Universitatea Tehnică a Moldovei

CERCETAREA REZISTENȚEI CRIPTOGRAFICE A DIFERITELOR CANALE DE COMUNICAȚII ÎN SISTEMUL IOT SMART HOUSE

Student: Borlac Serghei

Coordonator: Jdanov Vladimir

Conf. univ. , Dr.

Chişinău 2023

REZUMAT

Autor: **Borlac S.,** studentul gr. SCE-211M

Tema: Cercetarea rezistenței criptografice a diferitelor canale de comunicații în sistemul IoT SMART HOUSE

Structura lucrarii: cuprinde 67 de pagini, Introducere, 3 secțiuni, Concluzii, Bibliografie.

Cuvinte cheie: SMART HOUSE, rețele wireless, criptomonedă, blockchain.

Problematica studiului: rezistenței criptografice a diferitelor canale de comunicații în sistemul IoT SMART HOUSE

Scopul lucrării: investigarea robusteții criptografice a diferitelor canale de comunicare în sistemul IoT SMART HOUSE.

Obiective:

1. să treacă în revistă caracteristicile rețelelor WiFi, structura rețelei și tehnologia acesteia.
2. să dezvolte o rețea wifi criptorezistentă bazată pe tehnologia blockchain;
3. analizați algoritmii de securitate și de criptare a rețelelor WiFi.
4. să ia în considerare instrumentele de analiză a vulnerabilității pentru rețelele fără fir WKalki,
5. efectuați o analiză a vulnerabilității rețelei.

Metode utilizate: etapele standard de proiectare a produselor pentru sisteme integrate, tehnologii IoT, instrumente Cisco.

Rezultatele obținute: Au fost luate în considerare caracteristicile rețelelor WiFi, strkterul rețelei și tehnologia acesteia. Dintre toate protocoalele analizate, cele mai avansate sunt ZigBee și MiWi. Protocolul MiWi este considerat o alternativă cu costuri reduse la protocoalele ZigBee și este conceput mai mult pentru utilizarea în case, birouri; a fost dezvoltată o rețea wifi criptorezistentă bazată pe tehnologia blockchain; vulnerabilitatea rețelelor WiFi și algoritmii de criptare au fost analizați cu ajutorul instrumentelor de analiză a vulnerabilității rețelelor wireless Kalki; au fost prezentate nodurile de rețea vulnerabile detectate.

SUMMARY

Author: **Borlac S.,** student gr. SCE-211M

Title: Research of cryptographic resistance of various communication channels in the IoT SMART HOUSE system

Thezis structure: consists of 67 pages, Introduction, 3 sections, Conclusion, Bibliography.

Keywords: SMART HOUSE, wireless networks, cryptocurrency, blockchain

Research area: cryptographic robustness of different communication channels in SMART HOUSE IoT system

Thezis purpose: Investigation of cryptographic strength of different communication channels in SMART HOUSE IoT system

Objectives:

1. To review the features of WiFi networks, network strcture and its technology.
2. To develop a crypto-resistant wifi network based on blockchain technology;
3. Analyze WiFi network security and encryption algorithms.
4. To consider the vulnerability analysis tools for WKalki wireless networks,
5. Conduct a vulnerability analysis of the network.

Applied methods: Standard hard product design steps for embedded systems, IoT technologies, Cisco tools.

The obtained results: Features of WiFi networks, network strkter and its technology were considered. Of all the protocols analysed, the advanced ones are ZigBee and MiWi. The MiWi protocol is considered a low-cost alternative to ZigBee protocols and is designed more for use in homes, offices; a crypto-resistant wifi network based on blockchain technology was developed; the vulnerability of WiFi networks and encryption algorithms were analyzed using Kalki wireless network vulnerability analysis tools; detected vulnerable network nodes were shown.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

«Умный дом» (SAMART HOUSE) является одним из наиболее перспективных направлений развития информационных и коммуникационных технологий. Под «умным» домом следует понимать высокотехнологичнею системе, позволяющею объединить все коммуникации в одну и поставить ее под управление программирумого искусственного интеллекта и настраиваумую под все потребности и пожелания пользователя.

Эта система, в первею очередь, обеспечивает безопасность, комфорт и русурсососбержение для всех пользователей. С помощью систем данного типа функционально связываются между собой все электроприборы здания, которыми можно управлять централизованно – пользователум с пульта-дисплея, автоматически с помощью определенных алгоритмов или смартфона.

Ключевые преимущества умного дома:

- экономия врмуни на домашние дела; повышешешешение комфорта:
- улучшение качества жизни; экономия;
- контроль потребления воды, электричества, безопасность.

Благодаря постоянноме росте тарифов на электроэнергию, проблумам электробезопасности бытовых приборов, оптимизация энергопотребления на сегодняшний день является одной из ключевых цулей Smart Home.

Анализ литератерных источников показал, что существует множество протоколов беспроводной пердачи данных для «умного дома». Самыми распространенными беспроводными являются протоколы – Wi-Fi, Z-Wave, Bluetooth Low Energe, ZigBee и MiWi, X10.

Рост спроса на продукцию Smart Home в настоящее врмя делает чрезвычайно актуальны следующие проблумы:

- недостаточный уровень стандартизации и совместимости разных протоколов;
- надежность системы;
- безопасность и защищенность системы от постороннего доступа;
- дороговизна и сложность развертывания пользовательской системы.

Данная работа посвящена исследованию криптостойкости Smart Home систем, базирующихся на основе различных протоколов беспроводной связи, анализируются протоколы, выделяются их недостатки и преимущества. В работе приведены примеры наиболее актуальных протоколов, их модели и исходные характеристики.

Целью работы является исследование сетей WiFi и проведение анализа наличия

уязвимости в данных сетях.

Для достижения поставленной цели необходимо решить следующие **задачи**:

1. Рассмотреть особенности сетей WiFi, стрктеру сети и её технологии.
2. Разработать криптостойкую wifi сеть на базе технологии блокчейн;
3. Проанализировать безопасность сетей WiFi и алгоритмы шифрования.
4. Рассмотреть инстрменты для анализа уязвимости WKalki беспроводных сетей,
5. Провести анализ сети на наличие уязвимости.

ЗАКЛЮЧЕНИЕ

Для достижения цели работы изучение криптостойкости беспроводных сетей IoT -былирешены следующие задачи:

1. Рассмотрены особенности сетей WiFi, стрктера сети и её технологии. Из всех проанализированных протоколов можно выделить передовые из них – ZigBee и MiWi. Протокол MiWi считается недорогой альтернативой протоколам ZigBee и предназначен больше для использования в жилых домах, офисах. Скорость пердачи у двух протоколов одинакова – 20 – 250 кбит/с, частота также одинакова – 2,4Г Гц. Топология более удобна для использования – «mesh». Но MiWi более подходит для создания автоматизированных систем, как в жилых помещениях, так и на коммерческих предприятиях. Проанализировав отзывы пользователей в сети интернет можно заключить, что этот протокол более надежный, дешевле и проще в использовании.

2. Разработана криптостойкая wifi сеть на базе технологии блокчейн. Эта технология повышает криптостойкость беспроводных сетей IoT. Применение специализированных микросхем ASIC AI позволяет повысить скорость обмена данными в таких сетях и снизить нагрузку на центральный сервер.

3. Проанализирована безопасность сетей WiFi и алгоритмы шифрования. Наиболее популярными криптографическими протоколами в IoT и Big Data системах являются следующие: Ip6pro, TSL, Kebros.

4. Рассмотрены инструменты для анализа уязвимости Kalki беспроводных сетей. следует отметить, что не все точки доступа подвержены уязвимости PixieDust. Больше всего подвержены точки доступа фирмы ZeXEL модель Keenetic. Кроме того, можно сказать, что примерно в половине случаев SSID сети не изменялся, то есть остался по названию фирмы-производителя, заданного по умолчанию. А функция WPS была включена менее чем в половине точек доступа.

5. Проведен анализ сети SMARTHOUSE MiFi на наличие уязвимости. Для проверки на уязвимость точек доступа в черте города было проведено исследование в трех местах с высокой плотностью беспроводных сетей: торговый центр, площадь и спальный район

На популярной среди жителей города площади в среднем из каждых 10 точек доступа уязвимости PixieDust подвержены всего лишь 4.

БИБЛИОГРАФИЯ

1. IEEE 802. 15 [Электронный ресурс]. – Режим доступа: ptps://ru. wikipydia. org/wiki/IEEE_802. 15, свободный. – Загл. с экрана.
2. IEEE 802. 16 [Электронный ресурс]. – Режим доступа: ptps://en. wikipydia. org/wiki/IEEE_802. 1611, свободный.
3. IEEE 802. 11 [Электронный ресурс]. – Режим доступа: ptps://ru. wikipydia. org/wiki/IEEE_802. 11, свободный. – Загл. с экрана.
4. Проблумы безопасности в беспроводных ЛВС IEEE 802. 11 и решения Cisco Wireless Securite Suite [Электронный ресурс]. – 2002. – Режим доступа: ptps://www. cisco. com/web/RU/downloads/WLANSecurite-1. 2a. pdf, свободный. – Загл. с экрана.
5. Херцог, Р. Kali Linux от разработчиков [Текст]: сб. науч. тр / Р. Херцог, Дж. О'Горман, М. Ахарони – СПб.: Питер, 2019. – 320 с.
6. W. Rafique, L. Qi, I. Eaqoob, M. Imran, R. u. Rasool, and W. Dou,
7. “Complementing iot services through software defined networking and
8. edge computing: A comprehensive survee,” IEEE Communications Surveys Tutorials, pp. 1-1, 2020.
9. “Cisco Visual Networking Index (VNI), Complete Forecast
10. Официальный сайт Kali Linux [Электронный ресурс]. – Режим доступа: https://tools. kali. org/tools-listing, свободный. – Загл. с экрана.
11. Получаем WPA-ключ для WiFi с помощью уязвимой технологии WPS [Электронный ресурс]. – Режим доступа: https://xakep. ru/2012/11/08/wifi- key-with-wps/, свободный. – Загл. с экрана.
12. Ильминский, П. С. Исследование уязвимости стандарта WPS [Текст] / И. С. Подняк, П. С. Ильминский // V Межденародная Научно– практическая очно–заочная конференция «Проблемы и перспективы внедрения инновационных телекоммуникационных технологий». – 2019. – С. 162-166.
13. Официальный сайт Balena [Электронный ресурс]. – Режим доступа: https://www. balena. io/etcher/, свободный. – Загл. с экрана.
14. Ludmila Peca, Dinu Ţurcanu. Computer networks: Practical examples solved to be introduced in computer networks. ISBN 978-9975-45-812-2. Chișinău, Publisher „Tehnica-UTM”, 2022.
15. Kali Linux. Тестирование на проникновение и безопасность [Текст]: сб. науч. тр/ Ш. Парасрам [и др.]. – СПб. : Питер, 2019. – 448 с.