Универзитет у Новом Саду
Технички факултет „Михајло Пупин“
Зрењанин

Анализа безбедности бежичних сензорских мрежа

Security Analysis in Wireless Sensor Networks

- Мастер рад -

Студент:
Драго Катић
Бр. индекса:
МРТ 25/2015
Студијски програм:
Информатика и техника у образовању

Зрењанин, 2018.

Универзитет у Новом Саду
Технички факултет „Михајло Пупин“
Зрењанин

Анализа безбедности бежичних сензорских мрежа

Security Analysis in Wireless Sensor Networks

- Мастер рад -

Ментор:
Проф. др Далибор Добриловић

Студент:
Драго Катић
Бр. индекса:
МРТ 25/2015
Студијски програм:
Информатика и техника у образовању

Зрењанин, 2018.

Универзитет у Новом Саду

Технички факултет „Михајло Пупин” Зрењанин

Кључна документацијска информација

Редни број: РБР	
Идентификациони број: ИБР	
Тип документације: ТД	Монографска документација
Тип записа: ТЗ	Текстуални штампани материјал
Врста рада: ВР	Мастер рад
Име и презиме аутора: АУ	Драго Катић
Ментор: МН	Др Далибор Добриловић, професор
Наслов рада: НР	Анализа безбедности бежичних сензорских мрежа
Језик публикације: ЈП	Српски
Језик извода: ЈИ	Српски / енглески
Земља публиковања: ЗП	Србија
Уже географско подручје: УГП	Војводина
Година: ГО	2018.
Издавач: ИЗ	ауторски репринт
Место и адреса: МА	23000 Зрењанин, Ђуре Ђаковића бб
Физички опис рада: ФО	7/50/35/0/6/9
Научна област: НО	Информационе технологије
Научна дисциплина: НД	Заштита података и рачунарских мрежа
Предметна одредница, кључне речи: ПО	оптималне комуникационе путање, криптографски алгоритми, инфраструктура јавних кључева, бежични пренос електричне енергије
УДК	
Чува се: ЧУ	У библиотеци техничког факултета „Михајло Пупин” Зрењанин
Važna napomena: VN	
Извод: ИЗ	Предмет истраживања овог рада представља хардверска и софтверска имплементација безбедних бежичних сензорских мрежа са становишта оптималног рутирања, постизања тајности комуникације, аутентификације ентитета, обезбеђивања интегритета порука и расположивости система уз оптималну потрошњу електричне енергије и алтернативне видове снабдевања електричном енергијом.
Датум прихватања теме од стране НН већа: ДП	
Датум одбране: ДО	
Чланови комисије: КО	Председник: Члан: Члан:

University of Novi Sad

Tehnical Faculty "Mihajlo Pupin" Zrenjanin

Key word documentation

Accesssion number: ANO	
Identification number: INO	
Document type: DT	Monograph documentation
Type of record: TR	Textual printed material
Concents code: CC	M. Sc thesis
Author: AU	Drago Katić
Menthor: MN	Prof. dr Dalibor Dobrilović
Title: TI	Security Analysis in Wireless Sensor Networks
Language of text: LT	Serbian (Cyrillic)
Language of abstract: LA	English / Serbian
Country of publication: CP	Serbia
Locality of publication: LP	Vojvodina
Publication year: PY	2018.
Publisher: PU	Autor`s Reprint
Publication place: PP	23000 Zrenjanin, Đure Đakovića bb
Physical description: PD	7/50/35/0/6/9
Scientific field: SF	Information technology
Scientific discipline: SD	Data and Computer Network Security
Subject, Key words: SKW	optimal routhing, cryptographic algorithms, public key infrastructure, wireless power transfer
UC	
Holding data: HD	Library of Technical Faculty „Mihajlo Pupin” Zrenjanin
Note: N	
Abstract: AB	The subject of this thesis is the hardware and software implementation of safe wireless sensor networks from the perspective of optimal routing, achieving the secrecy of communication, entity authentication, ensuring the integrity of messages and system availability with optimal electricity consumption and alternative forms of electricity supply.
Accepted on Scientific Board on: AS	
Defended: DE	
Thesis Defend Board: DB	President: Member: Member:

САДРЖАЈ

Сажетак

Намера је да се у овом раду истраже питања и изазови у вези са безбедношћу бежичних сензорских мрежа. Овај рад се бави истраживањем оптималних комуникационих путања, проценом безбедносних потреба и потенцијалним безбедносним претњама у бежичним сензорским мрежама. Избор криптографских алгоритама је у директној вези са животним веком и ефикасношћу уређаја, потрошњом електричне енергије, потребним хардверским ресурсима, комплексношћу компјутерских прорачуна, пропусним опсегом и количином комуникације. Актуелна истраживања у овој области се баве превазилажењем ограничења која намећу оскудни хардверски ресурси, тако да су сада популарна решења која укључују једноставни, често наменски, хардвер који је развијен у складу са постојећим криптографским алгоритмима који се најчешће користе у сврху заштите бежичних сензорских мрежа. Поред тога, овај рад разматра решења која се заснивају на инфраструктури јавних кључева таквој да може да обезбеди размену јавних и приватних кључева и да омогући релативно висок ниво безбедности употребом кључева релативно мале комплексности употребом криптографије засноване на елиптичним кривим и хомоморфном шифровању. Како би се смањила потрошња електричне енергије хомоморфно шифровање се користи тако да обезбеди главним чворовима у мрежи агрегацију података и њихово шифровање без потребе за дешифровањем. Додатно, овај рад разматра проблем ефикасног и избалансираног бежичног снабдевања електричном енергијом уређаја у бежичним сензорским мрежама.

Кључне речи: оптималне комуникационе путање, криптографски алгоритми, инфраструктура јавних кључева, бежични пренос електричне енергије

Abstract

The intent of this paper is to look into the security related issues and challenges in wireless sensor networks. This paper explores optimal communication routing, security requirements and potential security threats in wireless sensor networks. The selection of a cryptographic algorithm will affect the lifespan and performance of the device, its battery life, necessary hardware and computation complexity, latency and communication bandwidth. Current research in this area explores overcoming the limitations imposed by scant hardware resource. For this reason, the trend is shifting towards lightweight algorithmic hardware designs developed in accordance with existing cryptographic algorithms, which are now most commonly now used for protection of wireless sensor networks. Moreover, this paper examines encryption schema based on public key infrastructure and optimal structure to exchange public and private keys and provide relatively high security with small key size using encryption schema based on Elliptic Curve Cryptography and homomorphic encryption. To reduce energy consumption, homomorphic encryption is used to allow cluster heads to aggregate the encrypted data without having to decrypt them. Additional, in this paper investigate the problem of efficient and balanced wireless power transfer in wireless sensor networks.

Keyword: optimal routing, cryptographic algorithms, public key infrastructure, wireless power transfer

1. Увод

Намера да се достигне ефикасна и оптимална безбедносна структура бежичних сензорских мрежа, које карактерише динамичка природа и ограничени ресурси, чини ову област непрестаним изазовом по питању истраживања. Употреба бежичних комуникационих технологија укључује бројне врсте безбедносних претњи док криптографски алгоритми представљају незаменљиво средство приликом заштите података и обезбеђивања њихове тајности. Избор криптографског система утиче на животни век мреже и на перформансе мрежних уређаја узимајући у обзир расположиву електричну енергију за њихово напајање, количину потребне меморије, комплексност интегралних кола по питању аритметичко логичких операција и комуникационе карактеристике уређаја. Бројна криптографска решења имају различите функционалности, специфичности и снагу, а избор одговарајућег зависи од намене и величине мреже као и од потребног нивоа безбедности. Потпуна реализација безбедних бежичних сензорских мрежа подразумева имплементацију алгоритама за креирање динамичких путања који ефикасно ангажују хардверске и софтверске ресурсе, имплементацију криптографских системе за обезбеђивање тајности, система за аутентификацију ентитета у мрежи, система за потврду интегритета порука и система за управљање криптографским кључевима. Сврха бежичних сензорских мрежа одређује неопходан безбедносни ниво, док њихова економичност одређује оправданост реализације.

2. Методолошки оквир истраживања

Циљ је да се у оквиру овог рада истраже питања и изазови у вези са безбедношћу бежичних сензорских мрежа и њиховим ефикасним функционисањем. Обрађене теме су у вези са одређивањем оптималних комуникационих путања, потенцијалним безбедносним претњама и криптографским решењима којима је могуће превентивно деловати по питању безбедносних претњи. Посебна пажња је посвећена имплементацији криптографских система којима је могуће обезбедити институције аутентичности, тајности, интегритета и непорецивости. Рад се бави превазилажењем ограничења која намећу скромни хардверски ресурси кроз оптимизацију криптографских алгоритама и на основу наменских хардверских решења. Такође, разматра решења која смањују потрошњу електричне енергије као и решења која могу омогућити снабдевање електричном енергијом из додатних, односно алтернативних извора.

2.1 Предмет истраживања

Хардверска и софтверска реализација безбедних бежичних сензорских мрежа.

2.2 Проблем истраживања

Бројна криптографска решења која су нашла своје место у информационо комуникационим технологијама нису адекватна за имплементацију у бежичним сензорским мрежама обзиром да њихова комплексност захтева сложеније хардверске ресурсе и већу количину енергије о чему говоре бројни научно-истраживачки радови, савремена литература из области информационих технологија и бројни извештаји са научних скупова. Док једни сматрају да хардверска ограничења не представљају препреку и да је довољно користити једноставне криптографске алгоритме обзиром да бежичне сензорске мреже често прикупљају велике количине података чија актуелност и значај варирају у зависности од намене мреже, други сматрају да уређаји у мрежама треба да буду довољно сложени како би на њима могли да се имплементирају довољно комплексни криптографски системи чиме би мреже имале одговарајући ниво безбедности и поузданости у раду.

2.3 Циљ и карактер истраживања

Настојање је да се овим истраживањем одговори на питање оптималног односа између нивоа безбедности бежичних сензорских мрежа и ангажовања хардверских ресурса због чега је битно размотрити карактеристике уређаја који се користе у реализацији ових мрежа и адекватна софтверска решења која могу бити имплементирана на тим уређајима са посебном пажњом на имплементацију криптографских система.

2.4 Задаци истраживања

Истраживање обухвата проучавање литературе, научних радова, извештаја са конференција и података који се појављују Интернет порталима.

2.5 Хипотеза

Бежичне сензорске мреже, без обзира на намену и величину, морају имати одговарајуће безбедносне механизме како њихова сврха и стабилан рад не би били угрожени.

2.6 Методе истраживања

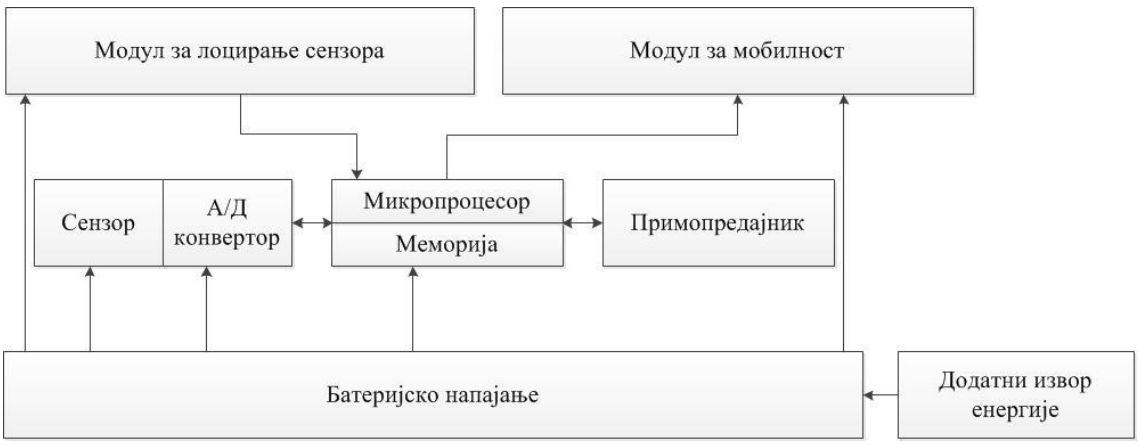
Ово истраживање ће бити реализовано дескриптивном методом. Дескрипција ће бити реализована на основу анализе доступног материјала, упоређивањем различитих извора, синтезом чињеница и утврђивањем каузалних веза.

2.7 Структура рада

Први део рада се бави архитектуром и основним карактеристикама бежичних сензорских мрежа. Други део рада обрађује карактеристике протокола рутирања и њихове предности и мане у зависности од намене и могућности за имплементацију. Трећи део се бави безбедносним претњама и начинима за њихову превенцију. Четврти део обрађује безбедносне механизме са аспекта имплементације различитих криптографских система. Пети део се бави животним веком бежичних сензорских мрежа, потрошњом уређаја и технологијама које омогућавају додатно снабдевање електричном енергијом.

3. Архитектура и карактеристике WSN

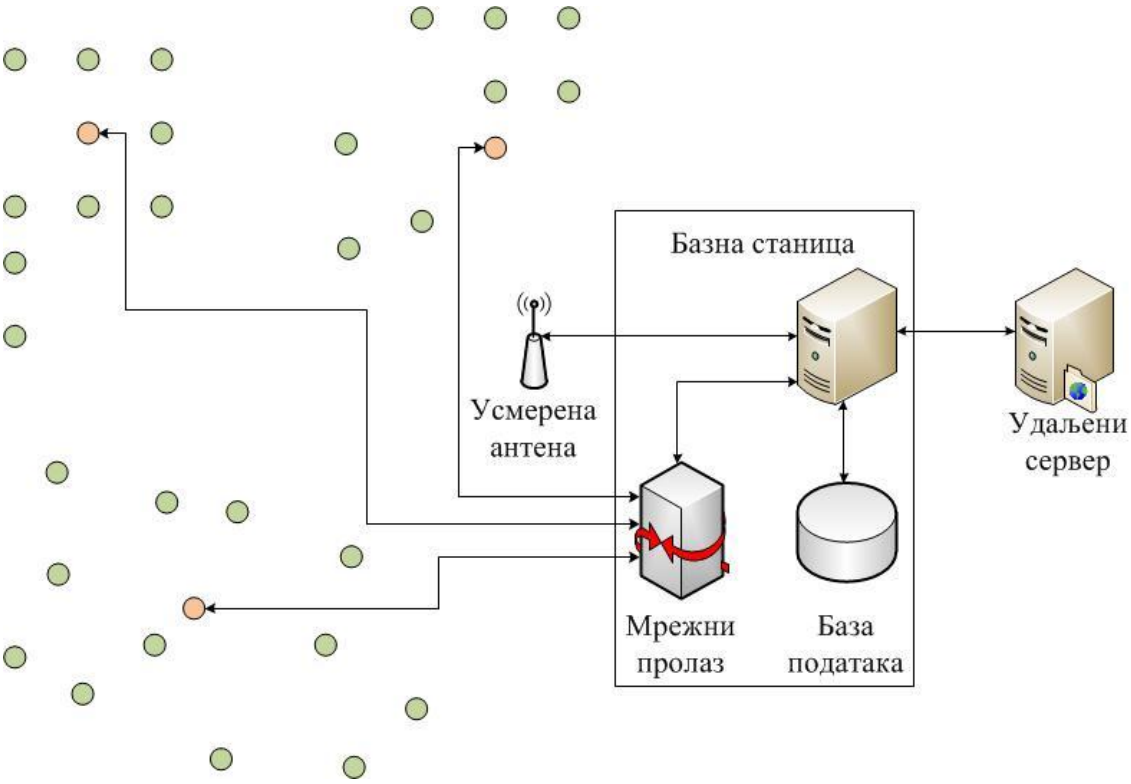
Развој бежичних комуникационих технологија је омогућио реализацију бежичних сензорских мрежа, WSN (енгл. Wireless Sensor Networks) употребом сензорских станица које карактерише мала потрошња електричне енергије и могућност комуникације ограниченог домета. Сензорске станице, или сензорски чворови, SN (енгл. Sensor Nodes) су релативно једноставан хардверски систем који чине сензорски подсистем са интегралним колима за прилагођавање сигнала и аналогно дигиталну конверзију, микропроцесор са интерним и/или екстерним меморијским модулима, комуникациони подсистем који омогућава да SN размењује податке са осталим чворовима и извор напајања. WSN су, услед релативно једноставне имплементације и релативно ниских трошкова, временом добијале на значају због бројних предности које пружају. Првенствено због могућности имплементације мреже на местима где то није могуће постићи жичаним инсталацијама, трошкови одржавања WSN су мањи у односу на трошкове обичних мрежа, флексибилност које пружају WSN је значајно већа када су у питању промене у конфигурацији мреже, док снага са којом раде SN-и је знатно мања од оног нивоа који може бити узрочник несрећа приликом њихове употребе у постројењима са експлозивним, или лако запаљивим материјама, такође ове мреже карактерише скалабилност високог нивоа. Са друге стране, постоје и недостаци који се у одређеној мери могу умањити, или предупредити. Отказ једног од чворова у WSN може узроковати отказ целокупног система, или једног његовог дела, што значајно усложњава проблематику комуникације када су у питању мреже које покривају велика подручја. Тржишне цене SN, иако релативно ниске, представљају значајан издатак када узмемо у обзир њихов животни век, док потрошња електричне енергије представља акутни проблем у свим мрежама оваквог типа. (Kong, et al., 2015)



Слика 1 Архитектура сензорског мрежног чвора

Сврха WSN је да се на одређеном простору распореде аутономни SN са циљем надзора физичких параметра окружења као што су температура, притисак, промене интензитета светлости, влажност, концентрација хемикалија и слично. Промене које региструју SN се преносе кроз мрежу ка сабирном месту, односно ка базној станици, BS (енгл. Base Stations) употребом одговарајућих комуникационих протокола. Обзиром на значајна хардверска ограничења по

питању радио примопредајника, пракса је да се комуникација у WSN подаци према BS преносе у више скокова (енгл. hops), односно не директно између SN и BS већ посредством чворова посредника који врше ретрансмисију. Чворови који, поред својих примарних улога, имају и улогу посредника често врше и фузију података у циљу додатног смањења броја порука које се преносе кроз мрежу у циљу оптималног ангажовања постојећих ресурса. Приликом реализације већих WSN пракса је да се мрежа подели у више група које чине SN међу којим се налази један главни чвор, CH (енгл. Cluster Head) који је задужен за ту групу. Поделом у мање групе се повећава се скалабилност мреже и њен животни век. Обзиром на ограничене хардверске ресурсе SN-а, поделом мреже је могуће организовати CH-е као чворове који располажу већим енергетским капацитетом и значајнијим хардверским потенцијалом тако да у њима може бити реализована агрегација података и извршавање криптографских функција. Уколико су сви мрежни уређаји једнаких карактеристика, они одређени од стране протокола могу преузети улогу CH-а чиме се омогућава бољу контролу саобраћаја и безбедности.



Слика 2 Архитектура бежичне сензорске мреже

WSN су претежно организоване тако да буду оријентисане ка подацима (енгл. data-centric), ретко као системи који су оријентисани ка адресама мрежних уређаја (енгл. address-centric). Оријентација ка подацима подразумева да се упити (енгл. queries) упућују чворовима, или мрежним регионима (енгл. cluster) у којима се реализује агрегација, а некада и анализа и обрада података. Након постављања упита ови мрежни чворови реагују и шаљу податке ка чворовима који су за то предодређени. Овако се у значајној мери редукују захтеви чиме се контролише ниво комуникације у мрежи и штеде њени ресурси, поред тога, сакупљање података на одређеним местима у мрежи повећава ниво тачности и умањује

редудантност података што утиче и на смањење потрошње електричне енергије и умањење кварова у чворовима. Обзиром да су SN делови мреже који се напајају електричном енергијом из сопствених извора који су ограничени, енергетска ефикасност оваквих чворова утиче на животни век WSN, или једног њеног дела. Протоколи за рутирање података и за економично ангажовање ресурса WSN су ти који одређују какав ће бити интензитет ангажовања мрежних чворова и у овом контексту WSN можемо окарактерисати као проактивне (енгл. Proactive Networks) где се SN периодично укључују, мере параметре окружења и предају податке од интереса, што је карактеристично за мреже у којима се толерише кашњење (енгл. Delay Tolerant Networks) и реактивне (енгл. Reactive Networks) где су SN непрестано будни и тренутно реагују на промене у окружењу, што је карактеристично за WSN које обрађују и шаљу податке у реалном времену (енгл. Real Time Networks). (Универзитет у Нишу, Електронски факултет, 2011)

WSN користе специфичне технике за пренос података између крајних тачака, предајника и пријемника. Подаци се кроз мреже простиру захваљујући простирању електромагнетних таласа са том разликом што се код жичаних мрежа подаци преносе кроз упредене каблове, коаксијалне каблове, оптичка влакна, док се код бежичних мрежа простирање електромагнетних таласа врши кроз ваздух, вакум, течности и чврсту материју. Преносни пут између две тачке се назива веза (енгл. link), а део везе који је намењен преносу називамо канал. Директна веза (енгл. direct link) подразумева пренос података између две крајње тачке без посредника у смислу других чворова уз употребу, или без употребе појачавача, или репетитора чија је основна улога да повећају снагу сигнала дуж преносног пута. Међутим, чешћи сценарио подразумева укључивање других чворова као посредника у комуникацији која се назива тачка-ка-тачки (енгл. point-to-point), или комуникацију у којој је медијум за пренос података дељив између више уређаја која се назива вишетачкаста (енгл. multipoint). Зависно од архитектуре WSN комуникација може бити симплекс (енгл. simplex), односно комуникација у којој се информације преносе само у једном смеру, полудуплекс (енгл. half-duplex) у којој се информације преносе у оба смера једним каналом, али наизменично и пун дуплекс (енгл. full-duplex) у којој је могуће истовремено преносити информације у оба смера засебним каналима.

WSN се најчешће реализују уз подршку алгоритама који обезбеђују динамичко креирање топологије мреже, односно самостално прилагођавање мреже (енгл. multihop) у зависности од постојања активних чворова креирањем једносмерних, односно двосмерних линкова. Пропусни опсег мрежних уређаја додатно се умањује у односу на номинални због постојања ефеката вишеструког приступа, слабљења сигнала, појаве шумова, или интерференције сигнала што је потребно узети у обзир приликом пројектовања WSN. Поред тога, WSN карактерише нижи ниво сигурности у односу на класичне жичане мреже што условљава потребу за пројектовањем мрежа са децентрализованом управљачком природом која омогућава реализацију додатне отпорности при појави појединачних отказа у односу на централизовани приступ. Стална промена стања мреже ствара потребу за алгоритмима који омогућавају чворовима да препознају прекид везе са чвором са којим су претходно били у вези и да пронађу алтернативни пут према одредишту због чега се користе алгоритми који омогућавају формирање више алтернативних путања до одредишног чвора (енгл. multipath) без понављања процеса њеног поновног откривања.

3.1 Комуникациони стандарди у WSN

WSN користе различите технологије бежичне комуникације у зависности од растојања између чворова и потребног протока: ZigBee, Wi-Fi, Bluetooth, WiMax и друге. (Dr. Shu Yinbiao, et al., 2016) Избор комуникационе технологије зависи од намене мреже а најчешће су заступљени стандарди које могу да подрже уређаји са малом потрошњом енергије, намењени раду на удаљености мањој од 50m и за мале протоке података, до 250Kb/s. Свим овим технологијама је заједничко да омогућавају умрежавање различитих уређаја од различитих произвођача, M2M, (енгл. Machine to Machine), као и технологију која се заснива на глобалној инфраструктури информатичког друштва која омогућава напредне услуге физичког и виртуелног умрежавања уређаја различитих намена направљених од стране различитих произвођача - IoT (енгл. Internet of Things). IoT је тековина савременог друштва и очекивана реакција произвођача на савремене тенденције, а ослања се на постојеће интероперабилне информационо комуникационе технологије. Комуникација између уређаја контролисаних од стране софтверског система може независно функционисати при чему је у могућности да се прилагођава условима окружења из ког преузима податке, анализира их и на основу резултата подешава параметре система. Најзахвалнији за то је Институт инжењера електротехнике и електронике (енгл. Institute of Electrical and Electronics Engineers) - IEEE који је развио неколико група стандарда у оквиру којих постоји већи број спецификација протокола који испуњавају битне критеријуме потребне за реализацију комуникације на којима се заснива комуникација у WSN.

Најзаступљенији комуникациони стандард за имплементацију WSN је IEEE 802.15.4. На основу овог стандарда је дефинисана спецификација за ZigBee протокол који се често среће код реализације WSN. Он омогућава реализацију WSN са уређајима мале потрошње за које је потребан мали пропусни опсег (енгл. bandwidth) и који могу да покрију релативно малу област. Битна карактеристика овог протокола је та што омогућава креирање мрежне топологије и путања у оквиру тог распореда само за конкретну прилику (енгл. ad-hoc network) што је са становишта WSN од пресудног значаја. За разлику од технологија као што су Wi-Fi, или Bluetooth, могућности ZigBee технологије су значајно скромније и омогућавају трансмисију на удаљености од 10m до максималних 100m у случају оптичке видљивости између уређаја, а у зависности од снаге примопредајника и утицаја окружења. Уређаји повезани на основу овог протокола стварају путање посредством других уређаја (енгл. mesh network) како би досегли оне удаљене уређаје. Номинални проток који подржавају ZigBee мреже је 250 Kb/s. ZigBee представља глобални стандард који је развијен првенствено за M2M мреже и поред штедљивости када су у питању ресурси WSN омогућава примену напредних криптографских алгоритама.(Милићевић, 2008)

Wi-Fi је технологија за комуникациону опрему која је се заснива на различитим верзијама IEEE 802.11 стандарда који омогућава комуникацију у фреквенцијском опсегу од 2,4GHz до 5GHz и уз теоријску брзину од 1Mb/s до 540Mb/. Прва верзија стандарда за Wi-Fi технологију, 802.11a, има теоријску брзину од 54Mb/s, али у пракси често износи 30Mb/s и представља скупљу опцију обзиром да комуникациони уређаји раде у фреквенцијском опсегу од 5GHz. Верзија 802.11б подразумева пренос података од 11Mb/s, што услед препрека и сметњи може бити

знатно мање, од 1Mb/s до 2Mb/s, али је најекономичнија опција за реализацију. 802.11g стандард је објединио претходна два, 802.11a и 802.11b и омогућава пренос података брзином од теоријских 54Mb/s при чему ради у фреквенцијском опсегу од 2,4GHz. Верзија 802.11n имплементира у себе претходне верзије и омогућава пренос података брзином од 54Mb/s до 600Mb/s при чему је могуће користити фреквенцијске опсеге од 2,4GHz, или 5GHz. Поред ових, постоје и други стандарди породице 802.11. Стандард IEEE 802.11 дефинише функционалности физичког слоја, а приступ мрежним уређајима се контролише уз помоћ механизама који омогућавају вишеструки приступ уз ослушкивање носилаца комуникације, CSMA (енгл. Carrier Sense Multiple Access), односно уз помоћ протокола који омогућава паралелно додељивање заједничких канала већем броју мрежних уређаја.

Када су у питању бежичне мреже, као у овом случају, овом механизму се додају механизми за избегавање колизија, CA (енгл. Collision Avoidance). CA механизам се обезбеђује уз помоћ дефиниција које омогућавају временски распоред приступа уређајима, DCF (енгл. Distributed Coordination Function). Иако је дизајниран за мреже којима управљају базне станице, DCF у оквиру IEEE 802.11 стандарда омогућава бежичним уређајима да приступе радио преносном путу без потребе за радио базном станицом. Већина уређаја намењених реализацији WSN подржава таласне форме за повезивање у складу са овим стандардом. WSN опрема може успоставити ad-hoc мрежу која се групише на малом простору, или може бити опслужена од стране hot-spot сервисног чвора који се налази у оквиру одређене области. Wi-Fi омогућава повезивање уређаја на удаљености до 45m у затвореном простору, или до 90m на отвореном. Уколико је потребно да се постигну веће брзине преноса и повезивање уређаја на већим удаљеностима, WSN се реализују тако што се у њихову инфраструктуру додају усмерене антене којима се минимизују последице преламања радио таласа и радио појачивачи, тако да омогући повезивање уређаја са оптичком видљивошћу до неколико километара.

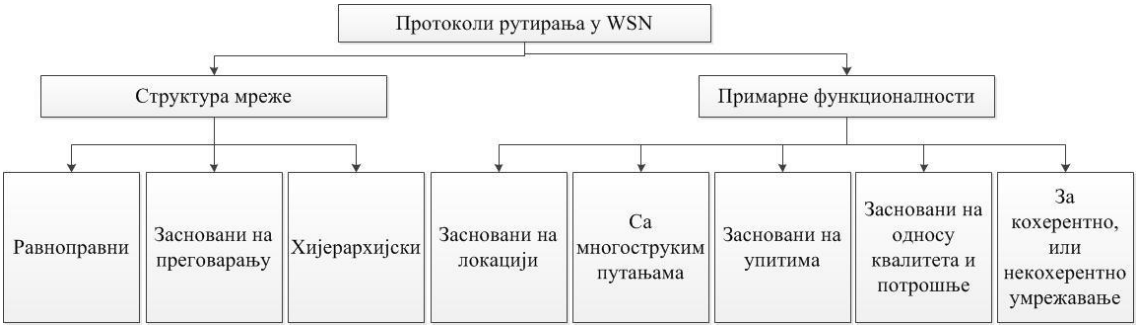
WiMAX (енгл. Worldwide Interoperability for Microwave Access) је бежична технологија која обезбеђује повезивање мрежних уређаја са великим пропусним опсегом и на великим растојањима. Овај стандард је дефинисан на основу IEEE 802.16 стандарда, а који је изведен из IEEE 802.11 Wi-Fi стандарда. За разлику од Wi-Fi технологија, WiMAX може да ради у вишим фреквенцијским опсезима и да обезбеди повезивање уређаја на удаљености до 50km уз постојање стационираних мрежних чворова са оптичком видљивошћу, или од 5km до 8km без директне оптичке видљивости, при чему је могуће остварити стабилну брзину преноса података до 50Mb/s. Ова технологија је нарочито погодна за WSN чија реализација подразумева управљање аудио, или видео надзором обзиром на могућности када је у питању проток и удаљеност. Посебна специфичност овог стандарда је у томе што се контрола приступа реализује тако што SN шаље захтев ка BS само једном, за прво пријављивање на мрежу, након чега му се додељује одређени временски период у ком ће се он обраћати тој базној станици. Тај временски период може да се мења, али остаје додељен конкретном SN, што онемогућава друге SN да се у том временском периоду обраћају BS. Системи који имају овакве алгоритме доделе, односно заказивања, су значајно стабилнији уколико у мрежама постоји велики број чворова, при чему BS контролишу квалитет и рационалну употребу мрежних ресурса. (Бојичић & Милосављевић, 2014)

Bluetooth технологија користи радио таласе високе фреквенције, UHF (енгл. Ultra High Frequency) у опсегу од 300MHz до 3GHz. Званично дефинисана стандардом IEEE 802.15, али се њеним даљим развојем и стандардизацијом баве различити произвођачи дигиталних технологија који се окупљају око заједничког имена Bluetooth SIG (енгл. Bluetooth Special Interest Group). Уз помоћ Bluetooth технологије могуће је повезати већи број мрежних чворова успостављањем point-to-point, или point-to-multipoint топологије у радијусу до 10m. Када се креира веза два, или више Bluetooth уређаја, креира се piconet. Сваки piconet може да садржи до 8 различитих уређаја, један master и седам slave уређаја, а више piconet-а може бити спојено у scatternet, највише 10, односно укупно 80 уређаја. Фреквенцијски опсег за Bluetooth се креће у границама од 2,4GHz до 2,48GHz. Теоријски, највећа могућа брзина преноса дефинисана овом спецификацијом износи 2,1Mb/s, док у пракси она износи 462Kb/s за двосмерну комуникацију, fullduplex. Асиметрична трансмисија омогућава брзину преноса од 721Kb/s у једном правцу и 56Kb/s у другом. Ова технологија је интересантна због поседовања независних система за избегавање интерференције са уређајима из ISM (енгл. Industrial, Scientific & Medical) опсега фреквенција и због поседовања независног система за уштеду енергије. Када је Bluetooth уређај у стању мировања он на сваких 1,28s ослушкује поруке других уређаја при чему се свако ослушкивање обавља на 32 различите фреквенције. (Веиновић & Јевремовић, 2008) Поред тога, Bluetooth технологија подразумева три безбедносна режима:

- Non-Secure - без процедура за сигурну трансмисију,
- Service-Level Enforced Security - са безбедносним процедурама након успостављања везе и
- Link-Level Enforced Security - са употребом процедура за сигурну трансмисију пре успостављања везе.

4. Протоколи рутирања у WSN

Рутирање у WSN може бити класификовано у зависности од структуре мреже на: равноправно (енгл. flat-based), хијерархијско (енгл. hierarchical-based) и рутирање засновано на локацији чворова (енгл. location-based). Код равноправног рутирања сви чворови имају једнаке улоге, или функционалности, у хијерархијском различите групе чворова имају различите улоге и различит значај у мрежи, док код рутирања заснованог на локацији, тачно одређени чворови имају улогу посредника у процесу. Протоколи могу да се класификују и у зависности од својих примарних функционалности на: оне који се заснивају на преговарању (енгл. negotiation-based), протоколе са многоструким путањама (енгл. multipath-based), оне који се заснивају на упитима (енгл. query-based), оне који балансирају између квалитета информација и потрошње електричне енергије (енгл. QoS-based) и протоколи за кохерентно (енгл. coherent-based), односно некохерентно умрежавање, зависно од тога да ли чворови независно обрађују податке пре њиховог слања, или се обрада врши само у одређеним чворовима. Највећи број WSN се заснива на протоколима који се могу окарактерисати као кооперативни што у основи подразумева да сви SN усмеравају податке ка централиним чворовима где се врши њихова агрегација и обрада. (Al-Karaki & Kamal, n.d.)



Слика 3 Протоколи рутирања у WSN

4.1 Софтверска архитектура WSN - OSI и TCP/IP

OSI модел (енгл. Open Systems Interconnection model) је најзаступљенији апстрактни модел мрежне архитектуре који омогућава да се опише интеракција између хардвера и софтвера, као да се на основу њега пројектују и проучавају мреже. Овај модел дели архитектуру мреже у седам слојева, али за потребе анализе WSN – а се обично користи систем од пет нивоа који у апликациони слој интегрише слој презентације (енгл. presentation layer) и сесије (енгл. session layer). Разлог за то је одсуство компоненти које су директно задужене за међу-системску комуникацију и чињеница да су функционалности ова три слоја у вези са корисничким процесима. Зависно од тога која технологија се користи за комуникацију у WSN, као референтни модел можемо посматрати и TCP/IP (енгл. Transmission Control Protocol / Internet Protocol). (N.Reka & M.Phil, 2015) У основи у WSN издвајамо пет слојева: слој апликације (енгл. Application layer), транспортни слој (енгл. Transport layer), мрежни слој (енгл. Network layer), слој везе (енгл. Data link layer) и физички слој (енгл. Physical layer).

Реализација WSN-а може да се посматра кроз три примарне функције које прожимају нивое дефинисане OSI референтним моделом: управљање енергијом (енгл. Power management), управљање повезивањем (енгл. Connection management) и управљање задацима (енгл. Task management).

4.1.1 Физички слој

Физички слој је задужен за пренос битова путем комуникационог канала. Овај слој дефинише правила по којима се битови преносе, који електрични напон је потребан, колико битова се шаље у секунди и какав физички облик каблова и конектора треба да буде. Овај слој је простор за реализацију енергетски ефикасних SN због чега има велики значај обзиром да од њега зависи животни век мреже. Комуникација у оквиру WSN - а се одвија на малим растојањима обзиром да повећавање домета чворова значајно повећава потрошњу електричне енергије када је у питању емисија радио таласа. Поред наведеног, физички слој је задужен за избор фреквенција, детекцију сигнала, шифровање података и модулацију сигнала: амплитудну (AM), фреквенцијску (FM) и фазну (PM).

Табела 1 Карактеристике модема заснованих на AM, FM и PM техникама

Тип модулације	Битска брзина преноса [bps]	Параметар који се мења	Параметар који остаје непроменљив	Додатне карактеристике
AM	5 Ширина канала једнака је битској брзини преноса	Амплитуда	Фаза и фреквенција	Обично се преносе два нивоа.
				Систем је веома осетљив на сметње.
				Структура модема није сувише комплексна.
FM	1200 Пропусност канала је два пута већа од биткске брзине	Фреквенција	Амплитуда	Пренос се заснива на промени фреквенције, обично логичкој нули одговара f1=1200Hz, а логичкој јединици f2=2400Hz, DTMF (енгл. Dual tone multifrequency).
				FM техника преноса је позната као FSK (енгл. frequency shift key) при чему разликујемо некохерентну (FSK-NC) која не обезбеђује континуитет фазне промене и кохерентну (FSK-C) која обезбеђује континуитет фазне промене.
				FSK је мање осетљива на сметње у односу на AM.
				FSK-C у поређењу са FSK-NC има боље карактеристике јер ефикасније користи пропусни опсег и може да оствари већу брзину преноса.
				Структура модема је сложенија.
PM	9600 Битска брзина може бити једнака фреквенцији носиоца	Фаза	Амплитуда и фреквенција	Ова техника је позната као PSK (енгл. phase shift key).
				Фазне промене између две вредности су функција вредности података на улазу при чему логичкој нули одговара фаза од 0º, а логичкој јединици фаза од 180º.
				PSK је мање осетљива на сметње.
				Структура модема је најсложенија.

4.1.2 Слој везе

Слој везе управља преносом путем физичког слоја и омогућава пренос ослобођен грешака на овом и физичком слоју. Задатак слоја везе јесте да заштити слојеве вишег нивоа од грешака насталих при преносу података. Слој везе управља форматом порука, односно дефинише почетак и крај поруке тако што формира и препознаје оквире (енгл. frame). Овај слој је задужен за мултиплексирање сигнала: фреквенцијско (истовремено одашиљање сигнала на различитим фреквенцијама), временско (наизменично слање више различитих сигнала у јединици времена), кодовано (емисија шифрованих сигнала) и просторно мултиплексирање (истовремено одашиљање на са више канала зависно од броја удружених антена које чине једну мултиплесирајућу антену). Обзиром на својства овог слоја у оквиру њега се реализују протоколи којима може да се уреди контрола приступа. Посебно значајна питање приликом реализације WSN-а је контрола будног стања чвора, односно стања у ком он троше електричну енергију. Протоколима за контролу приступа, односно MAC (енгл. Medium Access Control) протоколима је могуће контролисати пропусну моћ медија, његову поузданост, правичност (енгл. fairness), време које протекне од момента када је пакет спреман за слање до његовог слања (енгл. access delay), време које протекне од почетка емитовања преноса до успешног завршетка (енгл. transmission delay) и вишак саобраћаја који настаје услед губитка пакета и слања контролних пакета. (Универзитет у Нишу, 2011) (Rovčanin, 2008)

Како би се продужио животни век мреже осмишљено је више верзија MAC протокола који су намењени искључиво WSN и искључиво за комуникацију која се заснива на емисији електромагнетних таласа. Њихов задатак је контрола радио примопредајника који је највећи потрошач електричне енергије у систему. Циљ је да чвор буде укључен једино када прима, или шаље податке, односно да стање ослушкивања (енгл. idle listening) буде најкраће могуће. Чињеница је да ово није једини узрок расипања енергије него и колизија пакета, формирање додатног заглавља (енгл. protocol overhead), пријем и одбацивање пакета који су стигли на погрешно одредиште представљају додатне узроке трошења енергије.

Колизија пакета настаје када чвор покушава да пошаље поруку преко медијума који је већ заузет. Већина једноканалних радио примопредајника нема способност да прима и шаље пакете истовремено, тако да је једини начин да предајна страна буде информисана о успешном слању да добије потврду о пријему. Пропагацијско кашњење између удаљених чворова је време које је потребно примопредајнику да почне са емитовањем када је информисан о томе да је медијум слободан и обично износи од 250μs до 500μs, што је још један од узрока колизије. Ситуација у којој се приступ удаљеном чвору реализује посредством других чворова који се понашају као релеји (енгл. multi-hop routing) такође може узроковати колизију пакета. Нежељени ефекти колизије пакета се могу избећи употребом различитих механизама контроле као што су backoff алгоритам (IEEE 802.11), Multiple Access with Collision Avoidance for Wireless (MACAW), RTS/CTS (Request to Send / Clear to Send) механизмом, Time-division multiple access (TDMA) методом. RTS и CTS поруке у себи садрже поља у којима су уписана и време трајања размене тако да чворови који не учествују у комуникацији могу да подесе сопствене NAV (енгл. Network Allocation Vector) тајмере, што гарантује да чворови неће почети са слањем поруке све док се текућа трансмисија не заврши.

Креирање заглавља протокола додатно утиче на потрошњу енергије, као и на пропусни опсег. Наравно, MAC протоколи подразумевају имплементацију механизама који омогућавају реализацију поузданог система за пренос тако да је неопходно да пакети садрже поља која омогућавају уочавање грешака, идентификације примаоца и пошиљаоца као и податке на основу којих се чворови информишу о распореду свог рада. Стандардни подаци за уочавање и корекцију грешака удвостручују количину саобраћаја јер додају редундантне информације. Додавањем FCS (енгл. Frame Check Sequence) поља се умањује број порука које апликација може да пошаље у јединици времена, али се и знатно умањује вероватноћа за потребом поновног слања поруке услед грешке при преносу што је оптимална опција и ако се узме у обзир да заглавља MAC протокола има дужину често већу од дужине поруке која се преноси.

Још један узрок потрошње електричне енергије јесте обрада порука које су намењене другим чворовима (енгл. message overhearing). Уколико су у питању мреже у којима не постоји потреба за рационалном употребом електричне енергије пракса је да се не врши додатна контрола и спречавање обраде јер се тако повећава пропусна моћ мреже и смањује кашњење испоруке (енгл. latency). Обзиром да то није случај када су у питању WSN, нежељене последице услед погрешног усмеравања поруке, независно од тога да ли је у питању unicast, или broadcast слање, је могуће спречити раним одбацивањем пакета (енгл. early rejection), односно искључивањем примопредајника оних чворова којима порука није намењена. Пропуштање порука (енгл. message passing) је техника која је имплементирана у S-MAC (енгл. Sensor MAC) и T-MAC (енгл. Timeout MAC) протоколе која омогућава чворовима да подесе своје периоде мировања и да подесе NAV тајмере на основу података о дужини трајања трансмисије на основу размене RTS и CTS порука. Поред поменутих, међу често заступљеним протоколима за контролу приступа се налазе: B-MAC (енгл. Berkeley MAC) и G-MAC (енгл. Gateway MAC).

4.1.3 Мрежни слој

Задатак мрежног слоја јесте одређивање једне, или више путања којима ће порука бити прослеђена од изворишта до одредишта (енгл. routing). Мрежни слој је задужен да у сваком чвору мреже, између изворишта и одредишта, одреди који је следећи чвор коме ће порука бити прослеђена. Овај слој треба да обезбеди систем идентификовања чланова мреже и правила чијим ће поштовањем бити могућа испорука података на жељено одредиште. Примарни задаци овог слоја, када су у питању WSN, су у вези са оптималном употребом електричне енергије и ограничењима по питању количине података који служе за одређивање путања којима се повезују жељени чворови. Основна идеја је у дефинисању протокола за одређивање путања (енгл. routing protocol) који обезбеђује поуздане путање и оптималан број редундантних путања у зависности од метричких принципима који су одређени протоколом.

Поред поменутог, WSN треба да буду имплементиране тако да SN пошаљу податке убрзо након догађаја који прате, тако да модели који су уобичајени на компјутерске мреже, (енгл. sender/receiver model), нису адекватни за овакве мреже. Пријемна страна у WSN не мора увек да тражи информације од одређеног чворног места, већ чешће од чвора који се налази у близини а располаже жељеним

информацијама. Предајна страна не мора да располаже конкретним подацима о пријемној страни већ да понуди податке које ће пријемна страна преузети, или ће до њих доћи посредством мрежних чворова који су одређени протоколом. (Rollins, 2008)

4.1.4 Транспортни слој

Задатак транспортног слоја јесте обрада порука на крајњим тачкама, изворишту и одредишту. Овај слој успоставља, одржава и прекида виртуелне везе за пренос података између крајњих тачака, поред тога, задужен је за набавку идентификационе ознаке одредишта, превођење података у формат погодан за транспорт, поделу података у сегменте погодне за слање, прилагођавање брзине преноса могућностима стране са слабијим перформансама, осигуравање преноса свих сегмената, елиминисање дуплих сегмента и слично. Такође, овај слој може вршити додатну контролу грешака при преносу, додатну у смислу да је она већ извршена у оквиру слоја везе. Због његових функционалности, овај слој је погодан за обезбеђивање оптималне енергетске ефикасности и за одређивање квалитативних параметара у вези са вероватноћом губитака пакета и кашњења са краја на крај. Пракса је да се на овом слоју управља саобраћајем на основу, TCP-а (енгл. Transmission Control Protocol) који је развијен за уобичајене мреже, међутим тај протокол није погодан за WSN. WSN карактерише постојање релативно великог броја SN са предајницима и једног, њима надређеног одредишта (енгл. sink) које иницира пренос података: уникаст (енгл. unicast), бродкаст (енгл. broadcast), а најчешће мултикаст (енгл. multicast). Поред тога, WSN карактерише висок ниво редундантности, или корелације прикупљених података тако да не постоји потреба за поузданим преносом са краја на крај, односно између индивидуалних SN и BS-а, него само између тренутно активног SN и BS-а.

4.1.5 Слој апликације

Слој апликације представља највиши слој OSI и TCP/IP референтних модела и као такав се налази најближе кориснику. Елементе на овом слоју чине корисничке апликације којима се користе мрежни ресурси и управља комуникацијом. Зависно од начина реализације корисничких апликација, његови елементи се могу обраћати слоју сесије и слоју презентације, а постоје ситуације у којима се апликације директно обраћају нижим слојевима. Уколико постоји потреба за сесијама, апликације могу успостављати, одржавати прекидати логичке сесије између крајњих чворова. Сврха сесија јесте дефинисање стања, или фаза, сваког дијалога ради дефинисања валидних акција у сваком од њих. На основу тога је могуће реализовати управљање транспортним слојем и проверу података добијених од њега. Уколико је потребно додатно обрађивање података за презентовање кориснику, то је могуће реализовати у оквиру слоја презентације. Усклађени формат података се предаје апликативном слоју, а путем њега крајњем кориснику. Слој презентације може оригиналне податке компресовати ради ефикаснијег преноса, или их може трансформисати у облик погодан за презентовање крајњем кориснику.

4.2 Протоколи у MANET

Највећи број WSN је реализован као мобилна ad hoc мрежа, MANET-а (енгл. Mobile Ad Hoc Network). MANET мреже карактерише то што се сваки чвор, без обзира на његову намену, може појавити у улози транзитног чвора приликом успостављања комуникационог линка између крајњих тачака. Чворови се понашају као рутери што омогућава аутоматско конфигурисање мреже без централизованог управљања. Топологија мреже је динамичка а зависи од алгоритма по ком чворови објављују своје присуство након чега прате реакције суседних чворова и у складу са улогом и наменом, реагују. Алгоритми рутирања су задужени за проналажење рута, за пакетски пренос података од изворишног до одредишног чвора, затим за идентификацију и размену табела рутирања, откривање прекида у рутама, њихово поновно успостављање, или проналажење алтернативних рута, као и за њихову оптимизацију. Зависно од динамике одређивања путања протоколи могу да се окарактеришу као проактивни код којих су све путање одређене унапред, реактивни код којих се путање креирају на захтев и хибридни који представљају комбинацију претходна два. (Tepšić & Veinović, 2015)

4.2.1 Проактивни протоколи рутирања

Функционалност проактивних протокола рутирања се заснива на табелама у којима се чувају подаци на основу којих се успоставља линк између крајњих тачака. Сваки чвор у мрежи је задужен да својим суседима прослеђује податке о променама у вези са топологијом мреже. Такође, сваки чвор је задужен да ажурира табелу у складу са променама које настану у мрежи, а односе се на конкретан линк. Ово омогућава да табеле увек буду актуелне што обезбеђује оптималну функционалност мреже. Међусобне разлике између проактивних протокола рутирања се односе на начине на које откривају нове руте, начину ажурирања табела и скуповима података који се чувају у табелама. Заједничко за све проактивне протоколе је периодично генерисање и слање контролних порука на основу којих се комплетирају табеле у чворовима који нису били упознати са новонасталим изменама. Зависно од мреже, чворови могу одржавати једну, или више табела, а свака промена у топологији повлачи слање података ради корекције рута што одржава конзистентност мреже. Недостатак ових протокола се огледа у великом броју активних рута што увећава количину саобраћаја и успорава рад мреже, као и спора реакција услед поновног успостављања рута, или отказа. (Maheshbhai & Wandra, 2014)

Проактивни протоколи рутирања:

- DSDV (Destination Sequenced Distance Vector Routing)
- WRP (Wireless Routing Protocol)
- CGSR (Claster head Gateway Switch Routing)
- B.A.T.M.A.N (Better Approach To Mobile Ad hoc Networking)
- HSR (Hierarchical State Routing)
- OLSR (Optimized Link State Routing)

4.2.2 Реактивни протоколи рутирања

Карактеристично за реактивне протоколе рутирања је да они креирају руте на основу повремених захтева за ажурирање података у табелама за рутирање и то када један од чворова намерава да проследи податке ка одредишном чвору. Након захтева за слање података, чвор креира руту на основу алгоритма за њено откривање након чега је одржава све док је она потребна, односно све док је одредиште доступно. Ови протоколи се брзо прилагођавају променама у топологији мреже, не захтевају додатно ангажовање ресурса слањем контролних порука, као што се случај код проактивних протокола, међутим откривање нових рута на захтев ствара додатни саобраћај у виду поздравних порука, што може довести до загушења мреже, а често се догађа и да буду откривене лоше руте што има за последицу губљење пакета и додатно кашњење приликом успостављања нових рута. (Maheshbhai & Wandra, 2014)

Реактивни протоколи рутирања:

- AODV (Ad hoc On demand Distance Vector)
- HARP (Heading direction Angle Routing Protocol)
- DSR (Dinamic Source Routing)
- DSRFLOW (Flow State in the Dinamic Source Routing)
- ABR (Associatively Based Routing Protocol)
- SSA (Signal Stability Based Adaptive Routing Protocol)
- DYMO (Dynamic Manet On demand Routing)
- TORA (Temporally Ordered Routing Algorithm)

4.2.3 Хибридни протоколи рутирања

Ови протоколи комбинују предности проактивних и реактивних протокола и обично се имплементирају у апликације за WSN специфичних намена. Пракса да хибридни протоколи деле мрежу на регионе које се могу преклапати, или не. Са становишта чворова, региони су одређене њиховом удаљеношћу од суседних чворова, или су одређене географским подручјем на ком су чворови распрострањени. Најчешћи сценарио подразумева успостављање рута тако што се на основу проактивног протокола успоставља комуникација унутар региона, док региони међусобно комуницирају на основу рута које су одређене неким од реактивних протокола. (Maheshbhai & Wandra, 2014)

Хибридни протоколи рутирања:

- ZRP (Zone Routing Protocol)
- HSLS (Hazy Sighted Link State)
- HWMP (Hybrid Wireless Mesh Protocol)
- OORP (Orderoue Routing Protocol)

5. Анализа безбедносних захтева у WSN

Апликације за управљање WSN, у највећем броју случајева, подразумевају дизајн који укључује безбедносне протоколе и заштиту мреже од неауторизованог приступа. Компромитовање било које од значајних компоненти WSN, или њихових операција може утицати на целу мрежу и обесмислити њену сврху. Због тога се подразумева да развој апликација има интегрисане модуле који омогућавају достизање безбедносних циљева: тајност комуникације, интегритет података, расположивост система, аутентичност изворишта и одредишта, односно исправно функционисање WSN. Обзиром да су SN, у технолошком смислу, једноставни и релативно јефтини, ови чворови се не сматрају нарочито осетљивим у безбедносном смислу, чак и у случајевима када потенцијални нападач може да им приступи физички. Најгори сценарио у ком нападач приступи SN и, на основу тога, извуче осетљиве податке као што су кључеви, или да у SN имплементира неку малициозну апликацију, неће значајно угрозити функционалност WSN због постојања безбедносних модула у остатку система. Са друге стране, BS представља место које мора бити отпорно на нападе и поуздано у нормалном функционисању система. Претежно се BS имплементира у систем као чвор који има значајно боље хардверске и софтверске перформансе, а уз то и стабилан извор напајања електричном енергијом, његова улога у смислу безбедности система мора да буде доминантна.

Безбедносни циљеви у WSN се могу остварити кроз безбедносне протоколе рутирања, међутим протоколи се разликују зависно од врсте мрежа и апликација које контролишу рад WSN, тако да не постоји универзални алгоритам који омогућава остваривање свих циљева. Зависно од намене и величине мреже, безбедносни циљеви имају различите приоритете у складу са чим се имплементирају у хардвер и софтвер WSN-а.

Безбедносни циљеви:

- Поверљивост комуникације подразумева да само предајна и пријемна страна разумеју садржај поруке, док је неауторизованој страни то онемогућено што у основи подразумева употребу неког облика шифровања, а да би то било могуће и једна и друга страна морају располагати кључевима за шифровање, односно дешифровање. Неауторизовани учесници у комуникацији, обзиром да не поседују адекватне кључеве, нису у могућности да трансформишу шифрат у отворени текст. Кључни проблем у остварењу овог циља је дистрибуција криптографских кључева због чега је неопходно изградити безбедне канале којим се они могу дистрибуирати. Након шифровања података, они се могу кретати између чворова без бојазни да ће постати доступни злонамерним корисницима.
- Интегритет поруке подразумева да она на свом путу од пошиљаоца до примаоца није измењена, односно преправљана. Обзиром да потенцијални нападачи могу, релативно једноставно, пресрести поруку, изменити њен садржај и вратити је на њену путању ка пријемној страни, потребно је да постоји безбедносни механизам који ће омогућити проверу аутентичности порука. Захтеви у вези са

интегритетом порука се могу реализовати употребом једносмерних криптографских функција које на основу порука праве њихове отиске, или контролне суме.

- Аутентификација ентитета подразумева процес у оквиру ког ентитети који учествују у комуникацији, предајна, или и предајна и пријемна страна, потврђују своју аутентичност. Обзиром да се WSN највећим делом реализују путем бежичне комуникације, веома је значајно да у систему постоји модул за међусобну проверу аутентичности чворова. Постојање оваквог криптографског механизма онемогућава злонамерне кориснике да приступе неком од чворова и да реализују своје намере, јер аутентични чворови могу да провере изворе оригиналних пакета, да потврде идентитет пошиљаоца, и верификују учеснике у мрежној комуникацији.
- Доступност система, или операциона безбедност подразумева постојање модула који омогућавају нормално функционисање мреже и у случајевима када злонамерни корисници покушају да ометају њен рад. Губитак функционалности неког од чворова може узроковати необично понашање WSN, успорен рад мреже, појаву безбедносних шупљина, или отказивање целокупног система.

5.1 Напади на протоколе рутирања у WSN

Већина WSN се реализује без имплементације безбедносних механизама, међутим када су у питању мреже код којих постоји потреба за одређеним нивоом безбедности, протоколи рутирања и функционалности мрежног слоја представљају област у којој је могуће реализовати такве механизме. Највећи проценат WSN се имплементира као WANET (енгл. Wireless Ad Hoc Network), обзиром да ове мреже немају предефинисану структуру већ сваки чвор може да партиципира у процесу рутирања преносећи податке од једног чвора ка другом, што ствара потребу да се подаци шаљу путањама које се динамички креирају у зависности од протокола. Уколико узмемо у обзир да у неким WSN чворови нису статични, потребно је да њихово интегрисање у систем буде реализовано протоколима који омогућавају да самостално креирају руте и ако мењају свој положај, односно MANET. Овакве карактеристике WSN стварају специфична ограничења. Поред проблема снабдевања електричном енергијом, значајан ограничавајући фактор је простор за складиштење података, релативно мала процесорска снага и непоуздани комуникациони канал између чворова. Управо због тога, уобичајена мета напада су комуникациони канали, а обзиром на хардверска ограничења често је немогуће имплементирати уобичајене криптографске технике како би се заштитила функционалност WSN-а.

Нападе у WSN можемо поделити по више различитих основа. Прва подела је на пасивне и активне. Пасивни напади се односе на пресретање комуникације, њено праћење и прислушкивање, али без модификовања порука, док активни напади подразумевају манипулацију порукама, њихову измену и брисање. Друга подела категорише нападе као: нападе на податке током њиховог транспорта, нападе на одређени чвор, или чворове њиховим опонашањем, напади непотребним оптерећивањем мреже, DDoS (енгл. Distributed Denial of Service) напад и нападима на протоколе за рутирање. Да би протокол задржао своје

карактеристике и у условима напада мора имати могућност да пронађе исправне путање за усмеравање пакета и да открије неправилности у њима, односно мора осигурати откривање путања и успешно реализовати прослеђивање података. Највећи број напада на протоколе рутирања се може сврстати у једну од следећих категорија: лажне, поновљене, или промењене информације рутирања (енгл. Spoofing, altering, and replaying routing information), селективно прослеђивање пакета (енгл. Selective forwarding attack), напад типа Црна рупа (енгл. Sinkhole attack), Сибил напад (енгл. Sybil attack), Црвоточина напад (енгл Wormhole attack), напад преплављивањем (енгл. HELLO flood attack), лажне потврде, лишавање сна (енгл. Denial of sleep attack), откривање локације (енгл. Position estimation) и слично. Основна разлика између свих врста напада је у томе што једни манипулишу подацима, док други утичу на топологију мреже. (Zin, et al., 2015)

5.1.1 Лажне, промењене, или поновљене информације рутирања

Овај напад је усмерен на протокол рутирања у циљу да се информације које чворовима омогућавају да формирају руте лажирају, измене, или непотребно поново пошаљу. Овим врстама напада потенцијални нападачи могу да креирају руте по сопственој жељи, да утичу на количину саобраћаја, да изврше поделу мреже, да генеришу лажне поруке о грешци, да увећају кашњење са краја на крај и слично.

5.1.2 Селективно прослеђивање пакета

Multihop мреже у обично имплементиране на идеалном сценарију у ком чворови доследно прослеђују примљене поруке. Селективно прослеђивање пакета подразумева сценарио у ком малициозни чворови одбијају да проследе поруке при чему их одбацују у складу са уобичајеним понашањем дефинисаним протоколом. Овакав напад се реализује тако што се преузме контрола над једним од чворова након чега се он понаша као Црна рупа, односно да у њему нестају сви пакети које добије. Обичан сценарио у оваквој ситуацији је да суседни чворови препознају то понашање као неисправно и да потраже друге путање, међутим могуће је овакве нападе реализовати тако да се пакети селективно прослеђују само до неких од чворова чиме се умањује пропусна моћ мреже и непотребно троше ресурси.

5.1.3 Црна рупа (енгл. Sinkhole)

Код оваквих напада, нападач настоји да већину пакета, или комплетан саобраћај преусмери кроз компромитовани чвор и тиме креира област са малициозним чвором у средини. Ова врста напада се често користи да би се омогућили други напади. Уобичајен сценарио креирања Црне рупе настаје када нападач лажира приоритете рута у складу са протоколом, на пример може пошаље поруку са потврдама о поузданости руте са краја на крај уз додатне информације о поузданости, или толерантном кашњењу након чега се саобраћај усмерава жељеном путањом. Нападач са квалитетним хардвером и довољно јаким радио предајником може да симулира једну овакву путању трансмисијом са довољно снаге и да достигне BS у једном скоку, или да овај напад комбинује са нападом

Црвоточине. Мрежа ће се и у овом случају понашати у складу са протоколом и почеће да пропагира нову руту која ће водити кроз компромитовани чвор обзиром да су други чворови удаљени неколико скокова од BS, а обзиром на његове карактеристике, он ће наставити да привлачи сав саобраћај намењен BS. Обзиром да комплетан саобраћај иде кроз компромитовани чвор, нападач је у могућности да селективно одбацује пакете, да их модификује, или да криптоанализом дође до осетљивих података. WSN које располажу само једном BS су нарочито осетљиве на ову врсту напада јер сви пакети у мрежи су усмерени на једну крајњу адресу што ствара могућност за преузимање читаве мреже.

5.1.4 Сибил напад (енгл. Sybil)

Овај напад се реализује тако што један се малициозни чвор лажно представља другим чворовима у мрежи при чему мења идентитете што доводи до редундантности података у саобраћају. Овом врстом напада је могуће напасти алгоритме рутирања, могуће је ометати агрегацију података, гласање (сабирање различитих вредности ознака са различитих чворова, или сабирање успешно послатих пакета), коректну расподелу ресурса, или одржавање пожељне топологије мреже. Без обзира на врсту напада, све технике подразумевају вишеструке идентитете, тако да у случају гласања у WSN нападач користи вишеструке идентитете да би генерисао додатне гласове и преусмерио саобраћај, или у случају напада на протокол рутирања, малициозни чвор преузима идентитете чворова и усмерава саобраћај преко себе.

5.1.5 Црвоточина (енгл. Wormhole)

Креирање црвоточине је напад који подразумева креирање приватног тунела са ниском стопом кашњења који због добрих карактеристика почиње да преузима на себе део саобраћаја, или целокупан саобраћај. Најједноставнији сценарио је када малициозни чвор који се налази између два чвора прослеђује поруке уз мање кашњење, међутим ови напади најчешће функционишу тако што укључују два, или више малициозних чворова који креирају један, или више тунела који због смањивања удаљености између чворова, обзиром да се саобраћај одвија посредством спољашњег канала доступног само нападачу, постају приоритетни у процесу рутирања пакета. Овакав напад утиче на чворове који су неколико скокова удаљени од BS тако да усмере свој саобраћај кроз тунел који удаљеност између крајњих тачака чини мањом. WSN су осетљиве када се напади овог типа комбинују са селективним прослеђивањем, или прислушкивањем јер пружају могућност контроле и откривања осетљивих података чиме може бити компромитована читава WSN.

5.1.6 Преплављење

Овај напад се реализује захваљујући функционалности већег броја протокола која подразумева да сви чворови у мрежи изврше емисију „HELLO“ пакета како би се представили својим суседима, након чега чворови који приме такве пакете могу да меморишу податке о конкретним чворовима и да креирају потенцијалне руте. Уколико нападач са адекватном опремом и адекватном трансмисијом убеди

чворове да им је сусед, они ће покушати да податке усмере преко тог чвора. Уколико вештачки пропагира руту преко тог чвора сви чворови који су добили сигнал од њега ће започети слање пакета, а обзиром да не поседују радио предајнике адекватне снаге, ови чворови ће слати пакете у празно. На овај начин је могуће узроковати отказивање система, или његовог дела јер и ако неки од чворова установи да је одредиште сувише удаљено, преостали део чворова ће и даље слати пакете ка нападачу.

5.1.7 Лажне потврде

Неки од WSN алгоритама за рутирање се заснивају на имплицитним, или експлицитним потврдама на слоју везе о квалитету путања што омогућава потенцијалном нападачу да прислушкује и да лажира потврде за пакете адресиране суседним чворовима. На овај начин може да утиче да чворне тачке усмере своје пакете преко чворова који не представљају оптималну тачку у путањи, или који су онеспособљени услед квара, или услед недостатка напајања. Протоколи бирају чвор за наредни скок на основу поузданости путање, али вештачко одржавање лоших, или непостојећих чворова омогућава да се манипулише топологијом мреже и да се изврши напад селективним прослеђивањем и навођењем циљаних чворова да шаљу пакете кроз непостојеће путање. (Milovanović, et al., 2014)

5.1.8 Лишавање сна

Уобичајено је да се SN снабдевају електричном енергијом из батерија, а обзиром на карактеристике WSN, пуњење батерија, или није предвиђено, или је сведено на најмању могућу меру. Због овога је потребно обезбедити оптимално располагање енергијом и њеном уштедом што се постиже стављањем радио примопредајника SN у режим сна. Овај напад се реализује посредством малициозних чворова који манипулишу временом предвиђеним за различите активности SN, односно тако што онемогућава синхронизацију чворова у мрежи. (Naika & Shekokarb, 2015)

5.1.9 Откривање локације

Откривање локације мрежних чворова може угрозити безбедност мреже уколико потенцијални нападач жели да физички приступи неком од чворова, или уколико за остваривање својих намера треба да сагледа топологију мреже. Зависно од врсте WSN, чворна места могу да имају фиксне позиције, или могу да мењају свој положај. Неке мреже претпостављају да чворови имају своје уређаје за лоцирање, док неке друге реализују своју функцију уколико су чворови у домету чворова који су у њиховој близини. Уколико мреже имају SN који су мобилни, потребан је алгоритам за лоцирање како би се одредила удаљеност чвора од осталих релевантних чворова и да би се реализовало усмеравање пакета. Уколико су SN статични, није потребна имплементација таквог алгоритма, али то умањује безбедност уколико њихова локација буде откривена. У оба случаја је могуће одредити локацију чворова што отвара могућност напада и намеће потребу за имплементацијом превентивних безбедностних решења.

5.2 Одбрана од напада на протоколе рутирања

Већину спољашњих напада на протоколе рутирања је могуће предупредити шифровањем и аутентификацијом на нивоу слоја везе. Једноставни криптографски алгоритми могу спречити потенцијалне нападаче да реализују Сибил напад јер чворови неће реаговати уколико им се обраћа неаутентификовани мрежни уређај. Такође селективно прослеђивање и напад креирањем Црне рупе није могуће реализовати без одговарајуће акредитације мрежних уређаја, тако да потенцијални нападач неће бити у могућности да их дода у топологију мреже. Напади које није могуће спречити шифровањем података, или аутентификацијом мрежних уређаја на нивоу слоја везе су креирање Црвоточине и напад Преплављењем. Иако је нападач спречен да се убаци у мрежу, он може користити Црвоточину како би тунеловао податке које шаљу легитимни чворови једног дела мреже, другим, исто тако легитимним чворовима другог краја мреже и тиме их убедити да су суседи, или да проследи ухваћени broadcast пакет са довољном снагом тако да га сви чворови у мрежи приме. Криптографски механизми на нивоу слоја везе са употребом глобалног дељеног кључа су неефикасни у случају унутрашњих напада или у случају компромитованих чворова. Нападач који је успео да се убаци у мрежну топологију може да нападне WSN убацивањем лажних информација рутирања, креирањем Црне рупе, селективним прослеђивањем пакета, употребом Сибил напада и Преплављивањем.

5.3 Одбрана од унутрашњих напада

Нападач који је нашао начин да додај свој мрежни уређај у WSN не може бити спречен да користи неке од функционалности мреже, али он то мора учинити употребом идентитета компромитованих чворова. Уколико је успео да приступи једном од чворова, он је у могућности да екстрахује глобални дељени кључ на основу кога може равноправно учествовати у мрежној инфраструктури, некада и преко непостојећег, односно виртуелног чвора. Верификација идентитета мрежних уређаја на основу њиховог идентификатора, у оваквом сценарију не искључује безбедносну претњу, међутим решење може представљати третирање идентификационих ознака SN једносмерним криптографским функцијама и њихово уланчавање, или имплементација инфраструктуре јавних кључева, PKI (енгл. Public Key Infrastructure). Успостављање PKI је веома захтевно у хардверском смислу и често није могуће због ограничених ресурса SN који немају хардверске потенцијале да реализују генерисање и верификацију дигиталних потписа. Једно од решења може бити да сваки SN у мрежи дели јединствени симетрични кључ са BS чиме се омогућава међусобна верификација SN-а и успостављање заједничких дељених кључева као и аутентификована и шифрована комуникација. На овај начин BS може да ограничи сваки SN само на одређени број суседа са којима може да комуницира и уколико дође до компромитовања SN његова дејство је ограничено само на одређени број чворова, чак и у сценарију где нападач досегне BS и агрегационе чворове удаљене више скокова, обзиром да и они имају процедуре за верификовање суседа. Нападач може искористити Црвоточину да креира тунел између два чвора и да их убеди да су суседи, али није у могућности да прислушкује, или модификује комуникацију између њих.

Напад Преплављењем је могуће предупредити двосмерном верификацијом комуникационог канала пре отпочињања комуникације тим каналом. Уобичајени протоколи верификације намењени мрежним уређајима са скромнијим хардверским ресурсима су довољни да спрече овакву врсту напада. Двосмерна верификација онемогућава ефикасне нападе Црвоточином креираном на више места у WSN јер поуздане BS ограничавају број верификованих суседа за сваки чвор чиме се локализује ефекат Преплављења на мале сегменте WSN у околини компромитованих чворова, међутим није могуће направити савршену одбрану нарочито у случају када се напад креирања Црвоточине користи у комбинацији са креирањем Црне рупе. Црвоточину је тешко уочити због употребе приватних спољашњих канала који су невидљиви постојећој WSN и обзиром да WSN често користе додатне информације које обавештавају чворове о количини преостале енергије, или о процени поузданости путања што је неопходно како би се креирала топологија мреже. Такође, протоколи рутирања у WSN настоје да умање број скокова при чему се користе бројачи скокова који могу бити погрешно интерпретирани и злоупотребљени уколико је креирана Црвоточина. Једини начин за умањење негативних ефеката ових напада је да се протоколи рутирања пажљиво дизајнирају тако да и уколико се креирају Црвоточина, или Црна рупа нежељени ефекти буду бесмислени. Протоколи који креирају топологију WSN на иницијативу BS су веома осетљиви на овакве нападе, док су географски протоколи рутирања који креирају топологију на захтев употребом локалних информација у без учествовања BS значајно отпорнији обзиром да се саобраћај усмерава према физичким локацијама базних станица што смањује могућност злонамерног усмеравања саобраћаја. Напад Црвоточином је ефикасан када се користи за креирање Црне рупе, или вештачких путања које привлаче саобраћај. Овакве путање се једноставно препознају у географским протоколима јер чворови могу да утврде да је удаљеност између њих већа од уобичајеног радио домета.

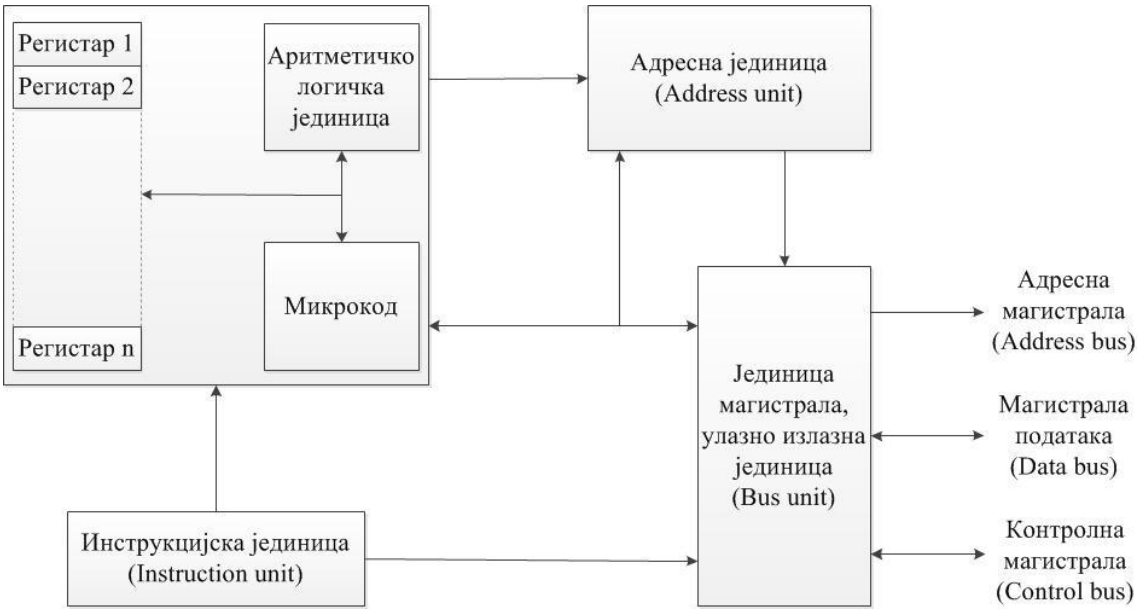
Уколико постоји компромитовани чвор, постоји релативно велика вероватноћа да је могуће извести напад селективним прослеђивањем пакета уколико је он стратешки постављен у близини SN, или BS. Multipath рутирањем је могуће успешно предупредити овакве нападе. Поруке које се усмеравају преко одређеног броја путања са потпуно раздвојеним чворовима су заштићене од напада селективног прослеђивања који укључује највише толико компромитованих чворова и нуде статистичку заштиту чак и у случајевима где је већи број чворова компромитован. Међутим, креирање путања које немају заједничке чворове је често неекономично и неефективно тако да је решење у уплетеним путањама које имају заједничке чворове, али на такав начин да се вишеструким уплитањем путања оствари статистичка заштита против селективног прослеђивања. Додатно, могуће је користити алгоритам који ограничава чворове да динамички бирају следећи скок из скупа могућих кандидата што додатно ограничава нападача да преузме контролу над током података.

Обзиром да BS располажу знатно комплекснијим хардверским могућностима у односу на SN, оне представљају чворове који су погодни за превенцију многих напада. Поуздане BS онемогућавају нападаче да лажирају broadcast, или поруке плављења што обезбеђује да сваки SN, иако постоји могућност да буде компромитован, не буде у могућности да лажира поруке од BS при чему може да верификује поруке од BS. Обзиром да већина протокола захтева broadcast HELLO поруку ка својим суседима, ове поруке морају да буду аутентификоване и отпорне

на лажирање. Стандардни протоколи за аутентификацију поздравних порука, или за употребу дигиталних потписа, нису увек прикладни за WSN. Имплементација криптографских механизама у WSN може бити реализована употребом симетричне криптографије обзиром да она захтева минимално увећање пакета. Са друге стране, употреба искључиво симетричних алгоритама није оптимално решење обзиром на сувише компликоване методе пуњења уређаја кључевима, или њихове замене, нарочито у случају великих WSN, или оних који се простиру на великим подручјима. Аутентификовани broadcast у пракси захтева одређени ниво асиметрије. Један од начина је употреба обелодањивања кључева са закашњењем и једносмерних ланаца кључева који се конструишу са јавним криптографским функцијама за креирање отиска поруке, хеш функцијама (енгл. hash functions) што онемогућава поновно слање порука обзиром да су све поруке аутентификоване, а оне које се појављују са обелодањеним кључевима се одбацују.

6. Безбедносни механизми у WSN

Зависно од намене, апликације за управљање WSN можемо поделити у три групе: уобичајене WSN које су намењене надгледању природних феномена где је безбедносни аспект на одржавању функционалности мреже што подразумева употребу мање комплексних криптографских алгоритама који пружају нижи ниво заштите, затим мултимедијалне WSN, WMSN (енгл. Wireless Multimedia Sensor Network) које карактерише употреба технологије која омогућава манипулацију сликама високе резолуције, звучним записима и видео записима релативно високог квалитета што подразумева балансирање између хардверских ресурса, потрошње енергије и комплексности безбедносних алгоритама и визуелне WSN, WVSN (енгл. Wireless Visual Sensor Network) које се реализују употребом ситних визуелних уређаја за праћење окружења и надгледање околине у реалном времену што подразумева употребу технологије која омогућава мало, или никакво кашњење комуникације и велику брзину обраде података. То је велики изазов обзиром да у оваквим мрежама није могуће правити компромисе када је у питању безбедност. (Kong, et al., 2015) Уобичајени сценарио реализације безбедног информационог система се заснива на употреби једносмерних функција за креирање отиска поруке и потврду њеног интегритета, употреби криптографских функција за шифровање података ради обезбеђивања тајности комуникације и имплементацији система за дистрибуцију криптографских кључева, међутим када су у питању WSN избор алгоритама и технологија се сужава на скуп оних који могу бити имплементиране у скученом хардверском окружењу.



Слика 4 Микропроцесорска јединица - MPU

Како би компоненте WSN биле прихватљиве по цени, у односу на њихову намену, пракса је да се у њих уграђују једноставнији микропроцесори, MPU (енгл. Microprocessing Unit). MPU се могу окарактерисати као слаби, напредни, и јаки зависно од њихових могућности када је у питању извршавање аритметичко логичких операција, односно у зависности од сложености аритметичко логичке јединице, ALU (енгл. Arithmetic Logic Unit), комплексности управљачке јединице, CU (енгл. Contrlol Unit), радног такта, броја регистара и њихове ширине, од

ширине унутрашњих магистрала и од могућности спољашњих магистрала, односно улазно-излазне јединице (енгл. BUS Unit). Поред набројаног, MPU чине адресна јединица (енгл. Address Unit) која управља приступом меморији, инструкциона јединица (енгл. Istruction Unit) која прикупља, припрема, чува и шаље инструкције у извршну јединицу и извршна јединица (енгл. Execution Unit) у оквиру које се налазе већ поменути ALU и скуп регистара и микрокод (енгл. microcode), односно блок у ком се налази скуп инструкција и табела специфичних инструкција и параметара за конкретну хардверску целину, које контролишу у одређују рад MPU.

6.1 Заштита интегритета података

Заштита интегритета података подразумева могућност детекције неауторизоване промене података. Шифровање не штити интегритет поруке чак и у идеалном сценарију у ком тајни криптографски кључ није откривен од стране нападача, тако да је потребно имплементирати технику која је у могућности да изврши тај задатак. Интегритет података се штити употребом функција за хеширање података које пресликавају бинарне низове произвољних дужина у бинарне низове фиксних дужина, 128 бита, 160 бита и слично. Основна карактеристика хеш функција је њихова једносмерност што подразумева да је практично немогуће пронаћи полазну вредност отвореног текста чија је хеш вредност унапред задата, односно позната, што обезбеђује отпорност на колизију обзиром да је веома мала вероватноћа да се добију две различите полазне поруке из исте хеш вредности. Овакве технике онемогућавају потенцијалног нападача да фалсификује оригиналну поруку, а да на крају добије исти отисак поруке, њену хеш вредност. Хеш функције су веома осетљиве на промене у улазној вредности, промена од само једног бита у изворном тексту покреће лавински ефекат и треба да створи промену бар половине бита у отиску. (Vidaković & Vučetić, 2005)

Највише заступљене хеш функције, у пракси и у теорији, су: MD5 (енгл. Message-Digest algorithm 5), SHA-1 (енгл. Sesure Hash Algoritam) и RIPEMD (енгл. RACE Integrity Primitives Evaluation Message Digest). Ове функције су развијене почетком деведесетих година XX века, али су и данас све оне у употреби са тим што се MD5 сматра мање безбедном обзиром да су се појавиле назнаке да се колизија може наћи већ са 2^{69} различитих порука, за разлику од преостала два алгоритма где је број могућих порука 2^{80}. Чињеница је да не постоји савршена хеш функција и да постоје хеш колизије одређеног нивоа, али то не повећава безбедносни ризик који би био значајан са становишта практичне имплементације ових алгоритама. Уколико је хеш дужине n бита, потребно је да се генерише 2^{n-1} порука како би се добио хеш исте вредности што потенцијални напад доводи на ниво напада грубом силом (енгл. brute force attack), тако да је у случају примене SHA-1, који генерише отисак од 160 бита, потребно извршити 2^{80} операција да се пронађе порука идентична полазној. Обзиром на потврђене слабости MD5 и SHA алгоритама и њихових претходника, препорука је да се користе комплекснији алгоритми попут напреднијих верзија SHA алгоритама: SHA-256, или SHA-512, затим BLAKE2s, BLAKE2b, RIPEMD-128, RIPEMD-160, Whirlpool за које још увек нико није демонстрирао успешан напад или теоријски образложио довољно значајне слабости, међутим ове препоруке важе за конвенционалне компјутерске мреже које су у малој мери ограничене хардверским ресурсима за разлику од WSN које имају бројна ограничења.

Табела 2 Упоредни преглед основних карактеристика криптографских хеш функција

Алгоритам	Дужина отиска поруке	Дужина блока	Највећа дужина поруке	Дужина компјутерске речи	Број рунди
BLAKE2b	512	512	Нема практичног ограничења	64	12
BLAKE2s	256	256	Нема практичног ограничења	32	10
MD2	128	128	Нема практичног ограничења	32	18
MD4	128	512	64	32	3
MD5	128	512	64	32	64
RIPEMD-128	128	512	64	32	64
RIPEMD-160	160	512	64	32	80
RIPEMD-320	320	512	64	32	80
SHA-0	160	512	64	32	80
SHA-1	160	512	64	40	80
SHA-256	256	512	64	56	64
SHA-512	512	1.024	128	64	80
WHIRLPOOL	512	512	256	8	10

6.1.1 Пирсон хеширање (енгл. Pearson)

Дужи низ година, дизајнери једносмерних хеш функција нису улагали додатне напоре у развој алгоритама, а након што су неке од функција проглашене практично, или теоријски небезбедним, повећавана је дужина отиска и број корака извршавања алгоритма. Већина актуелних хеш функција је оптимизована за 32-битне и 64-битне процесоре и веома су захтевне по питању времена извршавања и количини потребне енергије. Решења намењена скромнијим хардверским платформама, иако теоријски небезбедна, могу дати добре практичне резултате. Једно од таквих је Пирсон хеширање које је могуће реализовати на MPU са 8-битним регистрима. Ова функција генерише отисак за текст произвољне дужине тако што улаз дели на речи од одређеног броја карактера при чему се сваки карактер представља једним бајтом и везује за индексну вредност у опсегу од 0 до 255. У процесу хеширања користи се помоћна табела која је у функционалној зависности са индексираном табелом (енгл. auxiliary table). Ову табелу чини 256 бајтова псеудо случајних 8-битних целобројних вредности од којих се ни једна не понавља. Отисак поруке се генерише тако што се за сваки бајт из индексиране табеле на основу одређеног бајта из помоћне табеле израчунава 8-битна вредност логичком операцијом ексклузивне дисјункције, односно ЕКСИЛИ (енгл. XOR) логичком операцијом. (Pearson, 1990)

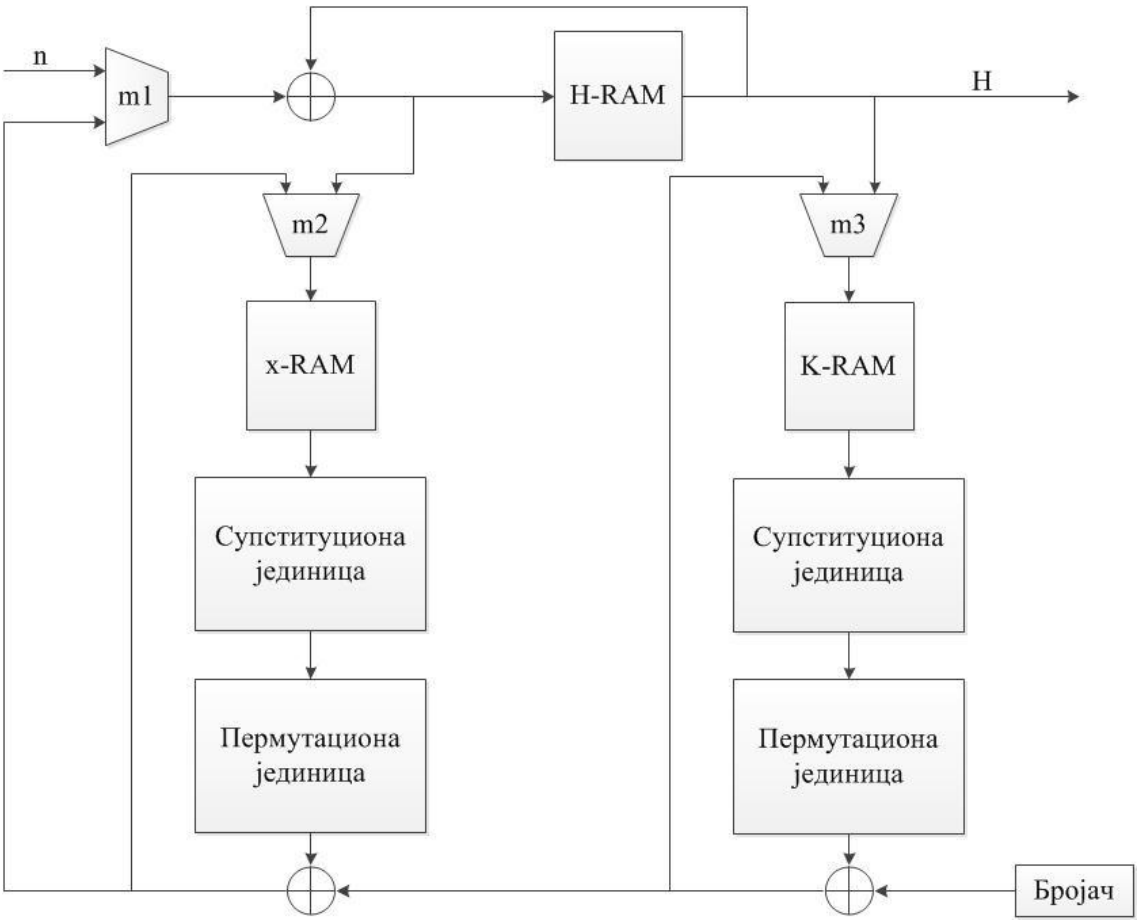
Помоћна табела је од суштинског значаја за овај алгоритам. Она мора бити генерисана за предајну и пријемну страну што умањује безбедност система јер се тако ствара могућност да потенцијални нападач, уколико дође до њеног садржаја, самостално генерише валидне отиске порука. Решења заснована на овом алгоритму која не користе помоћне табеле подразумевају коришћење функције пермутација која треба да буде смештена у меморији, међутим коришћење исувише једноставне функције ће резултовати повећањем колизије, док ће исувише комплексне функције негативно утицати на брзину њиховог извршавања. Обзиром да Пирсонов алгоритам нема ограничења по питању дужине поруке, потребно је крај поруке одредити неким од специјалних карактера и обезбедити да се такав карактер не појављује у садржају порука. Такође

потребно је обезбедити систем додатних пермутација за кључне речи, или за ознаке које се често појављују у конкретној врсти WSN обзиром да оне могу бити добар основ за криптоанализу. Поред тога, овај алгоритам је препоручен само за ASCII (енгл. American Standard Code for Information Interchange) односно за кодне стране (енгл. Code Page) где је сваки од карактера могуће представити из помоћ 8 бита. Такође, потреба за постојањем 256-бајтне табеле може додатно оптеретити MPU обзиром да често располажу меморијом од само неколико стотина бајтова.

6.1.2 Whirlpool алгоритам

Посебно интересантан алгоритам за генерисање отиска поруке, са становишта WSN је Whirlpool алгоритам. Whirlpool је итеративни блоковски алгоритам који улазну поруку дели у блокове од 512 бита које третира криптографским кључем дужине исте дужине. Иницијално, кључ који се користи за прву рунду чини низ нула, док се сваки следећи генерише зависно од улазног текста. Сваки од блокова се третира идентичним трансформацијама у десет рунди. Основне операције се извршавају над 8-битним регистрима на основу 512-битног стања тренутног хеша и стања ланчаних 512-битних кључева заснованих на вредностима улазне поруке и вредностима кључа из претходне рунде, односно актуелног стања хеша. Тренутно стање хеша је организовано као матрица стања од 8x8 бајтова над којом се, у току сваке од рунди, извршавају следеће операције: нелинеарно мешање бајтова, циклична замена колона, линеарно померање редова и додавања кључа рунде XOR операцијом на тренутну матрицу стања. Кључ се генерише на основу иницијалног 512-битног кључа након извршавања сваке рунде тако да у процесу извршавања алгоритма постоји 11 кључева, за сваку секвенцу по један. Пре извршења прве рунде улазна порука се третира XOR функцијом у односу на иницијални кључ на основу које се генерише кључ за прву рунду, док се сви наредни кључеви генеришу у односу на актуелну матрицу стања.

Whirlpool је дизајниран за 8-битне и 64-битне процесоре тако да се операције извршавају над речима од 8 бита уз највећу дужину блока од 64 бита. Обзиром да се у случају WSN често употребљавају једноставнији MPU који нису у могућности да у оптималном временском року изврше потребне операције, мрежни уређаји се често дизајнирану тако да омогуће хардверско извршавање тих операција. Извршавање Whirlpool алгоритма је, по својој математичкој структури, слично са Rijndael алгоритмом што отвара могућност хардверске реализације алгоритама којима се могу постићи и тајност порука и потврда њиховог интегритета. Основу структуре Whirlpool језгра чине две магистрале ширине 8 бита које креирају два одвојена тока података, један за стање хеша, а други за стање кључа. Whirlpool језгро садржи радну меморију, DPRAM (енгл. Dual-Port RAM) коју чине два 64x8-битна меморијска блока: X-RAM и K-RAM, затим две јединице за супституцију битова (енгл. S-box), две јединице за прермутацију битова (енгл. P-box), и XOR капију за додавање кључа. Тренутно стање хеша и резултат пермутација се комбинују и чувају у H-RAM-у чиме се увећавају перформансе мрежног уређаја јер употреба H-RAMA омогућава ишчитавање следеће речи, следећих 8 битова, током уписивања претходно третиране речи. (Alho, et al., 2007)



Слика 5 Хипотетичка структура Whirlpool језгра

Операције извршавања Whirlpool алгоритма са становишта хардверске имплементације је могуће поделити у три групе: учитавање, обраду и ишчитавање података. Учитавање података у првој вази подразумева формирање 64-битних блокова од улаза дужине n бита, (n<256) један по један бит. Први блок који се учитава из H-RAM-а чини низ нула, а сваки следећи представља међурезултат на крају претходне рунде. Током учитавања, мултиплескери m1, m2 и m3 одвајају низове бита тако да се у H-RAM и x-RAM учитавају актуелна верзија хеша, док се у K-RAM учитава актуелна верзија кључа. Обрада података подразумева десет паралелних итерација за стање хеша и за стање кључа. Свака рунда подразумева обраду једне по једне 8-битне речи које су смештене у x-RAM, један по један бит. Обрада сваке речи захтева 16 тактова од којих је осам намењено за ишчитавање операнада, а осам за смештање резултата. Током првих девет рунди, мултиплексери m2 и m3 усмеравају резултат сваке рунде ка x-RAM-у и K-RAM-у. Током последње рунде, након проласка кроз XOR капију, финални резултат се захваљујући мултиплексеру m1 смешта у H-RAM, тако да садржај у x-RAM-у и K-RAM-у није више потребан и може бити преписан у наредним корацима. Финални резултат H, смештен у H-RAM има дужину од 64 бита. Учитавање, обрада и исчитавање сваког блока захтева $64+10\cdot 8\cdot 16=1344$ тактова тако да је читав сет операција могуће извршити за 84s уколико се употребљава 8-битни MPU са радним тактом од 16Hz.

6.1.3 LOCHA алгоритам

LOCHA (енгл. Light-Weight One-way Cryptographic Hash Algorithm) генерише отисак фиксне и релативно мале дужине уз карактеристике које омогућавају примену у WSN. Због оптимизације, претпоставка је да ће улазне поруке чинити само 96 карактера ASCII (енгл. American Standard Code for Information Interchange) са кодним ознакама од 32 до 127 што би у нашем случају био знак за размак, све цифре, специјални карактери и сва велика и мала латинична слова, са том разликом што слова š, ž, č и ć не би имала квачице, а у случају слова đ би се користио дирграф 'dj'. (Chowdhury, et al., 2014)

Реализација LOCHA алгоритма започиње превођењем свих карактера улазне поруке у њихове бинарне репрезентације у складу са ASCII кодовима, након чега се врши допуњавање бинарног записа до величине дељиве са 512. Бинарни запис се допуњава нулама, а ако је дужина трансформисане поруке већ дељива са 512 додаје се још 512 нула како би се додатно увећала отпорност алгоритма. Преведена и допуњена порука се дели три пута: прво на блокове дужине 512 бита, онда сваки од њих на 8 блокова дужине 64 бита, а затим сваки од њих на још 8 блокова дужине 8 бита. Након поделе на блокове, сви 8-битни блокови се третирају на основу табеле за супституцију где се сваком коду додељује одговарајући парњак из табеле. Табелу за супституцију чини 97 простих бројева који су ограничени по величини како би се постигла боља оптимизација алгоритма. Замена карактера се извршава у сваком од осам 64-битних блокова након чега се за сваки од њих израчунава осам замењених вредности чиме се завршава први ниво трансформације. Друга трансформација се реализује на основу друге табеле за супституцију коју чини 67 простих бројева који су изабрани алгоритмом за псеудо случајни избор како би се обезбедила униформност и како би се омогућила рационална употреба меморије за складиштење података. Вредности друге табеле за супституцију се израчунава као логаритам синуса вредности коју чини збир броја 128 идентификационе вредности за сваки од простих бројева. Трећа трансформација се реализује на основу прве две где се вредности добијене за сваки од осам 64-битних блокова из децималног претварају у хексадецимални еквивалент од 3 карактера чиме се креира хексадецимални број од 24 карактера за читав полазни блок од 512 бита. Након реализације свих функција замене, финални отисак поруке има дужину од 96 бита за сваки улазни блок дужине 512 бита.

LOCHA задовољава све критеријуме једносмерне криптографске функције. Уколико би потенцијални нападач хтео да реализује напад грубом силом било би потребно да испита 2^n могућих комбинација. Обзиром да LOCHA генерише хеш дужине 96 бита, било би потребно испитати 2^{96} могућих комбинација. Потенцијални нападач који би успео да приступи неком од SN, обзиром на њихове скромне хардверске потенцијале не би био у могућности да успешно реализује напад. На пример, ATMega 128 располаже MPU-ом са радним тактом од 7,37MHz коме би за испитивање свих могућих комбинација требало $3{,}4x10^{14}$ година. LOCHA је отпоран на колизију јер је за проналажење две поруке са истим отиском потребно реализовати 2^{48} операција, за шта би поменутом MPU требало 1,21 година.

Табела 3 Упоредне карактеристике MD5, SHA-1 и LOCHA

Алгоритам	Дужина отиска	Ангажовање процесора (у циклусима)	RAM/ROM	Ангажовање регистара
MD5	128	36360	32 RAM-а од 32-битних блокова и ROM од 2368 бита	12 регистара од 32 бита
SHA-1	160	84272	32 RAM-а од 32-битних блокова	12 регистара од 32 бита
LOCHA	96	2952	1 ROM од 804 бита и 1 ROM од 970 бита	4 регистра од 16 бита и 18 регистара од 8 бита

6.2 Криптографски алгоритми за шифровање података

Симетричне криптографске алгоритме, који су у широкој употреби, често није могуће имплементирати у уређаје који су опремљени слабим MPU, међутим неке од њих, уз одговарајућу хардверску архитектуру могуће је релативно успешно имплементирати. На пример Rijndael, који је одређен као напредни шифрарски стандард, AES (енгл. Advanced Encryption Standard) од стране, NIST-а (енгл. National Institute of Standards and Technology), NESSIE-а (енгл. New European Schemes for Signature, Integrity and Encryption) и CRYPTREC-а (енгл. Cryptography Research and Evaluation Committees), ког је могуће успешно имплементирати на 8-битним, 32-битним и 64-битним MPU, или Twofish алгоритам који је оптимизован за 32-битне MPU ког је могуће успешно реализовати ангажовањем 8-битних регистара, односно MPU-а са 8-битном дужином речи. (Lee, et al., 2009) (Schneier, et al., 1998) Оба алгоритма су дизајнирана тако да омогуће имплементацију на различите платформе уз различите карактеристике по питању брзине шифровања, иницијализације кључа, употребе меморије и слично, на начин који не умањује безбедност система. Уколико су у питању 16-битни MPU, алгоритми као што је SkipJack се могу перфектно уклопити. Уређаји у WSN обично располажу са довољном количином сталне меморије за трајно чување података и оперативне меморије за смештање инструкција, програма, приватних кључева и других привремених података тако да избор криптографских алгоритама зависи од могућности MPU.

Проблематика дистрибуције кључева се у основи своду на њихов транспорт сигурним каналима између мрежних чворова. Обзиром да је ручно уношење криптографских неефикасно у случају великих WSN, потребно је реализовати систем који би омогућио да се тај задатак реализује на безбедан начин путем инфраструктуре WSN. Асиметрична криптографија и употреба јавних кључева која се данас успешно примењује у заштити информациони система није адекватно решење за већи део уређаја који се користе у реализацији WSN обзиром на њихове техничке карактеристике. Међутим, иако је симетрична криптографија супериорна у односу на асиметричну по безбедности, брзини извршавања операција и утрошцима електричне енергије, управљање кључевима у симетричној криптографији није једноставан задатак због чега се непрестано разматра опција имплементације различитих верзије асиметричне криптографије у WSN. Без обзира на одабир конкретних алгоритама безбедне WSN треба да испуне захтеве по питању тајности података, њиховог интегритета, потврде извора података, аутентификације ентитета који учествују у комуникацији, контроле приступа и доступности система, а то се успешно може реализовати

безбедним управљањем криптографским кључевима, препознавањем и превенцијом напада, безбедним рутирањем, обезбеђивањем подручја на којим се налазе уређаји, безбедним складиштењем података и другим специфичним безбедностним механизмима.

Блоковске алгоритме: SkipJack, RC5, RC6, Rijndael, Twofish, MISTY1, KASUMI, Camellia и друге могуће је успешно имплементирати у WSN, а у зависности од сценарија примене сваки има своје предности и мане. (Law, et al., 2008)

Табела 4 Упоредне карактеристике сензорских мрежних уређаја

Платформа	MPU	Радни такт	Напајање	Потрошња у стању мировања	RAM	Програмска меморија	Флеш меморија
Arduino BT	Atmel ATmega328	20 MHz	2.5-12 V	N/A	2 kB	1 kB (EEPROM)	32 kB
eyesIFXv2.1	TI MSP430F1611	8 MHz	2500 mAh (батерија)	N/A	10 kB	N/A	48 kB
iMote2	Intel PXA271 Xscale	13-416 MHz	3xAAA (4.5 V), батерија (3.2-4.5V) или Li-Ion/Li-Poly батерије	390 μA	256 kB	N/A	32 MB
Mica2	Atmel ATmega128L	8 MHz	N/A	15 μA	4 kB	4 kB (EEPROM)	128 kB
MicaZ	Atmel ATmega128L	8 MHz	2xAA или екстерно напајање (2.7-3.3 V)	< 15 μA	4 kB	4 kB (EEPROM)	128 kB
Cricket	Atmel ATmega128L	8 MHz	N/A	N/A	4 kB	4 kB (EEPROM)	128 kB
TMote Sky/TelosB	TI MSP430F1611	8 MHz	2xAA (3.0 V)	5.1 μA	10 kB	1 MB (Екстерна флеш меморија)	48 kB
BTnode rev3	Atmel ATmega128L	8 MHz	2xAA (3.0 V) или екстерно напајање (3.8-5 V)	11.6 μA	4 kB	4 kB (EEPROM)	128 kB
uAMPS	Intel StrongARM SA-1100	59-206 MHz	N/A	1 μA	16 MB	512 kB (ROM)	N/A
mPlatform	TI MSP430F1611/OKI ML67Q5003/ XC2C512	8/60/32-200 MHz	N/A	N/A	10/32/- kB	-/4/- kB	48/512/- kB

6.2.1 SkipJack

Анализа структуре алгоритма кроз зависност између отвореног текста и шифрата, односно диференцијална криптоанализа, или настојање да се открије линеарна апроксимација неких делова криптографског кључа, односно линеарна криптоанализа, у случају SkipJack алгоритма доводи до потребе за анализом података чија количина доводи ове нападе на ниво напада грубом силом чиме га карактерише као безбедан. Аналитичари се слажу да је SkipJack отпоран на све нападе и све познате методе диференцијалне и линеарне криптоанализе. За потребе истраживања су тестиране неке од модификованих верзија SkipJack алгоритма. Диференцијалном криптоанализом овог алгоритма, редукованог на 16 рунди, могуће је утврдити да ли је у питању SkipJack алгоритам или неки други

вид псеудослучајних пермутација. (Biham, et al., 1999) Оригинална верзија алгоритма реорганизује распоред бита криптографског кључа у зависности од стања бројача рунди, а уколико би се уклонила ова функција, простор за претрагу кључева би се смањио на 26% у односу на 50% што обично представља оквир претраге приликом напада грубом силом. Међутим криптоанализа овакве модификације алгоритма би подразумевала обраду $2^{78.06}$ могућих кључева што би и даље било практично неизводљиво. Модификована верзија, SkipJack-3XOR је карактеристична по томе што у њој недостају три XOR операције током 3. 15. и 16. рунде на начин који не нарушава постојећу Feistel структуру. Диференцијална криптоанализа ове верзије подразумева упоређивање 2^{71} парова отворених текстова и шифрата, међутим ако се анализирају разлике у оквиру 8. и 9. рунде, независно од осталих, простор се смањује за 2^{16} што омогућава анализу упоређивањем 2^{58} парова. Линеарна криптоанализа ове верзије алгоритма подразумева обраду 2^{64} што је, такође, практично неизводљиво обзиром временску и просторну сложеност обраде. Напад грубом силом, испитивањем свих могућих кључева би захтевао највише 2^{80} бинарних записа, међутим и када би се број потенцијалних кључева смањио на 50% обзиром на вероватноћу да се одговарајући налази у првој половини, не би било могуће извршити успешан напад. (Biham, et al., 1999)

Табела 5 Асимптотска сложеност диференцијалне криптоанализе SkipJack алгоритма у зависности од броја рунди и њихове заступљености

Број рунди	Број потребних отворених текстова за анализу	Асимптотска сложеност
25 (од 5. до 29.)	2^{38}	2^{27}
26 (од 4. до 29.)	2^{38}	2^{49}
28 (од 1. до 28.)	2^{34}	2^{77}
29 (од 1. до 29.)	2^{34}	2^{77}
30 (од 1 до 30.)	2^{34}	2^{77}
31 (од 1. до 31)	2^{41}	2^{78}
31 (од 2. до 32.)	2^{34}	2^{78}

6.2.2 Twofish

Структура Twofish алгоритма обезбеђује дифузију кључева њиховим дељењем на речи од 8 бита и ортогоналним распоређивањем у оквиру супституционих јединица чиме се спречава генерисање сличних чворова за сличне кључеве, што онемогућава напад сличним кључевима. Један бајт криптографског кључа утиче на измену четири зависна кључа на основу којих се реализује супституција. Овај алгоритам примењује пермутације бита употребом MDS матрице (енгл. Maximum Distance Separable), што обезбеђује генерисање различитих 12-бајтних иницијалних вектора на основу најмање 5 бајтова, али тако да сам алгоритам не буде превише захтеван када су у питању ресурси, што је значајно са становишта WSN. MDS матрице омогућавају довољно комплексне пермутације тако да нема потребе за употребом линераних функција, чиме се смањује сложеност, а постиже довољно квалитетна дифузија. Поред тога, напад сличним кључевима није изводљив ни због тога што супституционе јединице вредности кључа примењују у обрнутом редоследу у односу на подкључеве који се генеришу на почетку сваке рунде. Такође, ово омогућава и употребу једноставних криптографских кључева без снижавања нивоа безбедности, док оваква структура омогућава шифровање у оквиру само 64 бита радне меморије уз кључеве од 128 бита. (Schneier, et al., 1998)

Криптоанализа Twofish алгоритма редукованог на 5 рунди са предложеном дужином кључа без иницијалног третирања отвореног текста XOR функцијом у односу на криптографски кључ, захтева $2^{22,5}$ отворених текстова и асимптотску сложеност од 2^{51}, док 10 рунди без иницијалног мешања XOR функцијом и без завршног мешања шифрата и кључа истом функцијом захтева 2^{32} изабраних отворених текстова, 2^{11} прилагођених отворених текстова уз асимптотску сложеност од 2^{32}. Диференцијална криптоанализа пуних 16 рунди овог алгоритма би захтевала 2^{51} изабраних отворених текстова што би подразумевало обраду 32^{15} бајтова података. Претпоставка је да би најуспешнији напад на Twofish захтевао сложеност од 2^{128}, односно 2^{192}, или 2^{265}, зависно од дужине коришћеног кључа што је једнако нападу грубом силом.

6.2.3 RC5

RC5 алгоритам (енгл. Rivest Cipher) је присутан од 1995 године без појаве значајнијих слабости обзиром да је су за криптоанализу шифрата који је креиран на основу кључа стандардне дужине од 128 бита и данас потребне године, а обзиром да је дизајниран и за хардверску и за софтверску имплементацију, још увек представља довољно добро шифрарски систем. По конвенцији уз назив алгоритма додају се одговарајући параметри, RC5-w/r/b где w представља дужину компјутерске речи у битима, r број рунди, a b дужину кључа, такође у битима. Након успешне криптоанализе реализоване 1998. године на верзију алгоритма RC5-32/12/16 и то на основу 2^{44} изабраних комбинација отвореног текста, предложено је да се број рунди са 16, повећа на 18 што данас представља стандард у имплементацији RC5 алгоритма. За имплементацију RS5 алгоритма у WSN, RC5-32/18/b обезбеђује оптималне перформансе односа нивоа безбедности и ангажовања ресурса.

6.2.4 RC6

Алгоритам RC6 је нарочито значајан са становишта WSN због његових перформанси: релативно високог нивоа безбедности и могућности за имплементацију на велики број различитих платформи у оквиру WSN. Теоријски, испитивањем псеудослучајних секвенци на RC6 са 14 рунди могуће је доћи до отвореног текста испитивањем $2^{13,8+16,2}\cdot r$ комбинација, где r представља број рунди што у овом случају ствара простор од $2^{240,6}$ комбинација. Итеративни напади базирани на статистици карактеристичној за енглески језик на овај алгоритам у сценарију са истим бројем рунди захтевају 2^{118} познатих отворених текстова, меморију величине 2^{112} бита и 2^{122} операција. Уколико је циљ криптоанализе проналажење криптографског кључа дужине 64 бита који је имплементиран у шифровању применом RC6 алгоритма кроз 18 рунди, уз употребу релативно слабог криптографског кључа (који се јавља једном међу 2^{90} могућих кључева), могуће је из шифрата доћи до полазне вредности кључа са вероватноћом од 95% на основу многоструке линеарне криптоанализе уз употребу $2^{127,4}$ познатих комбинација бита, меморијом величине 2^{64} бита и $2^{193,4}$ операција. На основу овога се закључује да RC6-32/20/b представља оптимизовано решење.

6.2.5 Rijndael

Као и већина савремених блоковских шифрарских алгоритама, Rijndael је креиран тако да буде имун на диференцијалне и линеарне методе криптоанализе. На пример, диференцијална криптоанализа шифрата генерисаног овим алгоритмом на основу 128-битног кључа кроз 6 рунди захтева анализу $2^{91,5}$ бита шифрата. Криптоанализа шифрата након 7 рунди уз употребу кључа дужине 196 или 265 бита уз изабрани отворени текст од 2^{32} бита и доводи до приближно 2^{140} варијација и временску и просторну сложеност, односно асимптотску сложеност која је приближна оној потребној за напад грубом силом. Напад сличним криптографским кључевима на Rijndael са кључем дужине 256 бита и 9 рунди доводи до 2^{224} могућих комбинација што овакав напад чини практично немогућим. До сада није познат успешан напад на овај алгоритам уколико се шифровање реализује у процесу дужем од 7 рунди и ако безбедност овог алгоритма не расте експоненцијално броју рунди, међутим његова комплексност захтева хардверске ресурсе који су изнад просечних за WSN, тако да се AES имплементира само уколико постоје високи безбедносни захтеви.

6.2.6 IDEA

IDEA, (енгл. International Data Encryption Algorithm) је креиран да буде отпоран на диференцијалну криптоанализу и ту карактеристику још увек има под одређеним околностима. Такође, још увек нису забележени примери успешне линеарне криптоанализе. Диференцијална криптоанализа овог алгоритма редукованог на 6 рунди захтева упоређивање 2^{64} изабраних отворених текстова уз $2^{126,8}$ операција. Иако веома безбедан, IDEA захтева значајно ангажовање ресурса због чега не представља довољно добар избор за слабије MPU. Поред тога, овај алгоритам је веома осетљива на слабе криптографске кључеве. Током периода његове интензивне криптоанализе откривен је значајан простор слабих кључева, један у 2^{96} што је створило потребу за уношењем одговарајућих измена у алгоритам. Линеарном криптоанализом је откривено постојање алгебарских операција које је могуће поједноставити тако да је могуће извршити успешан напад на шифрат добијен након 2 рунде уз 2^{42} операција. Без обзира на слабости које IDEA показује у различитим сценаријима, практична примена овог алгоритма пружа довољно висок ниво безбедности.

6.2.7 MISTY1

MISTY1 је 64-битни алгоритам за шифровање који је дизајниран да буде имун на диференцијалну и линеарну криптоанализу. Поред тога, карактерише га једноставна хардверска, или софтверска имплементација и брзо извршавање обзиром да користи логичке операције у комбинацији са лукап табелама (енгл. table lookups). Такође, овај алгоритам је посебно погодан за 16-битне платформе што га чини значајним са становишта WSN. Након успешне криптоанализе шифрата генерисаног применом овог алгоритма кроз 5 рунди, створен је његов безбеднији наследник алгоритам KASUMI који је за разлику од претходника, уместо три, имао четири јединице за супституцију у оквиру FL (енгл. Feistel-like) структуре. Међутим, чак и слабија верзија, MISTY1 пружа довољно висок ниво безбедности обзиром да није могуће реализовати успешну криптоанализу у

времену у ком би то представљало претњу, јер је за примену диференцијалног напада након 4 рунде, потребна анализа 2^{34} изабраних отворених текстова и 2^{62} шифрата, док је за напад колизије потребно анализирати 2^{28} изабраних отворених текстова и 2^{76} шифрата. Чињеница је да је MISTY1 представља безбедносну маргину, али обзиром на једноставност извршавања овог алгоритма у односу на модерне 128-битне алгоритме за шифровање, његова потпуна имплементација са предложеним бројем рунди пружа оптималан безбедностни ниво.

6.2.8 KASUMI

Диференцијална криптоанализа зарад откривања тајних кључева коришћених приликом примене KASUMI алгоритма кроз 6 рунди би подразумевала 2^{55} одабраних отворених текстова и 2^{100} шифрата. Доказано је да реализација алгоритма кроз три рунде не генерише псеудослучајни низ довољне комплексности, али да се са већ четири рунде постиже довољно висок ниво комплексности. Уколико би се овај алгоритам имплементирао без FL структуре, за успешну криптоанализу би било потребно 1416 изабраних отворених текстова уз асимптотску сложеност од $2^{22,11}$ што би захтевало $2^{29.98}$ мање времена у односу на напад грубом силом. Наравно, уз број рунди који се сматра оптималним за овај алгоритам, могуће је постићи довољно добре безбедносне карактеристике.

6.2.9 Camellia

Camellia је 128-битни шифрарски алгоритам намењен за брзо извршавање уз хардверску, или софтверску имплементацију који шифрује отворени текст на основу логичких операција и лукап табела. Произвођачи овог алгоритма наводе да он користи само 7875 логичких капија (енгл. logic gates) што га карактерише као најмањи шифрарски алгоритам међу постојећим 128-битним блоковским алгоритмима. Camellia је дизајниран тако да буде отпоран на диференцијалну криптоанализу, линеарну криптоанализу, напад сличним кључевима и напад смањењем броја рунди. Нападом на супституционо-пермутациону мрежу (енгл. Square attack) могуће је извршити успешну криптоанализу чак и код шифрарских алгоритама са Feistel структуром. Комплексност оваквог напада у случају 6 рунди Camellia алгоритма захтева анализу 3328 изабраних отворених текстова и 2^{112} шифрата, док криптоанализа 7 рунди овог алгоритма без FL структуре захтева 192 шифрата и $2^{82,6}$ изабраних отворених текстова. Square напад на 11 рунди Camellia алгоритма уз употребу 256-битног кључа захтева 2^{93} изабраних отворених текстова и $2^{255,6}$ шифрата што овај напад доводи на ниво напада грубом силом и сврстава овај алгоритам међу довољно безбедне за примену у WSN.

Табела 6 Упоредне карактеристике шифрарских криптографских алгоритама

Алгоритам	Дужина кључа у битима	Број рунди	Дужина блока у битима
RC5-32	128	18	64
RC6-32	128	20	128
Rijndael	128	10	128
SkipJack	80	32	64
IDEA	128/256	16	64/128
MISTY1	128	8	64
KASUMI	128	8	64
Camellia	128	18	128
Twofish	256	16	128

Уколико су у питању WSN са потребом за релативно ниским нивоом безбедности, SkipJack представља оптимално решења за хардверску платформу на коју то може бити имплементирано, док је MISTY1 алгоритам који представља добро решење за WSN са компонентама нижих перформанси. Сви поменути алгоритми могу бити имплементирани на актуелним хардверским платформама, а у зависности од имплементације пружају различите резултате. (Ganesan, et al., 2003) (JINWALA, et al., 2008) MPU са смањеним скупом инструкција, RISC (енгл, Reduced Instruction Set Computing) и MPU са сложеним скупом инструкција, CISC (енгл. Complex Instruction Set Computing).

Табела 7 Упоредне карактеристике различитих хардверских платформи

Платформа	Дужина процесорске речи	Радни такт MPU	Архитектура
ATMega 103	8 бита	4 MHz	RISC
ATMega 128	8 бита	16 MHz	RISC
M16C/10	16 бита	16 MHz	CISC
StrongARM SA-1110	32 бита	206 MHz	RISC
Xscale PXA250	32 бита	400 MHz	RISC
UltraSparc2	64/32 бита	440 MHz	RISC

Табела 8 Упоредне карактеристике времена извршавања различитих криптографских алгоритама на различитим платформама изражено у μs

Алгоритам	Величина у битима	Активност	ATMega 103	Atmega 128	M16C/10	Strong ARM SA-1110	Xscale PXA250	UltraSparc 2
MD5	0	Хеширање	5863	1466	1083	46	26	23
	1-26	Хеширање	5890	1473	1075	46	26	23
	62-80	Хеширање	10888	2722	2011	74	45	39
SHA-1	1	Хеширање	15249	3812	2651	69	12	27
	3	Хеширање	15781	3945	5303	69	12.3	27
	56	Хеширање	14543	3636	7955	133	25.8	55
	64	Хеширање	31107	7777	10907	145	25.7	56
RC5	16	Иницијализација	9641	2410	2074	41	45	28
		Шифровање	1651	413	197	3	3	2
		Дешифровање	1636	409	202	3	3	2
IDEA	16	Иницијализација шифровања	1523	381	727	26	15.54	11
		Иницијализација дешифровања	9417	2354	1927	76	25.16	36
		Шифровање	2555	325	596	16	3.24	9
		Дешифровање	2614	325	597	16	3.27	9

6.3 Аутентификација мрежних уређаја у WSN

Како би уређаји у WSN били аутентификовани потребно је да постоји систем на основу ког би се та функција могла реализовати. Најчешће се користи аутентификациона порука која потврђује аутентичност извора, а како би се смањило ангажовање ресурса, њено генерисање се често реализује паралелно са шифровањем отвореног текста, или приликом генерисања отиска поруке. (Rehman, et al., 2012) Циљ је креирање аутентификационог кода, MAC (енгл. Message Authentication Code) у оквиру WSN на начин који не би значајно умањио перформансе комуникационих уређаја. Без обзира на избор криптографског алгоритма и на технику генерисања MAC вредности, сваки мрежни уређај у WSN мора располагати криптографским кључем. Уколико се користи симетрична криптографија, потребно је мање ресурса, али је управљање кључевима знатно комплексније, док код асиметричне криптографије не постоји такав проблем, али

то захтева значајно ангажовање ресурса. Поређења ради, 64-битно шифровање RC5 алгоритмом на ATmega128 8MHz уређају траје 5,6ms, а генерисање 160-битног SHA1 отиска само 7,2ms, што је две стотине пута брже од извршавања стандардних алгоритама криптографије са јавним кључевима.

Поредећи алгоритме симетричне криптографије, блоковски алгоритми (енгл. Block Cipher) су знатно безбеднији у односу на стрим алгоритме (енгл. Stream Cipher), а обзиром да не захтевају више ресурса представљају добар избор креирање MAC-а. Поред симетричних криптографских алгоритама, за креирање MAC-а често се користе једносмерне криптографске функције. Ова техника се користи и у дигиталном потписивању докумената где се исти криптографски кључ користи за потписивање поруке, односно за аутентификацију извора и за верификацију поруке, HMAC (енгл. Hashed Message Authentication Code). Међутим употреба једносмерних функција не пружа довољан ниво безбедности, обзиром да је могуће пресрести комуникацију, изменити поруку и генерисати нови отисак поруке, због чега се добијена хеш вредност додатно шифрује неким употребом симетричних шифрарских система, или се употребљава асиметрични шифрарски систем. Такође, могуће је користити искључиво HMAC, али је тада потребно да сваки пар учесника у комуникацији поседује тајни дељени кључ који се додаје на почетак, или крај поруке. Овакав приступ такође има слабост јер потенцијални нападач може изменити отворени текст и без познавања тајног кључа. Већина једносмерних криптографских функција раде блоковски, најчешће над блоковима дужине 512 бита. Израчунавање се врши тако што излаз из једне рунде представља улаз у другу, а трансформације се врше познатим функцијама што омогућава потенцијалном нападачу да допише део отвореног текста и на њега да дода отисак криптографског кључа. Због тога се у пракси криптографски кључ меша са отвореним текстом, након чега се израчунава хеш вредност.

6.3.1 Систем за управљање кључевима

Тајност комуникације се обезбеђује употребом криптографских алгоритама и кључева, а обзиром да су претежно у употреби јавни алгоритми, тајност се заснива на тајном кључу због чега је битно да WSN располаже системом за тајну дистрибуцију кључева. Такав систем је потребно реализовати у складу са могућностима WSN и потребној брзини преноса, очекиваном броју грешака у каналу, очекиваном броју ресинхронизација, дозвољеним кашњењима због шифровања и криптографске синхронизације, броју очекиваних порука у јединици времена и слично. На основу односа између захтеваног нивоа заштите, комуникационих карактеристика и расположиве технологије, реализује се дизајн алгоритма за шифровање: имплементација комплексног алгоритма, дужина кључева, период важења кључева, број и избор кључева, њихова дистрибуција и протокол за брисање у случају опасности. Није пожељно деградирати квалитет пренете поруке, комуникационих карактеристика и не смеју се појављивати значајнија кашњења. Поред идентификације ентитета и аутентификације уређаја, потребно је онемогућити аутоматски прелазак у отворени режим рада и потребно је заштитити кључеве који се дистрибуирају, што некада подразумева и заштиту уређаја од компромитујућег електромагнетног зрачења, заштиту од отклапања уређаја и филтрирање сигнала за напајање и комуникацију.

Симетрични шифрарски системи подразумевају да сваки учесник у комуникацији има кључеве од свих осталих учесника са којима комуницира. Због тога је потребно обезбедити посебни дистрибуциони канал, односно посебни тајни канал. Иако ангажују релативно малу количину ресурса, што им је највећа предност, безбедност симетричних шифрарских система угрожава откривање једног кључа, или њихове групе. Откривање једног кључа деконспирише све поруке и других учесника, такође деконспирише и све поруке послате у претходном периоду. Са друге стране, системи са јавним кључевима своју безбедност реализују кроз једносмерне функције, међутим увек постоји бојазан да је могуће реализовати приступ употребом пречице јер не постоји математички доказ који би ту бојазан отклонио. WSN, зависно од намене, могу имати посебне уређаје (модуле) за шифровање, или се шифровање може реализовати унутар SN, CH, или BS. Без обзира на избор уређаја, потребно је реализовати функције пуњења кључевима, њиховог чувања и брисања.

Пуњење кључева се врши периодично, мора да буде брзо реализовано без отварања уређаја, поред тога мора се вршити међусобна идентификација пуњача и уређаја, а саме кључеве је потребно контролисати израчунавањем контролних сума. Чување кључева мора онемогућити њихову деконспирацију и мора трајати неко одређено време. Уколико се кључеви чувају у EEPROM (енгл. electrically erasable programmable read-only memory), или FLASH EPROM медијуму јављају се проблеми са брисањем, а ако се чувају у батеријски напајаном RAM (енгл. Random-access memory) медијуму, јављају се проблеми са старењем батерије. Уколико се изузме брисање кључева, односно замена кључева након истека периода важности, потребно је обезбедити брисање у случају опасности, затим у случају престанка напајања уређаја електричном енергијом, као што је потребно заштити уређај од ненамерног брисања кључева. Зависно до врсте шифроване комуникације: заштита везе (енгл. Link encryption), тачка-тачка (енгл. Point-to-point), или с краја на крај (енгл. End-to-end), потребно је другачије управљање кључевима. Заштита везе се односи на шифровање између две чворне тачке при чему се са сваку везу користи другачији кључ, што подразумева дистрибуцију кључева између крајњих тачака које остварују везу. Тачка-тачка шифровање подразумевају постојање различитих парова кључева за сваку деоницу, односно шифровање и дешифровање се реализује на транзитним тачкама. Заштићена комуникација с краја на крај подразумева шифровање на целом преносном путу при чему транзитне тачке не врше модификовање садржаја, а свака од крајњих чворних тачака поседује кључеве само за оне чворне тачке са којима је у комуникацији.

Највећи део WSN је пројектован тако да омогући динамичко умрежавање уређаја због чега је потребно да систем за управљање кључевима буде у складу са таквим карактеристикама. Поред тога, он мора бити оптимизован у складу са могућностима уређаја који чине WSN, што подразумева постизање максималних безбедносних карактеристика уз минимално ангажовање ресурса. Управо због малог ангажовања ресурса, већина протокола се не бави безбедносним проблемима, као на пример: LEACH (енгл. Low-Energy Adaptive Clustering Hierarchy), или TEEN (енгл. Threshold sensitive Energy Efficient sensor). Међутим када је тајност комуникације важна најчешћи сценарио обухвата заштиту која се заснива на симетричној криптографији и управљање кључевима које се заснива на инфраструктури јавних кључева. (Cui, et al., 2015)

Првобитни системи за насумично додељивање кључева су подразумевали повезивање парова мрежних уређаја на основу иницијалне алокације кључева пре постављања SN-а, затим креирањем дељеног кључа и одређивањем путање чиме је превазиђен проблем непредвидиве мрежне топологије, а створена могућност за креирање заштићене комуникације. Након тога је креиран низ протокола који су имали своје предности и недостатке. (MURUKESVAN, 2006)

6.3.2 SPINS

Безбедносни протокол за WSN, SPINS (енгл. Security Protocols for Sensor Networks) обједињује два модула: SNEP (енгл. Secure Network Encryption Protocol) који обезбеђује тајност комуникације између две чворне тачке и µTESLA (енгл. Timed, Efficient, Streaming, Loss-tolerant Authentication) која обезбеђуje broadcast аутентификацију изворне стране употребом симетричне криптографије, такође обезбеђује тајност комуникације, аутентичност и интегритет података, као и њихову актуелност.

Овај протокол многе од својих карактеристика остварује захваљујући бројачима који обезбеђују семантичку безбедност. Зависно од стања бројача отворени текст се шифрује различитим алгоритмима чиме се онемогућава диференцијална криптоанализа. Такође, он обезбеђује MAC аутентификацију уређаја у WSN, док се увид у актуелност података обезбеђује на основу стања бројача где новији подаци имају већу вредност бројача. Међутим овај алгоритам не предвиђа могућност да SN реагују на промене, већ стање бројача иницира комуникацију, уколико је бројач достигао највећу могућу вредност, предајна страна није у могућности да шаље податке до његовог постављања на почетну вредност, због чега је потребно да вредност бројача буде предефинисана тако да његово поновно постављање на почетну вредност не доведе до колизије података.

Овај протокол обезбеђује аутентификацију извора у broadcast комуникацији. Обзиром на уобичајене карактеристике уређаја у WSN често је непрактично успоставити PKI, тако да се симетрично шифровање и аутентификација уређаја ослања на дељене симетричне кључеве. µTESLA примењује асиметрични алгоритам који се заснива на одложеном обелодањивању симетричних кључева што омогућава аутентификацију корисника. Уланчавање кључева се реализује њиховим генерисањем једносмерним функцијама које реализује мрежни пролаз (енгл. gateway). Овим мрежни пролаз преузима улогу дистрибуционог центра за кључеве, KDC (енгл. Key Distribution Center), односно треће стране од поверења која је задужена за додељивање кључева сваком мрежном чвору. Поред тога, што сви чворови треба да буду временски синхронизовани са мрежним пролазом, како би било могуће откривање кључева приликом креирања рута, они морају да имају адекватне MAC вредности како би били успешно аутентификовани од стране мрежног пролаза и како би добили кључ.

6.3.3 LEAP

LEAP (енгл. Localized Encryption and Authentication Protocol) је креиран са циљем да реализује комуникацију различитих безбедносних карактеристика у оквиру исте WSN. Како би то било могуће, LEAP омогућава класификацију

криптографских кључева у четири различите групе: индивидуалне кључеве које деле мрежни чворови и мрежни пролаз, парове кључева које међусобно деле мрежни чворови, кључеве региона које деле мрежни чворови у оквиру истог дела мреже и групе кључева које распоређене између свих мрежних уређаја у WSN:

- Индивидуални кључеви омогућавају тајност комуникације између мрежног пролаза и конкретног мрежног чвора, а обзиром да сваки чвор има јединствени кључ, они омогућавају израчунавање MAC-а што омогућава аутентификацију која је потребна за реализацију комуникације и додељивање нових кључева.
- Упарени кључеви, такође омогућавају тајност и аутентификацију извора, а распоређени су тако да чворови преко којих се остварује веза деле исти тајни кључ.
- Кључ региона деле сви мрежни чворови истог региона.
- Групни кључ који деле сви чворови у мрежи и који користи мрежни пролаз како би се обратио свим чворовима у мрежи. Овакав приступ захтева релативно честе измене вредности кључа обзиром да компромитовање само једног чвора омогућава преузимање читаве мреже.

6.3.4 Локална broadcast аутентификација

Локална аутентификација чворова је погодна за креирање динамичких рута у WSN које су реализоване по принципу пасивног учешћа чворова у комуникацији, због чега је важно реализовати аутентификацију у оквиру broadcast комуникације. LEAP то реализује уз помоћ аутентификационог кључа који је везан за одређени чвор и који је познат само суседима тог чвора. Тај кључ, односно AUTH кључ се генерише уз помоћ једносмерних криптографских функција и представља саставни део поруке који се заједно са поруком шифрује на основу дељеног тајног кључа. На пријемној страни мрежни чвор упоређује вредност AUTH кључа и у зависности од његове актуелности, на основу листе кључева коју поседује, класификује предајну страну као успешно, или неуспешно аутентификовану. За разлику од broadcast атуентификационе шеме μTESLA протокола, LEAP обезбеђује тренутну аутентификацију. μTESLA није погодан за локалну broadcast аутентификацију обзиром да не предвиђа тренутну аутентификацију зато што сваки чвор треба да чека одређени предефинисани период пре него што прими MAC кључ како би извршио аутентификовање. Насупрот μTESLA протоколу, LEAP користи уланчавање кључева који су генерисани једносмерним функцијама што омогућава тренутну аутентификацију.

6.3.5 LiSP

LiSP (енгл. Lightweight Security Protocol) је предвиђен за велике WSN са скромним хардверским ресурсима. Шема је предвиђена за поделу мреже у мање целине, односно регионе са једним CH (engl. cluster head), што омогућава креирање хијерархијске топологије. Сваки од CH-а има улогу сервера који додељује кључеве, KS (енгл. key server). KS је окружен мрежним чворовима који

се понашају као клијенти. Хијерархија коју одређује LiSP разликује две врсте кључева: привремени кључ, TK (енгл. Temporal Key) који се користи за шифровање и дешифровање података и главни кључ, MK (енгл. Master Key) који је јединствен и карактеристичан за сваки SN и који се користи за unicast рутирање. Сваки MK се чува у хардверу SN.

6.3.6 Управљање привременим кључевима

KS је задужен за додељивање TK и за њихово повлачење. Обзиром да LiSP тајност обезбеђује симетричним шифровањем обе стране у комуникацији морају имати исти дељени кључ како би успешно реализовале шифровање и дешифровање, због чега сваки SN чува копију одговарајуће крупе TK-а. LiSP користи једносмерне функције за уланчавање кључева и тиме креира хијерархијску структуру, а KS управља TK кроз три основне функције. Прва је у вези са генерисањем иницијалних вредности нових кључева, IinitKey, друга UpdateKey, која је задужена за периодично broadcast обраћање свим члановима одређеног региона при чему их обавештава о новим вредностима кључева и трећој RequestKey уколико одређени чвор није успео да прими нове вредности TK у предвиђеном временском периоду, а за то пошаље захтев ка KS.

6.4 Примена асиметричне криптографије у WSN

Основна карактеристика асиметричних шифрарских система употреба парова кључева којим се шифрује, односно дешифрује отворени текст тако да кључ за шифровање може бити јаван, а само кључ за дешифровање мора да буде тајан. Овакав приступ елиминише један од највећих безбедносних проблема симетричне криптографије, проблем сигурне дистрибуције криптографских кључева. Асиметрични шифрарски системи обезбеђују ефикасну аутентификацију, интегритет порука, непорецивост, али се ретко користе за обезбеђивање тајности, због чега се употребљавају у комбинацији са симетричним шифрарским алгоритмима. Највећи недостатак асиметричних шифрарских система, са становишта WSN, је велика асимптотска сложеност. Јавни и приватни криптографски кључ су повезани једносмерним функцијама са замком (енгл. trapdoor one way function) што омогућава аутентификацију предајне стране на основу јавног кључа, а само пријемна страна са одговарајућим приватним кључем може да дешифрује поруку.

Најпознатији алгоритми који се користи у асиметричној криптографији су RSA, Rivest–Shamir–Adleman, који се због своје комплексности често се користи за шифровање малих количина података и за генерисање дигиталних потписа и DH, Diffie–Hellman алгоритам за размену криптографских кључева употребом јавних канала, односно небезбедних канала, који је један од првих алгоритама за размену кључева, који је због оптимизоване структуре и данас у широкој примени. Посебно значајан аспект асиметричне криптографије за реализацију безбедних WSN представља криптографија се ослања на генерисање кључа применом елиптичних кривих, ECC (енгл. Elliptic-Curve Cryptography). Највећа предност елиптичне криптографије је ефикасност реализације алгоритама и могућност употребе релативно малих целих бројева, због чега је нашла своју примену у системима са ограниченим ресурсима као што су WSN.

6.4.1 Имплементација асиметричне криптографије у WSN

Тајност комуникације, интегритет порука, аутентификација учесника и аутентичност порекла порука су циљеви које се могу постићи применом асиметричне криптографије у оквиру WSN, узимајући у обзир скормне хардверске ресурсе. Тајност се може обезбедити применом симетричних шифрарских алгоритама: RC5, RC6, Rijndael, MISTY1, KASUMI и други, размена кључева захваљујући асиметричним алгоритмима: RSA, ECC, или HECC, (енгл. Hyperelliptic Curve Cryptography), а аутентичност порука захваљујући једносмерним хеш функцијама: MD5, SHA-1, LOCHA и друге. Зависно од потребног нивоа безбедности пројектује се потребан хардвер и имплементира решење које се сматра оптималним. Реализација WSN веома ретко подразумева имплементацију RSA алгоритма, обзиром да ECC пружа еквивалентан ниво безбедности употребом мањих кључева, мањим ангажовањем меморије, мањом количином саобраћаја и уз мању компјутерску сложеност. ECC располаже алгоритмом за размену кључева ECDH (енгл. Elliptic Curve Diffie-Hellman) док дигитални потписи могу бити генерисани и верификовани на основу ECDSA (енгл. Elliptic Curve Digital Signature Algorithm). Уобичајена дужина кључа за RSA алгоритам износи 1024 бита (RSA-1024) и омогућава безбедносни ниво еквивалентан снази ECC алгоритма уз дужину кључа од 160 бита, (ECC-160). Након 2010 године, RSA безбедносне препоруке наводе да је препоручена дужина кључа 2048 бита што је у нивоу са 224-битним кључем примењеним у ECC.

Међусобну аутентификацију чворова на основу PKI у оквиру WSN је могуће реализовати тако што би се количина података за генерисање дигиталног сертификата смањила на неопходну меру. Стандард који дефинише формат дигиталних сертификата, X.509 подразумева обраду 700 бајтова за RSA-1024, а 530 бајтова за ECC-160, а како је за аутентификацију уређаја у WSN потребан само њихов идентификациони број, дигитални сертификат у случају RSA може бити редукован на 262 бајтова, а у случају ECC на 86 бајтова. Аутентификација на основу дигиталних сертификата, чак и у случају редукованих верзија захтева релативно велику количину меморије и релативно велику количину саобраћаја, међутим потпуна имплементација PKI у оквиру WSN представља најбезбедније решење и може пронаћи своје место у случају реализације мрежа са високим безбедносним захтевима и адекватним хардверским ресурсима.

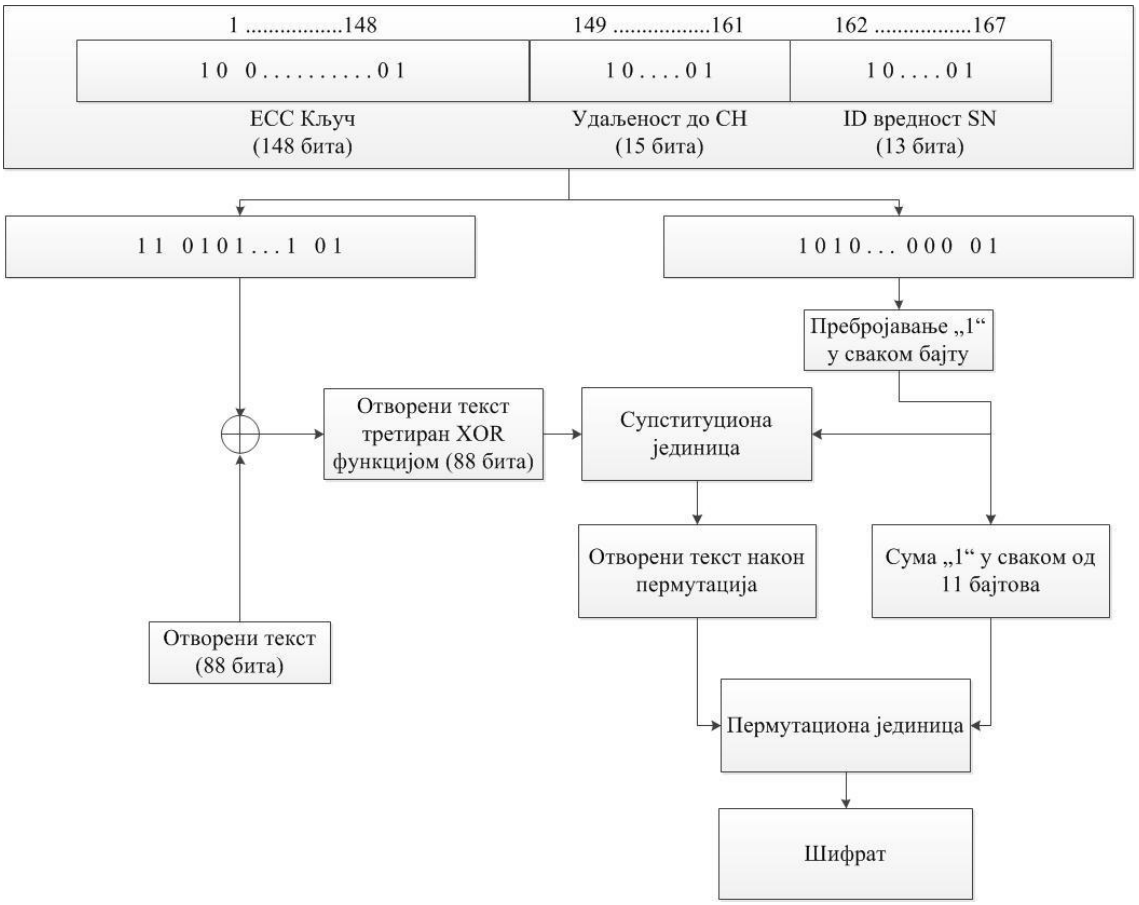
6.4.2 Асиметрична криптографија и GASONeC алгоритам

Једно комплетно криптографско решење за организацију WSN представља GASONeC алгоритам који обједињује асиметрични ECC шифрарски систем и хомоморфно шифровање који су подржани генеричким алгоритмом, GA (енгл. Genetic Algorithm) за динамичко креирање топологије мреже. GA дели мрежу у мање целине за које су задужени чворови који преузимају улогу CH. ECC се користи за размену приватних и јавних криптографских кључева, док се прилагођене, односно оптимизоване верзије дигиталних сертификата креирају на основу идентификационих бројева SN и њихове удаљености од CH. Како би се обезбедила уштеда електричне енергије, CH су задужени за агрегацију података који се чувају у облику шифрата. GA оптимизује поделу мреже на мање целине тако што испитује количину преостале енергије, прорачунава будуће енергетске

потребе и, у зависности од међусобне удаљености SN и BS и од броја чворова, динамички одређује који чвор ће преузети улогу CH чиме се настоји да се креира оптимална топологија WSN. (Elhoseny, et al., 2016)

Мрежна топологија се мења за сваки нови круг преноса у зависности од параметара чворова што подразумева њихову поновну аутентификацију и креирање новог криптографског кључа за сваки SN. Нови кључ чини 176 бита и укључује: 148 бита креираних од стране ECC алгоритма на основу ECC параметара који се налазе у меморији SN, од идентификационе вредности SN која је представљена уз помоћ 13 бита и од 15-битне вредности која представља удаљеност између SN и CH. Први део кључа се користи у процесу аутентификације између SN и BS, а у том процесу посредује CH тако што шаље ка BS хеширане ECC кључеве свих чланова дела мреже за коју је задужен док BS иницијализује дељени кључ за ту сесију који се генеришу SHA-2 једносмерном функцијом. Како би се креирао дељени јавни кључ, сваки SN бира псеудослучајни прост природан број, а како би вредност јавног кључа била довољно комплексна, изабрани број се множи вредношћу приватног кључа који се налази у меморији сваког SN.

Шифровање података се реализује кроз три различите операције: XOR, пермутацију и концентрацију. Отворени текст се конвертује у свој бинарни еквивалент и дели у блокове од 88 бита. Криптографски кључ дужине 176 бита се дели у два дела од којих се прва половина користи у логичкој XOR функцији са сваким улазним блоком отвореног текста, а у другој половини се броје бити са вредношћу „1“ за сваки од 11 бајтова како би се креирала вредност за процесе супституције и у 8 низова од 11 бита како би се креирала вредност за процес пермутације. Процес пермутације се реализује у зависности од броја битова са вредношћу „1“. Уколико је број јединица у првом бајту друге половине кључа n, места мењају битови који се налазе на местима n+1 и n+2 у првом бајту блока који је третиран XOP логичком функцијом. Процес се понавља за 11 пута за сваки бајт. Процес дифузије подразумева мешање низова од 8 бита након прва два процеса на основу броја јединица у 8 низова од 11 бајтова. Бајтови мењају своја места по истом принципу по ком се мењају места битима приликом пермутација у осам итерација. Уколико је број јединица у првих 11 бита m, своја места ће заменити бајтови са индексима m+1 и m+2. Овај процес се понавља осам пута са сваки следећи низ од 11 бита у оквиру сваког блока.



Слика 6 Процес шифровања GASONeC алгоритмом

Обзиром да су CH задужени за пријем, обраду и прослеђивање података они троше већу количину енергије у односу на остале мрежне чворове. Међутим, како би се умањила укупна потрошња енергије, CH су задужени за агрегацију података у облику шифрата при чему их не дешифрују. Обзиром да CH представљају безбедностно осетљива места, подаци који се ту чувају се додатно шифрују на основу хомоморфних шифрарских система. Хомоморфно шифровање омогућава додатно шифровање претходно генерисаног шифрата уз употребу произвољно комплексних функција које одговарају истим, или различитим функцијама којима је третиран основних текст у претходном поступку шифровања. Снага хомоморофног шифровања је у томе што се мрежни чворови са улогом CH не посматрају као страна од поверења у оквиру WSN, иако то заправо јесу, па као такви не треба да имају увид у садржај отвореног текста. Процес шифровања подразумева додавање 13 бита који представљају индекс сваког SN из ког је стигла порука ка CH што представља укупну величину поруке.

Процес дешифровања података се реализује у оквиру BS где се из сваке поруке издваја индекс SN-а. Обзиром да је у меморији BS сачуван индекс сваког SN, он пореди последњих 13 бита са вредностима сачуваним у табелама и реализује процес који је обрнут процесу хомоморофног шифровања порука. Одмах након издвајања шифрата започиње процес дешифровања. BS користи дељене тајне кључеве од сваког SN који су прослеђени од стране CH како би дешифровао пристигле поруке. BS дели шифрат у 176-битне блокове и сваки блок дели на два 88-битна дела након чега се одређује број бита са вредношћу „1“ у свих 11 бајтова и у свих 8 низова од 11 бита. Након тога се сваки блок трансформише у

одговарајући бинарни код и групише по редоследу за реализацију процеса дифузије који враћа распоред низова у стање пре реализације првог, истог таквог, процеса на предајној страни после чега се реализује процес пермутације који враћа шифрат у стање пре реализације првог процеса пермутације. На крају, BS претвара шифрат у отворени текст употребом НЕКСИЛИ (енгл. XNOR) логичке операције.

Табела 9 Упоредне карактеристике симетричних алгоритама

Алгоритам	MPU (циклуси)	Време (ms)	RAM (бајтови)	ROM (бајтови)
SkipJack	91224	12.353	292	7218
AES	68512	9.287	324	6994
LED	589652	78.972	378	5970
TWINE	128896	17.477	384	5280
BCC	91286	12.547	976	6240
Biswas	62396	8.547	542	5326
GASONeC	66201	8.619	281	3845

7. Закључак

Карактеристике WSN стварају бројне безбедносне ризике и отварају могућности за различите нападе који могу бити ефикасно предупређени различитим безбедносним механизмима. Протоколи за рутирање намењени WSN су дизајнирани тако да смање евентуалне утицаје сигурносних напада и да обезбеде несметано функционисање мреже уколико до њих дође. WSN се разликују по својој величини, конфигурацији и намени, па се протоколи бирају у зависности од карактеристика мреже, односно у зависности од процене безбедносних ризика и безбедносних циљева које је потребно остварити. Највећи број алгоритама користи лагане безбедносне механизме који претпостављају поделу мрежа на мање целине, хијерархијско уређење и mutipath рутирање. Идеалан протокол за рутирање би омогућио несметано функционисање мреже у ситуацијама када би она била изложена нападу без обзира на врсту, међутим ограничени хардверски ресурси и окружење које често није могуће надзирати представљају ограничења због којих је неопходно имплементирати решења која представљају компромис између ефикасности и безбедности. Сегментација и хијерархијско уређење WSN омогућава скалабилност мреже и продужавају њен животни век. Оптимално груписање мрежних чворова и ефикасно одређивање њихових улога подржава динамичку природу WSN, али не гарантује и сигурну мрежну структуру због чега је неопходна имплементација додатних безбедносних система.

Безбедне WSN подразумевају имплементацију система за аутентификацију мрежних чворова, система за обезбеђивање тајности комуникације, система за потврђивање интегритета порука и система за управљање криптографским кључевима. Аутентификацију ентитета у мрежи је могуће реализовати употребом протокола који идентификују мрежне чворове додељујући им јединствене називе. Из безбедносних разлога, идентификационе ознаке мрежних чворова је потребно шифровати неким од симетричних шифрарских алгоритама или/и употребом једносмерних хеш функција за генерисање отиска идентификатора мрежног чвора при чему се комуникационе путање креирају у зависности од успешности аутентификације. Тајност се постиже употребом симетричних шифрарских алгоритама обзиром да је за њихово извршавање потребно мање ресурса, док се за потврду интегритета порука користе технике упоређивања отисака порука креираних неком од хеш функција. Употреба симетричних шифрарских система усложњава управљање криптографским кључевима због чега се развијају решења која имплементирају асиметричне криптографске системе. Примена класичне асиметричне криптографије у WSN није довољно оптимизовано решење због оскудних хардверских ресурса који нису у могућности да изврше алгоритме за шифровање, односно за размену и генерисање криптографских кључева. Једно од решења које може бити имплементирано у WSN представља употреба алгоритама асиметричне криптографије који се ослањају на елиптичне криве.

Криптографија елиптичних кривих омогућава довољно висок ниво безбедности уз употребу криптографских кључева релативно мале дужине и могућност потпуне имплементације на релативно скромним хардверским платформама. Употребом асиметричне криптографије се отклањају сви недостаци парцијалних решења, при чему се рационално ангажују постојећи ресурси. Оваква решења обједињавају системе за аутентификацију ентитета, потврду интегритета порука и знатно поједностављују управљање криптографским кључевима, док се тајност комуникације обезбеђује употребом симетричне криптографије заснованој на тајним кључевима којима се управља захваљујући алгоритмима асиметричне

криптографије. Тајност података је могуће додатно повећати применом хомоморфног шифровања чиме се без значајног ангажовања ресурса добија комплекснији шифрат и смањује могућност реализације успешног напада на шифрат јер нападнути мрежни чвор не поседује податке за шифровање обзиром да није задужен за потпуно креирање шифрата. Избор симетричних шифрарских алгоритама, односно њихова комплексност зависи од хардверских потенцијала WSN, а најчешће су у употреби блоковски алгоритми чија се имплементација ослања на хардверску структуру мрежних уређаја.

Са становишта животног века WSN пресудну улогу има оптимизација процеса која обезбеђује уравнотежену потрошњу електричне енергије. Сви протоколи намењени оваквим мрежама обухватају алгоритме за оптималну потрошњу, међутим ни најбољи алгоритми не могу обезбедити неограничено дугачак животни век мреже. Једно од решења представља додавање уређаја који могу обезбедити допуњавање батерија мрежних уређаја. Обзиром на карактеристике WSN најбоље решење представља додавање бежичних пуњача у инфраструктуру WSN и имплементација алгоритама за контролу њиховог рада. Пуњачи могу имати перманентни извор напајања уколико то дозвољава окружење у ком се налази WSN, или могу бити предвиђени за допуњавање. Мануелно допуњавање оваквих уређаја локализује ову активност на релативно мали број мрежних уређаја, односно пуњача, док се посредством њих може обезбедити допуњавање великог броја осталих мрежних чворова. Ово је нарочито значајно уколико WSN чини велики број мрежних уређаја који су распоређени на великом подручју, или уколико се налазе у областима које нису лако доступне.

Литература

1. Alho, T., Hämäläinen, P., Hännikäinen, M. & Hämäläinen, T. D., 2007. *IEEE Computer Society.* [Online]
   Available at:
   https://www.computer.org/csdl/proceedings/date/2007/2/00/04211978.pdf
2. Al-Karaki, J. N. & Kamal, A. E., n.d. *Routing Techniques in Wireless Sensor Networks: A Survey*, Iowa: Iowa State University, Dept. of Electrical and Computer Engineering.
3. Biham, E. et al., 1999. Initial Observations on Skipjack: Cryptanalysis of Skipjack-3XOR. *SAC*, pp. 362-375.
4. Biham, E., Biryukov, A. & Shamir, A., 1999. Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. *EUROCRYPT*, pp. 12-23.
5. Chowdhury, A. R., Chatterjee, T. & DasBit, S., 2014. LOCHA: A Light-Weight One-way Cryptographic Hash Algorithm for Wireless Sensor Network. *Procedia Computer Science*, Volume 32, pp. 497-504.
6. Cui, B. et al., 2015. Enhanced Key Management Protocols for Wireless Sensor Networks. *Baojiang Cui et al.*
7. Dr. Shu Yinbiao, P. L. M. M. S. et al., 2016. *Internet of Things : Wireless Sensor Networks*, s.l.: IEC Market Strategy Board.
8. Elhoseny, M., Elminir, H., Riad, A. & Yuan, X., 2016. A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic encryption. *Journal of King Saud University – Computer and Information Sciences*, Volume 28, pp. 262-275.
9. Ganesan, P. et al., 2003. Analyzing and Modeling Encryption Overhead for Sensor Network Nodes. *WSNA.*
10. JINWALA, D. C., PATEL, D. R. & DASGUPTA, K. S., 2008. Investigating and Analyzing the Light-weight ciphers for Wireless Sensor Networks.
11. Kong, J. H., Ang, L.-M. & Seng, K. P., 2015. A comprehensive survey of modern symmetric cryptographic solutions. *Journal of Network and Computer Applications.*
12. Kong, J. H., Ang, L.-M. & Seng, K. P., 2015. A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments. *Journal of Network and Computer Applications*, Volume 49, pp. 15-50.
13. Law, Y. W., Doumen, J. & Hartel, P., 2008. *Survey and Benchmark of Block Ciphers for Wireless Sensor Networks*, Netherlands: University of Twente, Faculty of Electrical Engineering, Mathematics and Computer Science.
14. Lee, H., Lee, K. & Shin, Y., 2009. AES Implementation and Performance Evaluation on 8-bit Microcontrollers. *International Journal of Computer Science and Information Security*, 6(1), pp. 70-74.
15. Maheshbhai, L. A. & Wandra, K. H., 2014. Survey on Mobile Ad Hoc Network Routing Protocols. *International Journal of Computer Applications* , 101(12), pp. 28-33.
16. Milovanović, S., Pantelić, I. & Marković, M., 2014. Napadi na protokole rutiranja i sigurnosna rešenje u bežičnim senzorskim mrežama. *Naučni skup Mreža,* Tom VI, pp. 46-52.
17. MURUKESVAN, A., 2006. *Distributed Overlays in Wireless Sensor Networks*, Kista: KTH Information and Communication Technology.

18. N.Reka & M.Phil, 2015. Wireless Sensor Networks (WSN). *International Journal of Computer Science and Information Technologies*, 6(4), pp. 3706-3708.
19. Naika, S. & Shekokarb, d. N., 2015. Conservation of energy in wireless sensor network by preventing. *International Conference on Advanced Computing Technologies and Applications*, Volume 45, pp. 371-379.
20. Pearson, P. K., 1990. Fast Hashing of Variable-Length Text Strings. *Communications of the ACM*, 33(6), pp. 677-680.
21. Rehman, S. U. и други, 2012. Comparison Based Analysis of Different Cryptographic and Encryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN). *IJCSI International Journal of Computer Science Issues*, 9(1), pp. 96-101.
22. Rollins, S., 2008. *Data-centric Routing.* [Online] Available at: https://www.cs.usfca.edu/~srollins/courses/cs686-f08/web/notes/datacentric.html
23. Rovčanin, M., 2008. SMAC protokol u bežičnim senzorskim mrežama. *Telekomunikacioni forum TELFOR 2008*, Tom 16, pp. 894-897.
24. Schneier, B. et al., 1998. Twofsh: A 128-Bit Block Cipher.
25. Tepšić, D. M. & Veinović, M. Đ., 2015. KLASIFIKACIJA MANET PROTOKOLA RUTIRANJA. *VOJNOTEHNIČKI GLASNIK / MILITARY TECHNICAL COURIER*, LXIII(1), pp. 84-101.
26. Vidaković, D. & Vučetić, Z., 2005. Zaštita integriteta podataka u praksi. *Telfor*.
27. Zin, S. M., Anuar, N. B., Kiah, M. L. M. & Ahmedy, I., 2015. Survey of secure multipath routing protocols for WSNs. *Journal of Network and Computer Applications*, Volume 55, pp. 123-152.
28. Бојичић, С. & Милосављевић, В., 2014. Препоруке ТМ Форума за уговарање SLA у случају пружања IPTV услуге. *YU INFO 2014 - ОБЛАСТ ИНФОРМАЦИОНИ СИСТЕМИ*, 09-13 03, pp. 155-158.
29. Веиновић, П. д. М. & Јевремовић, м. А., 2008. *Увод у рачунарске мреже.* Београд: Универзитет "Сингидунум".
30. Милићевић, З., 2008. Мултимедијални H.264/AVC стандард у војним комуникационим системима. *XXVI Симпозијум о новим технологијама у поштанском и телекомуникационом саобраћају - PosTel 2008, Београд, 16. і 17. децембар 2008.*, 16 - 17 12.
31. Универзитет у Нишу, Електронски факултет, 2011. [На мжрежи] Available at: http://es.elfak.ni.ac.rs/rmif/Prenos-podatak-februar-2011/Pre.-pod-%202010/Pdf-2010/Pogl-03-Tehnike%20za%20pren%20%20pod%20(40-98).pdf
32. Универзитет у Нишу, Е. ф., 2011. *Prenos podatka – Tehnike za prenos podataka.* [Na mreži] Available at: http://es.elfak.ni.ac.rs/rmif/Prenos-podatak-februar-2011/Pre.-pod-%202010/Pdf-2010/Pogl-03-Tehnike%20za%20pren%20%20pod%20(40-98).pdf

Списак слика

Списак табела