Проблемы Информационной Безопасности Беспроводных Систем Мониторинга Здоровья Пациентов

Рамиз Шыхалиев
Институт Информационных Технологий НАНА, Баку, Азербайджан
ramiz@science.az

Аннотация– Беспроводный мобильный мониторинг здоровья пациентов является очень важным сервисом здравоохранения. При этом обеспечение информационной безопасности систем беспроводного мобильного мониторинга здоровья пациентов является жизненно важной задачей. В статье рассматриваются проблемы безопасности, угрозы безопасности, а также меры по обеспечению безопасности систем беспроводного мобильного мониторинга здоровья пациентов.

Ключевые слова– мониторинг здоровья пациентов, беспроводные сенсорные сети, информационная безопасность, угрозы информационной безопасности, меры информационной безопасности

I. ВВЕДЕНИЕ

В последнее время с развитием технологий улучшились условия работы и жизни людей, что привело к повышению продолжительности жизни. Однако это привело к увеличению количества старшего поколения и людей, имеющих хронические болезни и нуждающихся в постоянной медицинской помощи. Кроме того, из-за нехватки больничных коек обычно большинство пациентов рано выписываются из больниц и нуждаются в дополнительной медицинской помощи и мониторинге состояния здоровья вне больниц. Таким образом появляется необходимость в создании новых способов обеспечения людей постоянной хорошей медицинской помощью. Для оказания такой услуги более подходящим методом является беспроводной мобильный мониторинг здоровья пациентов.

Сегодня для мониторинга здоровья пациентов используются сенсорные сети, которые существенно изменяют многие аспекты традиционной медицинской помощи [1]. Для этого строятся так называемые беспроводные нательные сенсорные сети – WBAN (Wireless Body Area Networks) [2–4]. Подключение к телу пациентов беспроводных и носимых датчиков для сбора жизненно важных данных в реальном времени значительно упрощает и облегчает мониторинг их здоровья. Датчики позволяют следить за изменениями, происходящими в организме пациента, и обеспечивают обратную связь, чтобы помочь поддерживать оптимальное состояние здоровья. А также эти системы могут оповещать медицинский персонал об изменениях, угрожающих жизни пациентов. Кроме того, эти системы могут быть использованы для контроля за состоянием здоровья пациентов в амбулаторных условиях. Например, могут быть использованы для диагностики, поддержания оптимального состояния здоровья пациентов, контролируемого восстановления после острых приступов или хирургических операций, а также для мониторинга эффекта проводимой лекарственной терапии. При этом собранные жизненно важные данные и медицинские записи о здоровье пациентов передаются через различные беспроводные соединения и Интернет в центр сбора данных.

Несмотря на преимущество применения беспроводных сенсорных сетей для мониторинга здоровья пациентов, также имеются некоторые проблемы. В частности, беспроводные сенсорные сети должны обеспечить групповую топологию маршрутизации, мобильность узлов, высокую скорость передачи данных и быть надежными и безопасными.

Перечисленные проблемы являются очень актуальными, и каждая из них является темой отдельного исследования. В данной статье рассматриваются проблемы информационной безопасности систем беспроводного мобильного мониторинга здоровья пациентов.

II. ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ WBAN

Из-за беспроводного характера связи в сенсорных сетях при их использовании для мониторинга здоровья пациентов могут появляться различные угрозы и атаки информационной безопасности. Эти угрозы и атаки могут создавать серьезные проблемы в социальной жизни пациентов и даже для жизни в прямом смысле. Поэтому исследование вопросов обеспечения информационной безопасности медицинских беспроводных сетей, используемых для мониторинга здоровья пациентов, является очень актуальным [5–7].

Основными проблемами информационной безопасности системы беспроводного мониторинга здоровья пациентов являются обеспечение конфиденциальности, целостности и доступности данных пациентов, а также контроль доступа в систему. При этом вопросы конфиденциальности и безопасности персональных данных пациентов должны рассматриваться на двух уровнях, а именно на уровнях инфраструктуры и приложений, и эти уровни должны рассматриваться как в отдельности, так и вместе. Вопросы конфиденциальности и целостности решаются с помощью шифрования данных.

Контроль доступа должен предотвратить несанкционированный вход в сеть, и узлы сети должны идентифицировать несанкционированные узлы и сообщения. При решении этих и других проблем информационной безопасности систем мониторинга здоровья пациентов необходимо, однако, достичь баланса между безопасностью, эффективностью и практичностью системы.

В WBAN злоумышленники могут скомпрометировать узлы (сенсоры), нарушить целостность данных, перехватывать передаваемые в системе сообщения, вводить в сеть ложные сообщении и т.п. Обычно они пытаются проникнуть в узлы сетей, чтобы получить персональные данные пациентов. При этом, если основная часть данных пациентов в зашифрованном виде будет непосредственно храниться в узлах вместе с ключом шифрования, то компрометация этих узлов приведет к раскрытию персональных данных пациентов.

Основными требованиями к хранению персональных данных пациентов являются конфиденциальность, целостность и надежность. При обеспечении конфиденциальности только авторизованные узлы будут иметь возможность получить доступ к данным из сети. Это требование достигается с помощью шифрования данных, для которого должны быть использованы криптоустойчивые методы шифрования, которые обеспечат высокий уровень устойчивости к атакам по раскрытию персональных данных пациентов, а также снизят вероятность компрометации узлов.

Обеспечение целостности состоит в том, чтобы персональные данные пациентов в течение срока хранения не были изменены, а также должны быть механизмы динамической проверки и обнаружения изменения данных, которые позволили бы узлам контролировать целостность данных. Кроме того, персональные данные пациентов должны настолько надежно храниться, чтобы при сбое узлов их можно было легко восстановить. Для обеспечения конфиденциальности, целостности и надежности хранимых в WBAN данных в литературе предлагаются различные решения [8, 9].

III. Угрозы информационной безопасности WBAN

В системах беспроводного мобильного мониторинга здоровья пациентов всегда существует вероятность нарушения информационной безопасности. Поскольку беспроводная среда передачи информации является более уязвимой, чем проводная, злоумышленники могут легко осуществлять атаки на эти системы. При этом угрозы и атаки могут быть разделены на две категории – пассивные и активные [5]. При этом злоумышленники, а также угрозы могут быть как внутренними, так и внешними [10]. Так как внешние злоумышленники не являются частью системы, то очень трудно предотвратить их атаки, и основной целью таких атак является получение персональных данных пациентов.

Пассивные атаки в основном направлены против конфиденциальности персональных данных пациентов. При осуществлении пассивных атак злоумышленники могут украсть данные о состоянии здоровья пациентов путем прослушивания среды беспроводной связи между узлами WBAN. Атакующий проводит мониторинг незашифрованного трафика WBAN. Эти атаки состоят из анализа трафика, мониторинга коммуникации, дешифрования слабозашифрованного трафика, а также сбора информации аутентификации. Перехват сетевых операций позволяет злоумышленникам увидеть предстоящие действия, что может привести к раскрытию информации или файлов, находящихся в узлах. Кроме того, злоумышленники могут изменить назначение пакетов или нарушить маршрутизацию пакетов.

В отличие от пассивных атак, при активных атаках злоумышленники принимают активные меры для контроля за сетью. Активные угрозы являются более опасными, чем пассивные, так как посредством прослушивания злоумышленники могут найти местоположение пользователя, что может привести к угрозе для жизни пациентов. В качества примера атак на систему беспроводного мониторинга здоровья пациентов можно привести такие атаки, как DoS (Denial of Service – отказ в обслуживании), модификация данных, воспроизведение (записанная информация в автономном режиме), спуфинг (подмена), «человек в середине», избирательное перенаправление, ложный узел и т.п. Эти и другие атаки более подробно описываются в работах [11–15].

IV. Меры обеспечения информационной безопасности WBAN

Для противостояния угрозам информационной безопасности WBAN в качестве основных мер безопасности обычно используются механизмы шифрования и аутентификации. При передаче по сети персональных данных о состоянии здоровья пациентов они обязательно должны быть зашифрованы. При этом предотвращение несанкционированных изменений данных гарантируется тем, что только законные пользователи и устройства могут создавать и вводить данные в сеть. Это может, в свою очередь, позволить предотвратить многие из вышеуказанных атак. При этом для безопасной передачи различных видов информации в WBAN, а также для аутентификации используются различные криптографические методы, такие как симметричное и асимметричное шифрование.

В литературе для обеспечения безопасности сенсорных сетей на основе симметричного шифрования предложены множества решений [16–22], которые могут использоваться в WBAN. В этих решениях особое внимание уделяется эффективности создания и использования ключей. Причем управление ключами является динамичным, что создает дополнительные трудности атакующим. Однако при увеличении числа узлов сети симметричные решения не очень хорошо масштабируются, а программная реализация симметричной криптографии является очень сложной. Потому во многих работах по обеспечению безопасности сенсорных сетей исследования также были сосредоточены на использовании асимметричных криптографических алгоритмов [23–29].

Механизмы аутентификации используются для обеспечения идентификации узлов, от которых поступают данные, а также пользователей (врачей, медицинских

работников и т.п.) системы. Аутентификация данных является обязательной для узлов, чтобы идентифицировать введенные в систему новые пакеты [30]. Кроме того, наряду с сильными мерами аутентификации четко определенная иерархия пользователей может предотвратить нарушения безопасности в WBAN, то есть только авторизованные пользователи могут получить доступ к данным.

Заключение

Последние достижения в области беспроводных сенсорных сетей позволили использовать их для мобильного мониторинга состояния здоровья пациентов. WBAN является одним из важнейших элементов системы беспроводного мобильного мониторинга состояния здоровья пациентов. При этом обеспечение информационной безопасности является очень важным.

В статье были проанализированы проблемы информационной безопасности, возникающие при мобильном мониторинге состояния здоровья пациентов, а также существующие решения, которые могут быть использованы.

Использование этих решений может свести к минимуму риски по информационной безопасности при мобильном мониторинге состояния здоровья пациентов и обеспечить целостность и надежность персональных данных пациентов, а также системы в целом.

ЛИТЕРАТУРА

[1] T. Sheltami, A. Mahmoud and M. Abu-Amara, Warning and monitoring medical system using sensor networks, Proc. of the 18th National Computer Conference, Riyadh, Saudi Arabia, 2006, pp. 63–68.

[2] L. Wolf and S. Saadaoui, Architecture Concept of a Wireless Body Area Sensor Network for Health Monitoring of Elderly People, Proc. of the IEEE Consumer Communications and Networking Conference 4th, 2007, pp. 722–726.

[3] K. Yazdandoost et al., Channel Model for Body Area Network (BAN), Proc. of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2008, pp. 1549–1552.

[4] T. O’Donovan, J. O’Donoghue, C. Sreenan, P. O’Reilly, D. Sammon, K. O’Connor, A Context Aware Wireless Body Area Network (BAN), Proc. of the Pervasive Health Conference, 2009, pp. 1-8.

[5] S. Ng, L. Sim, and M. Tan, Security Issues of Wireless Sensor Networks in Healthcare Applications, Computer Journal of BT Technology Journal, vol. 24, no. 2, pp. 138–144, 2006.

[6] K. Chelli, Security Issues in Wireless Sensor Networks: Attacks and Countermeasures, www.iaeng.org/publication/WCE2015/WCE2015_pp519-524.pdf

[7] J. Mary, M. Buvana, A Survey: Security Issues and Design Challenges in Healthcare Monitoring System using Wireless Sensor Network, International Journal of Innovative Research in Science, Engineering and Technology, vol. 4, no. 11, pp. 10758–10765, 2015.

[8] Q. Wang, K. Ren, W. J. Lou and Y. C. Zhang, Dependable and secure sensor data storage with dynamic integrity assurance, Proc. of the IEEE International Conference on Computer Communications, Rio de Janeiro, Brazil, 2009, pp. 954–962.

[9] S. Chessa and P. Maestrini, Dependable and secure data storage and retrieval in mobile, wireless networks, Proc. of the International Conference on Dependable System and Networks, 2003, pp. 207–216.

[10] T. Dimitriou, K. Ioannis, Security issues in biomedical wireless sensor networks, Proc. of the First International Symposium on Applied Sciences on Biomedical and Communication Technologies, 2008, pp. 1–5.

[11] F. Kargl, E. Lawrence, M. Fischer and Y. Lim, Security, Privacy and Legal Issues in Pervasive eHealth Monitoring Systems, Proc. of the 7th International Conference on Mobile Business, 2008, pp. 296–304.

[12] A. Sastry, S. Sulthana and S. Vagdevi, Security Threats in Wireless Sensor Networks in Each Layer, International Journal of Advanced Networking and Applications, vol. 4, no. 4, pp. 1657–1661, 2013.

[13] H. Marzi, A Marzi, A security model for wireless sensor networks, Proc. of the IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications, 2014, pp.64-69.

[14] S. Kaplantzis, Security Models for Wireless Sensor Networks, http://members.iinet.com.au/~souvla/transferfinal-rev.pdf

[15] C. Karlof and D. Wagner, Secure routing in wireless sensor networks: attacks and countermeasures, Ad Hoc Networks Journal, vol.1, no. 2–3, pp. 293–315, 2003.

[16] A. Jain, K. Kant, Security Solutions for Wireless Sensor Networks, Second International Conference on Advanced Computing & Communication Technologies, 2012, pp. 430–433.

[17] S. Zhu, S Setia, S Jajodia, LEAP: efficient security mechanisms for large-scale distributed sensor networks, Proc. of the 10th ACM Conference on Computer and Communications Security (CCS 03), 2003, pp. 62–72.

[18] R. Blom, An optimal class of symmetric key generation systems, Proc. of the Eurocrypt 84 Workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques (Springer), 1985, pp. 335–338.

[19] C. Blundo, A. D. Santix, A. Herzberg, S. Kutten, U. Vaccaro, M. Yung, Perfectly-secure key distribution for dynamic conferences, Proc. of the 12th Annual International Cryptology Conference on Advances in Crypto-logy, Berlin, Germany (Spring), 1992, pp. 471–486.

[20] D. Liu, P. Ning, Location-based pairwise key establishments for static sensor networks, Proc. of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (CCS '03), 2003, pp. 72–82.

[21] L. Eschenauer, V. D. Gligor, A key-management scheme for distributed sensor networks, Proc. of the 9th ACM Conference on Computer and Communications Security, 2002, pp. 41–47.

[22] R. Anderson, H. Chan, A Perrig, Key infection: Smart trust for smart dust, Proc. of the 12thIEEE International IEEE International Conference on Network Protocols (ICNP '04), 2004, pp. 206–215.

[23] N. Gura, A. Patel, A. Wander, H. Eberle, S. C. Shantz, Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs, Sun Microsystems Laboratories, www.research.sun.com/projects/crypto.

[24] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn and P. Kruus, TinyPK: Securing Sensor Networks with Public Key Technology, Proc. of the 2nd ACM workshop on security of ad hoc and sensor networks SASN’04, 2004, pp. 59–64.

[25] D. J. Malan, M. Welsh, M. D. Smith, A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography, Division of Engineering and Applied Sciences, Harvard University, Dec 2007.

[26] H. Wang, B. Sheng, C. C. Tan, Q. Li, Comparing Symmetric-key and Public-key based Security Schemes in Sensor Networks: A Case Study of User Access Control, College of William and Mary Williamsburg, VA 23187-8795, USA.

[27] H. Wang and Q. Li, Efficient implementation of public key cryptosystems on mote sensors, Proc. of the International Conference on Information and Communication Security (ICICS ’06), 2006, pp. 519–528.

[28] J. Girao, D. Westhoff, E. Mykletun, and T. Araki, TinyPEDS: Tiny Persistent Encrypted Data Storage in Asynchronous Wireless Sensor Networks. Elsevier Ad Hoc Journal, vol. 5, no.7, pp. 1073–1089, 2007.

[29] L. B. Oliveira, M. Scott, J. Lopez, R. Dahab, TinyPBC: Pairings for Authenticated Identity Based Non-Interactive Key Distribution in Sensor Networks, CAPES (BrazilianMinistry of Education) grant 4630/06-8 and FAPESP grant 2005/00557-9.

[30] S. Stanković, Medical Applications Based on Wireless Sensor Networks, Transactions on Interbet Research, vol.4, no. 2, pp. 19–23, 2009.