- Частичное делегирование по доверенности. Доверенному лицу выдается ключ, сгенерированный на основании секретного ключа оригинального подписывающего и доверенности.

Процесс подписи документа с использованием схем доверенной подписи зачастую состоит из четырех этапов:

- настройка системы. Данный этап заключается в установке публичных или приватных параметров пользователей;

- генерирование подписи. На данном этапе генерируется подпись для подписи документа;

- подпись документа. Непосредственно встраивание сгенерированной подписи в документ;

- проверка. На данном этапе происходит проверка подлинности подписи, подтверждение доверенности подписи и пр.

Заключение

В настоящее время существует достаточное количество реализаций схем доверенной подписи, которые отличаются типами делегирования, алгоритмами генерирования и подписи документов. Каждая реализация может использоваться в зависимости конкретных потребностей пользователей в быстродействии или криптографической стойкости, а также могут быть предложены новые модификации.

Список цитированных источников

1. Proxy signatures: Delegation of the power to sign messages/M.Mambo, K.Usuda, E.Okamoto. IEICE Transactions Fundamentals. – Vol. E79A, 1997.

2. Designated-Verifier Proxy Signature Schemes / G. Wang. Security and Privacy in the Age of Ubiquitous Computing (IFIP/SEC 2005). – Springer, 2005.

УДК 004.8.032.26

СИСТЕМА УПРАВЛЕНИЯ ТРАНСПОРТОМ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

Войцехович О.Ю.

УО «Брестский государственный технический университет», г. Брест

Научный руководитель – Шуть В.Н., доцент, к.т.н.

1. Постановка задачи

Задача состоит в разработке адаптивной системы управления транспортом, работающей в режиме реального времени вдоль городской магистрали, способной координировать светофоры для улучшения дорожной ситуации в целом. Еще одна задача состоит в моделировании, тестировании и оценке разработанной системы.

Для решения поставленной задачи предложен подход, координирующий время горения сигналов светофоров путем распознания и предсказания движения групп транспортных средств (пачек) на магистрали и прилегающих к ней улицах с помощью полученных с детекторов и отфильтрованных данных. Для тестирования разработанного подхода в управлении транспортом была реализована имитационная модель.

2. Описание системы

Адаптивная система управления состоит из 3 частей: предсказание прибытий и очередей (обрабатывает данные с детектора и осуществляет предсказание); система принятия

решений (строит дерево решений и выбирает оптимальные времена и длительности горения зеленого и красного сигналов для магистрали и прилегающих дорог); продвижение (модифицирует массив, где хранятся данные о распознанных пачках транспортных средств).

Разрабатываемая система управления работает на уровне пачек автомобилей и их скоростей. Критерием оптимизации являются средние задержки, которые необходимо свести к минимуму. Система предсказывает транспортный поток (предсказание осуществляется в пространстве и времени), чтобы осуществить упреждающее управление. С помощью построения бинарного дерева решений выбираются оптимальные настройки светофоров, которые отвечают сделанным предсказаниям.

Большинство существующих подходов, управляющих транспортным потоком, используют статистические сглаженные данные. Такие системы основаны на временных планах светофоров, оперирующих временем цикла, расколами и смещением. Такой подход пригоден для медленно меняющихся характеристик, но не подходит, если рассматривать реальные колебания транспортного потока, которые статистические подсчеты не могут учесть.

В разрабатываемой системе акцент смещается от модификации временных параметров, реагирующих на уже случившиеся изменения транспортного потока, к упреждающей настройке параметров светофора для предсказываемого состояния транспортного потока. И это ее главное преимущество, которое делает систему гибкой. То есть мы не устанавливаем временные планы в терминах времени цикла, расколов и сдвигов фаз. А, скорее, в терминах длительности и последовательности фаз.

Система нуждается: 1) в обмене данными в режиме реального времени с процессором; 2) в вычислительных возможностях на уровне PC, 3) во входной информации о характеристиках транспортного потока, считываемой с датчиков в реальном времени. Система централизованная, т.к. данные со всех датчиков собираются в центр управления, где происходит прогнозирование и выбор оптимальных фаз.

Для предсказания необходимы следующие входные данные: 1) время проезда от детектора к детектору; 2) коэффициент очистки очереди и 3) доля сворачиваемого транспорта. Выходные данные используются алгоритмом управления.

За основу был взят алгоритм управления, предложенный P. Dell'Olmo и P.B. Mirchandani [1]. Если прогнозируется, что две или более пачки подъедут к перекрестку и создадут конкурирующий спрос на время горения зеленого сигнала светофора для конфликтных направлений, тогда должно быть определено, какому направлению движения отдать время горения зеленого сигнала. Решение что сделать зависит от полученного значения выбранного критерия эффективности. Оптимальное разрешение конфликтов в реальном времени, или иными словами, оптимизация движения распознанных пачек автомобилей – это основная цель алгоритма управления.

Для разрешения конфликтных ситуаций алгоритм заблаговременно строит дерево решений. Каждый возникающий конфликт формирует узел в дереве решений; типы решений в этом узле включают: а) дать зеленое время пачке А, т.е. остановить пачку Б (пачка А подъезжает раньше); б) расколоть пачку А (т.е. зеленое время предоставить пачке Б). Каждая ветка дерева рассматривается далее, чтобы сохранить путь от начального узла к потенциальному решению. Построение дерева заканчивается, когда разобраны все конфликты. Конечные узлы будут представлять собой полную стоимость всех решений, которые идут от корня к конечному узлу дерева решений. Выбор единственного решения с минимальной задержкой, дает конечную стоимость траектории решения конфликтов. Путь по дереву от корня к выбранному листу обеспечивает фазовый план – конечная цель всего алгоритма.

3. Вопросы реализации

В системе был использован алгоритм идентификации пачек, основанный на двух пороговых параметрах: максимальное расстояние между двумя автомобилями в пачке и минимальное число автомобилей, которые составляют пачку.

Алгоритм начинает работу с начального решения о распределении фаз, которое может быть получено с использованием статистических данных и определяет первый узел в дереве решений. Критерий эффективности, связанный с начальными фазами, становится верхней границей при выполнении алгоритма.

4. Моделирование

Для тестирования системы была создана микроскопическая стохастическая имитационная модель, и в настоящий момент происходит ее кооперация и синхронизация с системой управления. Генерация автомобилей рассматривается как неоднородный пуассоновский процесс. Количество прибытий автомобилей следует распределению Пуассона с параметром λ, где λ – среднее количество прибытий в единицу времени. Моделирование транспортных потоков было выполнено с помощью клеточного автомата (КА) [2]. КА - это модели, которые являются дискретными в пространстве, времени и переменных состояния. Из-за дискретности КА являются чрезвычайно эффективными в реализации на компьютере. Самый простой набор правил, который приводит к реалистичному поведению, был введен в 1992 году учеными Nagel и Schreckenberg [3]. Он состоит из 4 шагов, которые должны применяться одновременно для всех автомобилей (параллельно или синхронно). Вышеприведенный набор правил является минимальным в том смысле, что отсутствие одного из 4 шагов будет вести к не реалистичному поведению. **Шаг 1: разгон.** Все машины, не достигшие максимальной скорости $v_{max,}$ ускоряются на одну единицу: v -> v+1 **Шаг2: безопасная дистанция.** Если у машины есть d пустых ячеек перед собой и ее скорость v (после шага 1) больше, чем d, то она уменьшает скорость до d: v -> min{d,v} **Шаг 3: эффект случайности.** С вероятностью p транспортное средство уменьшает скорость на одну единицу (если v после шага 2): v -> v-1 **Шаг 4: езда.** После шагов 1-3 новая скорость v_n для каждой машины n определяет продвижение на v_n ячеек: x_n -> x_n+v_n.

Заключение

Была создана адаптивная система управления транспортным потоком, способная координировать сигналы светофоров,, с целью достичь минимальной средней задержки и снизить необходимость постоянного наблюдения за перекрестком и настройки светофоров. Целью алгоритма управления является гибкое реагирование на стохас-тическое поведение транспортного потока. В данный момент проводится тестирование системы управления с помощью имитационной модели.

Список цитированных источников

1. Dell'Olmo, P. REALBAND: An Approach for Real-Time Coordination of Traffic Flows on a Network / P. Dell'Olmo, P.B. Mirchandani // Transportation Research Record. – 1995. – 1494. – P. 106-116.

2. Chowdhury, D. Statistical physics of vehicular traffic and some related systems / D. Chowdhury, L. Santen, A. Schadschneider // Physics Reports. – 2000. – 329. – P. 199.

3. Nagel, K. A cellular automaton model for freeway traffic / K. Nagel, M. Schreckenberg // J. Physique. – 1992. – 2. – P. 2221.