ефективно. У результаті, впровадження та використання нових сервісів, для роботи яких необхідна наявність вільних частотних діапазонів, стає важким, а в деяких випадках зовсім неможливим.

Дане завдання стає все актуальнішим і виходить на передній план, розв'язання якого дало б можливість суттєво підвищити основні характеристики протоколу IEEE 802.22.

Косолапов А.А.
(Дніпропетровський національний університет залізничного транспорту імені академіка В. Лазаряна)

ДО ПИТАННЯ ОЦІНКИ ВИМОГ ДО СИСТЕМ ЗАХИСТУ WEB-СЕРВЕРІВ ВІД DDOS-АТАК

Сучасні інформаційні системи будуються на основі інтегрованих корпоративних мереж, що об'єднують величезні інформаційні ресурси з доступом до них великої кількості віддалених користувачів через мережу WWW. Прикладом таких систем є автоматизована система керування вантажними перевезеннями АСК ВП УЗ-Є, інформаційна система українського центру оцінювання якості знань,