

УДК 004.056

С.С. Беляев, Г.П. Жигулин

**ПОВЫШЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЦЕССОВ
УПРАВЛЕНИЯ МОБИЛЬНЫМИ ОБЪЕКТАМИ В СИСТЕМАХ
УПРАВЛЕНИЯ НА ОСНОВЕ СЕТЕЙ СОТОВОЙ СВЯЗИ ТРЕТЬЕГО
ПОКОЛЕНИЯ**

Рассматриваются проблемы применения каналов передачи данных с коммутацией пакетов сотовых сетей мобильной связи третьего поколения, используемых в качестве основы для построения систем мониторинга и управления мобильными объектами. Рассмотрены факторы, повышающие риски информационной безопасности процессов удаленного управления, характерные для каналов передачи данных такого рода. Проанализирована возможность повышения уровня информационной безопасности процессов мониторинга и управления посредством оперативного прогнозирования состояния радиоканала. В качестве базы прогноза предложено использовать математическую модель учитывающую динамику параметров радиоканала, которая позволяет оценить вероятность изменения его состояния. Описан программно-аппаратный комплекс, реализованный для проведения экспериментального исследования с целью выявления корреляции между параметрами радиоканала и показателями процесса информационного обмена. По результатам исследования предложена прогнозная модель, основанная на выявленной корреляции, позволяющая повысить уровень информационной безопасности процесса управления в рассматриваемых системах.

Система управления мобильным объектом; информационная безопасность; сотовые сети мобильной связи; моделирование.

S.S. Belyaev, G.P. Zhigulin

**IMPROVING OF INFORMATION SECURITY OF MOBILE OBJECTS
CONTROL PROCESSES IN THIRD GENERATION CELLULAR NETWORK
BASED MANAGEMENT SYSTEMS**

The paper is concerned with problems of third generation cellular network packet switching channels employment as a basis of remote mobile objects management systems. The factors that increase the information security risks of remote control processes in such kind of data transmission channels are considered. The possibility of increasing of information security level of monitoring and control processes via operative forecasting of channel state is analyzed. The mathematical model taking into account the dynamics of radio channel parameters is offered as the base of forecasting of changing radio channel status. The experimental hardware and software system is described. The purpose of that system is to reveal the correlation between radio channel parameters and information transmission process indicators. Forecasting model based on revealed correlation, allowing improving the information security level of control process in described management systems is offered as the result of experimental research.

Mobile object management system; information security; cellular networks; modeling.

Введение. За последние два десятилетия широкое распространение получили сотовые сети мобильной связи (сети подвижной связи). Активно развиваются технологические возможности различных мобильных устройств по передаче цифровой информации, а также растет спектр соответствующих услуг, предоставляемых операторами сотовой связи. Существует уже несколько поколений стандартов передачи цифровых данных, позволяющих мобильным устройствам получить доступ к сети Internet [1]. Таким образом, вполне естественным является интерес к применению возможностей средств сотовой связи в качестве одной из альтернативных основ при построении систем удаленного мониторинга и телеуправления мобильными системами. Идеи применения глобальной сети Internet в таком качестве существуют уже достаточно давно и были многократно реализованы на практике [2, 3].

Конечно же, такой подход позволяет решить проблему физической реализации канала связи с объектом мониторинга и управления, для которого требуется высокая степень мобильности, предоставляя последнему возможность информационного обмена с удаленной системой управления из любой точки области уверенного приема сигнала базовых станций. Тем не менее при применении средств сотовой связи для организации удаленного информационного обмена остается ряд проблем, лежащих как в плоскости информационной безопасности, так и в плоскости надежности систем удаленного управления, которые требуют дальнейших исследований [4].

Обзор исследуемой технологии. Ввиду особенностей архитектуры сотовых сетей мобильной связи и используемых в них технологий передачи цифровых данных, порой не представляется возможным получить канал информационного обмена, характеристики которого соответствовали бы требованиям, специфичным для систем удаленного мониторинга и управления мобильным объектом.

Если говорить о построении канала передачи цифровой информации на основе сотовых сетей мобильной связи, то, прежде всего, стоит сказать, что на сегодняшний день наиболее перспективным как с точки зрения организации теоретических исследований, так и с точки зрения внедрения разработанных решений на практике, является применение возможностей сетей мобильной связи третьего поколения. Сети мобильной связи третьего поколения также известны как сети универсальной системы мобильной связи или сети UMTS (Universal Mobile Telecommunications System). Стандартизация и создание технических спецификаций сетей UMTS в глобальном масштабе проводится международным партнерским проектом по системам подвижной связи третьего поколения 3GPP (3rd Generation Partnership Project), что позволяет обеспечить универсальность применяемых технологий в глобальном масштабе, и, как следствие, расширяет географическую применимость результатов разработок, основанных на возможностях сетей UMTS. Кроме того, сети мобильной связи третьего поколения на данный момент имеют достаточно большую зону покрытия, которая продолжает расширяться. Также следует отметить, что, несмотря на появление сетей мобильной связи четвертого поколения, которые предлагают услуги по передаче цифровых данных более высокого качества, ввиду технических и особенно экономических особенностей процесса эволюции сетей мобильной связи, можно быть уверенным в том, что сети UMTS будут эксплуатироваться ещё достаточно долго и их вытеснение новыми технологиями связи произойдёт лишь в долгосрочной перспективе.

Использование оборудования совместимого с сетями UMTS позволяет осуществлять передачу данных со скоростью до 384 Кбит/с (скорость передачи в направлении к мобильному терминалу может быть увеличена до 7,2 Мбит/с в режиме высокоскоростной передачи данных в нисходящем направлении HSDPA). Такие показатели, разумеется, нельзя назвать избыточными, особенно с учётом того, что они достижимы только в благоприятных для функционирования сети радиодоступа условиях. Тем не менее они оказываются достаточными для решения многих задач удаленного управления и мониторинга.

Основными преимуществами применения сетей UMTS в качестве основы для организации информационного обмена является:

- ◆ Минимальное время развертывания системы управления удаленным мобильным объектом в пределах зоны покрытия сети.
- ◆ Высокая степень мобильности объекта управления, что бывает критически важно во многих приложениях.
- ◆ Сравнительно невысокая стоимость технической реализации системы управления с учетом ее возможностей.

Однако, как уже упоминалось выше, существует ряд проблем и ограничений, которые следует учитывать при передаче данных по каналам с коммутацией пакетов сетей UMTS. В первую очередь, речь идёт об устойчивости канала связи. В данном контексте возникают такие проблемы информационной безопасности процесса управления, как доступность объекта управления, целостность информационных сообщений, а также актуальность управляющих сигналов и информации о состоянии объекта управления.

Так как опорная сеть операторов связи достаточно надёжна и обладает высоким быстродействием, она, как правило, не является узким местом канала передачи данных. Кроме того, ее защищенность от воздействий, несущих угрозу информационной безопасности, как случайных, так и преднамеренных гораздо выше, чем у сети радиодоступа. Последняя, напротив, остается уязвимой. На практике именно в сети радиодоступа локализируются причины возникновения проблем перечисленных выше. Также, негативное влияние оказывают технологические ограничения сети радиодоступа. С одной стороны, приёмы, применяемые для увеличения ёмкости соты в сотовых сетях третьего поколения с широкополосным множественным доступом с кодовым разделением каналов WCDMA (Wideband Code Division Multiply Access), позволяют повысить качество работы сети с большим количеством абонентов в целом. Однако, с другой стороны, они не позволяют обеспечивать постоянное качество предоставляемых услуг отдельно взятому мобильному абоненту [5].

Таким образом, можно заключить, что системы управления и мониторинга, построенные на основе сетей UMTS, с учетом описанных выше ограничений, могут быть применены в гражданских приложениях, область перемещения объекта управления и/или мониторинга в которых ограничена зоной покрытия сети.

Теоретические основания исследования. При использовании систем управления и мониторинга на основе сетей UMTS требуются меры по повышению надёжности канала передачи цифровой информации и снижению рисков информационной безопасности процесса управления и мониторинга. Сложность заключается в том, что у конечного пользователя практически нет рычагов воздействия на механизмы работы сети радиодоступа. Причём не только отсутствует возможность воздействия на работу базовых станций и прочего оборудования сети, но и на процедуры радиодоступа оконечного пользовательского оборудования. Это обусловлено тем, что в сотовых сетях мобильной связи UMTS применяются достаточно сложные технологии для рационализации расходования радиоресурса. Эти технологии требуют от всех участников радиообмена определённого поведения в эфире, и бесконтрольное вмешательство в процессы радиодоступа может повлечь негативные последствия в работе сети.

В условиях невозможности прямого воздействия на канал передачи информации с целью повышения его надёжности и безопасности следует сосредоточить внимание на прогнозировании его поведения, выявлении закономерностей между параметрами, отражающими его состояние и показателями процесса информационного обмена. Конечному пользователю могут быть доступны различные параметры состояния сети, позволяющие косвенно судить о радиоусловиях, в которых находится его мобильное оборудование. Это, в частности, уровень мощности принимаемого сигнала RSSI (Received Signal Strength Indication), мощность принимаемого сигнала кода соты RSCP (Received Signal Code Power), мощность передачи TxPwr (Transmission Power) и другие. С другой стороны, в качестве показателей процесса информационного обмена могут выступать скорость информационного обмена, количество потерь информационных пакетов, задержка передачи пакета.

Ясно, что показатель RSSI, на значении которого, в частности, основана индикация приёма сети в мобильных телефонах, сам по себе, а также его динамика уже могут служить основанием для прогнозирования состояния процесса информационного обмена в канале связи. Так или иначе, его абсолютное значение характеризует радиоусловия, в которых находится мобильное оборудование. Чем ниже этот показатель, тем выше вероятность сбоев при обмене информацией. Также приближение его величины к достаточно низким значениям (порядка -100 dBm) свидетельствует о том, что осуществление информационного обмена скоро может оказаться невозможным.

Немаловажным показателем для оценки состояния канала передачи информации в сети UMTS является $TxPwr$. Примечательно то, что мощность передачи оконечного мобильного оборудования в сети UMTS подвергается весьма точному и динамичному регулированию со стороны механизмов управления радиоресурсом сети RRM (Radio Resource Management). Столь высокое внимание к данному параметру со стороны механизмов саморегуляции сети (периодичность обновления параметра $TxPwr$ – 1500 раз в секунду) обусловлено необходимостью минимизировать взаимные помехи при одновременной передаче разных абонентов в условиях WCDMA. При этом мощность передачи каждого абонента должна быть достаточной для обеспечения надлежащего качества связи [5]. Таким образом, динамика параметра $TxPwr$ тесно связана с текущими возможностями передачи данных по радиоканалу и, соответственно, должна коррелировать с возможными сбоями в процессе информационного обмена.

Изложенные выше факты позволяют сделать предположение о наличии корреляции между параметрами, характеризующими состояние радиоканала, и показателями процесса информационного обмена, осуществляемого по нему. Наличие такой корреляции может составить базу для прогнозирования возможности стабильной передачи данных по данному радиоканалу.

Методика проведения эксперимента. Для выявления корреляции между параметрами радиоканала и показателями процесса информационного обмена необходимо на практике реализовать информационную систему, состоящую из подвижного хоста, осуществляющего доступ в сеть Internet посредством оконечного пользовательского оборудования UMTS, и неподвижного хоста, имеющего надёжное высокоскоростное подключение к сети Internet. В данной системе между хостами необходимо осуществить непрерывный обмен информацией. Далее, в условиях постоянного перемещения подвижного хоста в зоне покрытия сети, необходимо накапливать статистические данные как о величинах параметров радиоканала, так и о параметрах, характеризующих процесс информационного обмена. Особенно следует отметить тот факт, что подключение неподвижного хоста к сети Internet должно быть достаточно надёжным и быстродействующим, чтобы не вносить со своей стороны существенных изменений в параметры информационного обмена.

При организации описанной выше информационной системы следует учесть, что подвижный хост при подключении к сети Internet получит внутренний IP-адрес, который пройдя через систему преобразования сетевых адресов NAT (Network Address Translation) будет преобразован в связку внешний IP-адрес – порт. Конечно, некоторые операторы могут предоставить услугу выделенного IP-адреса, однако в данном эксперименте будем рассматривать общий случай с NAT-преобразованием. Также для общности положим, что адрес неподвижного хоста также подвергается преобразованию системой NAT. В таком случае для организации обмена информацией между хостами необходимо в экспериментальную систему включить сервер адресов. Такой сервер должен быть наделён внешним IP-адресом и способен по запросу осведомлять хост, участвующий в эксперименте

о присвоенной его партнёру по информационному обмену связке внешний IP-адрес – порт. Также наличие сервера адресов важно ввиду того, что в определённых случаях со временем связка внешний IP-адрес – порт, выделенная подвижному хосту, может измениться. Поэтому обращение хостов, участвующих в эксперименте, должно быть периодическим и достаточно частым.

Информационный обмен между подвижным и неподвижным хостами организуется по протоколу UDP (протокол без гарантированной доставки пакетов). Каждый пакет имеет поле с уникальным номером и поле, содержащее время его отправки. Эти поля нужны для определения потерь и задержек пакетов. Остальную часть пакета составляет балласт для создания нагрузки на канал передачи. Неподвижный хост формирует пакеты и отправляет их подвижному хосту с заданной периодичностью. Подвижный хост работает в эхо-режиме, направляя принятый пакет обратно отправителю. На рис. 1 представлена схема экспериментальной информационной системы.

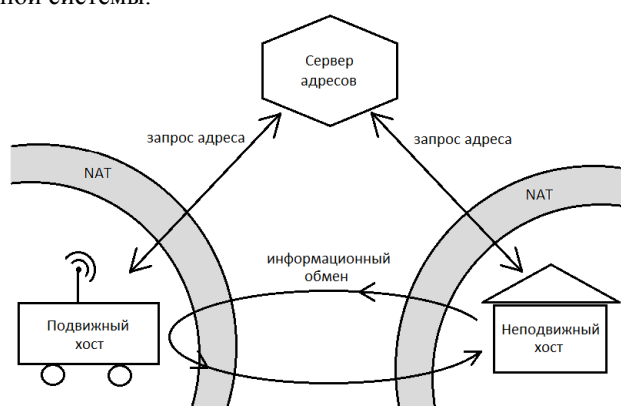


Рис. 1. Экспериментальная информационная система

Организация проведения эксперимента. В качестве подвижного хоста использовался ноутбук, перемещаемый на автомобиле в г. Санкт-Петербург со средней скоростью 40 км/ч в зоне покрытия сети. В качестве оконечного пользовательского оборудования использовался UMTS-модуль UC-864 фирмы Telit. На ноутбуке было установлено программное обеспечение для осуществления всех необходимых для проведения эксперимента операций: опрос сервера адресов, эхо-отправка пакетов на неподвижный хост, отслеживание задержки между приходом пакетов от неподвижного хоста, опрос UMTS-модуля для сбора информации о состоянии радиоканала.

Роль неподвижного хоста исполнял стационарный компьютер, имеющий проводное подключение к сети Internet со скоростью 10 Мбит/с. На данном компьютере было установлено программное обеспечение для опроса сервера адресов, информационного обмена с подвижным хостом и накопления статистических данных о процессе информационного обмена. В качестве сервера адресов выступал виртуальный сервер, выделенный на оборудовании Data-центра с подключением к сети Internet со скоростью 1 Гбит/с.

Запросы с подвижного и неподвижного хостов к серверу адресов осуществлялись с периодичностью в 500 мс. Неподвижный хост отправлял информационные пакеты подвижному хосту с периодичностью 100 мс, размер каждого пакета составлял 512 байт. Мгновенный снимок параметров радиоканала и процесса информационного обмена для накопления статистической информации делался с периодичностью в 1 секунду.

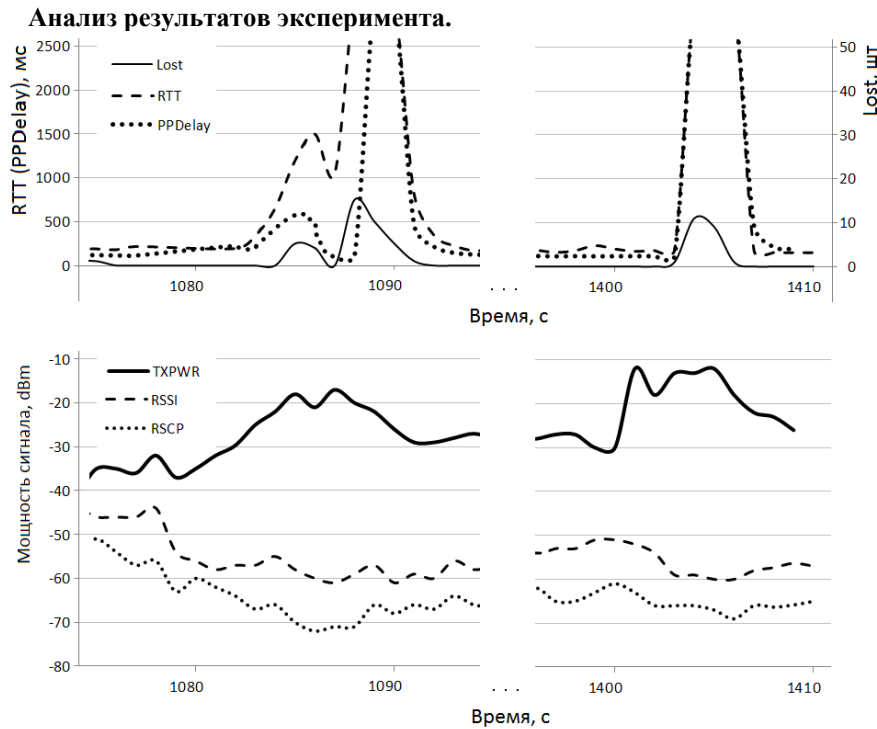


Рис. 2. Результаты эксперимента

На рис. 2 представлены два временных отрезка, на которых видны характерные признаки нестабильности передачи данных по радиоканалу, а так же его временной неработоспособности. В частности, наблюдается появление потерь пакетов (Lost), возрастание времени двойной пересылки пакета (RTT) и интервала приема пакетов подвижным хостом (PPDelay). Также очевидно наличие корреляции между динамикой параметров радиоканала и периодами временной неработоспособности канала. Начало таких периодов предваряется возрастанием параметра TxPwr. Очевидно, механизмы саморегуляции сети радиодоступа совершают попытку скомпенсировать вхождение подвижного хоста в зону неблагоприятных радиоусловий, что подтверждается одновременным снижением значений параметров RSSI и RSCP. С выходом из зоны неблагоприятных радиоусловий производится корректирующее снижение параметра TxPwr и соответствующее возрастание значений параметров RSSI и RSCP.

Таким образом, радиоканал можно упрощенно промоделировать как объект с двумя состояниями: 1 – стабилен и 2 – нестабилен. При этом величина

$$T(t) = \frac{dTxPwr(t)}{dt} - \frac{d(RSSI(t)+RSCP(t))}{dt},$$

основанная на динамике параметров радиоканала, может служить индикатором потенциальной возможности смены состояния. Её положительное значение служит сигналом к возможному переходу радиоканала из состояния 1 в состояние 2, а отрицательное – к переходу из состояния 2 в состояние 1, причем, чем больше значение модуля этой величины, тем более вероятен переход. Результаты такого моделирования могут быть применены в алгоритмах управления мобильными объектами и роботами, а также при оперативном планировании использования системой управления канала передачи данных. В частности, на их основе можно

принять решение о применении превентивных мер, позволяющих минимизировать возможные последствия реализации рисков информационной безопасности процесса управления.

Заключение. Каналы передачи данных сетей UMTS могут быть применены в качестве основы для построения систем управления и мониторинга мобильных объектов и роботов с учётом описанных ограничений. Кроме того, уровень информационной безопасности процессов управления и мониторинга, осуществляемых с применением таких систем, может быть повышен с помощью прогнозной модели состояния радиоканала, базирующейся на параметрах, характеризующих его текущее состояние. В дальнейшем планируется произвести значительное расширение базы экспериментальных данных для уточнения прогнозной модели и четкого определения границ применимости технологий пакетной передачи данных сети UMTS в качестве основы систем управления и мониторинга мобильными объектами и роботами.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Гельгор А.Л., Попов Е.А.* Сотовые сети мобильной связи стандарта UMTS: Учеб. пособие. – СПб.: Изд-во Политехнического университета, 2010. – 227 с.
2. *Moutaouakkil F., El Bakkali M., Medromi H.* New Approach of Telerobotic over Internet // Proceedings of the World Congress on Engineering and Computer Science. – San Francisco, 2010. – P. 213-221.
3. *Al-Ali A.R.* GSM Based Control System // Information and Communication Technologies: From Theory to Applications. Proceedings. – Damascus, 2004. – P. 326-341.
4. *Беляев С.С., Васильева О.В., Жигулин Г.П.* Проблемы удаленного управления мобильными системами через Internet с использованием средств сотовой связи // Сборник тезисов докладов конгресса молодых учёных. Вып. 1. – СПб.: Изд-во НИУ ИТМО, 2013. – С. 100-101.
5. *Кааранен Х., Ахтиайнен А. и др.* Сети UMTS. Архитектура, мобильность, сервисы. – М.: Техносфера, 2007. – 464 с.

Статью рекомендовал к опубликованию д.т.н. О.Ю. Гаценко.

Беляев Сергей Степанович – Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»; e-mail: belss751@rambler.ru; 197101, г. Санкт-Петербург, Кронверкский проспект, 49, лит. А; тел.: 88122979787; кафедра мониторинга и прогнозирования информационных угроз, аспирант.

Жигулин Георгий Петрович – e-mail: ikvo@grv.ifmo.ru; тел.: 88125954132; к.т.н.; доцент; декан ИКВО.

Belyaev Sergey Stepanovich – Saint Petersburg National Research University of Information Technologies, Mechanics and Optics; e-mail: belss751@rambler.ru; 49, Kronverkskiy ave., lit. A, Saint-Petersburg, 197101, Russia; phone: +78122979787; the department of monitoring and forecasting of information threats; postgraduate student.

Zhigulin Georgy Petrovich – e-mail: ikvo@grv.ifmo.ru; phone: 88125954132; cand. of eng. sc.; associate professor; dean ИКВО.