УДК 004.78:004.056

ОЦЕНКА БЕЗОПАСНОСТИ НАТЕЛЬНОЙ КОМПЬЮТЕРНОЙ СЕТИ

Меркурьев Р.О.

ФГБОУ ВО «Дальневосточный государственный университет путей сообщения», Хабаровск, e-mail: o-radik@ya.ru

Последние достижения электроники дают возможность создавать беспроводные сенсорные сети в, на, или вокруг тела человека. Беспроводные нательные сети используются не только в медицинских приложениях, но также в немедицинских областях, таких как развлекательные и военные. Беспроводные нательные сети имеют громадный потенциал для революционного преобразования будущих оздоровительных технологий. В данной статье рассмотрено, чем является беспроводная нательная сеть и каковы области ее применения как в медицинской, так и в немедицинской областях. Произведена оценка безопасности и требования по защите беспроводной нательной сети. Рассмотрены ключевые требования к нательной компьютерной сети (конфиденциальность, целостность, доступность) и обозначено, что перечисленные требования вместе гарантируют надежное сохранение данных, их передачу и беспрепятственный доступ к ним уполномоченными лицами.

Ключевые слова: нательная компьютерная сеть, требования безопасности, защита нательной сети

ESTIMATION OF SAFETY OF BODY AREA NETWORKS

Merkurev R.O.

Far Eastern State Transport University, Khabarovsk, e-mail: o-radik@ya.ru

Recent advances in electronics allow the creation of wireless sensor networks inside, inside or around the human body. Wireless internal networks are used not only for medical purposes, but also in non-medical areas, such as entertainment and the military. Wireless networks have enormous potential for transforming future health technologies. This article examines what is the wireless network and what are the areas of its application in both medical and non-medical fields. The security and requirements for the protection of the wireless network are assessed. The main requirements for the computer network (confidentiality, integrity, availability) are considered and indicated that the listed requirements together guarantee reliable storage of data, their transfer and unhindered access to authorized persons.

Keywords: body area networks, security requirements, protection of the network

Интеграция вычислительных устройств и здравоохранения изменила представление современной медицины. Имплантируемые медицинские устройства (Implantable medical devices (IMDs), ИМУ), или медицинские приборы, встроенные внутри человеческого тела, сделали возможным непрерывно и автоматически управлять состоянием здоровья, начиная нарушением сердечного ритма, и заканчивая болезнью Паркинсона. Беспроводные нательные сети (Body Area Networks (BAN), БНС, называемые также беспроводными нательными сенсорными сетями – БНСС)) позволяют осуществлять удаленный мониторинг состояния здоровья пациента.

Беспроводная нательная сеть (Body Area Network (BAN), беспроводная нательная компьютерная сеть WBAN, также нательная компьютерная сеть) – беспроводная сеть надеваемых компьютерных устройств. БНС устройства могут быть встроены в тело, имплантированы, прикреплены к поверхности тела в фиксированном положении или совмещены с устройствами, которые люди носят в различных местах (карманах, на руке или в сумках) [1].

Описание беспроводной нательной сети

Нательная компьютерная сеть позволяет провести недорогой и продолжительный мониторинг тела в реальном времени через Интернет. Несколько интеллектуальных физиологических аппаратов могут быть интегрированы в надеваемые устройства, которые могут использоваться для компьютерной реабилитации или заблаговременного обследования состояния здоровья. Эта область основывается на возможности имплантации очень маленьких датчиков внутрь человеческого тела, которые очень удобны и не нарушают нормальную деятельность человека.

Применение БНС

БНС имеют большой потенциал для нескольких применений, включая удаленную медицинскую диагностику, интерактивные игры и военные применения.

Приложения внутри тела включают мониторинг и программу изменений для пейсмейкеров и имплантируемых сердечных дефибрилляторов, контроль функций мочевого пузыря и реабилитацию движения ко-

нечностей [2]. Медицинские применения на теле человека включают в себя мониторинг ЭКГ, давления крови, температуры и дыхания. К немедицинским применениям относятся: мониторинг забытых вещей, создание социальных сетей, снижение усталости солдат и повышение боеготовности. Ниже подробнее рассмотрены некоторые применения.

Сердечно-сосудистые болезни. Традиционно холтеровские мониторы использовались для сбора нарушений сердечного ритма в режиме “offline” без обратной связи. Однако, в таком режиме использования иногда трудно обнаружить переходные аномалии. Например, многие сердечные заболевания ассоциируются с эпизодическими, а не с непрерывными аномалиями, такими как волны перехода в кровяном давлении, мерцательная аритмия или индуцированные эпизоды ишемии миокарда, и время их наступления на может быть точно предсказано. БНС является ключевой технологией предупреждения наступления инфаркта миокарда, мониторинга эпизодических событий и других аномальных условий и может быть использована для амбулаторного наблюдения за здоровьем.

Обнаружение рака. Рак остается одной из самых больших опасностей для жизни человека. Согласно Национальному центру статистики здоровья, в 1999 году 9 миллионов жителей США имели диагноз ракового заболевания. Множество миниатюрных сенсоров, способных обнаружить раковые клетки могут быть равномерно интегрированы в БНС. Это позволит медикам диагностировать новообразования без биопсии.

Астма. БНС могут помочь миллионам людей, страдающих от астмы, путем мониторинга аллергенов в воздухе и предоставления медикам обратной связь в режиме реального времени. Предложен прибор на основе GPS-технологии, который осуществляет мониторинг факторов окружающей среды и включает сигнал тревоги при обнаружении информации об аллергенах для пациента.

Искусственная сетчатка. Чипы с протезом сетчатки могут быть имплантированы в глаз человека, что помогает пациенту с ослабленным зрением, или незрячему видеть на адекватном уровне.

Поле боя. БНС могут быть использованы для связи между солдатами на поле боя и передачи данных об их активности командиру – бежит солдат, стреляет или ползет. В данном случае солдаты должны иметь секретный канал связи, чтобы предотвратить засады [3].

Оценка требований безопасности

Безопасность и конфиденциальность физиологических и неврологических данных пациентов, генерируемых BAN, являются двумя незаменимыми компонентами BAN. Эти требования вместе гарантируют, что данные надежно хранятся, передаются и доступны уполномоченным лицам. С этой целью конфиденциальность, целостность и доступность данных являются ключевыми требованиями. Эти свойства должны сохраняться на протяжении всего жизненного цикла устройств IMD и BAN, включая надлежащую утилизацию эксплантированных устройств.

1. Конфиденциальность: данные, информация об устройствах и устройства системы должны быть доступны только уполномоченным организациям (то есть соответствующим объектам), и эти объекты должны быть аутентифицированы (то есть идентификация объектов, взаимодействующих с устройствами, должна поддаваться проверке). В частности, данные должны храниться конфиденциально как при хранении, так и при передаче.

Данные должны храниться в надежном месте во время хранения на центральном сервере. Даже если взломан узел или сервер, злоумышленник не должен иметь возможность получить какую-либо информацию.

2. Целостность: данные, информация об устройствах и устройства системы не должны модифицироваться несанкционированными лицами. Система должна также удовлетворять аутентификации источника данных; источник любых полученных данных должен поддаваться проверке.

Целостность данных относится к обеспечению того, что несанкционированные изменения данных не могут быть сделаны во время хранения или передачи. Любые вредоносные изменения должны быть обнаружены перед использованием и соответствующие лица должны быть предупреждены. Это может быть достигнуто посредством протоколов аутентификации данных. Аутентификация данных позволяет получателю убедиться, что заявленный отправитель отправил сообщение. Очень важно проверить, что данные были отправлены доверенным датчиком, а не злоумышленником, который взломал узел или контроллер, чтобы принять ложные данные. В BAN

аутентификация данных может быть выполнена с использованием симметричных методов.

3. Доступность: данные, информация об устройствах и устройства системы должны быть доступны по запросу уполномоченных лиц.

Доступность данных означает, что подлинным пользователям доступны правильные данные. Невозможность получить правильные данные может стать угрозой для жизни. Также необходимо аутентифицировать любой обмен данными с другими машинами или людьми. Если злоумышленники смогут захватить важные узлы, здоровье пациентов будет подвергаться риску.

Таким образом, данные, хранящиеся в распределительном порядке в узлах BAN, должны отвечать, иногда противоречивым требованиям. Они должны быть безопасными, безопасно передаваться на центральный сервер через Интернет, когда пациент прибывает в больницу или в другое место; следует контролировать латентность (скрытность); также и для своевременной диагностики, и для лечения, новые данные всегда должны быть доступны для врача. Помимо перечисленных выше основных требований безопасности и конфиденциальности, BAN должны также удовлетворять следующим требованиям.

1. Личная конфиденциальность устройства: неавторизованные лица не должны иметь возможность определить, что у пациента есть IMD или BAN.

2. Конфиденциальность устройства: если конфиденциальность существования устройства невозможна, неавторизованные лица не должны иметь способность определить, какой тип IMD или BAN используется.

3. Индивидуальная идентификация конкретного устройства: неавторизованные лица не должны иметь возможность определять уникальный идентификатор датчика IMD или BAN.

4. Измерение и конфиденциальность журнал защиты: неавторизованные лица не должны иметь возможность определять частную телеметрию или доступ к хранимым данным о пациенте.

5. Личная конфиденциальность пользователя: неавторизованные лица не должны использовать свойства IMD или BAN для идентификации пациента.

6. Отслеживание: несанкционированные объекты не должны использовать физический уровень (например, контролировать аналоговые датчики или сопоставлять радиоприемник отпечатка пальца), чтобы отслеживать или находить пациента.

7. Контроль доступа: тип и объем данных, доступных для различных заинтересованных сторон, таких как врачи, вспомогательный персонал, аптеки и страховые агентства, должны быть четко контролируемыми. Система должна предоставлять разные права доступа для разных пользователей.

8. Свежесть данных: злоумышленник может воспроизводить старые данные. Наряду с конфиденциальностью и целостностью важно обеспечить отправку данных в том порядке, в котором они были созданы. Существует два типа свежести данных: слабая свежесть, которая гарантирует упорядочение частичных данных, но не гарантирует задержку и сильную свежесть, которая гарантирует упорядочение данных, а также задержку. Некоторые приложения, такие как мониторинг артериального давления, могут хорошо работать при слабой свежести, в то время как во время синхронизации требуется сильная свежесть, например, когда контроллер передает сигнал.

9. Масштабируемость: по мере роста сети и увеличения числа пользователей система должна масштабироваться без чрезмерной задержки. Требуется контролировать вычислительные и накладные расходы хранилища. Он не должен быть ресурсоемким для реализации политик доступа, а также накладные расходы на управление также должны быть под контролем.

10. Гибкость: пациент может поменять местами больницы или врача, и можно будет легко переносить центральные серверы и средства контроля доступа. В случае возникновения чрезвычайных ситуаций врачи, которые раньше не видели пациента, должны получить разрешение немедленно. Система должна также обрабатывать непредвиденные обстоятельства, связанные с тем, что пациент находится в бессознательном состоянии или психически неспособен контролировать работу БАН.

11. Подотчетность и неотказуемость: отправитель сообщения не должен впоследствии ложно отрицать, что он отправил сообщение, и этот факт должен быть поддающимся проверке независимо третьим лицом, не зная слишком много о содержании оспариваемого сообщения.

12. Безопасное распределение ключей: это необходимо для обеспечения шифрования и дешифрования для достижения желаемой безопасности и конфиденциальности.

Контроллер должен иметь возможность выполнять безопасную ассоциацию и диссоциацию узлов [4].

Заключение

Безопасность в BAN является одним из наиболее важных вопросов. Имеются некоторые реализации криптографии с симметричным ключом. Однако криптография с открытым ключом обеспечивает более высокую безопасность, но при высоких затратах на энергию.

Необходимы дополнительные исследования, чтобы поднять безопасность и конфиденциальность BAN-систем на новый уровень, а также необходимо исследовать эффективные схемы аутентификации, основанные на человеческих чертах лица и сигналах ЭЭГ. Для бессознательных пациентов необходим определенный метод, основанный на биометрии и аутентификации на основе физиологических сигналов.

Список литературы

1. IEEE 802.15 WPAN. Body Area Networks [Электронный ресурс]. – Режим доступа: http://www.ieee802.org.

2. Связь RF и несколько протоколов доступа в сети датчиков для тела / Сана Улла, Генри Хиггинс // Международный журнал по технологии цифрового контента и его приложениям, 2008. – С. 9–16.

3. Инструменты для публикации и обмена информацией [Электронный ресурс]. – Режим доступа: http://docplayer.ru/.

4. Исследование беспроводных нательных сетей / Бенуа Латр, Барт Брем, Ингрид Моерман, Крис Блондия // Беспроводная сеть, 2011. – С. 1–18.