УДК 004.056.2

В. П. Бубнов, д-р техн. наук,
А. Д. Хомоненко, д-р техн. наук,
В. В. Яковлев, д-р техн. наук,
С. В. Клименко

Кафедра «Информационные и вычислительные системы»,
Петербургский государственный университет путей сообщения
Императора Александра I

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ДАННЫХ ЛОКАЛЬНОГО СЕРВЕРА СИСТЕМЫ АВТОМАТИЗИРОВАННОГО ГЕОДЕЗИЧЕСКОГО МОНИТОРИНГА

Рассматривается совершенствование архитектуры программного обеспечения локального сервера системы автоматизированного геодезического мониторинга объектов в аспекте защиты передаваемых данных путем проверки подлинности при их получении локальным сервером. Описан программный комплекс автоматизированной системы геодезического мониторинга. Исследуется выявление поврежденных данных на основе анализа архитектуры комплекса. Для решения исследуемого вопроса предлагается механизм контроля целостности получаемых данных при их передаче по зашумленным каналам, которые вносят повреждения. Предложены алгоритмы проверки целостности передачи данных между датчиком и локальным сервером, а также между датчиком и удаленным сервером, поскольку целостность передаваемой информации от датчиков к программному комплексу важна: от ее достоверности зависит объективный анализ собираемой информации, на основании которого необходимо реагировать на опасные отклонения искусственных сооружений от нормы. Дана экспериментальная оценка временной эффективности расчета контрольной суммы для контроля целостности передачи данных.

опасный объект; программный комплекс; сервер; система автоматизированного геодезического мониторинга; датчики

Введение

Одним из основных направлений по предотвращению аварий и разрушений объектов, таких как автодорожные и железнодорожные мосты, тоннели метрополитена и другие критически важные сооружения, что приводит к порче и уничтожению значительных материальных ценностей и даже к человеческим жертвам, является организация системы мониторинга технического состояния этих объектов.

Под мониторингом критически важных и опасных объектов понимается процесс инструментального автоматизированного круглосуточного наблюде-

ния за определенными параметрами ранее перечисленных объектов. Задачей мониторинга является предотвращение опасных ситуаций, нанесения ущерба объектам или их разрушения.

Для объективного анализа собираемой информации и своевременного реагирования на опасные отклонения искусственных сооружений от нормального состояния необходимо, чтобы в состав системы комплексной безопасности движения входила подсистема автоматизированного мониторинга искусственных сооружений. В [1] представлена Концепция Федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры Российской Федерации и опасных грузов, принятая в 2005 г. Проблема мониторинга искусственных сооружений также рассмотрена в [2–7].

Актуальными направлениями развития программного комплекса системы автоматизированного геодезического мониторинга (САГМ) являются проверка подлинности (целостности) данных при их получении, а также шифрование данных перед передачей между локальным и удаленным серверами и устройствами пользователя, поскольку от достоверности данных зависит объективный анализ собираемой информации, на основании которого необходимо реагировать на опасные отклонения искусственных сооружений.

1 Обзор системы автоматизированного геодезического мониторинга

Комплекс САГМ описан в [8, 9], а процесс выбора системы управлениями базами данных (СУБД), наиболее пригодной для использования на локальном сервере САГМ, – в [10]. Он дает возможность подключить любые наборы датчиков, производить сбор, передачу, анализ и хранение данных. Возможности комплекса могут расширяться в соответствии с актуальными техническими требованиями к подобным комплексам.

Перечислим основные компоненты комплекса:

1) программное обеспечение локального сервера (ПОЛС);

2) программное обеспечение удаленного сервера (ПОУС, REST API);

3) графический интерфейс (Web Application).

Обобщенные функции элементов системы, представленной на схеме рис. 1, состоят в следующем.

ПОЛС обеспечивает настройку, контроль состояния, сбор информации со всех датчиков, установленных на контролируемом сооружении. Его основная задача – считывание информации с датчиков.

ПОУС ведет круглосуточный анализ получаемых данных, а также предоставляет возможность визуализировать обработанный результат.

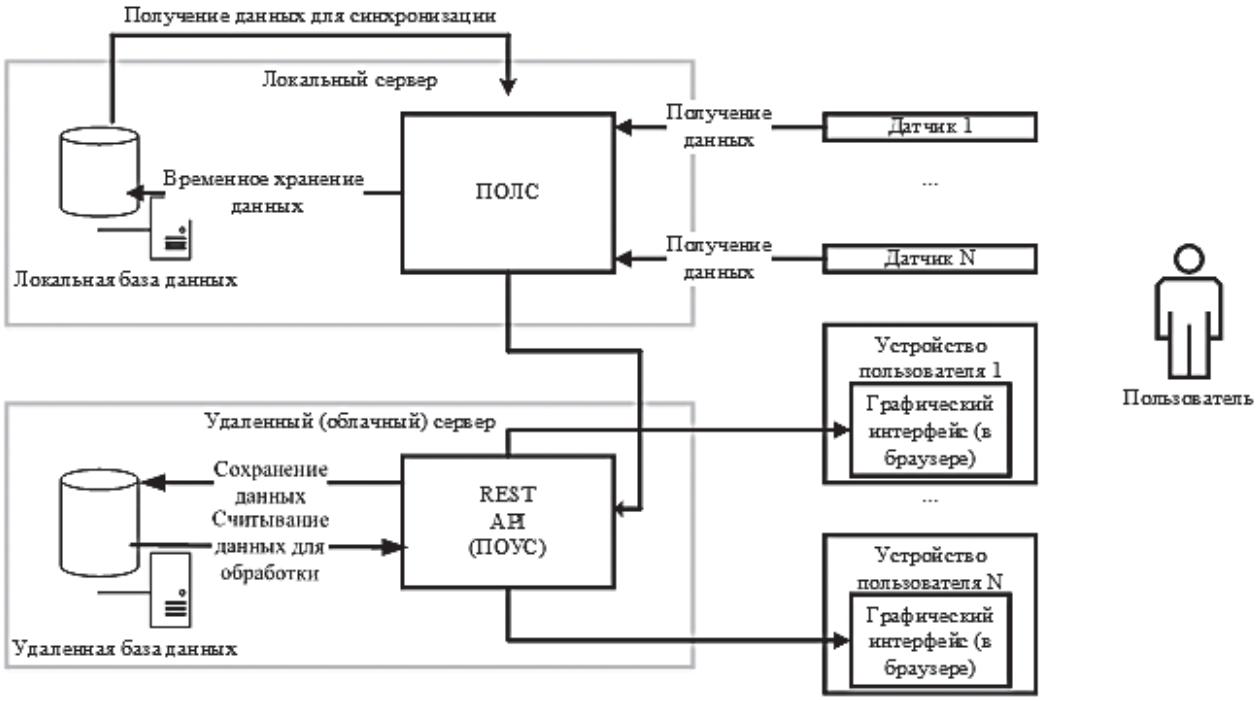

Рис. 1. Схема САГМ

Графический интерфейс – клиентская часть программного комплекса. Его основными задачами являются визуализация данных, поступающих с удаленного сервера в виде графиков, и контроль доступа к данным.

Основные ограничения, наложенные на локальный сервер, состоят в следующем.

К локальному серверу подключаются датчики одного типа.

Через равные интервалы времени в систему поступают данные от nd подключенных к локальному серверу датчиков. Поскольку все датчики одного типа и заявки от них обрабатываются непрерывно, группы заявок объединяются и приходят одновременно как единая заявка первого типа.

Через равные интервалы времени поступают заявки второго типа, связанные с технологическим циклом синхронизации данных между локальным и удаленным сервером.

Важно, чтобы после одновременного поступления двух заявок второго и первого типа они успели пройти обслуживание до момента поступления последующей заявки.

ПОУС представляет собой HTTP-сервер, который получает данные от объектов в формате JSON (Java Script Object Notation – текстовый формат данных), проверяет, с какого объекта и датчика присланы данные, и сохраняет их в соответствующей таблице в базе данных (рис. 2). Анализ данных заключается в проверке правильности принимаемых данных, в том, что они не выходят за рамки позволенных диапазонов, а также в проверке временных интервалов:

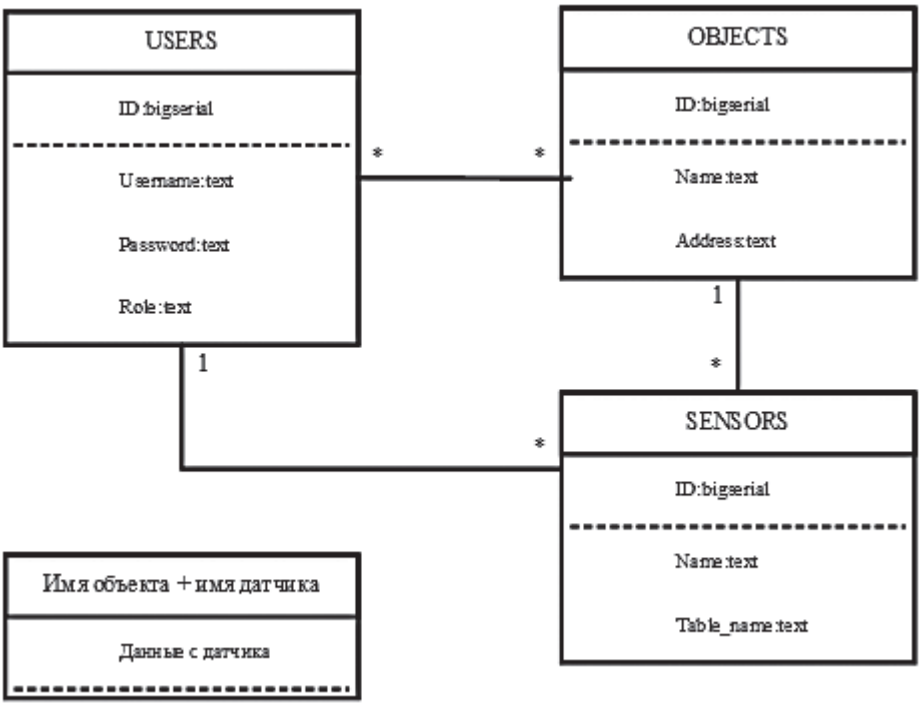

Рис. 2. Схема базы данных

когда временные интервалы поступления данных от датчика неравномерны, следует заполнять их средними показателями, рассчитанными на основе последних десяти значений, что необходимо, так как во многих датчиках существует вероятность задержек данных на несколько секунд. Эта информация есть в документации датчиков, а для математических алгоритмов анализа данных требуются значения, поступающие с одинаковым интервалом.

Связь между приложением графического интерфейса и ПОУС осуществляет WebSockets. WebSockets – это надстройка над HTTP-протоколом, предоставляющая API для разработки интерактивных web-приложений. Такие параметры приложения, как порты HTTP-сервера и Websocket-сервера, подключение к базе данных, конфигурируют с помощью XML-файла. Необходимо отметить, что важной задачей для систем такого рода является защита данных, поэтому ПОУС не принимает никаких запросов по WebSocket, кроме запросов авторизации при новых подключениях.

На рис. 3 показан скриншот работы графического интерфейса в момент просмотра данных, поступающих от датчика в режиме реального времени.

Все три программных компонента САГМ могут находиться как на одном сервере, так и на трех разных, что делает программный комплекс достаточно гибким в использовании. Время от поступления данных на локальный сервер до их отображения на компоненте «Графический интерфейс» зависит от задержек в канале связи, а также от интервала синхронизации удаленного и локального серверов.

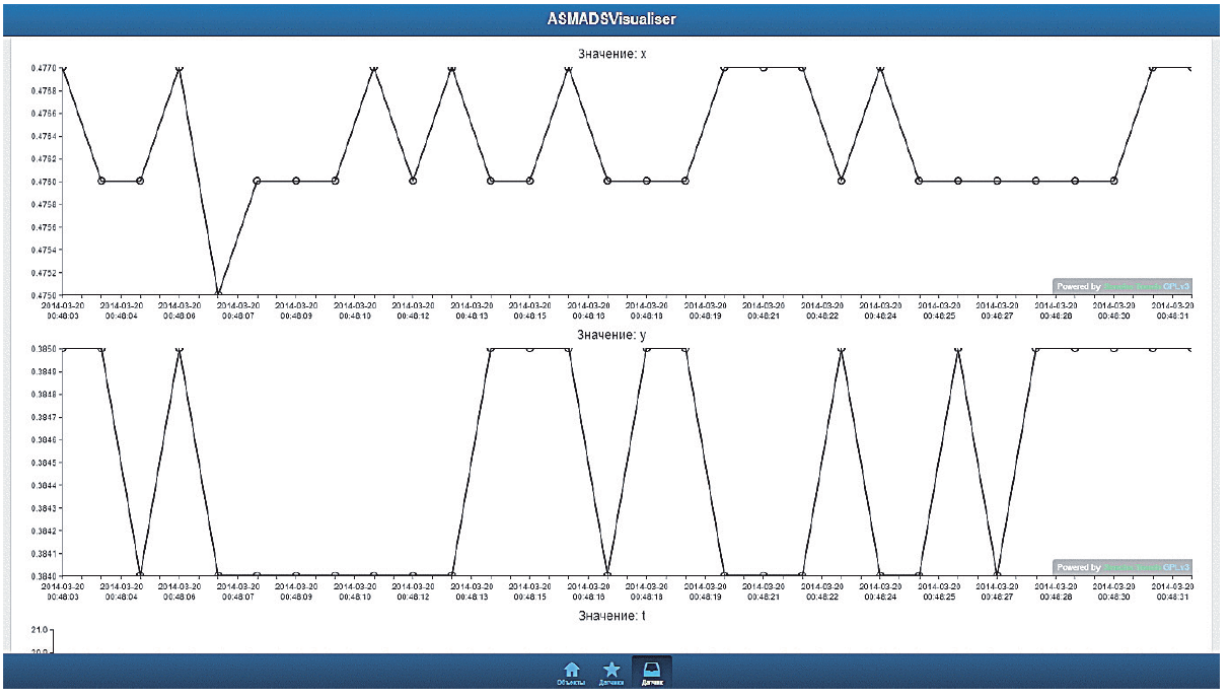

Рис. 3. Данные с датчика Nivel220

Архитектура программных компонентов устроена таким образом, что для сбора информации с каждого датчика выделяется отдельный поток вычислений. ПОЛС и REST API разработаны на языке JavaSE, что делает их платформенно независимыми.

Таким образом, САГМ способна в реальном времени получать, передавать, накапливать и анализировать данные со всех датчиков исследуемого объекта, а при необходимости ее можно дополнить неограниченным количеством новых типов сенсоров без прекращения функционирования.

2 Постановка задачи

Как отмечалось, актуальными направлениями развития описанного программного комплекса являются проверка подлинности (целостности) данных при их получении и шифрование данных перед передачей между локальным и удаленным серверами и устройствами пользователя.

На схеме рис. 1 видно, что ПОЛС обеспечивает настройку, контроль состояния, сбор информации со всех датчиков, установленных на контролируемом сооружении. Именно компонент ПОЛС должен обеспечивать проверку целостности данных от датчиков, поскольку в дальнейшем эта информация будет передаваться на удаленный сервер и визуализироваться для конечного пользователя. Между компонентами ПОЛС и ПОУС необходимо предусмотреть аналогичную проверку, так как при условии проверки только между

ПОЛС и датчиками нельзя гарантировать корректную передачу от ПОЛС к ПОУС. Таким образом, для защиты информации, содержащейся в пакете и передаваемой от датчика к ПОЛС и от ПОЛС к ПОУС, необходим подсчет контрольной суммы передаваемых данных.

3 Методы и результаты

Подсчет контрольной суммы можно отнести к методу обнаружения ошибок, предназначенному для выявления повреждений сообщений при их передаче по зашумленным каналам, которые и приносят эти повреждения. Для этого передающие устройства (в нашем случае это ПОЛС и датчики), создают некоторое число, называемое контрольной суммой, и добавляют его к передаваемому сообщению. Приемное устройство, используя тот же алгоритм, рассчитывает контрольную сумму принятого сообщения и сравнивает ее с переданным значением.

Под контрольной суммой, или хешем, понимается некоторое значение, рассчитанное по набору данных путем применения математических алгоритмов, обеспечивающих устойчивость к хеш-коллизиям, например, CRC-32 (Cyclic Redundancy Code 32) или MD5 (Message Digest 5) [11]. Названые алгоритмы имеют широкое практическое применение и количество реализаций, адаптированных под различные высокоуровневые языки программирования. Отметим, что подсчет контрольной суммы на высокопроизводительных системах занимает немного времени [12].

CRC-32 чаще всего используется в работе программ-архиваторов, а MD5 – не только для проверки целостности данных, но и получения довольно надежного идентификатора файла. Последний часто используется при поиске одинаковых файлов на компьютере, чтобы не сравнивать все содержимое, но только хеш.

Данные, передаваемые цифровым способом, отправляются фрагментами, и часты случаи, когда эти фрагменты теряются или повреждаются [13]. Хеш предназначен для проверки целостности данных и выявления поврежденных фрагментов.

Специальный алгоритм (CRC32 или MD5) рассчитывает сумму полученного файла, и, если она совпадает с контрольной суммой оригинала, это может означать, что передача прошла успешно. В противном случае возникает ошибка контрольной суммы, которая свидетельствует о нарушении целостности файла.

Таким образом, при помощи одного из алгоритмов вычисляется контрольная сумма пакета данных, передаваемая вместе с ним. Принимающее устройство (ПОЛС) повторно вычисляет контрольную сумму пакета данных. Несовпадение рассчитанной и принятой контрольной суммы расценивается как ошибка передачи данных, при этом, как правило (в зависимости от типа

передаваемого пакета), принимающее устройство (ПОЛС) производит запрос повторной передачи ошибочного пакета.

Алгоритм проверки целостности данных при их передаче между ПОЛС и датчиками представлен на рис. 4.

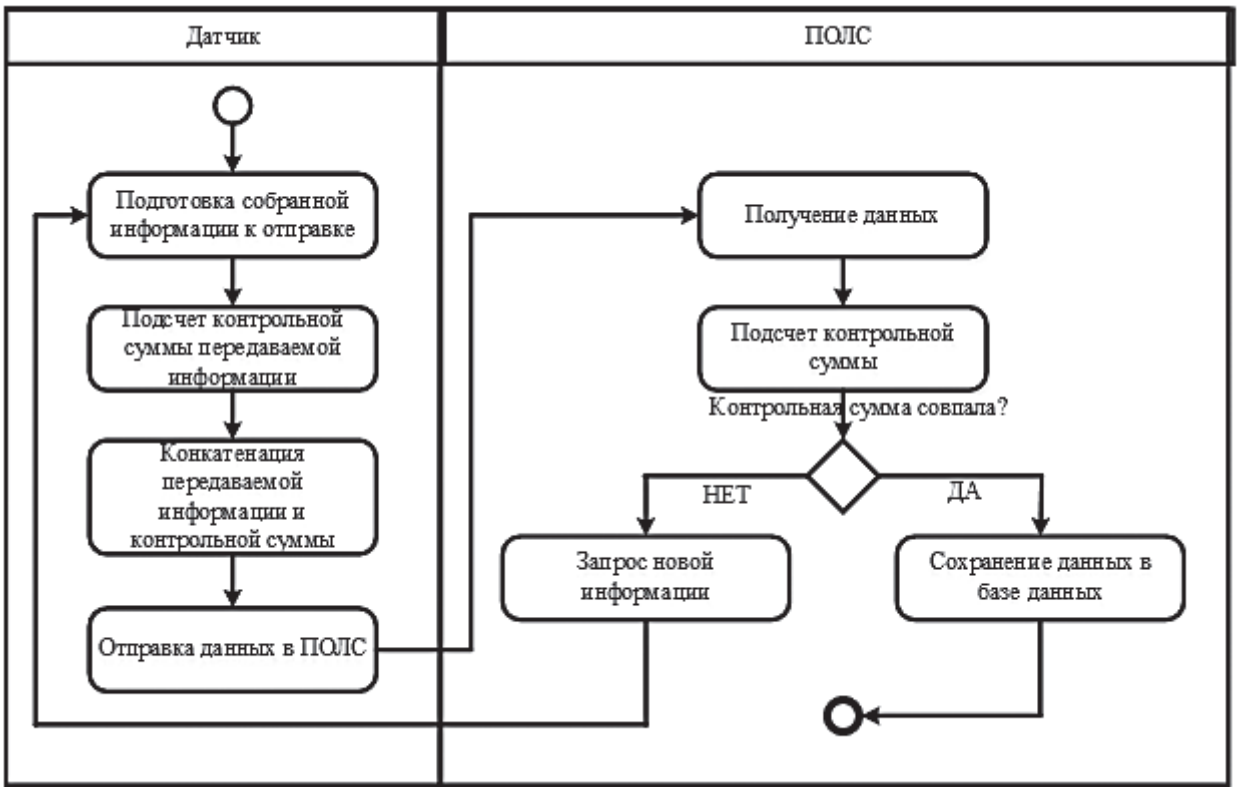

Рис. 4. Алгоритм проверки целостности данных при передаче между датчиком и ПОЛС

Алгоритм проверки целостности данных при их передаче между ПОЛС и ПОУС будет выглядеть так, как показано на рис. 5.

Вычисления CRC возможно реализовать на любом языке, так как операции XOR и SHL встроены практически в любой язык программирования. Алгоритм (G – порождающий полином, $k_{код}$ – битовое сообщение) можно записать так:

1. Дополнить исходное сообщение нулями для выравнивания (количество нулей определяется степенью порождающего полинома). Например, для порождающего полинома 10011 исходное сообщение дополняется четырьмя нулями, $k_{доп0} = k_{код}0000$.

2. Инициализировать начальное значение CRC. Например, если $r_{код} = 4$, то начальное значение CRC = 0000.

3. Выполнить операцию сдвига влево последовательности битов сообщения $k_{доп0}$ до тех пор, пока бит в ячейке (том месте, где изначально находился старший бит $k_{доп0}$) не станет равным единице или количество битов станет меньше, чем в делителе.

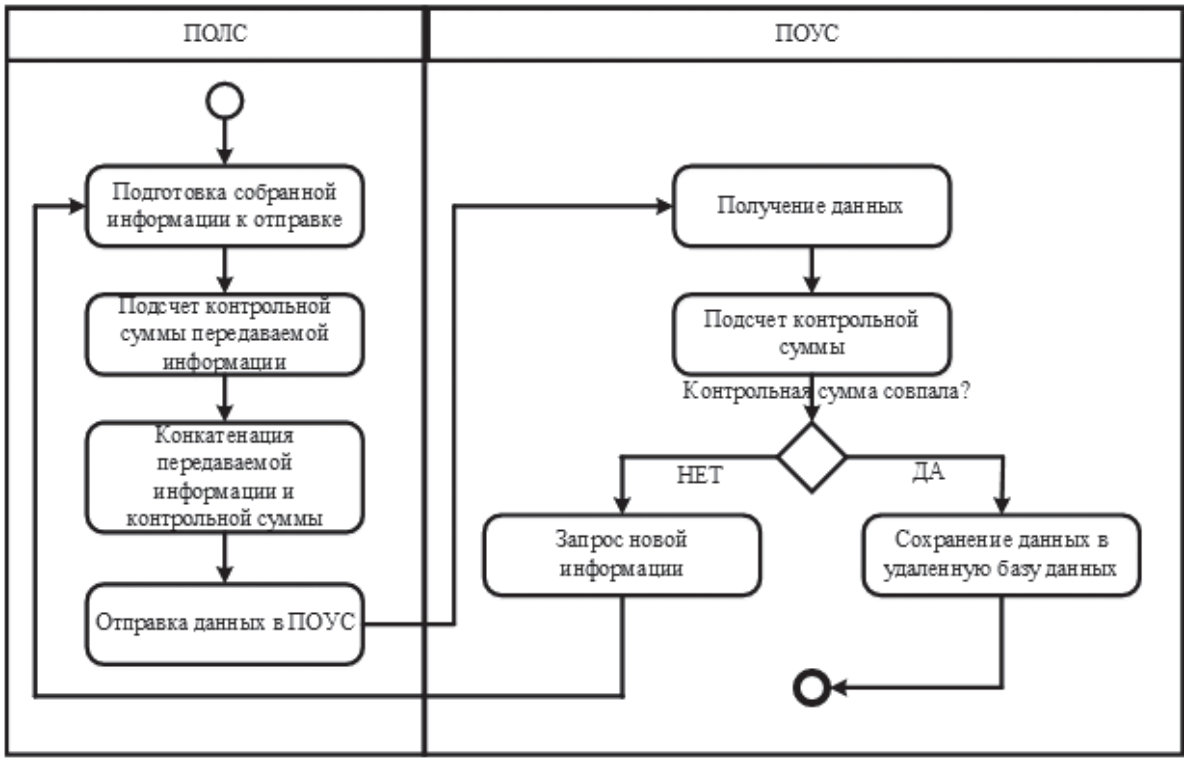

Рис. 5. Алгоритм проверки целостности данных при передаче между ПОЛС и ПОУС

4. Если старший бит станет равным единице, производим операцию XOR между сообщением и порождающим полиномом и повторяем шаг 2.

То, что в конце остается от последовательности $k_{доп0}$, называется CRC-остатком.

Пример выполнения алгоритма вычисления CRC-остатка приведен на рис. 6, где в качестве порождающего выбран полином 10011.

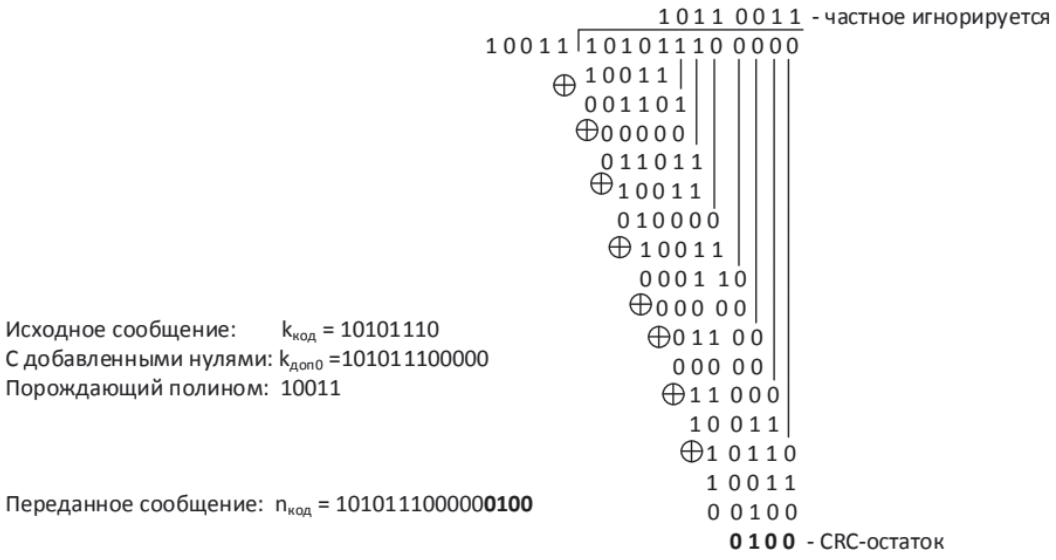

Рис. 6. Вычисление CRC-остатка

Существуют алгоритмы, работающие быстрее вышеописанного (табличный, зеркальный и др.).

4 Оценка временно́й эффективности

Под временной эффективностью понимается время отклика от момента отправки запроса (на получение контрольной суммы) до его выполнения. Современные системы хранения данных обладают расширенными функциональными возможностями и могут производить подсчет контрольных сумм по запросу, в частности, могут подсчитывать контрольную сумму всей дорожки диска [12].

Если принять во внимание, что ПОЛС и ПОУС отвечают за подсчет и проверку контрольных сумм полученной информации, то справедлива оценка временной эффективности, для которой была собрана статистика, отражающая время отклика на исполнение запросов в зависимости от числа дорожек. Время отклика получено для дорожек, где $i = 1, 5, 10, 15$.

Для вычисления среднеарифметического значения времени отклика на исполнение запроса использовалась формула

$$\overline{t} = \frac{1}{n} \cdot \sum_{i=1}^{n} t_i, \tag{1}$$

где t_i – время отклика i-го запроса на получение CRC кода; n – общее количество обращений к дорожке.

Среднеквадратичное отклонение рассчитывалось по формуле

$$\sigma = \sqrt{\frac{1}{N-1} \cdot \sum_{i=1}^{n} (t_i - \overline{t})^2}, \tag{2}$$

где $\overline{t}$ – среднеарифметическое значение времени отклика.

Результаты измерений представлены в табл. 1 и 2.

ТАБЛИЦА 1. Результаты запроса к группам дорожек

Тип запроса к дорожке	Количество дорожек	Количество запросов	Среднее время получения запроса, с	Среднеквадратичное отклонение
Получение CRC-кода	1	100	0,0011	0,0001
	5	50	0,0040	0,0011
	10		0,0068	0,0015
	15		0,0092	0,0008

ТАБЛИЦА 2. Результаты выполнения запросов к группам дорожек

Тип запроса к дорожке	Количество дорожек	Количество запросов	Среднее время получения запроса, с	Среднеквадратичное отклонение
Получение содержимого	1	100	0,001	0,0007
	5	50	0,0038	0,0017
	10		0,0063	0,0013
	15		0,0094	0,0015

Из рис. 7 видно, что подсчет контрольной суммы оказывает незначительное влияние на время передачи данных от датчиков к ПОЛС и от ПОЛС к ПОУС, его использование позволяет обеспечить целостность пересылаемых данных между этими компонентами.

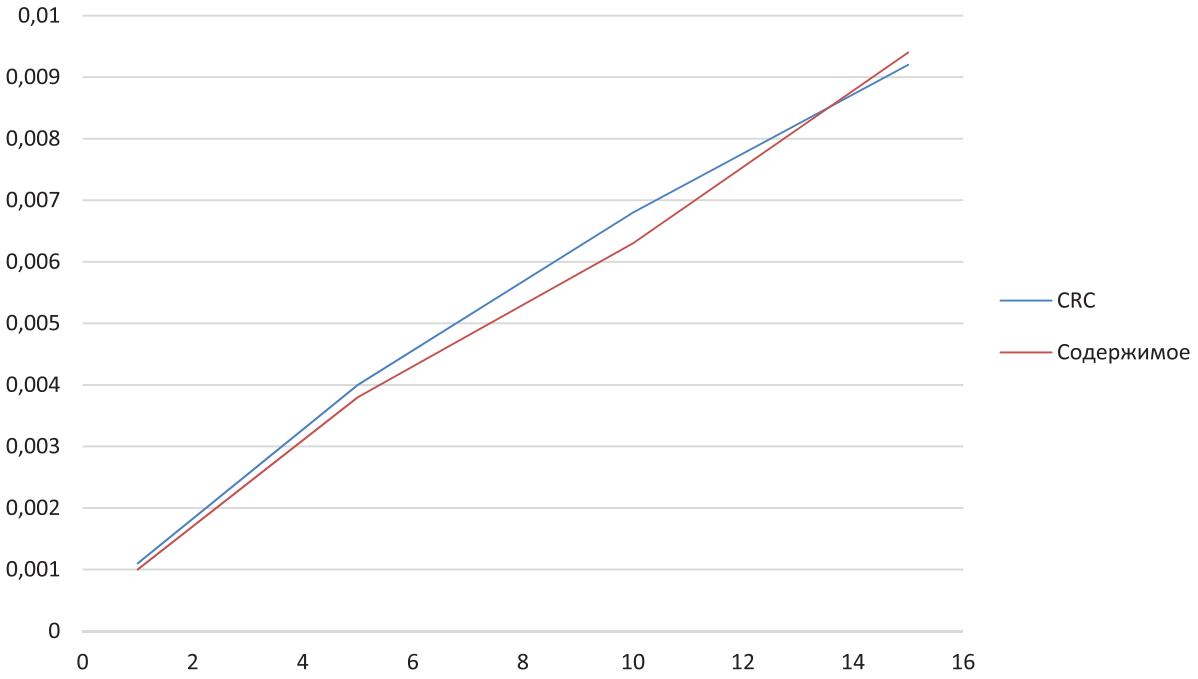

Рис. 7. График зависимости между количеством запрашиваемой информации от времени

Заключение

В системах автоматизированного мониторинга состояния критически важных сооружений (автодорожные и железнодорожные мосты, тоннели метрополитена и т. п.) важно обеспечение безопасности данных, передаваемых между датчиками и основными компонентами САГМ.

Приведенные алгоритмы передачи данных между ПОЛС и датчиками, а также между ПОЛС и ПОУС позволяют обеспечить целостность пересылаемых данных между этими компонентами. От целостности и достоверности информации, передаваемой от датчиков к ПОЛС и от ПОЛС к ПОУС, зависит объективный анализ, на основании которого необходимо реагировать на опасные отклонения искусственных сооружений от нормы. Описанный в статье подход предназначен для выявления повреждений сообщений при их передаче по зашумленным каналам связи. Источниками повреждений могут служить случайные шумы в каналах связи, а также преднамеренные искажения данных со стороны злоумышленников.

Библиографический список

1. Концепция Федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры Российской Федерации и опасных грузов» (ФСМ КВО и ОГ) : распоряжение Правительства Российской Федерации от 27 августа 2005 г. № 1314-р // Собрание законодательства РФ, ст. 3660. – 2005. – № 35, 29 авг.
2. Watanabe E. On longevity and monitoring technologies of bridges : a survey study by the Japanese Society of Steel Construction / E. Watanabe, H. Furuta, T. Yamaguchi, M. Kano // Structure and Infrastructure Eng. – 2014. – Vol. 10. – N 4. – Pp. 471–491.
3. Li S. L. SMC structural health monitoring benchmark problem using monitored data from an actual cable-stayed bridge / S. L. Li, H. Li, Y. Liu, Ch. Lan, W. Zhou, J. Ou // Structural Control and Health Monitoring. – 2014. – Vol. 21. – N 2. – Pp. 156–172.
4. Li A. Q. Analysis and assessment of bridge health monitoring mass data – progress in research/development of Structural Health Monitoring / A. Q. Li, Y. L. Ding, H. Wang, T. Guo // Science China Technological Sci. – 2012. – Vol. 55. – N 8. – Pp. 2212– 2224.
5. Spencer B. F. Campaign Monitoring of Railroad Bridges in High-Speed Rail Shared Corridors using Wireless Smart Sensors / B. F. Spencer // Report No NSEL-040, Department of Civil and Environmental Eng. Univ. of Illinois at Urbana-Champaign, June 2015.
6. Брынь М. Я. Геодезический мониторинг деформаций вантовых мостов на основе спутниковых технологий / М. Я. Брынь, А. А. Никитчин, Е. Г. Толстов // Известия Петербургского гос. ун-та путей сообщения. – 2009. – № 2. – С. 120–128.
7. Брынь М. Я. Программный комплекс для мониторинга деформаций особо опасных объектов / М. Я. Брынь, А. Д. Хомоненко, В. П. Бубнов, А. А. Никитчин, С. А. Сергеев, П. А. Новиков, А. И. Титов // Проблемы информационной безопасности. Компьютерные системы. – 2014. – № 1. – С. 36–41.
8. Бубнов В. П. Программный комплекс автоматизированного геодезического мониторинга искусственных сооружений для высокоскоростной железнодорожной магистрали Москва – Казань – Екатеринбург / В. П. Бубнов, А. А. Никитчин,

С. А. Сергеев // Интеллектуальные технологии на транспорте. – 2015. – № 4. – С. 27–33.
9. Сергеев С. А. Программный комплекс для мониторинга и анализа деформаций сооружений / С. А. Сергеев, А. Д. Хомоненко, В. П. Бубнов ; свид. о гос. регистрации программы ЭВМ № 2014619426. – М., 2014.
10. Бубнов В. П. Выбор СУБД и определение оптимального числа датчиков для локального сервера в составе САГМ / В. П. Бубнов, А. В. Мочалов, В. Г. Соловьева // Интеллектуальные технологии на транспорте. – 2017. – № 3. – С. 26–31.
11. Мыцко Е. А. Особенности программной реализации вычисления контрольной суммы CRC32 на примере PKZIP, WINZIP, ETHERNET / Е. А. Мыцко, А. Н. Мальчуков // Вестник науки Сибири. – 2011. – № 1. – С. 279–282.
12. Клименко С. В. Сравнение производительности способов получения содержимого дорожки CKD-тома и ее CRC-кода / С. В. Клименко // Интеллектуальные технологии на транспорте. – 2017. – № 3. – С. 45–50.
13. Яковлев В. В. Оценка влияния помех на производительность протоколов канального уровня / В. В. Яковлев, Ф. И. Кушназаров // Известия Петербургского университета путей сообщения. – 2015. – № 1. – С. 133–138.

Vladimir P. Bubnov,
Anatoly D. Khomonenko,
Valentin V. Yakovlev,
Sergey V. Klimenko
«Information Technology Systems» department
Emperor Alexander I St. Petersburg state transport university

Increase the safety improvement of data transmission on the local server of the automated geodetic monitoring system

The issue of improving the software architecture of the local server for automated geodetic monitoring of objects is considered. The issue of ensuring the protection of transmitted data from unauthorized access is investigated. For its solution, we propose a mechanism of control of integrity of the received data. This approach is intended to detect damage to messages when they are transmitted over noisy channels, which bring these damages. Algorithms for checking the integrity of data transfer between the sensor and the local server, as well as between the sensor and the remote server are proposed. An experimental estimation of the time efficiency of calculating the checksum for monitoring the integrity of data transmission is performed.

dangerous object; software complex; server; automated geodetic monitoring system; sensors

References

1. Order of the Government of the Russian Federation of August 27, 2005 «Concept of the Federal system of monitoring critical important objects and (or) potentials of dangerous objects of infrastructure of the Russian Federation and dangerous goods» [Kontseptsiya Federalnoy sistemy monitoringa kriticheski vazhnykh obyektov i (ili) potentsialno opasnykh obyektov infrastruktury Rossiyskoy Federatsii i opasnykh gruzov], issue 35.
2. Watanabe E., Furuta H., Yamaguchi T., Kano M. (2014). On longevity and monitoring technologies of bridges: a survey study by the Japanese Society of Steel Construction, Structure and Infrastructure Eng, vol. 10, issue 4. – Pp. 471–491.
3. Li S. L., Li H., Liu Y., Lan Ch., Zhou W., Ou J. (2014). SMC structural health monitoring benchmark problem using monitored data from an actual cable-stayed bridge, Structural Control and Health Monitoring, vol. 21, issue 2. – Pp. 156–172.
4. Li A. Q., Ding Y. L., Wang H., Guo T. (2012). Analysis and assessment of bridge health monitoring mass data – progress in research/development of Structural Health Monitoring, Science China Technological Sci, vol. 55, issue 8. – Pp. 2212–2224.
5. Spencer B. F. (2015). Campaign Monitoring of Railroad Bridges in High-Speed Rail Shared Corridors using Wireless Smart Sensors, Report No NSEL-040, Department of Civil and Environmental Eng. Univ. of Illinois at Urbana-Champaign, June.
6. Bryn M. Ya., Nikitchin A. A., Tolstov Ye. G. (2009). Geodetic monitoring of deformations of cable-stayed bridges on the basis of satellite technologies [Geodezicheskiy monitoring deformatsiy vantovykh mostov na osnove sputnikovykh tekhnologiy]. Proceedings of Petersburg state transport university [Izvestiya Peterburgskogo universiteta putej soobshcheniya], issue 2. – Pp. 120–128.
7. Bryn M. Ya., Khomonenko A. D., Bubnov V. P., Nikitchin A. A., Sergeev S. A., Novikov P. A., Titov A. I. (2014). Software complex for monitoring deformations of especially dangerous objects [Programmnyy kompleks dlya monitoringa deformatsiy osobo opasnykh obyektov]. Problems of information security. Computer systems [Problemy informatsionnoy bezopasnosti. Kompyuternyye sistemy], issue 1. – Pp. 36–41.
8. Bubnov V. P., Nikitchin A. A., Sergeyev S. A. (2015). Software for automated geodetic monitoring of artificial structures for high-speed railway Moscow – Kazan – Yekaterinburg [Programmnyy kompleks avtomatizirovannogo geodezicheskogo monitoringa iskusstvennykh sooruzheniy dlya vysokoskorostnoy zheleznodorozhnoy magistrali Moskva – Kazan – Yekaterinburg]. Intellectual technologies on transport [Intellektualnyye tekhnologii na transporte], issue 4. – Pp. 27–33.
9. Sergeyev S. A., Khomonenko A. D., Bubnov V. P. (2014). Software for monitoring and analyzing deformations of structures [Programmnyy kompleks dlya monitoringa i analiza deformatsiy sooruzheniy]. The Federal Service for Intellectual Property, Patents and Trademarks. Certificate of state registration of the computer program № 2014619426, Moscow.
10. Bubnov V. P., Mochalov A. V., Solovyeva V. G. (2017). DBMS selection and determination of the optimal number of sensors for a local server within the SAGM [Vybor SUBD i opredeleniye optimalnogo chisla datchikov dlya lokalnogo servera v sostave SAGM]. Intellectual technologies on transport [Intellektualnyye tekhnologii na transporte], issue 3. – Pp. 26–31.

11. Mytsko Ye. A., Malchukov A. N. (2011). Features of the software implementation of calculating the CRC32 checksum on the example of PKZIP, WINZIP, ETHERNET [Osobennosti programmnoy realizatsii vychisleniya kontrolnoy summy CRC32 na primere PKZIP, WINZIP, ETHERNET]. Bulletin of Siberian Science [Vestnik nauki Sibiri], issue 1. – Pp. 279–282.
12. Klimenko S. V. (2017). Comparison of the performance of ways to get the content of a CD-ROM track and its CRC code [Sravneniye proizvoditelnosti sposobov polucheniya soderzhimogo dorozhki CKD-toma i yeye CRC-koda]. Intellectual technologies on transport [Intellektualnyye tekhnologii na transporte], issue 3. – Pp. 45–50.
13. Yakovlev V. V., Kushnazarov F. I. (2015). Estimating the effect of interference on the performance of link-layer protocols [Otsenka vliyaniya pomekh na proizvoditelnost protokolov kanalnogo urovnya]. Proceedings of Petersburg state transport university [Izvestiya Peterburgskogo universiteta putey soobshcheniya], vol. 1. – Pp. 133–138.

Статья представлена к публикации членом редколлегии Д. С. Марковым
Поступила в редакцию 25.12.2017, принята к публикации 26.02.2018

БУБНОВ Владимир Петрович – доктор технических наук, профессор кафедры «Информационные и вычислительные системы» Петербургского государственного университета путей сообщения Императора Александра I.
e-mail: bubnov1950@yandex.ru

ХОМОНЕНКО Анатолий Дмитриевич – доктор технических наук, профессор кафедры «Информационные и вычислительные системы» Петербургского государственного университета путей сообщения Императора Александра I.
e-mail: khomon@mail.ru

ЯКОВЛЕВ Валентин Васильевич – доктор технических наук, профессор кафедры «Информационные и вычислительные системы» Петербургского государственного университета путей сообщения Императора Александра I.
e-mail: jakovlev@pgups.ru

КЛИМЕНКО Сергей Витальевич – аспирант кафедры «Информационные и вычислительные системы» Петербургского государственного университета путей сообщения Императора Александра I.
e-mail: s.klimenko@live.ru