Ministerul Educației, Culturii și Cercetării al Republicii Moldova
Universitatea Tehnică a Moldovei
Facultatea Electronică și Telecomunicații
Departamentul Telecomunicaţii şi Sisteme Electronice

Admis la susţinere
Șef departament:
conf.univ.dr. Sava L.
„____”_____ 2020

Analiza securității privind localizarea sigura in rețele de senzori fără fir

Анализ защищенности безопасного местоположения в беспроводных сенсорных сетях

Teză de master

Studenta: **Serluceanu Iana, grupa SISRC-191M**

Coordonator: **Cerbu Olga, conf. univ.dr.**

Chişinău, 2020

РЕЗЮМЕ

Serluceanu Iana

Тема: Анализ защищенности безопасного местоположения в беспроводных сенсорных сетях.
Структура работы: Введение; Глава 1: Общие сведения о беспроводных сенсорных сетях WSN; Глава 2: Анализ и применение структуры данных фильтра Блума для повышения безопасности сетей WSN; Глава 3: Анализ и применения алгоритмов для оптимизации топологии беспроводной сенсорной сети; Заключение, Библиография; Анекса; 37 таблиц; 31 фиг.

Ключевые слова: WSN - Беспроводные сенсорные сети, Триангуляции Делоне, AES, Share and Master, фильтр Блума.
Цель работы: изучение и анализ алгоритмов работы сенсорной сети (существующих протоколов), позволяющих обеспечить безопасное местоположение в сети.
Задачи: 1. Анализ современного состояния в области исследований WSN;
2. Определение наиболее важных характеристик и структуры беспроводных сенсорных сетей;
3. Анализ методов улучшения безопасности;
4. Анализ существующих алгоритмов маршрутизации;
5. Определение факторов, влияющих на безопасность системы;
Применяемые методы: Шифрование и «одноразовый номер», блочный шифр AES-128, Фильтр Блума, Триангуляция, алгоритм «Share and Master» на языке java.
Полученные результаты:1. Тематика сенсорных беспроводных сетей еще недостаточно изучена, имеются на данный момент ряд нерешенных проблем и ограничений, но преимущества привлекают компании для разработки стандартов передачи информации в сенсорных сетях.

2. Были проанализированы основные топологии БСС. Разработаны математические модели топологии, узлов, механизма их конкурентного доступа к каналу передачи данных, коммуникаций БСС, адаптированные к использованию в алгоритме оптимизации топологии.

3. Были проанализирлованны методы по защите БСС такие как криптографические примитивы, поддержка управления ключами, обеспечение аутентификации на уровне Mac, безопасное агрегирование данных. Механизм защиты атаки подразделяется на два типа протокола связи и архитектуру управления ключами. Проблемы надежности могут быть решены путем полного планирования и управления архитектурой сети до ее развертывания.

4. В качестве инструментов для анализа существующих алгогритмов маршрутизации использовался алгоритм Триангуляции Делоне, алгоритм симметричного блок шифрования AES, Алгоритм «Share and Master», для обработки результатов использовался язык JAVA.

5. Разработка сенсорных сетей зависит от многих факторов, которые включают в себя отказоустойчивость, масштабируемость, издержек производства, вид операционной среды, топологию сенсорной сети, аппаратные ограничения, модель передачи информации и потребление энергии.

REZUMAT

Serluceanu Iana

Tema: Analiza securității privind localizarea sigură in rețele de senzori fară fir.
Structura lucrării: Introducere; Capitolul 1: Prezentare generală a rețelelor de senzori fără fir WSN; Capitolul 2: Analizați și aplicați o structură de date a filtrului Bloom pentru a îmbunătăți securitatea WSN; Capitolul 3: Analiza și aplicarea algoritmilor pentru optimizarea topologiei rețelei senzorilor fără fir; Concluzie, Bibliografie; Anexa; 37 tabele; 31 fig.
Cuvintele-Cheie: WSN - Rețele de senzori fără fir, Triangulații Delaunay, AES, Share and Master, Bloom Filter.
Scopul lucrării: studierea și analiza algoritmilor rețelei de senzori (protocoale existente), permițând asigurarea unei locații sigure în rețea.
Obiectivele: 1 Analiza stadiului actual al tehnicii în domeniul cercetării WSN;
2. Determinarea celor mai importante caracteristici și structură a rețelelor de senzori fără fir;
3. Analiza metodelor de îmbunătățire a siguranței;
4. Analiza algoritmilor de rutare existente;
5. Identificarea factorilor care afectează securitatea sistemului;
Metodele aplicate: Criptare și nonce, cifrare bloc AES-128, filtru Bloom, triangulare, partajare și algoritm master în java.
Rezultatele obținute: 1. Subiectul rețelelor de senzori fără fir nu a fost încă suficient studiat, în prezent există o serie de probleme și limitări nerezolvate, dar avantajele atrag companiile să dezvolte standarde pentru transmiterea informațiilor în rețelele de senzori.
2. Au fost analizate topologiile de bază ale BSS. Au fost dezvoltate modele matematice ale topologiei, nodurilor, mecanismul accesului competitiv la canalul de transmisie a datelor și comunicațiile BSS, adaptate pentru utilizarea în algoritmul de optimizare a topologiei.
3. Au fost analizate metode pentru protejarea FSU, cum ar fi primitive criptografice, suport pentru gestionarea cheilor, furnizarea autentificării la nivel de Mac, agregare sigură a datelor. Mecanismul de apărare a atacurilor este clasificat în două tipuri de protocol de comunicare și arhitectură de gestionare a cheilor. Problemele de fiabilitate pot fi rezolvate prin planificarea și gestionarea completă a arhitecturii rețelei înainte de implementare.
4. Algoritmul de triangulare Delaunay, algoritmul de blocare de criptare simetrică AES, algoritmul Share și master au fost utilizate ca instrumente pentru analiza algoritmilor de rutare existente, limbajul JAVA a fost utilizat pentru a procesa rezultatele.
5. Dezvoltarea rețelelor de senzori depinde de mulți factori, care includ toleranța la erori, scalabilitatea, costurile de producție, tipul de mediu de operare, topologia rețelei senzorilor, constrângerile hardware, modelul de comunicare și consumul de energie.

SUMMARY

Serluceanu Iana

Title: Security analysis on secure location in wireless sensor networks.

Thesis structure: Introduction; Chapter 1: Overview of WSN Wireless Sensor Networks; Chapter 2: Analyze and Apply a Bloom Filter Data Structure to Enhance WSN Security; Chapter 3: Analysis and Application of Algorithms to Optimize Wireless Sensor Network Topology; Conclusion, Bibliography; Anexa; 37 tables; 31 fig.

Keywords: WSN - Wireless Sensor Networks, Delaunay Triangulations, AES, Share and Master, Bloom Filter.Purpose of the work: study and analysis of algorithms for the sensor network (existing protocols), allowing to ensure a safe location in the network.

Thesis purpose: study and analysis of the algorithms of the sensor network (existing protocols), allowing to ensure a safe location in the network.

Objectives: Objectives: 1. Analysis of the current state of the art in the field of WSN research;

2. Determination of the most important characteristics and structure of wireless sensor networks;
3. Analysis of methods for improving safety;
4. Analysis of existing routing algorithms;
5. Identification of factors affecting the security of the system;

Applied methods: Encryption and nonce, AES-128 block cipher, Bloom filter, Triangulation, Share and Master Algorithm in java.

Results obtained: 1. The subject of wireless sensor networks has not been sufficiently studied yet, there are currently a number of unresolved problems and limitations, but the advantages are attracting companies to develop standards for information transfer in sensor networks.

2. The basic topologies of the BSS were analyzed. Mathematical models of the topology, nodes, the mechanism of their competitive access to the data transmission channel, and BSS communications, adapted for use in the topology optimization algorithm, have been developed.

3. Methods for protecting the FSU were analyzed, such as cryptographic primitives, key management support, providing Mac-level authentication, and secure data aggregation. The attack defense mechanism is categorized into two types of communication protocol and key management architecture. Reliability issues can be resolved by fully planning and managing the network architecture prior to deployment.

4. The Delaunay Triangulation Algorithm, AES Symmetric Encryption Block Algorithm, Share and Master Algorithm were used as tools for the analysis of existing routing algorithms, the JAVA language was used to process the results.

5. The design of sensor networks depends on many factors, which include fault tolerance, scalability, production costs, type of operating environment, sensor network topology, hardware constraints, communication model and energy consumption.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Одной из областей телекоммуникаций, которая в настоящее время широко используется широким сообществом, являются беспроводные сети (WLAN) и Интернет. Эта беспроводная сеть быстро развивалась, примером которой является передача данных через инфракрасный порт (IrDA) и Bluetooth. Из-за его способности передавать данные люди во всем мире используют его в различных приложениях, связанных с беспроводными сетями, одним из которых является его использование для передачи данных. Чтобы справиться с развитием передачи данных с использованием беспроводных сетей, есть надежда, что будущие сети связи смогут лучше использовать беспроводные сети, как на локальных, так и на больших территориях. Простая сеть состоит из двух или более компьютеров, соединенных друг с другом. Основными компонентами сети являются компьютеры, соединяющие сеть, среда подключения, программное обеспечение сетевой операционной системы, концентратор или Switch Hub - это очень простое устройство, которое соединяет сетевые компоненты, отправляя пакеты данных на все подключенные устройства. К ним относятся традиционные телефонные системы, мобильная сотовая связь, беспроводные локальные сети и корпоративные веб-сайты, интрасети, экстрасети, а также стеки LAN и WAN, включая Интернет. Этот набор сетей развивается из двух принципиально различных типов сетей: телефонных сетей и компьютерных сетей.

Беспроводные каналы открыты для всех и имеют радио интерфейсы, настроенные на одном частотном диапазоне. Таким образом, любой может контролировать или участвовать в общении по беспроводному каналу. Это дает злоумышленникам простой способ проникнуть в сеть.

Как и в случае с интернетом, большинство протоколов для WSN не учитывают механизмы безопасности, необходимые на этапе проектирования. С другой стороны, большинство протоколов широко известны из-за необходимости стандартизации. По этой причине злоумышленники могут легко запускать атаки, используя дыры в безопасности в протоколе.

Ограниченные ресурсы сенсорных узлов очень затрудняют реализацию надежных алгоритмов безопасности на сенсорных платформах из-за их сложности. Кроме того, большое количество сенсорных узлов отправляет запросы на простые, гибкие и масштабируемые протоколы безопасности.

Более строгие протоколы безопасности потребляют больше ресурсов на узлах датчиков, что может привести к снижению производительности приложений. В

большинстве случаев приходится искать компромисс между безопасностью и производительностью. Однако слабые протоколы безопасности могут быть легко взломаны злоумышленником.

WSN обычно размещаются во враждебных зонах без постоянной инфраструктуры. После развертывания сети сложно вести постоянное наблюдение. Из-за этого он может столкнуться с различными потенциальными атаками.

Цель работы и задачи исследования

Целью магистерской работы является изучение и анализ алгоритмов работы сенсорной сети (существующих протоколов), позволяющих обеспечить безопасное местоположение в сети.

Для достижения поставленной цели в магистерской работе решаются следующие **задачи**:

1. Анализ современного состояния в области исследований WSN
2. Определение наиболее важных характеристик и структуры беспроводных сенсорных сетей
3. Анализ методов улучшения безопасности;
4. Анализ существующих алгоритмов маршрутизации,
5. Определение факторов, влияющих на безопасность системы,

Актуальность магистерской работы:

Защита беспроводных сенсорных сетей является актуальной проблемой, так как узлы сети имеют небольшую вычислительную мощность, ограниченный заряд батареи и располагаются в незащищенных местах, а информация передается по беспроводным каналам, то любое нарушение работы сети может привести к нежелательным последствиям. На сегодняшний день разработано большое количество методов защиты БСС, а также систем обнаружения вторжений, но данные методы в основном предназначены для статических БСС. Также существует необходимость в разработке комплексного подхода к защите БСС, который смог бы противодействовать большинству существующих атак.

БИБЛИОГРАФИЯ

1. Агафонов Н. Технологии беспроводной передачи данных,
    a. «Беспроводные технологии» №1, 2014 г.
2. Варгаузин В.А. Радиосети для сбора данных от сенсоров, мониторинга и управления на основе стандарта IEEE 802.15.4 // ТелеМультиМедиа. 2015. № 6. – С. 23-27.
3. Talipov E. Sensor network 802.15.4 AODV simulation [Электронный ресурс]. – Режим доступа: http://elmurod.net/
4. David Gascon Understanding 802.15.4 [Электронный ресурс]. – Режим доступа: http://www.sensor-networks.org/
5. B. Bloom. Space/Time Tradeoffs in Hash Coding with Allowable Errors,CACM,13(7):422-426, July 1970.
6. A. Broder and M. Mitzenmacher, Network Applications of Bloom Filters: A Survey, Internet Mathematics, 1(4):485-509, 2004.
7. F. Hao, M. Kodialam, and T.V. Lakshman, Building High Accuracy Bloom Filters using Patitioned Hashing, Joint International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS), pp:277 - 288, San Diego, California, USA, 2007.
8. Yi Lu, Balaji Prabhakar, and Flavio Bonomi, Perfect Hashing for Network Applications, IEEE International Symposium on Information Theory (ISIT), Seattle, USA, July 9-14, 2006.
9. A. Pagh, R. Pagh, and S.S. Rao, An Optimal Bloom Filter Replacement, Proceedings of the sixteenth annual ACM-SIAM symposium on Discrete algorithms (SODA), Vancouver, B.C., Canada, 2005.
10. S.C. Rhea and J. Kubiatowicz. Probabilistic Location and Routing, Proceedings of INFOCOM 2002
11. Varber, C. B.; Dobkin, D. P.; and Huhdanpaa, H. T. “The Quickhull Algorithm for Convex Hulls.” ACM Trans. Mathematical Software 22, 469–483, 1996.
12. Hinton, P. J. “qh-math: A MathLink Interface To Qhull’s Delaunay Triangulation.”
13. Lee, D. T. and Schachter, B. J. “Two Algorithms for Constructing a Delaunay Triangulation.” Int. J. Computer Information Sci. 9, 219–242, 1980.
14. Okabe, A.; Boots, B.; and Sugihara, K. Spatial Tessellations: Concepts and Applications of Voronoi Diagrams. New York: Wiley, 1992.
15. Preparata, F. R. and Shamos, M. I. Computational Geometry: An Introduction. New York: Springer-Verlag, 1985.
16. (2020), J. A.-i.-O. (б.д.). *Doug Lowe.*

17. Daniel Deogun, D. B. (б.д.). *Secure By Design (2019).*
18. Hyde, R. (б.д.). *Write Great Code, Volume 2, 2nd Edition (2020).*