7. *Kwitt R., Hofmann U.* Robust Methods for Unsupervised PCA-based Anomaly Detection. IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation, Tuebingen, Germany, September 28–29, 2006.

8. *Lincoln labs*. KDDCup'99. http://kdd.ics.uci.edu/databases/kddcup99/kdd-cup99.html, 2003.

9. *Gu G., Fogla P., Dagon D., Lee W., Skoric B.* Measuring Intrusion Detection Capability: An Information-Theoretic Approach. ASIACCS'06, March 21–24, 2006 Taipei, Taiwan.

10. *Levin I.* KDD-99 Classifier Learning Contest: LLSoft's Results Overview. ACM SIGKDD Explorations 2000, pp. 67–75, January 2000.

11. *Pfahringer B.* Winning the KDD99 Classification Cup: Bagged Boosting. ACM SIGKDD Explorations 2000, pp. 65–66, January 2000.

12. *Miheev V., Vopilov A., Shabalin I.* The MP13 Approach to the KDD'99 Classifier Learning Contes». ACM SIGKDD Explorations 2000. – P. 76–77, January 2000.

13. *Карайчев Г.В., Нестеренко В.А.* Применение весовых функций для определения локальных статистических характеристик потока пакетов в сети // Известия высших учебных заведений. Северо-Кавказский регион. Естественные науки. – Ростов н/Д, 2008. № 1. – С. 10–14.

Карайчев Глеб Викторович
Южный федеральный университет.
E-mail: kgv_rostov@mail.ru.
344091, г. Ростов-на-Дону, пр. Стачки, 235/1, кв. 47.
Тел.: +7 (928) 1252607.
Факультет математики, механики и компьютерных наук; кафедра информатики и вычислительного эксперимента; ассистент.

Karaychev Gleb Viktorovich
South Federal University.
E-mail: kgv_rostov@mail.ru.
App. 47, 235/1, prosp. Stachki, Rostov-on-Don, 344091, Russia.
Phone: +7 (928) 1252607.
Faculty of mathematics, mechanics and computer science; Department of informatics and computing experiment; junior member of teaching staff.

УДК 510.6:656.001

Е.А. Пакулова

МОДЕЛЬ СОВРЕМЕННОЙ СИСТЕМЫ МОНИТОРИНГА ПОДВИЖНЫХ ОБЪЕКТОВ С ГАРАНТИРОВАННОЙ ДОСТАВКОЙ СООБЩЕНИЙ В ГЕТЕРОГЕННОЙ БЕСПРОВОДНОЙ СЕТИ

Основной целью данной статьи являлось построение модели системы мониторинга транспортных средств (ТС) с использованием нескольких беспроводных технологий связи. В связи с этим были решены следующие задачи: выбраны методы исследования, основанные на теории множеств и теории конечных автоматов, построена модель системы мониторинга ТС, определены события и команды в модели, а также связи между компонентами модели. В заключение статьи выделены дальнейшие планы работы, направленные на разработку и реализацию методов рационального управления технологиями беспроводной связи.

Моделирование; теория множеств; беспроводные технологии связи; система мониторинга транспортных средств.

E.A. Pakulova

THE MODEL OF MODERN MONITORING SYSTEM OF MOBILE OBJECTS WITH ASSURED DELIVERY OF MESSAGES IN HETEROGENEOUS WIRELESS NETWORK

The main subject of this article is development of transport monitoring system model with the usage of wireless technologies. In this connection the following tasks were decided: the research methods were chosen, which are based on the set theory and the finite automata theory, the events and commands were defined in the model, the connections between the components of the model were specified. The future plans of work directed to development and realization of methods of efficient management of wireless technologies were given in the conclusion.

Modeling; set theory; wireless technologies; transport monitoring system.

Сегодня, в условиях современной жизни, в виду террористических угроз, мы все чаще задумываемся о своей безопасности. Правительства различных стран принимают решения о тотальном контроле значимых объектов, транспортных средств, своих граждан. Для этого разрабатываются новые и с успехом применяются уже зарекомендовавшие себя технологии: системы охранного телевидения, системы управления и контроля доступа, охранно-пожарные сигнализации и многое другое.

Отдельной задачей становится обеспечение безопасности граждан на транспорте. В августе 2008 года Правительством РФ было принято постановление №641 «Об оснащении транспортных, технических средств и систем аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS». Согласно данному постановлению оснащению аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS подлежат космические средства, морские и воздушные суда, а также автомобильные и железнодорожные транспортные средства (ТС), используемые для перевозки пассажиров, специальных и опасных грузов [1].

На этом фоне получили большое развитие системы мониторинга ТС. Как правило, они предназначены для определения местоположения ТС, контроля и учета технических и эксплуатационных характеристик ТС, контроля маршрута передвижения рейсовых ТС, оповещения владельца в случае тревоги через сервисы беспроводной связи. Большинство современных систем мониторинга имеют схожую архитектуру. В ее состав входят множество бортовых устройств (или трекеров), устанавливаемых на ТС, и диспетчерский пункт (ДП), куда стекается информация с подвижных объектов, и где она анализируется. Для осуществления изложенных функций наиболее часто используется следующий набор технологий: GPS/ГЛОНАСС для определения местоположения объекта и GSM/GPRS для обмена информацией между ДП и ТС. При нормальных погодных условиях, а также полном охвате обслуживаемой зоны GSM этих средств вполне достаточно. Однако для служб, отслеживание местоположения транспорта которых является критически важным, требуются принципиально новые подходы. Система мониторинга в этом случае должна предоставлять резервные работоспособные каналы для передачи информации, в случае выхода из строя основных. Примерами таких служб могут являться:

- инкассаторская служба;
- милицейские службы;

- службы быстрого реагирования.

В данной статье рассматривается статичная модель системы мониторинга ТС с использованием нескольких альтернативных друг другу беспроводных технологий передачи данных.

Прежде всего, дадим краткое описание рассматриваемой системы. Предположим, что система мониторинга ТС состоит из следующих компонентов:

- бортовые устройства или трекеры – устройства, устанавливаемые на подвижных объектах и собирающие информацию о технических и эксплуатационных характеристиках ТС, а также информацию, полученную с GPS приемников;
- ретрансляционные станции (РС) – неподвижные объекты, устанавливаемые в городе и выполняющие роль ретрансляторов в системе;
- ДП – пункт, выполняющий функции сбора, анализа и хранения информации, полученной от РС или трекеров.

Все перечисленные компоненты находятся в тесной взаимосвязи: трекер собирает информацию со штатных датчиков и диагностических систем ТС, формирует пакет и отправляет его ДП. Если передача данных ДП в силу каких-либо причин невозможна, то трекер передает пакет ближайшей к ДП РС или другому трекеру, используя выбранную по определенному алгоритму технологию связи. Если отправленный пакет получила РС, то она, в свою очередь, отправляет его ДП. Если пакет получил другой трекер, что он также пытается отправить его ДП. Если ДП недоступен, то пакет перенаправляется другому трекеру, ближайшему к ДП, или РС.

Заметим, что в системе может быть большое количество бортовых устройств и станций. Также предположим, что в системе функционирует несколько ДП, например, для каждой службы. При этом передача пакета от одного трекера к другому трекеру или РС не зависит от принадлежности трекеров к определенному ДП.

Дадим представление рассматриваемой модели, построенное на теории множеств.

Представим компоненты системы мониторинга ТС как непустое конечное множество K_S. Оно состоит из подмножеств, то есть $K_S = \{TU , SU , CU\}$, где

$TU = \{t_{u1}, t_{u2}, \ldots, t_{ur}\}$ (Tracker Unit) есть непустое конечное множество бортовых устройств (или трекеров) в системе,

$SU = \{s_{u1}, s_{u2}, \ldots, s_{us}\}$ (Station Unit) – непустое конечное множество РС,

$CP = \{c_{u1}, c_{u2}, \ldots , c_{uc}\}$ (Control Point) есть непустое конечное множество ДП в системе.

Определим каждое из перечисленных подмножеств. Множество TU будем считать множеством-универсумом, содержащим в себе элементы с определенными свойствами. Для описания свойств всех элементов универсума введем базу переменных $P_1, P_2, \ldots, P_p$, характеризующих показатели соответствующих свойств элементов из множества TU и принимающих значения из множеств

$$A_i = \{a_0, a_1, \ldots, a_a\}, \text{ где } i = 1,\ldots, e.$$

Таким образом, выделим некоторые из свойств:

- P1 есть значение из множества A1 = {a11, a12, … , a1r}, определяющее номер конкретного трекера в системе (каждое бортовое устройство имеет определенный идентификатор или номер, по которому его можно однозначно отличить от других трекеров системы);

- P2 есть значение из множества A2 = {a21, a22 , … , a2w}, обозначающее принадлежность ТС, на котором установлен трекер, к определенной службе;
- P3 есть значение из множества A3 = {a31, a32 , … , a3v}, определяющее количество подключаемых к трекеру датчиков ТС (в составе каждого ТС есть штатные датчики, измеряющие все необходимые эксплуатационные параметры, они могут быть дискретными или аналоговыми);
- P4 есть значение из множества A4 = {a41, a42 , … , a4o}, определяющее наличие сетевых средств (Как правило, современные ТС имеют в своей составе различные сетевые среды для передачи сигналов и команд. Они могут использоваться для подключения новых блоков и устройств, не входящих в базовый набор любого ТС [2]);
- P5 есть значение из множества A5 = {a51, a52 , … , a5g}, определяющего наличие диагностической системы на ТС (как правило современные ТС имеют в своем составе системы бортовой диагностики, позволяющие контролировать состояние систем двигателя, топливной системы, системы зажигания, системы рециркуляции отработавших газов и т.п.).

Аналогичным образом опишем множество PC SU. Для описания свойств всех элементов данного множества введем базу переменных Q_1, Q_2, …, Q_q, характеризующих показатели соответствующих свойств элементов из множества SU и принимающих значения из множеств $B_i = \{b_0, b_1, …, b_b\}$, где i = 1,…,h.

Опишем некоторые из свойств:

- Q1 есть значение из множества B1 = {b11, b12, … , b1S}, определяющее номер конкретной РС в системе (каждая РС имеет определенный идентификатор или номер, по которому ее можно однозначно отличить от других РС системы);
- Q2 есть значение из множества B2 = {b21, b22, … , b2D}, определяющее местоположение определенной станции (РС являются неподвижными компонентами системы, их координаты местоположения неизменны).

Предположим, что множество СР также является множеством универсумом, содержащим в себе элементы с определенными свойствами. Для описания свойств всех элементов универсума введем базу переменных O_1, O_2,…, O_c, характеризующих показатели соответствующих свойств элементов из множества СР и принимающих значения из множеств

$$R_i = \{r_0, r_1, …, r_k\}, \text{ где } i = 1,…, c.$$

Получим некоторые из свойств:

- O1 есть значение из множества R1 = {r11, r12, … , r1r}, определяющее номер ДП в системе (поскольку ДП в системе может быть несколько, то для однозначной идентификации каждого ДП им присвоены номера);
- O2 есть значение из множества R2 = {r21, r22, … , r2d}, определяющее местоположение определенного ДП (ДП являются неподвижными компонентами системы, их координаты местоположения неизменны).
- O3 есть значение из множества R3 = {r31, r32, … , r3w}, определяющее принадлежность к определенной службе (каждый ДП принадлежит к какой-либо службе);
- O4 есть значение из множества R4 = {r41, r42, … , r4u}, определяющее количество обслуживаемых трекеров (как было указано выше, каждый трекер закреплен за определенным ДП);

Таким образом, каждый элемент подмножеств TU, SU и CP можно выделить среди множества других подобных элементов с помощью баз переменных P_1, P_2,…, P_p, Q_1, Q_2, …, Q_q и O_1, O_2,…, O_c.

Следует также выделить, что все компоненты системы осуществляют долговременное хранение данных, за исключением PC. На ДП осуществляется долговременное хранение данных и их анализ. Трекеры сохраняют информацию в энергонезависимой памяти. Срок хранения данных у трекеров гораздо короче, чем у ДП, но его достаточно для получения необходимой информации через определенный промежуток времени в случае сбоя работы системы. Кроме того, в процессе функционирования в компонентах системы происходят различные процессы обработки информации.

Таким образом, компоненты системы можно представить как непустое конечное множество процессов обработки информации P_S (Processing) и память (или множество блоков памяти) M_S (Memory), то есть

$$K_S = \{M_S, P_S\},$$

где $P_S = \{P_{S1}\, P_{S2}, P_{S3}\}$, причем P_{Si} определяет подмножества процессов обработки информации элементов компонентов системы, например,

$P_{Si} = \{ P_{Si,1}\, P_{Si,2}, \ldots, P_{Si,r} \}$ есть множество процессов обработки информации любого из подмножеств TU, SU или CP, где $P_{Si,j} \neq \varnothing$.

$M_S = \{DB, MT\}$ – множество блоков памяти элементов компонентов системы, где DB (Data Base) есть множество блоков памяти ДП (или баз данных) и MT (Memory Tracker) – множество блоков памяти трекеров в системе:

$$DB = \{db_1, db_2, \ldots, db_c\},$$
$$MT = \{mt_1, mt_2, \ldots, mt_r\}.$$

Из вышесказанного можно сделать вывод, что каждый элемент множеств TU, SU и CP можно представить как множество процессов обработки информации $P_{Si,j}$ и блок памяти $M_{Si,j}$.

Взаимодействие элементов компонентов системы происходит через информационные потоки. Информационные потоки обеспечивают все необходимые операции обмена информацией между элементами компонентов системы. Определим информационные потоки как непустое конечное множество I_S (Information). Поскольку любая передача данных в системе между элементами компонентов инициируется событиями или командами, то определим непустое конечное множество событий в системе EM (Event Message) и непустое конечное множество команд CM (Command Message).

$$EM = \{em_1, em_2, \ldots, em_m\},$$
$$CM = \{cm_1, cm_2, \ldots, cm_{cd}\}.$$

Оба множества характеризуют множество информационных потоков I_S. Тогда определим множество информационных потоков следующим образом:

$$I_S = \{EM, CM\}.$$

Под событиями будем понимать сообщения, формируемые в результате выполнения каких-либо условий в трекере и отправляемые на ДП системы по определенному алгоритму. Выделим основные события в системе:

- события определения местоположения;
- события включения/выключения бортового устройства;
- события изменения значений, подключенных к устройству аналоговых и дискретных датчиков;
- события изменения значений на входах от сетевых устройств;
- события изменения значений на входе разъема бортовой диагностической системы;
- события приема входящего пакета;
- события тревоги (в случае чрезвычайного происшествия водитель ТС может подать сигнал тревоги);
- события выхода из строя трекера (в случае несанкционированного воздействия на трекер, его поломки);
- события попытки несанкционированного доступа к данным на трекере.

Под командами будем понимать сообщения, инициирующие какие-либо действия со стороны участников взаимодействия. Как правило, команды формируются на ДП и предназначаются для РС и трекеров.

Выделим некоторые из команд в системе:

- команды запроса данных с трекера (имеют место быть в случае, если ДП не получал никаких данных с трекера в определенный период времени);
- команды дистанционного конфигурирования и обновления программного обеспечения трекеров и РС;
- команды управления исполнительными механизмами ТС (например, блокировка двигателя в случае тревоги);
- команды авторизации трекера или РС (имеют место быть при первом запуске трекера или С);
- команды оповещения трекеров и РС о неисправности других трекеров и РС (участники взаимодействия должны оперативно получать информацию о неисправных РС и трекерах);
- команда оповещения водителя о неисправности трекера;
- команды повторного запроса пришедшего пакета.

Для РС и трекеров существуют команды оповещения получения пакета с ошибкой.

При формировании множества информационных потоков I_S возможно будет удобно рассматривать их по отношению к компонентам системы, то есть, рассматривая компоненты системы, выделять их информационные потоки. Тогда множество информационных потоков системы может быть получено объединением множеств информационных потоков компонентов системы:

$$I_S = ITU \cup ISU \cup ICP.$$

Количество информационных потоков, функционирующих в определенный момент времени – величина переменная, так как элементы компонентов системы находятся в движении. В связи с этим мы можем определить максимальное количество информационных потоков, а в процессе функционирования системы будут возникать одни информационные потоки и исчезать другие.

Предполагается, что в системе мониторинга ТС функционирует несколько технологий связи (как проводные, так и беспроводные). Представим их как непустое конечное множество технологий $T_S = \{T_{S1}, T_{S2}, \dots, T_{St}\}$ (Technology).

При использовании беспроводных технологий связи всегда следует учитывать возможность их недоступности при определенных условиях или при наличии каких-либо преград. Поэтому выделим непустое конечное множество преград распространению сигнала $N = \{N_1, N_2, \dots, N_{sp}\}$ (Noise).

Множество помех информационных потоков составляется путем наложения множества элементарных помех обмена информацией на информационный поток:

$$NI_{Si} = \{ N_1 I_{Si}, N_2 I_{Si}, \dots, N_{sp} I_{Si}\}.$$

Тогда множество помех распространению сигнала в информационном потоке может быть получено следующим образом:

$$NI_S = I_S \times N.$$

Таким образом, в общем виде модель системы мониторинга ТС можно представить как $ISYS = \{TU, CP, SU, P_S, M_S, I_S, N_S, T_S\}$ (рис. 1).

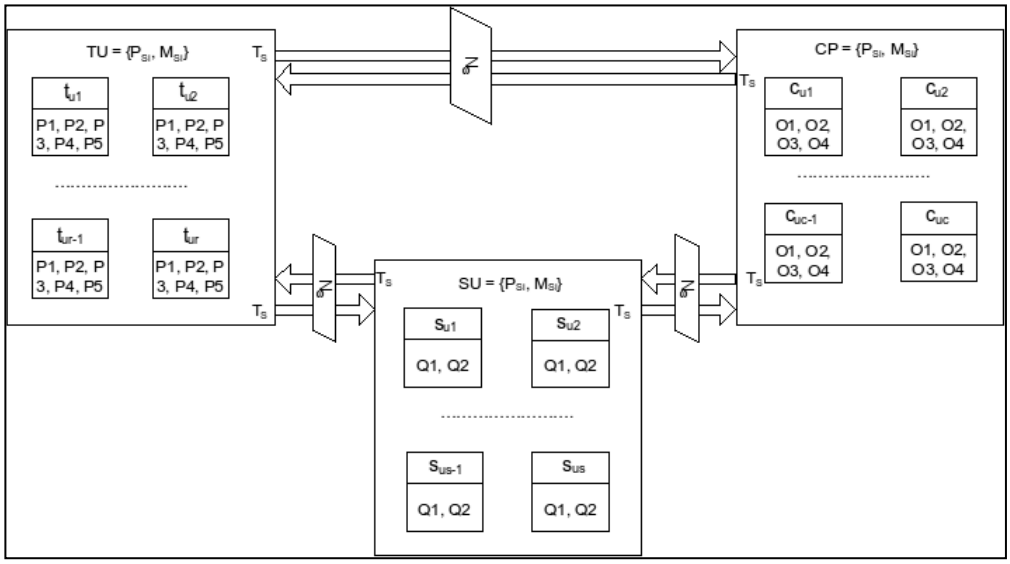

Рис. 1. Структурная схема модели системы мониторинга ТС

В результате мы получили формальную модель системы мониторинга ТС, построенную на теории множеств. Она представлена в статичном виде и не передает динамичности системы. Для описания динамики происходящих в системе процессов предполагается использовать теорию конечных автоматов. В перспективе также планируется детализировать полученную модель системы мониторинга ТС, разработать и реализовать методы рационального управления технологиями беспроводной связи. Это позволит получать информацию с трекеров критически важных подвижных объектов в режиме реального времени, даже при плохих погодных условиях, преградах или помехах.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Постановление Правительства Российской Федерации от 25 августа 2008 г. N 641 "Об оснащении транспортных, технических средств и систем аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS" // Собрание законодательства Российской Федерации. – М.: "Юридическая литература администрации президента Российской Федерации", 2008. – №35. – С. 4037.

2. *Пакулова Е.А.* Аспекты безопасности в системе мониторинга транспортных средств // Материалы I Всероссийская молодежная конференция по проблемам информационной безопасности ПЕРСПЕКТИВА-2009. – Таганрог: Изд-во ТТИ ЮФУ, 2009. – С. 24 – 28.

Пакулова Екатерина Анатольевна
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: pakulova_e@mail.ru.
347928, г. Таганрог, ул. Чехова, 2, корпус "И".
Тел.: 8 (8634) 312-018.
Кафедра безопасности информационных технологий; аспирант.

Pakulova Ekaterina Anatolyevna
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education "Southern Federal University".
E-mail: pakulova_e@mail.ru.
Block "I", 2, Chehov str., Taganrog, 347928, Russia.
Phone: 8 (8634) 312-018.
The Department of Security of Information Technologies; post-graduate student.

УДК 681.324

Е.С. Абрамов

ПОСТРОЕНИЕ АДАПТИВНОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Предлагается методика построения системы защиты информации, позволяющая с помощью методов теории иммунных систем, нечёткой логики, искусственных нейронных сетей, нечеткого многокритериального выбора решений и численных методов оптимизации создать и поддерживать в актуальном состоянии систему защиты информации, в которой обеспечивается поддержание уровня защищенности, адекватного текущим угрозам. Кроме того, решается задача оценки эффективности получившейся новой структуры СЗИ без изменения режима функционирования текущей конфигурации средств защиты.

Иммунные системы; нечёткая логика; искусственные нейронные сети; нечеткий многокритериальный выбор; имитационное моделирование.

E.S. Abramov

DEVELOPMENT OF ADAPTIVE SYSTEM OF INFORMATION SECURITY

There is method of constructing a system of information protection, which allows using the methods of the theory of immune systems, fuzzy logic, artificial neural net-