DOI: 10.5937/voidelo1906222S

ВОЈНА ПРИМЕНА БЕЖИЧНИХ СЕНЗОРСКИХ МРЕЖА И ЊЕНИ СИГУРНОСНИ И БЕЗБЕДНОСНИ АСПЕКТИ

Милан Станојевић*
Министарство одбране Републике Србије
Ahmad Mohammed Salih
Higher Institute of Telecommunications, Iraq, Baghdad
Majid Alsadi
Noontech Company, Iraq, Baghdad

Употреба бежичних сензорских мрежа пружа поуздану слику у реалном времену и бољу оперативну слику. Она ће додатно помоћи да се побољша спремност трупа и смањи време реакције сопствених снага. Коришћењем прикупљених података може се планирати ефикасније управљање и распоређивање јединица. У случају цивилних апликација, критичне инфраструктуре као што су нафтна поља, рудници, електране, луке, аеродроми и сл., могу се заштитити од уљеза и нападача.

Кључне речи: *сензори, бежичне сензорске мреже, војна примена, надзор, оперативна слика бојишта, критичне инфраструктуре*

Увод

Бежична мрежа је технологија која се развија и постаје најбрже растућа технологија у 21. веку у области бежичних телекомуникација. Користећи ову технологију телекомуникационе мреже избегавају скупе процесе увођења каблова као медијума за повезивање између различитих типова опреме лоцираних на различитим локацијама. Овај тип мрежа се генерално имплементира и администрира помоћу радио комуникација. Уобичајене технологије које се користе у бежичним мрежама су: Bluetooth, Wi-Fi, WiMax и сл. Бежичне мреже играју важну улогу на пољу телекомуникација, међутим, опсег апликације бежичне мреже је огроман.

Савремене војне операције постају све комплексније, вишеструке и непредвидиве. Како технолошки капацитети националних војски, савеза и њихових противника напредују, већи је притисак на војне заповеднике да предвиде, процене и предузму адекватне мере у условима са све већим притиском проузрокованим ограниченим временским, људским и материјалним ресурсима. Такође, за сваког заповедник у процесу доношења одлуке, од круцијалног значаја су информације са бо-

* milan.stanojevic@mod.gov.rs

јишта, са територије или одређеног простора. Често у таквим ситуацијама се не располаже са довољно људских ресурса који би ту информацију прикупиле, обрадиле и доставиле у командни центар.

Нове технологије у настајању, као што су информационе мреже, подржавају војне операције тако што брзо и поуздано пружају критичне информације правом појединцу или организацији у право време, чиме се значајно побољшава ефикасност борбених операција. Нове мисије, настале и вођене данашњим светским догађајима, омогућавају технологијама да значајно утичу на војне операције. Те нове технологије морају се брзо интегрирати у свеобухватне доктрине и начине вођења борбених операција војске која жели да буде ефективна и ефикасна.

Глобални рат против тероризма карактерише лоше дефинисано и у стварности примењено – асиметрично ратовање. На пример, урбане операције су тешке за извођење и са потенцијално великим жртвама у људству и борбеној техници, због саме природе и динамичности урбане средине која не дозвољава сагледавање свих њених потенцијалних опасности на почетку саме операције. Без могућности да се урбани простор даљински истражи, људски животи су у опасности, што је неприхватљив недостатак оперативних и борбених способности једне јединице. Зато је потребан флексибилан и модуларан технички систем, да би се откриле претње и прикупили подаци у реалном времену за јединствену оперативну слику бојишта или урбане средине.

Крај „Хладног рата“ почетком деведесетих и стварност коју су изазвали драматични догађаји у свету у наредним деценијама довели су до померања фокуса војних операција на „операције које нису рат“ (*енг.* Operations Other Than War – OOTW) са нагласком на очување, стварање и изградњи мира. Правила ангажовања у вези са овим мисијама значајно су ограничавали опције које су биле доступне борбеним јединицама ангажованим на војним операцијама на урбаном терену. У ствари, већина реалности коју су искусили ови ратници имају више сличности са националном безбедношћу и противтерористичким операцијама него са традиционалним војним операцијама. Сходно томе, многи оперативни концепти су били заједнички за оба типа сценарија, као и захтеви за примењеним технологијама које би пружале информативну подршку извођењу самих борбених акција. Карактеристика употребе борбених јединица у XXI веку и сама одлика асиметричног ратовања је да употреба несразмерне и неограничене силе није могуће, а у урбаним срединама није ни прихватљива. На примеру ангажовања коалиционих и руских снага на ратиштима у Ираку, Авганистану и Сирији, могло се уочити да су услови у борби захтевали чишћење непријатељских урбаних подручја од блока до блока. Сам контекст ангажовања је био близак тзв. „Троструком блоковском рату“, где су ангажоване борбене снаге у једном тренутку, храниле и облачиле избеглице – пружали хуманитарну помоћ, да би у наредном тренутку, раздвајали зарађене стране – спроводећи мировну операцију. И коначно се борили у оружаној борби малог или средњег интензитета. Све то у истом дану, све то унутар једног града, унутар три градска блока [1]. Сложеност и величина бојишта, као и мешовитост руралних и урбаних средина унутар самих бојишта, имплицира потпуно свест и познавање ситуацији на истом. Када на све наведено додамо и чињеницу да се од противника очекује да боље разуме оперативно окружење, онда ангажовање борбених снага представља значајан ризик за живот и интегритет бораца. У таквим мисијама, мрежноцентрично ратовање које је потпомогнуто робусним сензорским умрежавањем

представља једно од најважнијих корака којим се смањује несигурност у борбеним и неборбеним ситуацијама, пружајући рано упозорење и праћење непредвиђених догађаја, као на пример упад у области које се сматрају штићеним и виталним за друштво и државу, или пак надзор над већ очишћеним теренима од непријатељских снага, чиме се ускраћује предност изненађења и обезбеђује правовременост реаговања.

Интеграцијом сензорских система, комуникацијских уређаја, актуатора и система контроле у постојећу војну инфраструктуру, војска може постати ефикаснија. Бежичне сензорске мреже су потенцијално решење овог проблема. Бежичне сензорске мреже (*скр.* БСМ, *енг.* Wireless sensor network – WSN) представљају скуп просторно дистрибуираних аутономних сензорских модула (чворова БСМ) којима се врши детекција и естимација различитих параметара околине [2]. Војна апликација бежичних сензорских мрежа показала се од значајног утицаја на војнике на бојишту. Кроз концепт „повезаног војника“, се непосредном заповеднику путем система комуникације омогућава приступ битним информација и оперативној слици бојишта кроз сензорску мрежу размештену у оперативном захвату јединице. На тај начин се пружа сигурност и обезбеђује успех мисије, а самом војнику на бојном пољу у сваком тренутку су на располагању правовремене и потпуне информације.

Иако су бежичне сензорске мреже првобитно замишљене за коришћење у војне сврхе, оне данас налазе широку примену у индустрији, осматрању и заштити животне средине, прецизној пољопривреди и другим областима. У свом раду ћемо се поред активне војне примене БСМ, осврнути на њихову примену и у другим безбедносним ситуацијама, као што је безбедносна заштита критичних инфраструктура, ванредни догађаји, хемијски акциденти, трагање и спасавање лица, природних катастрофа – поплава, пожара и невремена. За примене у којима је неопходно детектовати и реаговати на појаву критичне ситуације, БСМ треба опремити напредним функцијама у циљу поуздане и благовремене детекције критичних догађаја.

Ниво угрожености критичних инфраструктура од напада различитих терористичких, криминалних или активистичких група у протеклим годинама је значајно порастао. Појам “критична инфраструктура” није добио своју званичну дефиницију у Србији. Међутим консултујући позитивну светску праксу на том пољу можемо доћи до тога да се термин “критична инфраструктура” односи на средства и имовину која је неопходна за свакодневно функционисање друштвеног, економског, политичког и културног система једне државе [3]. Да би се постигао успех у једном тако захтевном подухвату неопходно је користити модерне информационе технологије.

У вези са тим, битан искорак у безбедносној заштити представља концепт интернет ствари (*енг.* Internet of Things – IoT) који повезује велики број електронских уређаја и дигиталних сензора у једну велику интерактивну мрежу дајући тако један велики помак у односу човека према Интернету[1], истовремено наглашавајући предности, али и изазове човечанства на пољу заштите критичних инфраструктура [4]. Основу развоја ове парадигме чине сензорске мреже, а као посебна категорија бежичне сензорске мреже са напредном анализом и фузијом података добијених од сензора [5].

[1] Када разматрамо концепт Интернета у примени бежичних сензорских мрежа, треба имати на уму да се у војним апликацијама може користити светска информациона мрежа, која користи комерцијалне или јавне мрежне уређаје, али исто тако се у већини случајева користи приватна (војна) информациона мрежа, која пак користи војне телекомуникационе преносне путеве и војне мрежне уређаје.

Бежичне сензорске мреже због својих карактеристика: агилности, самоорганизованости, скалабилности, мобилности, бидирекционој комуникацији, аутономији и великог броја разноврсних типова сензора представљају интелигентан информациони систем. Бежична сензорска мрежа се састоји од великог броја хомогених чворова, који се креће од пар стотина па до неколико хиљада. Бежичне сензорске мреже представљају дистрибуирани систем сензора различитог типа међусобно повезаних комуникационом мрежом у одређеном простору, формирајући на тај начин сензорска поља [6]. Сензори детектују физичке појаве у свом окружењу које у форми података деле кроз дистрибуиран систем комуникацијских чворова ради њихове процене. Задатак овакве мреже је да на основу података добијених са сензора издвоји највероватнију информацију о физичкој појави која се надгледа. Карактеристике оваквих система су способност да надзиру унутар и ван граница додељене зоне, како претње са земље тако и из ваздуха, а све у зависности од домета и нивоа осетљивости сензора.

Овај рад описује инжењерско решење за побољшање операционе слике на бојишту. Ова решења су заснована на основним тактичким концептима, изводљивим технологијама, концептуалним доктринама и способностима потребним за развој снага у операцијама у све три мисији. Овај рад пружа могућност за избор поузданог решења било да је у питању систематично или ad hoc постављена бежична сензорска мрежа, која узима у обзир хардверске и софтверске недостатке и у реалном времену повезује сензоре на терену са оперативном командом (или командним центром за надзор), преко интероперабилних чворишта уз употребу бежичне технологије. Такође, циљ овог рада је да понуди могуће решење за један сигурносни систем чија би улога била да спајајући модерне комуникационе технологије (бежичне сензорске мреже, интернет ствари и телекомуникације) са традиционалним захтевима, обезбеди заштиту критичних инфраструктура од потенцијалних претњи.

Могуће војне примене бежичних сензорских мрежа

Бежичне сензорске мреже имају различите примене као што су војна, цивилна и здравствена заштита, откривање шумских пожара, контролу инвентара, управљање енергијом, управљање процесима, надзор, научна истраживања и сл. Примена БСМ у војним операцијама и подршци су првенствено предодређене за управљање и препознавање на бојишту, односно да открију, препознају и прате суседне мете у свом окружењу. Овако употребљене мреже захтевају велику поузданост и интегритет у добијању прецизних података о непријатељу при чему морају бити енергетски ефикасне да би дале подршку дуговечност своје мисије на терену. Примена БСМ за управљање и надзор се обично користе да би се открили циљеви, као што су непријатељ или уљез на борбеном пољу или у тешко приступачној области. То је важно приликом додељивања задатака јединицама, дистрибуцији логистичких информација, обавештајних података и навођења сопствених снага.

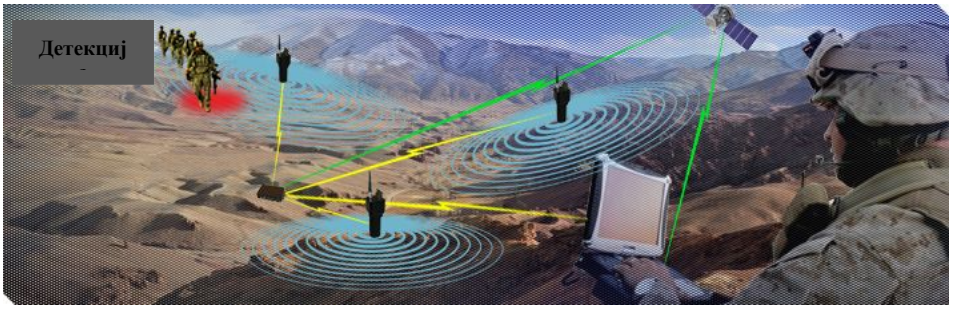
Војне комуникације, било којим средствима па и БСМ, морају бити заштићене у простору и времену где то околности налажу [7]. Војна примена БСМ битно је дефинисана могућностима сензора као основним елементом мреже. Сензори могу детектовати и евентуално мерити хемијске, биолошке и експлозивне паре, као и

постојање људи или објеката. У случају бојишта, урбаног ратовања и очувања снаге, коришћење БСМ може смањити сумњу у погледу тога где ће се непријатељске снаге распоредити или каква ће бити њихова улога. Такође бежичне сензорске мреже могу се користити од стране војске за низ циљева као што су контролисање и праћење непријатељских и милитантних активности у удаљеним областима (граница, удаљена складишта, објекти посебне намене) и заштита снага.

Начин размештаја великог броја сензора може бити плански и прецизан или насумичан (ad hoc) и мање прецизан. Плански размештај великог броја сензора би захтевао велико време и дуг временски период за постављање истих (лика 1). Стога се у том случају постављају сензори већег домета и дужег животног века, како би се надоместила величина простора који се надгледа.

Слика 1 – *Плански размештај сензора бежичне сензорске мреже*

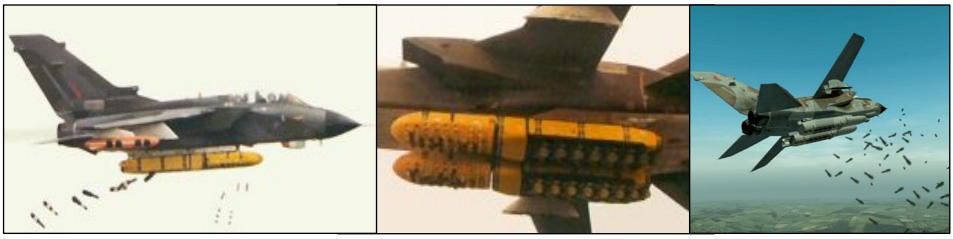
Овакви сензори могу бити георефернцирани приликом размештаја, чиме се постиже боље одређивање позиција самих циљева у надзираној области. Самим тим физичка величина и тежина сензора не морају бити главна ограничења. Ови уређаји су дизајнирани за имплементацију у релативно дугом периоду – од неколико дана па до пар година. Циљ је откривање покрета непријатељских возила и војника у удаљеним или неприступачним подручјима (слика 2).



Слика 2 – *Бежичне сензорске мреже пружају тактичким снагама решење за праћење угрожених тачака у изазовним окружењима*[2]

[2] Слика преузета са сајта: https://www.pinterest.com/pin/178666310200610115/

Насумичан распоред уобичајено подразумева размештај великог броја сензора у веома кратком временском периоду. У таквим случајевима цена коштања, величина, тежина, животни век и хардверске могућности сензора су значајно ограничене. У већини случајева, сензорски чворови могу бити испуштени или размештени употребом ракетних бацача, артиљеријских граната, ваздухоплова, беспилотних летелица, балона и сл. Употреба ватрених оруђа подразумева да такви сензори морају бити додатно ојачани услед великих сила напрезања. Употреба летелица за размештај („засејавање“) сензора подразумева коришћење подвесних контејнера – диспенсера (Слика 3) или подкалибарних контејнера (Слика 4).



Слика 3 – *Подвесни контејнери за размештај – „засејавање“*[3]

Слика 4 – *Подкалибарни контејнери за размештај – „засејавање“*[4]

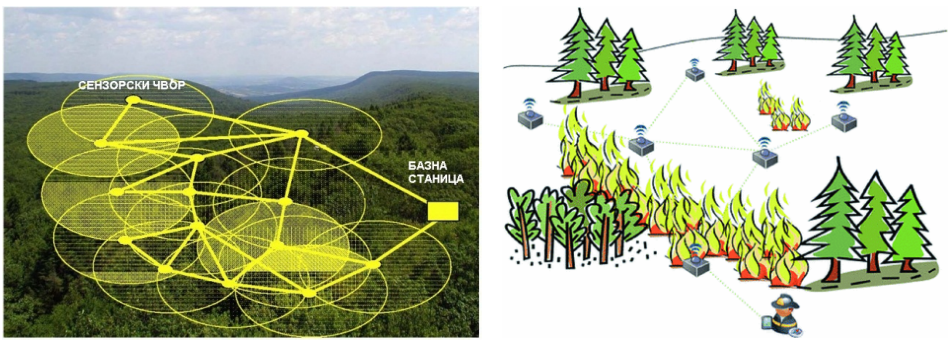
На овакав начин је могуће покрити велике површине бојишта или потенцијалне правце уласка уљеза у заштићену или надгледану зону. Време потребно за готовост за рад овако распоређене бежичне сензорске мреже је кратко и подразумева: време потребно за размештај, време потребно за побуду појединачних сензорских чворова, време потребно за повезивање појединачних чворова у потпуно функционалну мрежу. Овакав распоред војне бежичне сензорске мреже подразумева животни век у трајању од само неколико дана до неколико месеци.

[3] Слике преузете са сајтова https://www.pinterest.de/pin/379146862371116983/; http://craymond.no-ip.info/awk/twbomb2.html.

[4] Слике преузете са сајтова https://www.taringa.net/+imagenes/como-funcionan-las-bombas-de-racimo_hkh7h; https://defenceanalyzist.blogspot.com/2010/11/south-korea-to-integrate-textron.html?m=0; http://news.bbc.co.uk/2/hi/americas/2788573.stm.

Честа употреба бежичних сензорских мрежа је у заштити од ванредних ситуација. Постављањем бежичне сензорске мреже са сеизмичким сензорима могу се предупредити последице земљотреса, ерупције вулкана, клизишта или одрона. Један од најчешћих ванредних догађаја у последњим деценијама су шумски пожари, у којима бивају уништени милиони квадратних километара шума, често изгубљени људски животи и претрпљена велика материјална штета. Употреба бежичних сензорских мрежа је нарочито ефикасна у превенцији од шумских пожара, због чега је добила је на замаху последњих година.

Бежичне сензорске мреже размештене на великим шумским пространствима, често и ненасељеним, ће дати рани пожарни аларм у случају пожара у шуми или планинском подручју. Откривање такве ватре пре него што се прошири преко великог подручја је важно како би се избегли огромни губици и катастрофа. Бежичне мреже сензора се могу ефикасно користити у ту сврху. Мрежа сензорских чворова може бити размештена у шуми да би се открило када и где је пожар почео (Слика 5). Чворови могу бити опремљени сензорима за мерење температуре, влажности и гасова који се производе сагоревањем дрвећа или вегетације. Ако сензор открије пожар, он шаље алармну поруку (заједно са својом локацијом) на базну станицу. Због брзог развоја сензора, микропроцесора и мрежне технологије, омогућено је поуздан и аутоматизован надзор над шумским пожарима у реалном времену. Овакав систем реаговања у ванредним ситуацијама представља нови тип раног упозорења који користе бежичну сензорску мрежу за прикупљање информација о могућим шумским пожарима и деловима који су склони за шумске пожаре. Бежични сензорски чворови чине "паметну" мрежу надзора и контроле, који кроз непрекидну самоорганизацију сензорских чворова обезбеђује активан надзор над великом површином. Сталном комуникацијском везом са контролним центром преко мреже, постиже се даљинско управљање шумским пожарима. Бежичне сензорске мреже непрекидно процењују и анализирају информације о животној средини, као што су температура, влажност, звук, вибрације, присуство дима и слике зграда и шуме.



Слика 5 – *Архитектура бежичне сензорске мреже у превенцији шумских пожара*

Употреба БСМ налази своју широку примену у свакодневним војним пословима, па тако уз помоћ БСМ заповедници и команданти могу увек вршити мониторинг пријатељских снага, опреме и муниције, пратити статус војника, стање и доступност опреме и ватрене моћи на линији фронта. Мали сензори се додају сваком војнику, возилу, опреми и наоружању који непрекидно прате стање и очитане параметре и статус достављају непосредно одговорним заповедницима (Слика 6) [8].

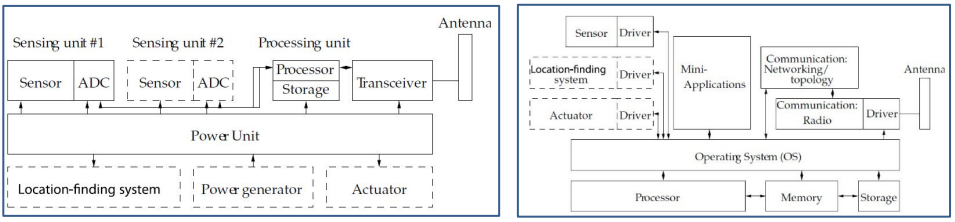
Слика 6 – *Широк спектар система и других "паметних ствари" ће комуницирати и сарађивати на бојном пољу [9]*

Анализа дизајна и карактеристика система

Сагледавајући комплексност задатка и начина употребе својих оперативних снага у испуњењу задатог циља требају се размотрити проблеми који ће се превазићи одговарајућом употребом бежичних сензорских мрежа. Свакако њихова употреба доприноси бољем разумевању слике бојишта и олакшавања функцију командовања и контроле. Напослетку тако добијене информације се процесирају и дистрибуирају другим учесницима. Ако би смо могли да групишемо војну примену бежичних сензорских мрежа онда би смо свакако могли да издвојимо три доминантна поља употребе и то: прикупљање података са бојишта; безбедносна заштита војних инфраструктура и подршка живљењу у њима; и логистика. Прикупљањем података са различитих војних платформи, као што су авиони, системи оружја, борбених возила или самих војника – војна организација може повећати ефикасност својих система интелигенције, надзора и извиђања. Овако прикупљене информације ће омогућити оружаним снагама да брже и прецизније идентификују кључне претње.

Да би један такав систем задовољио основне безбедносне услове, потребно је да заповедници у командном центру могу благовремено и адекватно да реагују на догађаје и инциденте изазване од потенцијалних претњи.

Бежична сензорска мрежа састоји се од великог броја малих и јефтиних сензорских чворова са минималном рачунарском снагом и потрошњом енергије. На Слици 7 приказана је генерална архитектура сензорског чвора БСМ.



Слика 7 – *Хардверске и софтверске компоненте сензорског чвора БСМ*

Главни циљ мреже је да ослушкује, осећа, делује и шаље информације из своје околине ка јединици за прикупљање података – чворишту података (енг. Data Sink), која их обрађује [10]. Мултидимензионалне претње и појаве кроз које се они манифестују наглашавају употребу разноврсних сензора за потпуну детекцију догађаја. Систем мора бити аутономан и без потребе за претераним одржавањем и присуством техничког особља. У случајевима када се систем користи у безбедносној заштити инфраструктуре, тада он може бити независан и у том погледу може се гледати као потпуно независан и изолован систем, на чији рад не утиче функционисање саме критичне инфраструктуре [11]. Да би извршавао своју основну безбедносну функцију неминовно се намеће услов да овакав систем мора бити сигуран. Интегритет и поузданост бежичне сензорске мреже размештена у условима изузетно густог РФ окружење на бојишту са бројним системима који се ослањају на РФ везе за комуникацију, навигацију, као и пренос података и видеа за реалну операцијску слику бојишта, услед „непријатељске“ или чак „пријатељске“ интерференције може бити озбиљно угрожена. Откривањем „пријатељских“ извора сметњи, њиховом елиминацијом или ублажавањем утицаја на рад БСМ може се поузданост саме мреже довести у прописане параметре. Међутим ако је извор сметњи непријатељске природе, тада систем мора поседовати способност да се том облику напада супротстави различитим контрамерама. Аутономан рад система без надзора техничког особља отвара могућности за напад на систем, попут тамперовања, физичке манипулације и компромитовања сензорских чворова.

У циљу постизања основне функције бежичне сензорске мреже за потребе војне примене, потребно је у њега уградити јединствен безбедносни концепт, који се састоји од безбедне комуникације унутар саме мреже, механизма који ће обезбедити функционалну сигурност у току рада и самозаштитну функцију. Идеја је да систем своју основну функцију дефинише кроз три основна задатка, а то су: (1) да изврши детекцију, (2) да оствари локализацију и (3) да обезбеди класификацију објекта претње у надгледаној зони [6], [12]. Систем треба да обезбеди такву осетљивост и дискриминативност сензора, како би могао правовремено да обавести о потенцијалној претњи и обезбеди реакцију корисника на настале промене у надгледаној области.

Због ограниченог приступа енергетском напајању, енергетска ефикасност мреже мора бити пажљиво испланирана како у хардверском, тако и у софтверском дизајну. Ово је нарочито важно ако се има у виду да сензорски уређаји унутар мрежа треба да поседује способност међусобне комуникације 24 часа, 7 дана у недељи.

У БСМ сваки сензорски чвор има ограничен сензорски опсег r_s и ограничени домет комуникације r_c. Скуп свих сензорских опсега свих сензорских чворова сматра се сензорском покривеношћу читаве мреже, што имплицира колико добро је неко подручје сензорски покривено. Поред тога, одржавање повезаности сензорских чворова БСМ је такође важно, јер се прикупљени подаци са сензора морају послати у командни центар. Претпоставља се да сваки сензор има ограничен домет комуникације r_c, који обично може бити различит од опсега сензора r_s[5].

Систем мора да прикаже могућност креирања интелигентног система за надзор који може да ради у свим временским условима. Дизајн система треба да је такав да може да надзире и област иза границе надгледане зоне, како би правовремено и адекватно реаговао на земаљске и ваздушне претње. Систем мора донети праву одлуку нпр. да ли у сензорском пољу има људских бића. Током овог процеса детектовања присуства, систем не сме да неживе предмете региструје као живе. У сценарију, ако су непријатељски војници авионом десантирани на сопствену територију, велика је вероватноћа да ће се у циљу заштите сопствених снага или обмане непријатељ користити и лутке. У том случају систем не сме да их замени за војнике, јер би то било озбиљно питање поузданости. Систем треба да има низак ниво лажних аларма (нпр. због животиња или других не ризичних догађаја) у комбинацији са високом осетљивошћу детектора претњи. Једна од важних особина система мора бити дискриминативност, како би број непријатељских војника који су ушли у надгледану зону био тачно идентификован, што има тактички значај за сопствене борбене јединице које треба да донесу адекватне одлуке.

Могућност система да изврши лоцирање циљева је веома важно за изненадне нападе на непријатеља, тако да га можемо довести у ситуацију, без идеје шта да учини. У неком сценарију лоцирање циља је веома важно, тако да можемо елиминисати претњу са индиректним елементима као што су минобацачи, артиљеријске гранате или вођене ракете.

Правац кретања непријатељских јединица или уљеза временом се може променити, због чега се он мора стално проверавати тј. пратити. Процес праћења је сличан процесу лоцирања, али се он мора стално понављати у дугом временском периоду. Такође сам процес мора имати елементе интелигенције, како би у одређеном периоду времена предвиђао будућу локацију циља. Сопствене снаге у том случају морају бити стално ажуриране најновијим информацијама, како би се одржала реална оперативна слика ситуације на терену.

Физичке одлике система су да се у већини случајева сензорски чворови ручно размештају и превозе на терен возилима или у ранцима војника, што значи да сензор мора бити мали по величини и тежини [13]. У неким случајевима сензори могу бити испуштени из ваздуха помоћу авиона или беспилотних летелица, што изискује да сензорски чвор мора бити физички ојачан како би остао неоштећен приликом пада на земљу.

[5] На пример, опсег комуникације платформе Extreme Scale Mote је око 30 m, док је опсег осетљивости акустичког сензора за детекцију возила око 55 m.

Самоорганизовање је основна одлика бежичних сензорских мрежа и поступак који се непрекидно одвија у БСМ. Наиме размештени сензорски чворови морају идентификовати свој пријатељски сензорски чвор у оквиру свог радио домета како би кроз бежичну комуникацијску мрежу извршили пренос података до базне станице и командног центра користећи технике вишеструког скакања (*енг.* multi-hop). Техником вишеструког скакања сензорски чворови чувају преко потребну енергију и велике дистанце до базне станице преваљују кооперативним комуницирањем више сензорских чворова у низу. Једном постављени сензорски чворови требају да буду статични, јер приликом сваког померања чвора он мора да реконфигурише своју комуникацијску везу са чворовима у окружењу и мрежом уопште.

Током раних фаза концепта БСМ технологија, ток података, посебно у периоду прве генерације БСМ, је био једносмеран и таква врста комуникација је била сасвим довољна. Међутим, напредак технологије нас је довео у нову фазу, другу генерацију сензорских мреже где у неким ситуацијама командант мора преузети контролу над сензорским чвором за шта су нам потребне дуплекс комуникационе везе, како би се нпр. управљало електро-оптичким сензорима као што су камере или актуаторима [14].

Покривеност одређеног простора и величина БСМ у директној је вези са бројем размештених сензорских чворова. Општеприхваћени стандарди за војне бежичне сензорске мреже је да су домети њихових сензора значајно већи, а број размештених сензора сразмеран је важности задатка који та мрежа треба да испуни. Мрежа мора имати својство робусности, самоизлечења и самоконфигурисање.

Неке операције трају недељама, а неке чак и месецима. У таквом случају, животни век БСМ мора да буде довољно дуг како би омогућио прикупљање информација о оперативној слици бојишта, а то се посебно односи на оне које се налази у непријатељском окружењу. Ако је БСМ постављена за заштиту границе, оперативних праваца, критичних инфраструктура и стратешких локација, треба размотрити употребу БСМ којима је могуће заменити извор напајања како би се додатно продужио животни век БСМ. У неким режимима сензорски чворови не треба да функционишу у пуном капацитету и непрекидно. За ту потребу се користе алгоритми за планско ангажовање одређених сензорских чворова БСМ, који одређене сензоре држе у хибернацији, стању приправности или потпуној спремности за рад. Циљ је уштедети више енергије и тиме продужити живот БСМ.

Употреба БСМ на сопственом терену, а нарочито на непријатељској територији подразумева да је она невидљива за људске очи. Међутим, данас невидљивост не подразумева само бити невидљив у видном делу спектра. Невидљивост (*енг.* Stealthy characteristics) подразумева одсуство било какве емисионе карактеристике и то одсуство: електронског, електромагнетног или термални потписа. У ту сврху размештени чворови морају емитовати у веома широком опсегу (*енг.* Ultra Wide Band-UWB), како би имали веома мали електронски потпис. Предност оваквог система је: мала интерференција са тренутним ускопојасним и широкопојасним радио-системима, велики капацитет канала, рад испод нивоа шума, мала предајна снага, отпорност на ометање, високе перформансе у каналима са вишеструким простирањем и једноставна архитектура примопредајника.

Сигурност и поузданост БСМ су функционални елементи који имају веома висок степен разматрања у дизајну било које, а нарочито војне БСМ. Ово нарочито има велику важност када прикупљени подаци морају бити поуздани за команданта да

донесе одлуку у делићу секунде. Мрежа мора да обезбеди неопходну безбедност да би се избегло прислушкивање, ометање и пресретање. У случају било каквог напада на сензорске чворове, они морају бити способни да обавесте командни центар о нарушеном интегритету неким резервним каналом. Сваки сензорски чвор треба да има у себи уграђен механизам за контролу неовлаштеног приступа, јер сваки појединачни податак који се налази у њему може довести до отицања поверљивих података и нарушавања националне безбедности, ако дође у руке друге стране.

Један од одлучујућих фактора за примену БСМ у реалном времену је укупни трошак система у смислу имплементације и одржавања. Дакле, овај фактор се мора узети у обзир пре, током и након развоја дизајна БСМ за примену у специфичним војним условима.

Све наведене карактеристике система треба да буду обједињене и као такве да представљају безбедносни концепт који треба да гарантује поверљивост, интегритет и доступност система у сваком тренутку [15]. Једино на такав начин мрежа ће бити безбедна, флексибилна и употребљива да у датој ситуацији, одговори на захтеване услове рада [16]. Поред могућности креирања извештаја и бележења догађаја (инцидената), систем треба да омогући захтеваној страни да врши надзор над активностима у мрежи, конфигурисање и управљање из јединственог командног центра. Нарочито, систем треба да пружи подршку безбедносним структурама да правовремено детектује и одговори на претње и упаде у раним фазама, како би се осујетио елеменат изненађења од стране непријатеља.

Модел сигурне бежичне сензорске мреже

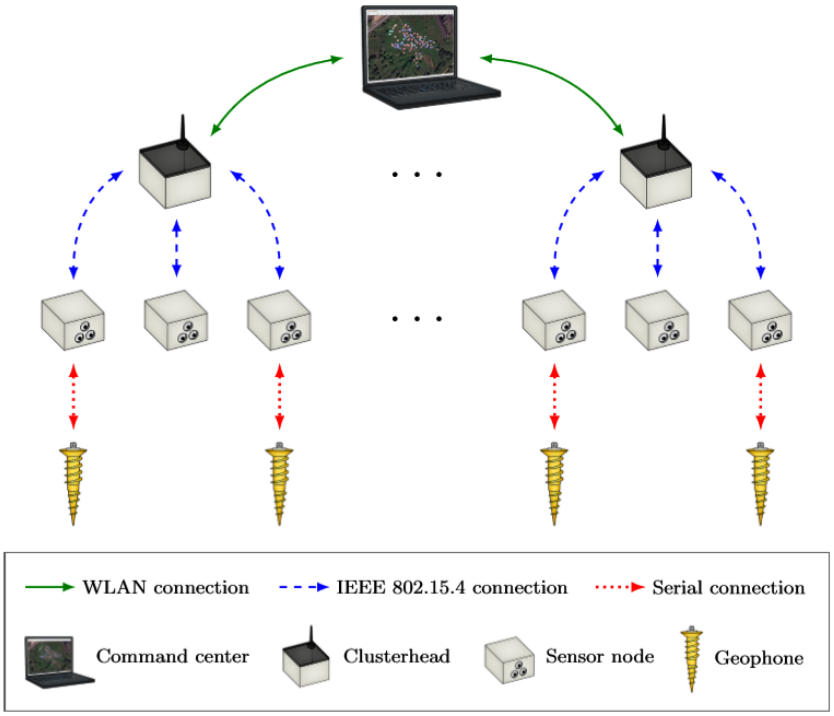
Топологија бежичне сензорске мреже је хијерархијски уређена и динамички самоорганизована мрежа равноправних чворова (*енг.* Nodes). На њих су повезани различите врсте сензора, који на тај начин формирају јединствени сензорски чвор (*енг.* Sensor Node – SN). Овакви чворови хијерархијски су организовани у скупове или групе вишег нивоа који се називају кластери (*енг.* Cluster), где се у оквиру кластера бира један чвор који ће имати улогу вође, тзв. вођа кластера (*енг.* Cluster Head – CH). Он регионално повезује више сензорских чворова и понаша се као базна станица (*енг.* Data Sink/BS). У оквиру планиране бежичне сензорске мреже и самих кластера међусобна комуникација чворови (*енг.* peer-to-peer) се своди на неопходни минимум. Циљ оваквог ограничења је да се радио комуникација и пренос података врши унапред дефинисаним путањама, како би се очувала енергетска ефикасност мреже. Поред тога, потребно је да мрежа користити енергетски ефикасну модулацију за комуникацију са сензорским чворовима и да су чворови у стању да подрже режим са смањеном потрошњом [15].

Основни дизајн система би био такав да више вођа кластера (CH) буду увезани са командним центром (*енг.* Command Center – C), где би основна функција центра била да прикупља податке од сензорских чворова (SN). Вође кластера би имали улогу да управљају и обједињавају информацијама у процесу преноса података од сензорских чворова ка командном центру [5] [6] [10] [17]. Сензорски чворови могу бити опремљени различитом комбинацијом сензора приказаним у табели 1. Намена оваквих сензора је пре свега детекција људи, возила и предмета, а управо је то оно што би овакав систем требао да детектује.

Табела 1 – *Типови сензора [6]*

Тип сензора	Намена
AMR	Феромагнетни сензор
Акцелерометар	Сензор брзине и убрзања
Singl-PIR	Сензор покрета
Multi-PIR	Вишеструки сензор покрета
Longrange-PIR	Сензор покрета за детекцију на великим удаљеностима
Геофон	Сензор вибрација (сеизмички)
ГПС	Сензор позиције

Хардвер бежичне сензорске мреже



Слика 8 – *Дизајн уопштеног система бежичне сензорске мреже [6]*

Као што је приказано на Слици 8 бежична сензорска мрежа би била организована у три хијерархијска нивоа:

– командни центар,
– вође кластера и
– сензорска чворишта.

Командни центар

Намена командног центра (C) је да прикупља податке од вођа кластера (CH) и приказује информације кориснику. Информације добијене од сензорских чворова се преко вођа кластера уз помоћ алгоритма за детекцију достављају софтверу за визуелизацију мреже. Намена софтвера је да обједињава све вредности добијене од сензорске мреже, врши графички приказ сензорске мреже и статуса њених елемента, управља сензорском мрежом на основном нивоу. На тај начин коришћењем софтвера може се рестартовати чвор, послати порука одређеном броју чворова или пак извршити репрограмирање чворова.

Вођа кластера (ClusterHead)

Сваки вођа кластера (CH) би се састоји од два дела:

– уграђене мини-PC плоче (процесор треба да буде енергетски ефикасан, са одређеном RAM и ROM меморијом) и

– хардвера сензорског чвора.

Улога мини-PC плоче је да одржава WiFi комуникацију са командним центром (C), обавља претходну обраду података прикупљених од сензора и да изводи одређене задатке на мрежи.

Улога хардвера сензорског чвора је да комуницира са осталим сензорским чворовима у нижој хијерархији. Он поседује свој централни модул (*енг.* Core Module), мрежни пролаз (*енг.* Gatway Module) са могућношћу повезивања на мини-PC и ГПС модул за временску синхронизацију.

Сензорски чвор

У зависности од намене БСМ и у зависности од облика и својства надгледане зоне у употреби би се налазиле различите конфигурације сензорских чворова (CH) који се разликују према врсти повезаних сензора. У јединственом кућишту били би смештени различити модули хардверске платформе сензорске мреже. Централни модул поседује контролер који треба да има довољне капацитете ROM, RAM и Flash меморије за инструкције и податке, као и радио интерфејс компатибилан са IEEE 802.15.4 стандардом на фреквенцији 2.4 GHz са 16 различитих радио канала, са брзином преноса од 250 kB/s и AES енкрипцијом [18]. Поред тога централни модул би поседовао ултра стабилни real-time часовник (*енг.* Real time clock – RTC) са максималним 6 ppm, регулатором напона и великом палетом конектора за спајање са сензорима [6]. Употреба акцелерометра унутар сваког кућишта сензорског чвора је обавезна, са основном улогом да региструју сваку могућност тамперовања, тј. отварања кућишта сензорског чвора.

Сензори

Сензорска мрежа би подразумевала имплементацију четири врсте сензора претходно наведене у овом раду, који би морали бити прилагођени за посебну намену. Први тип сензора би био пасивни инфрацрвени сензор (*енг.* passive infrared –

PIR), који би имао своје три различите верзије у зависности од захтеваних карактеристика. Верзије сензора су:

– једноструки PIR (singl-PIR), са могућношћу детекције до 10 метара,

– вишеструки PIR (multi-PIR), са више појединачних PIR сензора различитих карактеристика са могућношћу детекције до 5 метара и

– PIR сензор великог домета (long-range – PIR) са могућношћу детекције до 50 метара.

Употреба појединих врста сензора има специфичну намену и улогу, па тако multi-PIR сензори имају за циљ да дају податке на основу којих би се извршила процена о правцу кретања објекта, док употреба long range-PIR сензора има за циљ да детектује објекте који се крећу тик уз надгледану зону и евентуално сваки његов улазак у зону. Други тип сензора за детекцију би био геофон (*енг. Geophone*) као на Слици 9 [19].

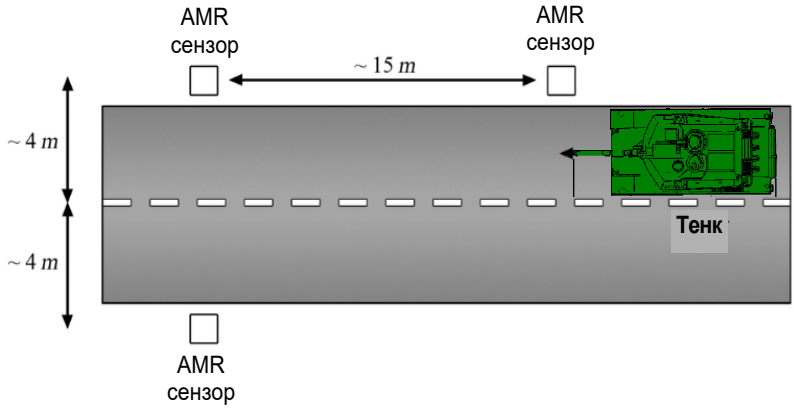
Слика 9 – *Сензор за детекцију вибрација – геофон*

Намена геофонских сензора је детекција сеизмичких покрета и вибрација које се преносе кроз тло. У овом конкретном случају њихова намена би била да детектује подрхтавање тла услед кретања објекта (животиње, човека, возила, тенка и сл.) као на Слици 10.

Слика 10 – *Детекција човека и возила геофоном*

Конкретан модел се састоји од три сензорске капсуле које су смештене у водоотпорно кућиште, са циљем детекције вибрација у све три осе. Сензорске капсуле су преко А/Д конвертора, спојене на микропроцесорску јединицу. Комплетно кућиште је спојено на сензорско чвориште преко комуникацијског и напојног кабла.

За потребе детекције металних објеката, користио би се феромагнетни или AMR (енг. Anisotropic-magneto-resistive – AMR) сензори [20]. Овакви сензори се користе за потребе класификације објекта, а мање за детекције истог. Наиме због своје енергетске неекономичности (просечна потрошња 20-25 mA) овакви сензори се користе у комбинацији са PIR сензорима, где се укључују по потреби, као што је приказано на Слици 11 [6].



Слика 11 – *Употреба AMR сензора у комбинацији са PIR сензором [6]*

Последњи сензор је акцелерометар, који би био саставни део сваког сензорског чворишта. Његова основна намена је да детектује и најмање покрете, због чега се користи у физичкој заштити само сензорског чвора од могуће тамперовања [21]. Оваква структура једног вишефункцијског сензорског чвора може дизајном бити прилагођена за амбијент у којем ће се користити, а нарочито ако је та средина непријатељска. Сензорски чвор је могуће маскирати у елементе окружења као што је то приказано на Слици 12.

Слика 12 – *Бежични сензорски чворови маскирани у елементе у окружењу (камен)*

Софтвер бежичне сензорске мреже

Софтверска архитектура идејног модела бежичне сензорске мреже састоји се од: (1) хијерархијске комуникацијске структуре, (2) безбедносне структуре и (3) алгоритма за детекцију, локализацију и класификацију [22].

Хијерархијска комуникацијска структура

Хијерархијска комуникацијска структура обезбеђује скалабилност мреже [10] [15] [23] [24] [25]. Сама мрежа, као што смо раније рекли, састоји се од командног центра, вођа кластера (спој mini-PC и сензорског чвора) и сензорских чворова увезаних на вође кластера. Као што је то приказано на Слици 8, комуникација између командног центра и вођа кластера се одвија преко стандардног TCP/IP протокола путем WiFi мреже, док се комуникација у самој сензорској мрежи базира на енергетски ефикасном IEEE 802.15.4 стандарду. Замисао је да сензорски чворови очитане вредности прослеђују вођама кластера, где се врши претходна обрада очитаних вредности, а онда се прослеђују командном центру где се они спајају, обрађују, визуализују и презентују оператеру [6] [26] [27] [28]. Такође постоји проток података од командног центра ка нижим хијерархијским уређајима у облику конфигурацијских инструкција, захтева за репрограмирањем сензорских чворова или пак команди за ресетовање чвора [26] [29]. Да би вођа кластера и сензорски чворови започели комуникацију, прво вођа шаље захтев за идентификацијом (*енг.* heartbeat message) свим чворовима. Након провере идентитета и валидности вође, сензорски чвор одговара са поруком где у једном биту исказује свој статус, а у другом квалитет везе између учесника. Вођа такође утврђује идентитет и валидност сензорског чвора, након чега шаље поруку потврде (*енг.* cluster advertisement message) и поруку о времену сензорском чвору. Након тога је комуникација сензорске мреже успостављена, где су све поруке које се размењују заштићене.

Безбедносна функционалност

Безбедносна функционалност треба да обезбеди:
– комуникацијску безбедност и
– функционалну сигурност система.

Комуникацијском безбедношћу се гарантује потребан ниво заштите системских операција, док се функционалном сигурношћу гарантује детекција отказа у хардверу система. Иако стандард IEEE 802.15.4 пружа могућност неколико безбедносних опција, њих не користимо из два главна разлога. Први разлог је тај што се као додатна заштита безбедносни протоколи требају држати одвојено од основних комуникацијских протокола. Самим тим се и систем чини жилавијим и отпорнијим на нападе. Други разлог је тај што се безбедносне заштите понуђене у оквиру IEEE 802.15.4 стандарда не сматрају довољно безбедним за примену у оквиру предложеног сценарија. Идејно решење за комуникацијску безбедност је да се у оквиру система интегришу безбедносне функције које ће моћи да детектују било какву повреду интегритета система. Комуникацијска безбедност је зами-

шљена кроз два нивоа заштите, где истичемо ниво адаптивно фреквенцијског скакања (АФС) и безбедносна заштита. Оба начина заштите су независна један од другог током процеса прикупљања података и њихове процене. Ниво AFS подразумева адаптивно фреквенцијско скакање, временску синхронизацију, управљање тренутно расположивим комуникационим каналима и процедуре за иницирање заједничке сесије између чвора и кластера [30]. Циљ безбедносне заштите је да се постигне поверљивост, интегритет и доступност. Да би се поруке заштитиле од кривотворења и манипулације, врши се шифровање корисне информације AES кодирањем, који је доступан у оквиру крипто копроцесора, доступног у свим сензорским чворовима. Процес шифровања је веома брз и енергетски ефикасан. Циљ свега је да постигне отпорност система на нападе. Напомињемо да је комуникација између вођа кластера и командног центра реализована путем стандарда IEEE 802.11g WiFi која у оквиру својих безбедносних функција нуди WPA2 енкрипцију, која се сматра и више него довољном за заштиту података у бежичној сензорској мрежи [31].

Функционална сигурност бежичне сензорске кључно се односи на физички интегритет и целовитост чворова, као и њихових сензора. Константним надзором мреже и њених делова постигла би се детекција тренутних и сталних грешака и отказа компонената. Када се грешке уоче, онда се са њима може управљати и самим тим постићи сигурније стање сензорске мреже. Поузданост мреже је веома битна у процесу детекције претњи. Не детектована претња услед отказа сензора или дела система, може створити рупе у надгледаној зони. Због тога се у систем уграђују функционалне сигурносне мере како би се откриле грешке у функционисању и предузеле мере да се обезбеди правилно функционисање система. Неке од мера које систем периодично обавља су:

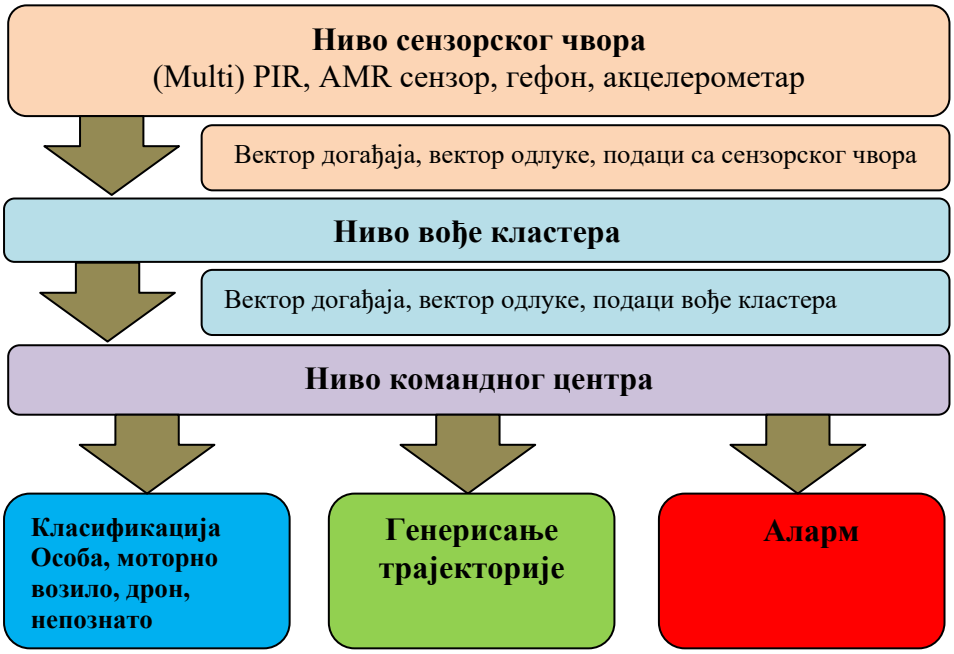
– провера интегритета меморија (RAM, ROM, Flash меморије),
– провера кода уписаног у меморији са оригиналним кодом,
– провера CPU (ради се по потреби због велике потрошње енергије),
– провера сензора на делимични или потпуни отказ и
– логовање очитаних грешака у командном центру.

Након завршених провера корисник у командном центру може да сагледа исправност мреже и да по потреби реагује на такво стање. У случајевима отказа први корак је поновно конфигурисање мреже тако да суседни елементи мреже преузму део функција, а ако отказ уређаја битно утиче на безбедност, одмах се приступа замени неисправног исправним уређајем [6] [32].

Алгоритам за детекцију, локализацију и класификацију

Захтеване особине бежичне сензорске мреже у дуготрајним условима надзора су робусност и поузданост. Због тога методе детекције, локализације и класификације морају бити једноставно и ефективно имплементиране у хијерархијску мрежу. На Слици 13 је приказан ток информација у предложеном алгоритму за детекцију, локализацију и класификацију [6]. Сензорски чвор је лоциран на најнижем хијерархијском нивоу и као такав је одговоран за аквизицију података од сензора. У идејном решењу би у бежичној сензорској мрежи након првог укључења,

алгоритам за детекцију ушао у стање чекања док број сензорских догађаја не достигне значајан број. Ако тај број догађаја расте то би значило да је објекат ушао у надгледану зону, међутим ако тај број догађаја остане мали, то би значило да су они узрок случајног шума или других извора (ветра, птица и сл.). Такође активност сваког сензора указује на могућу локацију објекта који се детектује у сензорском пољу [28].



Слика 13 – *Алгоритам за детекцију, локализацију и класификацију [6]*

Подаци који су стигли до сензорских чворишта се након претходне обраде прослеђују непосредно надлежним вођама кластера, где се додатно обрађују. Сваки сензорски чвор може да сугерише могућу позицију објекта на основу догађаја проистеклих са сензора. Тренутну позицију објекта вођа кластера одређује усредњавањем сугерисаних позиција сензорских догађаја, узимајући у обзир претходну позицију објекта. Након тога се у обзир узимају само сензорски догађаји у близини тренутне позиције детектованог објекта, све док објекат не напусти надгледану зону [33].

Подаци пристигли у командни центар се анализирају и на основу њих се врши класификација објеката детектованих и локализованих у надгледаној зони. Анализирајући податке добијене од AMP и геофон сензора командни центар класификује тип објекта (лице, лице које пушку, ауто, тенк или непознато) [6] [34] [33] [35] [36].

Снабдевање енергијом

Због енергетске ефикасности система и ограниченог приступа енергији, потрошња унутар сензорских чворова мора бити строго ограничена. У прилог целокупној штедњи енергије иде и изабрани сценарио и изглед мреже. Безбедност и поузданост система не сме бити угрожена. С тим у вези треба избећи да дође до отказа неког сензорског чвора услед недостатка енергије. За те потребе се уграђује систем раног упозорења, који периодично мери ниво енергије у батеријским ћелијама и активира аларм у случају достизања критичних вредности. Да би систем измерио преосталу вредност енергије, уграђени модел енергетске потрошње прерачунава укупно потрошену и преосталу енергију у батеријским ћелијама. Ово се изводи тако што модел мери време које је чвор и са њим повезани сензори провели у „будном стању“ (у раду) и „стању спавања“ (чвор и сензори неактивни). На такав начин је могуће извршити апроксимацију расположиве енергије у зависности од капацитета напојне ћелије. Целокупни подаци о стању утрошене и расположиве енергије се смештају у меморију, како би се сачувало стварно стање услед губитка енергије или ресетовања уређаја. У табели 2 и 3 су дате апроксимативне енергетске потребе различитих компоненти и различитих чворова респективно [5] [6] [37].

Табела 2 – *Преглед апроксимативних енергетских потреба различитих компоненти [6]*

Тип сензора	Будно стање	Спавајуће стање
AMR	40mA	0μA
Акцелерометар	650μA	1μA
Singl-PIR	300μA	0μA
Multi-PIR	900μA	0μA
Геофон (GP)	10mA	5mA
ГПС пријемник	50mA	0mA
Централни модуле (Core)	6mA	40μA
ФМ примопредајник	16mA	0mA

Табела 3 – *Преглед апроксимативних енергетских потреба различитих чворова [6]*

Тип чвориште	Будно стање	Спавајуће стање
Воћа кластера	672mA	480mA
Чвор са singl-PIR без геофона	63mA	41μA
Чвор са singl-PIR са геофоном	73mA	5mA
Чвор са multi-PIR без геофона	64mA	41μA
Чвор са multi-PIR са геофоном	74mA	5mA

Имплементација сигурне бежичне сензорске мреже

Бежичне сензорске мреже у војним применама се највише користе за надзор одређене границе или периметра, откривање и праћење непријатеља у непријатељском окружењу како би се војне јединице осигурале од изненађења. Такође се на

овакав начин смањују трошкови ангажовања војног особља на обављању оваквих врста послова. Употреба БСМ може заменити ангажовање значајног броја војних јединица, које би морале бити ангажоване на пословима обезбеђења и запречавања одређених оперативних праваца. Овакав надзор треба имати способности да открије, прати, идентификује и класификује непријатеље и приоритете према претњи.

Дизајна конкретне бежичне сензорске мреже везан је за одређен тип намене исте. У поступку планирања и пројектовања, потребно је извршити процену адекватног и економичног хардвера. Могућност избора хардвера је велика, али се приликом реализације треба водити ниском ценом хардвера и малим трошковима одржавања. У зависности од значаја објекта који се чува (нпр. војна база, складиште, караула, затвор, државна граница и сл.) могућа је примена и дела фиксне инфраструктуре са сталним напајањем. Употреба мултисензорских чворова са већом осетљивошћу значајно увећава цену мреже, али то може бити оправдано значајем објекта који се штити.

Због свега наведеног бежична сензорска мрежа се мора ослонити на добро осмишљену сигурносну архитектуру која мора да укључује следеће [38] [39] [40]:

– потпуно униформан хардвер са савременим сигурносним механизмима,

– континуирано скенирање мреже у потрази за фалсификованим или компромитованим хардвером или софтвером,

– проверљив интегритет информација и система, како би се открио сваки неовлаштени приступ, измена података или њихова крађа,

– непрекидну контролу и надзор над мрежним конекцијама како би се обезбедила безбедна комуникација између сензорских чворова,

– планиране поступке и мере у случају компромитације мреже или једног његовог дела, како би се предупредиле озбиљније последице по људе и имовину,

– непрекидно истраживање безбедносних пропуста у мрежи кроз планирана тестирања,

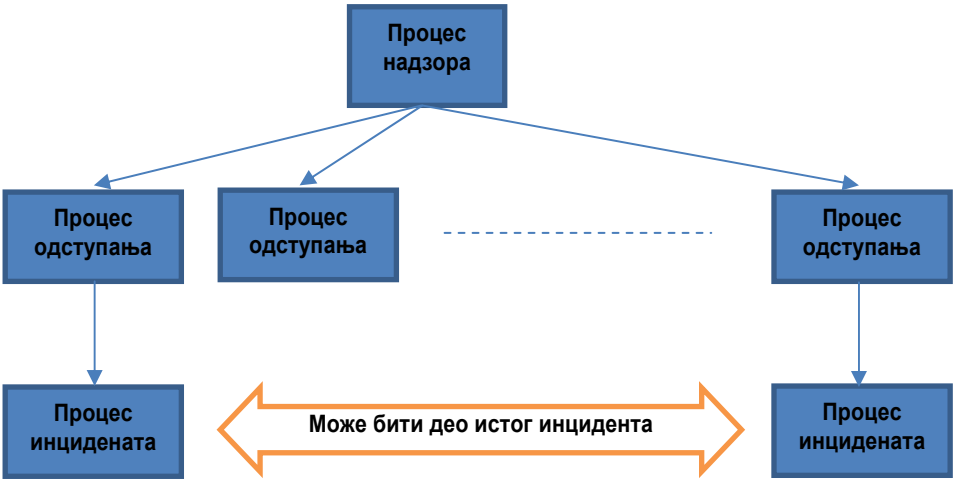
– континуирано унапређење сигурносних система у бежичним сензорским мрежама.

Имплементација бежичне сензорске мреже за специфичну намену указује на потребу усмереног истраживања и развоја сензорске мреже која ће одговорити захтевима и задацима који се испред те мреже постављају. Сигурна бежична сензорска мрежа треба да представља систем са нултом толеранцијом на грешке. Имплементирани систем се базира на могућностима бежичне сензорске мреже, структуре једне такве мреже и њених процеса.

Могућност једне мреже се огледа кроз могућности њених подсистема. Главни подсистем је анализа сензорских података и њихова централизована обрада. Систем треба да поседује могућност праћење, детектовања и надгледања. Такође, на основу ових могућности мрежа треба да поседује могућност селективног укључивања појединих делова мрежа како би систем задржао своју енергетску ефикасност. У зависности од захтева, у мрежи по потреби треба бити имплементирана могућност управљања заштитом критичне инфраструктуре. Подсистем сензора треба да омогући информације из сензорског поља који се анализирају и обједињавају. Резултат анализе се употребљава за подсистеме детектовања, надгледања и праћења.

Структура система треба да се састоји од: корисничког интерфејс модула, модула за командовање и контролу и сензорских модула. Кориснички интерфејс треба да омогући поред праћења ситуације у мрежи (стања исправности, инцидената и промена) и визуалну контролу над сензорима у мрежи. Командно-контролни модул управља процесима надзора, процесима одступања од задатих параметара мреже и процесима инцидената. Сензорски модули доносе информације о детектованим објектима и праћењу тих објеката.

Способност управљања заштитом критичне инфраструктуре представља најважнију могућност једне мреже којом се одређују процеси унутар мреже. Управљање надзором, поремећајима и инцидентима у мрежи одговарају процесима надзора, процесима одступања од задатих параметар и процесима инцидената (Слика 14).



Слика 14 – *Општа структура процеса*

Процес надзора је јединствен и треба да траје све док постоји (функционише) бежична сензорска мрежа. Процес одступања треба да активира аларм и он региструје појединачно сваки догађај који је јединствен случај и како се у мрежи могу десити вишеструки догађаји мање или више симултано, због неких непријатељских и координисаних активности то може довести до активирања вишеструких процеса одступања, а сваки може заузврат може иницирати појединачни процес инцидента. Сваки утврђени инциденти ће довести до почетка процеса инцидента, али како је назначено на слици, вишеструки инциденти могу на вишем нивоу бити део истог текућег инцидента са више догађаја или акција које предузима непријатељска група због чега командни центар мора да одлучи да ли вишеструки догађаји у одређеним инцидентним процесима припадају истом укупном инциденту. Када се било који од догађаја у било којем процесу одступања и инцидента доведе до краја, завршавају се одговарајући процеси. У зависности од процеса, систем треба да изврши активирање аларма, како би особље знало када и како да делује у случају угрожавајућег догађаја.

Закључак

Свакодневни захтеви за употребом бежичних сензорских мрежа превазилазе могућности истраживача и испред њих постављају јако пуно изазова са којима се треба суочити. Иако су бежичне сензорске мреже једно од најбрже растућих поља у оквиру информационо-телекомуникационих технологија, развој хардвера и софтвера покушава да држи корак са захтевима и потребама корисника. Проблеми који су били заступљени уназад десет година у пројектовању и имплементацији бежичних сензорских мрежа, готово да се ни данас нису променили: ограничена енергија, позиционирање сензора, ограничења у хардверу сензорских чворова, агрегација података, оптимизација података кроз протоколе усмеравања и скалабилност мреже. Управо због тога сваки технолошки напредак на пољу ИТ технологија изнова актуелизује оптимизацију бежичних сензорских мрежа на свим овим пољима у погледу поузданости и ефикасности мреже да детектује, локализује и класификује појаве у сензорском пољу, а да након тога безбедно и сигурно проследи те податке до крајњег корисника. Због тога су главни циљеви развојних инжењера да заштите бежичну сензорску мрежу од малициозних намера и развију брзу и рану детекцију напада на мрежу. Имајући у виду да свака особа са непријатељским намерама и лаптоп рачунаром веома лако може да пресретне ток података, да их измени и убаци као малициозни кôд у бежичну сензорску мрежу, још више се наглашава неопходност заштите мреже и поверљивости података у њој.

Управо због тога безбедносне структуре (војска, полиција, гранична полиција и сл.) које се брину о заштити виталних и за друштво у целини критичних инфраструктура дефинишу захтеве у погледу окружења у којој ће бежична сензорска мрежа радити, задатке које треба да обави и циљева које та мрежа треба да испуни. Рад даје осврт на поље бежичних сензорских мрежа и једно од могућих решења, које би се користило и у сопственом и у непријатељском окружењу за стицање пуне оперативне слике над простором или објектом од интереса, са нагласком на архитектуру мреже, њене саставне делове, топологију као и протоколе и алгоритме који се користе у доношењу одлуке.

Литература

1] C. Krulak, "The Strategic Corporal: Leadership in the Three Block War," *Marine Corps Gazette,* vol. 83, no. 1, pp. 18-22, 1999.

[2] M. Milanović, M. Stojilović, M. Oklobdžija and G. Dimić, "Adaptacija bežične senzorske mreže u cilju detekcije i dojave kritičnih situacija," in *INFOTEH*, Jahorina, 2012.

[3] E. Jungert, N. Hallberg and E. Wadströmer, "A system design for surveillance systems protecting critical infrastructures," *Journal of Visual Languages and Computing Vol. 25,* pp. 650-657, 2014.

[4] M. Maksimović and V. Vujović, "Uloga Internet baziranih bežičnih senzorskih mreža u zaštiti od požara," in *Infoteh*, Jahorina, 2013.

[5] I. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless sensor networks: A survey," *Computer Networks Vol. 38,* pp. 393-422, 2002.

[6] M.Niedermeier, X.He, H.Meer, C.Buschmann, K.Hartmann, B.Langmann, M.Koch, S.Fischer and D.Pfisterer, "Critical Infrastructure Surveillance Using Secure Wireless Sensor Networks," *Journal of sensor and actuator networks, Vol. 4, Iss. 4,* pp. 336-370, 2015.

[7] P. S. Cannon and C. R. Harding, "Future Military Wireless Solutions, Ch.8," in *Wireless Communications: The Future*, John Wiley & Sons, Ltd, 2007, pp. 91-116.

[8] A. Chatterjee and M. Pandey, "Practical Applications Of Wireless Sensor Network Based On Military, Environmental, Health And Home Applications: A Survey," *International Journal of Scientific & Engineering Research,* vol. 5, no. 1, pp. 1043-1050, 2014.

[9] A. Kott, A. Swami and B. J. West, "The Internet of Battle Things," *Computer,* vol. 49, no. 12, pp. 70-75, 2016.

[10] G. B. Marković and M. L. Dukić, "Bežične senzorske mreže, I deo: Osnovna arhitektura, karakteristike i primene," *Telekomunikacije, Vol.3, RATEL,* 2008.

[11] K. Romer and F. Mattern, "The Design Space of Wireless Sensor Networks," *IEEE Wireless Communications,* vol. 11, no. 6, pp. 54-61, 2004.

[12] A. Oračević, "Ad hoc wireless sensor networks," *Faculty of engineering Bihać, University Bihać,* 2013.

[13] H. A. A. Al-Asadi, "Energy Efficient Hierarchical Clustering Mechanism for Wireless Sensor Network Fields," *International Journal of Computer Applications,* vol. 153, no. 8, pp. 42-46,, 2016.

[14] B. Prabhu and N. Balakumar, "Enhanced Clustering Methodology for Lifetime Maximization in Dense WSN Fields," *International Journal for Technological Research in Engineering,* vol. 4, no. 2, pp. 343-348, 2016.

[15] G. B. Marković and M. L. Dukić, "Bežične senzorske mreže, II deo: Pregled komunikacione arhitekture," *Telekomunikacije, Vol.7, RATEL,* 2008.

[16] S. Prasanna and S. Rao, "An Overview of Wireless Sensor Networks-Applications and Security," *International Journal of Soft Computing and Engineering,* vol. 2, no. 2, pp. 538-540, 2012.

[17] D. Niculescu, "Communication paradigms for sensor networks," *IEEE Communications Magazine,* vol. 43, no. 3, pp. 116-122, 2005.

[18] IEEE 802.15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs) (2003), 3 Park Avenue, New York, USA: IEEE.

[19] "PE-6/S case – 'The Spike," ION Geophysical Corporation, 18 August 2011. [Online]. https://www.iongeo.com/content/documents/Resource%20Center/Brochures%20and%20Data%20Sheets/Brochures/BR_SEN_Spares_091509.pdf. [Accessed 10 september 2017].

[20] "iSense Modules & Devices: Outstanding Extensibility," Coalesenses, [Online]. ww.quarbz.com/Wireless%20Sensor%20Network/2.%20iSense%20Devices%20and%20Modules.pdf. [Accessed 20 septembar 2017].

[21] R. P. Narayanan, T. V. Sarath and V. V. Vineeth, "Survey on Motes Used in Wireless Sensor Networks: Performance & Parametric Analysis," *Wireless Sensor Network,* vol. 8, pp. 51-60, 2016.

[22] J. Edgar H. Callaway, Wireless Sensor Networks: Architectures and Protocols, Boca Raton, FL: Auerbach Publications, 2004.

[23] S. K. Singh, M. Singh and D. Singh, "Routing Protocols in Wireless Sensor Networks- A Survey," *International Journal of Computer Science&Engineering Survey,* vol. 1, no. 2, pp. 63-82, 2010.

[24] M. S. Rajković, G. B. Marković and M. L. Dukić, "Hijerarhijski DSCC protokol rutiranja za energetski heterogene WSN," *Infoteh-Jahorina,* vol. 11, pp. 367-372, 2012.

[25] M. Mrkaja, "Prilagodljivi (dinamički) algoritmi za rutiranje," in *Infoteh*, Jahorina, 2005.

[26] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEEE wireless communications,* vol. 11, no. 6, pp. 6-28, 2004.

[27] I. Akyildiz and M. Vuran, "Wireless Sensor Networks, Series in Communications and Networking," *John Wiley & Sons,* vol. 6, pp. 17-33, 2010.

[28] D. Boyle and T. Newe, "Security Protocols for Use with Wireless Sensor Networks: A Survey of Security Architectures," in *Third International Conference on Wireless and Mobile Communications* , Guadeloupe, French Caribbean, 2007.

[29] D. Goyal and M. R. Tripathy, "Routing Protocols in Wireless Sensor Networks: A Survey," in *Second International Conference on Advanced Computing & Communication Technologies*, Rohtak, Haryana, India, 2012.

[30] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos and G. Pantziou, "A survey on jamming attacks and countermenasures in WSNs," *IEEE Communications Surveys & Tutorials,* vol. 11, pp. 42-56, 2009.

[31] A. H. Lashkari, M. M. S. Danesh and B. Samadi, "A Survey on Wireless Security protocols (WEP, WPA and WPA2/802.11i)," in *2nd IEEE International Conference on Computer Science and Information Technology*, Beijing, China, 2009.

[32] A. R. M. Kamal, C. J. Bleakley and S. Dobson, "Failure detection in wireless sensor networks: A sequence-based dynamic approach," *ACM Transactions on Sensor Networks,* vol. 10, no. 2, 2014.

[33] A. Oracevic, S. Akbaş, S. Ozdemir and M. Kos, "Secure Target Detection and Tracking in Mission Critical Wireless Sensor Networks," *International Conference on Anti-Counterfeiting, Security and Identification (ASID),* pp. 1-5, 2014.

[34] M. Fayyaz, "Classification of object tracking techniques in wireless sensor networks," *Wireless Sensor Network,* vol. 3, no. 4, pp. 121-124, 2011.

[35] "MOVEDETECT–Secure Detection, Localization and Classification in Wireless Sensor Networks," *Internet of Things, Smart Spaces, and Next Generation Networking,* vol. 8121, p. 284–297, 2013.

[36] A. Oračević and S. Ozdemir, "Secure and Reliable Prediction Based Target Tracking for Wireless Sensor Networks," in *5th International Conference on Intelligent Systems, Modelling and Simulation*, Langkavi, Malezija, 2014.

[37] D. Lee, "Energy Harvesting Chip and the Chip Based Power Supply Development for a Wireless Sensor Network," *Multidisciplinary Digital Publishing Institute - Sensors ,* vol. 8, pp. 7690-7714, 2008.

[38] S. K. Singh, M. P. Singh and D. K. Singh, "Routing Protocols in Wireless Sensor Networks – A Survey," *International Journal of Computer International Journal of Computer,* vol. 1, no. 2, pp. 63-83, 2010.

[39] A. Diaz and P. Sanchez, "Simulation of Attacks for Security in Wireless Sensor Network," *Multidisciplinary Digital Publishing Institute - Sensor,* vol. 16, no. 11, pp. 1-27, 2016.

[40] M. Mansouri, A. Sardouk, L. Merghem-boulahia, D. Gaiti, H. Snoussi, R. Rahim-amoud and C. Richard, "Factors that May Influence the Performance of Wireless Sensor Networks," in *Smart Wireless Sensor Networks*, London, InTech, 2010, pp. 31-48.

[41] T. Simon, "Critical infrastructure and te Internet of Things," *Global Commission on Internet Governance,* pp. 1-11, 2017.

[42] S. Yinbiao, L. Kang, P. Lanctot and F. Jianbin, "Internet of Things: Wireless Sensor Networks," *International Electrotehnical Commission - White Papier,* pp. 1-78, 2014.

[43] L.Seder, Ž.Ilić and M.Kos, "Sigurno usmeravanje u ad hoc mrežama," *Automatika,* vol. 52, pp. 269-278, 2011.

[44] E. Cayirci and C. Rong, Security in Wireless Ad Hoc and Sensor Networks, New Jersey: John Wiley & Sons, 2009.

[45] J. Stankovic, "Wireless Sensor Networks," *IEEE Computer Society, Computer,* vol. 41, no. 10, pp. 92-95, 2008.

[46] J. Liu, F. Zhao and D. Petrovic, "Information-Directed Routing in Ad Hoc Sensor Networks," *IEEE Journal on Selected Areas in Communications,* vol. 23, no. 4, pp. 851-861, 2005.

[47] L. J. G. Villalba, A. L. S. Orozco, A. T. Cabrera and C. J. B. Abbas, "Routing Protocols in Wireless Sensor Networks," *Sensors,* vol. 9, pp. 8400-8421, 2009.

[48] S. Alam and D. De, "Analysis of security threats in wireless sensor network," *International Journal of Wireless & Mobile Networks,* vol. 6, no. 2, pp. 35-46, 2014.

[49] D. R. Raymond and S. F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," *Article in IEEE Pervasive Computing 7(1),* pp. 74-81, 2008.

[50] M. Dener, "Security Analysis in Wireless Sensor Networks," *International Journal of Distributed Sensor Networks,* vol. 10, no. 10, pp. 1-9, 2014.

[51] S. K. Singh, M. P. Singh and D. K. Singh, "Intrusion Detection Based Security Solution for Cluster-Based Wireless Sensor Networks," *International Journalof Advanced Science and Technology,* vol. 30, 2011.

[52] "Analysis of Security Protocols in Wireless Sensor Network," *International Journal Advanced Networking and Applications ,* vol. 2, no. 3, pp. 707-713, 2010.