Обзор методов, применяемых при проектировании защищенных систем связи геоинформационных систем

Overview of methods used in the design of secure communication systems of geoinformation systems

Карманов / Karmanov A.
Андрей Геннадьевич
(karmanov.nip@gmail.com)
кандидат технических наук, доцент.
ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» (Университет ИТМО), доцент кафедры ГИС.
г. Санкт-Петербург

Чжао Лэй
(zl_2321@hotmail.com)
Университет ИТМО,
аспирант кафедры ГИС.
г. Санкт-Петербург

Бондаренко / Bondarenko I.
Игорь Борисович
(igorlitmo@rambler.ru)
кандидат технических наук.
Университет ИТМО,
доцент кафедры ГИС.
г. Санкт-Петербург

Иванова / Ivanova E.
Евгения Анатольевна
(karmanov.nip@gmail.com)
Университет ИТМО,
аспирант кафедры ГИС.
г. Санкт-Петербург

Ключевые слова: геоинформационная система – geoinformation system; живучесть – survivability; экспертные системы – expert systems; искусственные нейронные сети – artificial neural networks; ранжирование – ranging; нейроны – neurons; оптимизация – optimization; протоколы – protocols; радиосеть – radio network.

В работе рассмотрен набор методов, использованных для проектирования систем связи с наземными подвижными объектами при построении геоинформационных систем. Представленная методология опирается на методы экспертных оценок, оптимизации, аппарат искусственных нейронных сетей, математическую статистику. Позволяет производить оценку применимости компонентов беспроводных сетей для разработки защищенных систем связи на основе анализа параметров живучести.

The article considers a set of methods used to design communication systems with terrestrial mobile objects in the construction of geoinformation systems. The presented methodology is based on methods of expert evaluations, optimization, the device of artificial neural networks, mathematical statistics. Allows evaluating the applicability of wireless network components for the development of secure communication systems based on the analysis of survivability parameters.

Введение

Геоинформационные системы (ГИС) представляют собой бурно развивающееся направление, имеющее военное, промышленное и гражданское применение. Средствами ГИС решаются задачи картографирования, кадастра, мониторинга экологии и чрезвычайных событий, геомаркетинга и т.п. [1, 2].

ГИС – программно-технические комплексы, включающие в себя: технические средства обработки данных, средства обмена данными в ЛВС с выходом в разнотипные сети, а также резервированные средства хранения данных и осуществляющие взаимодействие с внешними организациями по коммутируемым и выделенным каналам связи. Анализ структуры ГИС и типа системы управления базами данных позволяют отнести такие системы к распределенным. Развитие беспроводных протоколов связи позволило получить доступ к ресурсам ГИС практически из любой точки планеты.

Большое число разнородных пользователей ГИС, таких как государственные и ведомственные организации, коммерческие предприятия, частные лица, – диктует необходимость обеспечения защиты конфиденциальной информации, содержащей сведения, составляющие государственную, служебную и коммерческую тайну, а также персональные данные пользователей

[3]. Еще одной проблемой при защите данных в ГИС является их большой объем, что затрудняет использование методов защиты, требующих значительных временных затрат.

Для устойчивого функционирования ГИС при влиянии негативных воздействий разработчикам необходимо решать ряд задач, таких как: выявление узких мест каналов, узлов при перегрузке, обеспечение безопасного обмена между источниками и приемниками информации и т.д.

Ведущие производители оборудования активно ведут исследования и разработки в области мобильных систем связи с целью повышения пропускной способности и скорости передачи цифровых данных. Несмотря на то что в беспроводных сетях используются встраиваемые протоколы безопасности, которые включают в себя шифрование и аутентификацию пользователя, системам связи, особенно на этапе их разработки, необходимо уделять повышенное внимание. В связи с этим тематика статьи является актуальной.

Предложенные методы при организации защиты систем радиосвязи

Для построения и развертывания ГИС может использоваться широкая номенклатура сетевых протоколов, поддерживающих сети подвижной связи сухопутные, морские, авиационные, спутниковые и общего пользования. Проанализировав беспроводные стандарты связи, используемые в настоящее время для передачи данных, сделан вывод о том, что организации, особенно службы по обеспечению безопасности, испытывают дефицит радиочастотных каналов для развертывания систем связи. Каналов становится еще меньше из-за продажи прав использования некоторых диапазонов частот коммерческим операторам связи. Это влечет к сужению полосы частот (F_c):

$$F_c = nF_n,$$

где n – количество выделенных каналов с шириной полосы F_n у каждого.

Основными параметрами средств связи, определяющими их разделение на различные классы профессионального использования, являются:

– плотность абонентов в обслуживаемой зоне;

– площадь покрытия, которая определяет масштаб системы;

– уровень сервиса;

– автоматический или ручной выбор канала;

– возможности и глубина группообразования;

– наличие индивидуальных и аварийных вызовов;

– идентификация абонентов;

– выход в телефонную сеть, полный дуплекс на уровне абонентского терминала;

– передача коротких сообщений;

– передача данных и др.

Далее были проанализированы угрозы системе радиосвязи для ГИС. Основными угрозами системе радиосвязи являются следующие.

1. Внешняя помеха, источником которой может быть как внешняя среда (неумышленная), так и аппаратура злоумышленника (злонамеренная).

2. Перехват (прослушивание) информации с целью дальнейшей расшифровки. Удобство и легкость развертывания беспроводной сети оборачивается мобильностью не только пользователей, но и злоумышленника, местоположение которого определить достаточно сложно.

3. Искажение информации с целью препятствия приему пакета, искусственного сбоя.

4. DDoS-атака с целью перегрузки канала и/или аппаратуры радиостанций. Такие атаки очень эффективны и трудно поддаются анализу.

5. Подмена информации.

6. Клонирование SIM-карт, аппаратуры.

Злоумышленником могут реализовываться одновременно несколько из перечисленных. Например, если уровень злонамеренно генерированной помехи превосходит допустимый уровень, при котором приемо-передающей аппаратуре невозможно выделить полезный сигнал, возникает глушение. Глушение мобильной станции абонента производится с целью ее подмены аппаратом злоумышленника, или чтобы не дать клиенту реализовать соединение с базовой станцией (БС). Может осуществляться постановкой помех или направленными DoS-атаками. Глушение БС опять же может осуществляться для лишения пользователя услуг связи или для подмены БС пользователя базовой станцией злоумышленника.

Доступность аппаратуры для беспроводной связи делает возможным организацию ложной точки доступа с имитацией работы с фирменными сетевыми ресурсами.

Наиболее действенными способами защиты является контроль системы связи, резервирование, шифрование, аутентификация и идентификация пользователей и операторов, надежные схемы управления доступом пользователей к ресурсам сети.

При построении беспроводных сетей различных стандартов возможны следующие источники возникновения уязвимостей: среда передачи данных, технические параметры стандартов беспроводных сетей, системы аутентификации, криптографические методы и алгоритмы, программное и аппаратное обеспечения, человеческий фактор.

Модель оценки живучести ГИС от параметров системы включает следующие компоненты: топология сети **G**, множество целей **C** и условия функционирования ГИС **U**, надежность **P**, а также множество решаемых задач **Z**. Общий показатель живучести системы **Q** имеет интегральный и комплексный характер зависимости от живучести входящих подсистем Q_i:

$$\mathbf{Q} = F(Q_1, Q_2, ..., Q_k),\ Q_i = f(G_i, C_i, U_i, Z_i, P_i) \quad (1)$$

Запас структурной живучести системы будет определяться ее избыточностью и обеспечиваться резервированием элементов. Надежность системы – сложный функционал, включающий как надежность входящих в ГИС элементов, так и структуру подсистем:

$$\mathbf{P}_{\text{сист}} = f(P_i, G_i),\ i = \overline{1,n}. \quad (2)$$

С увеличением сложности ГИС растет сложность моделей (1) и (2) и уменьшается уровень негативных воздействий, достаточный для перехода ГИС в худшее состояние.

Параметры математических моделей, характеризующих живучесть ГИС, были получены с помощью метода экспертных оценок [4, 5]. То есть определены параметры протоколов беспроводной связи, которые сильнее всего влияют на их защищенность.

Вес j-го фактора w_j определим по выражению:

$$w_j = \frac{1}{k}\sum_{i=1}^{k}\frac{x_{ji}}{\sum_{j=1}^{n} x_{ji}}, \quad (3)$$

где n – число параметров; k – количество экспертов.

Коэффициент конкордации (при наличии связанных рангов в ответах экспертов) определим по соотношению:

$$W = \frac{12S}{k^2(n^3 - n) - k\sum_{i=1}^{k} H_i}, \quad (4)$$

где

$$H_i = \sum_{p=1}^{Z_i}(h_p^3 - h_p), \quad (5)$$

H_i – показатель связанных рангов для i-й ранжировки; Z_i – число групп равных рангов в i-й ранжировки; h_p – число равных рангов в p-й группе связанных рангов при ранжировке i-м экспертом; величина S рассчитана по соотношению:

$$S = \sum_{j=1}^{n}\left(\sum_{i=1}^{k} x_{ji} - 0{,}5k(n+1)\right)^2. \quad (6)$$

Коэффициент конкордации W, рассчитанный по соотношениям (4–6), изменяется в диапазоне [0, 1]. Его максимум означает, что все эксперты сошлись во мнении при расстановке рангов, а минимум – что оценки экспертов рассогласованы.

Для определения показателей живучести системы радиосвязи был использован аппарат искусственных нейронных сетей (ИНС), описанный, например, в источниках [6, 7]. Сложность использования аппарата ИНС на практике представляет: подбор структуры сети нейронов и ее обучение.

Путем последовательного приближения к оптимальному варианту сети было определено количество слоев, число нейронов во внутренних и внешних слоях в многослойном персептроне, метод оптимизации ошибки сети при ее обучении с помощью процедуры обратного распространения ошибки. Конец обучения ИНС наступает при условии:

$$\varepsilon_{\text{опт}} = \min\left[\frac{1}{2N_S}\sum_{i=1}^{N_S}(OUT_i - E_i)^2\right] \quad (7)$$

В соотношении (7): N_s – количество обучающих пар; OUT_i – полученное с помощью сети значение выходного нейрона при i-м наборе обучения; E_i – требуемое значение выходного нейрона при i-м наборе обучения.

Полная ошибка ИНС из выражения (7):

$$\varepsilon = \varepsilon(\mathbf{W}, \mathbf{K}, \mathbf{L}_t \ldots) = \frac{1}{2N_S}\sum_{i=1}^{N_S}\Delta_i^2, \quad (8)$$

где $\mathbf{W}$, $\mathbf{K}$, $\mathbf{L}_t$... – множества весов входного, выходного и скрытых слоев (t –количество скрытых слоев) соответственно, Δ_i – ошибка i-го выхода сети. Функция (8) является неотрицательной, а из условия (7) при $\varepsilon = 0$ она имеет глобальный экстремум: в этом случае сеть не допускает ошибок. Выбор метода оптимизации ошибки осуществлялся из следующего набора: метод наискорейшего (градиентного) спуска, метод параллельных касательных, сопряженных градиентов, BFGS и DFP.

Результаты экспериментов и выводы

По соотношениям (3–6) был рассчитан коэффициент конкордации $W = 0{,}403$ по результатам опроса экспертов. Полученное значение означает согласованность экспертов. В результате были определены значимые параметры: общее количество каналов, используемая полоса частот, мощность БС, разнос каналов, наличие идентификации абонента, типичный радиус ячейки, зависимость от ландшафта, ограничение по доступу, область применения связи, наличие шифрования и оплата за использование. Остальные показатели не учитывались при дальнейшем анализе. Далее было сформировано обучающее множество для ИНС, на выход которой подавалось значение времени живучести протокола связи, взятое из открытых источников информации. С помощью программного средства NeuroPro и имитационных экспериментов была определена структура сети и ее параметры. Сеть имеет структуру 11 нейронов на входе, 8 нейронов в скрытом слое и 1 – выходной. Наилучшими методами оптимизации ошибки стали: сопряженных градиентов и BFGS. При значении точности ±2 % понадобилось 524

цикла обучения ИНС до 100%; максимальная ошибка 1,65. Обученная таким образом сеть была использована для нахождения прогнозного значения времени живучести системы связи на основе технологии *NFC* (Near Field Communication – высокочастотной связи малого радиуса действия). Полученный прогноз составил 23,5 года. Предложенная методология позволяет также проводить анализ структурной живучести беспроводной сети связи для ГИС, но данное описание выходит за рамки объема данной статьи.

Литература

1. Защита данных геоинформационных систем / Л.К. Бабенко [и др.]. – М.: Гелиос АРВ, 2010. – 587 с.

2. Завгородний, В. И. Комплексная защита информации в компьютерных системах: Учебное пособие / В.И. Завгородний – М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. – 264 с.

3. Малик, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малик. – М.: ИНФРА-М, 2004. – 282 с.

4. Рыбина, Г. В. Особенности современных подходов к построению экспертных систем / Г.В. Рыбина // Труды конгресса «Искусственный интеллект в XXI веке». Научное издание. – М.: Изд. Физ.-мат. Лит., 2001. – С. 383–390.

5. Галушкин, А. И. Теория нейронных сетей / А.И. Галушкин. – М.: ИСПЖР, 2000. – 325 с.

6. Каллан, Р. Основные концепции нейронных сетей / Р. Каллан. – М.: Вильямс, 2001. – 288 с.

7. Прикладной статистический анализ данных. Теория. Компьютерная обработка. Области применения : Учебно-практическое пособие для вузов : [В 2-х книгах] / С.В. Алексахин [и др.] – М.: Приор, 1998. – 224 с.