KRIPTOGRAFSKI RADNI OKVIR ZA BEŽIČNE SENZORSKE MREŽE

Bogdan Brkić*,
Dejan Živković,
Mladen Veinović

Univerzitet Singidunum,
Beograd, Srbija

Rezime:

Bežične senzorske mreže doživjele su veliku ekspanziju u svim oblastima ljudskog života. Neke od primjena su komercijalne prirode, a neke su takvog karaktera da je gotovo nemoguće zamisliti bilo koju drugu tehnologiju koja bi mogla da ih zamijeni. Zbog sve niže cijene komponenti bežičnih senzorskih mreža i sve masovnije upotrebe one prikupljaju ogromne količine podataka koji bi, ukoliko bi bili nezaštićeni, mogli biti zloupotrebljeni. Predmet ovog rada je istražiti na koji način se štite podaci u bežičnim senzorskim mrežama uzimajući u obzir tehnološka i ograničenja u realizaciji koja su specifična za ovu vrstu uređaja.

Ključne reči:

simetrični i asimetrični kriptografski algoritmi, eliptične krive, programabilne logičke mreže.

1. UVOD

Bežične senzorske mreže (Wireless Sensor Networks - WSN) predstavljaju grupu umrežanih uređaja koje nazivamo nodovi ili čvorovi. Njihova osnovna karakteristika je da obavezno sadrže senzorsku komponentu. Najčešće se radi o malim, jeftinim, multifunkcionalnim i autonomnim uređajima koji pored senzora imaju: sklop za obradu i čuvanje podataka, vlastito napajanje, mogućnost komunikacije sa drugim uređajima najčešće bežičnom komunikacijom, a nerijetko posjeduju i aktuatore koji im omogućavaju upravljanje drugim uređajima. Informacije prikupljene sa nodova kao i upravljački signali za aktivaciju aktuatora čine skup podataka koji se prenosi bežičnim putem unutar oblasti koju mreža pokriva. Bez obzira na namjenu bežične senzorske mreže kao i na značaj podataka koji se unutar nje prenosi jasno je da ovakav protok informacija treba obezbijediti od neovlaštenog čitanja i modifikovanja. Kao i u većini današnjih komunikacionih uređaja kao logično rješenje zaštite podataka nameće se primjena kriptografskih tehnika. Poznato nam je da izvođenje kriptografskih algoritama može zahtijevati upotrebu značajnih resursa. Neke od osnovnih karakteristika bežičnih senzorskih mreža upravo su u suprotnosti sa zahtjevima koje postavljaju kriptografske tehnike - procesorski i memorijski resursi su skromni, a energetski resursi najčešće su ograničeni i za obavljanje bilo kakvih funkcija unutar nodova očekuje se što manja potrošnja energije.

Odgovorno lice:
Bogdan Brkić

e-pošta:
bogdan.brkic.08@singimail.rs

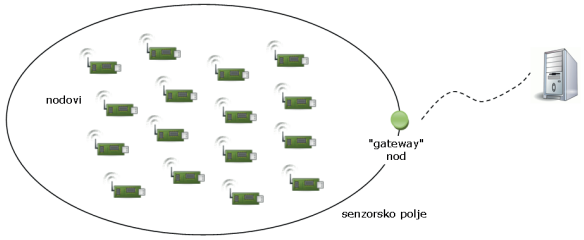
DOI: 10.15308/Sinteza-2019-526-533

2. BEŽIČNE SENZORSKE MREŽE

Nodovi

Osnovna namjena nodova je registrovanje i mjerenje različitih pojava iz okoline i slanje izmjerenih vrijednosti na neko centralno mjesto na kom će se vršiti obrada podataka. Nodovi su obično gusto raspoređeni u području koje se naziva senzorsko polje i prikupljaju i prosleđuju podatke iz okruženja u kom se nalaze. Ukoliko postoje aktuatori, sa centralnog mjesta za obradu podataka prema nodu se mogu slati i upravljački signali. Današnje tehnologije proizvodnje integrisanih kola omogućavaju dobijanje veoma minijaturnih nodova u kojima se nalaze sve pobrojane komponente. Jedna od važnih karakteristika ovih uređaja jeste mala potrošnja energije, tako da ako se radi o baterijskom napajanju mogu da rade veoma dugo sa jednim punjenjem. Mala potrošnja energije omogućava i napajanje „konstantnim“ izvorima energije kao što su npr. solarna ili energija kretanja.

Senzorsku mrežu čini grupa nodova od kojih svaki ima mogućnost komunikacije sa jednim ili više susjednih nodova. Najčešće se jedan od nodova tzv. “gateway nod” konfiguriše tako da ostvaruje i dodatnu funkciju - interkonekciju sa susjednom bežičnom mrežom ili nekim drugim informacionim sistemom. Oblast koju pokrivaju svi senzori jedne mreže u smislu registrovanja određene pojave na nekom prostoru predstavlja senzorsko polje.



Slika 1. Model bežične senzorske mreže

Senzori su konvertori koji jednu fizičku veličinu pretvaraju u drugu. Danas se najčešće vrši pretvaranje u digitalne električne impulse koje je poslije moguće obrađivati različitim uređajima.

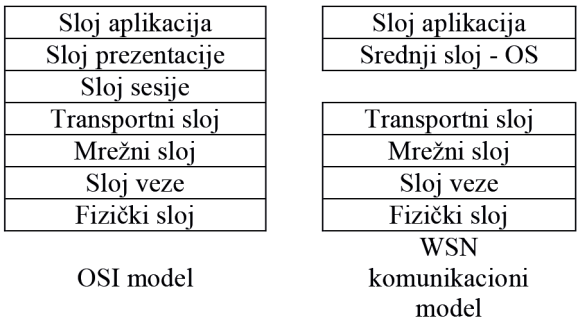
Oblasti primjene senzorskih mreža

Velika raznolikost pojava koji današnji vještački senzori mogu da detektuju, prate i izmjere naslućuje i široku oblast upotrebe ovih uređaja. Neke od oblasti primjene senzorskih mreža [1] su:

- industrija – praćenje stanja mašina i postrojenja, praćenje proizvodnih procesa, ...
- vojna industrija – detekcija pokretnih predmeta, neprijateljskih formacija i ciljeva, hemijskih i bioloških agenasa, nuklearnog zračenja, ...
- geolokacija
- javna bezbjednost – nadgledanje područja, praćenje različitih pojava, ...
- poljoprivreda – praćenje promjena u mikroklimi, praćenje kretanja štetočina i nametnika
- seizmologija – praćenje geoloških aktivnosti
- zdravstvo – praćenje zdravstvenog stanja pacijenta pomoću senzora koji se nalaze unutar i na organizmu, kretanje pacijenata unutar zdravstvene ustanove, pomoć hendikepiranim osobama, udaljeni monitoring pacijenta, ...
- saobraćaj i logistika – praćenje gužvi u saobraćaju, monitoring čvorova i parkinga, monitoring zaliha u skladištima, ...
- biološke i ekološke primjene – monitoring kvalitete vazduha i vode, praćenje šumskih požara, detekcija klizišta, sprečavanje prirodnih katastrofa, upozoravanje na poplave i cunamije, praćenje kretanja otpada i opasnih materija, ...
- kućna automatizacija – pametne kuće, upravljanje elektronskim uređajima na osnovu detektovanih promjena u okolini bez asistencije čovjeka, energetska efikasnost, upravljanje mikroklimatskim uslovima i privatnim i javnim prostorima

Komunikacioni model WSN

Komunikacioni model koji opisuje proces komuniciranja unutar WSN [2] sličan je OSI (Open Systems Interconnection) modelu i u odnosu na njega ne posjeduje jedino sloj sesije.



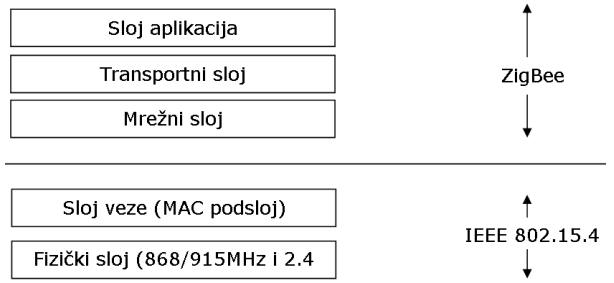
Slika 2. OSI i komunikacioni model WSN

Fizički sloj izvršava sledeće funkcije: odabir frekvencije, detekcija signala, zaštitu podataka, prenos podataka između čvorova, modulacija i briga o potrošnji energije. Sloj veze zadužen je za: formiranje zaglavlja i multipleksiranje paketa podataka, fizičko adresiranje i kontrolu toka paketa, kontrolu grešaka pri prenosu i kontrolu pristupa, osluškivanje medijuma, ponovljena slanja zbog nastalih kolizija, udvostručeni prijem kao i slanje podataka za kontrolu koji nisu neophodni. Mrežni sloj obezbjeđuje razmjenu podataka između transportnog, aplikacionog i MAC podsloja. Zadatak mrežnog sloja jeste da se pravilno formira mrežna topologija, konfigurišu i adresiraju uređaji, vodi računa o susjedstvu između čvorova, pronađe najbolji put da se poruka dostavi na odredište i da se uključivanjem i isključivanjem čvorova s mreže kontroliše potrošnja energije. Kako TCP kao transportni protokol ne garantuje pouzdan prenos zbog postojanja velikog broja čvorova i predajnika kao i potrebe pojedinih pristupnih uređaja da iniciraju multicast saobraćaj, na transportnom sloju koriste se protokoli: PFSQ (Pump Slow Fetch Quickly), RMST (Reliable Multi-Segment Transport), ESRT (Event to Sink Reliable Transport) i CODA (Congestion Detection and Avoidance). Operativni sistem utiče na potrošnju, responsivnost, kvalitet, bezbjednost i brzinu razmjene podataka. Shodno takvim potrebama pojedini operativni sistemi posebno su napravljeni za primjenu u WSM. Jedan od osnovnih zadataka operativnog sistema je optimizacija potrošnje energije noda koja se realizuje: uključivanjem ili isključivanjem dijelova senzorskog čvora, promjenom frekvencije sistemskog sata ili praćenjem upisivanja ili čitanja iz i u memoriju. Na aplikativnom sloju koriste se protokoli: SMP (eng. Sensor Management Protocol), TADP (eng. Task Assignment and Data Advertisement Protocol) i SQDDP (eng. Sensor Query and Data Dissemination Protocol).

Komunikacioni model je važno poznavati jer se na osnovu njega mogu klasifikovati i vrste napada na komunikaciju unutar mreže kao i mogućnosti primjene različitih kriptografskih tehnika na različitim slojevima.

Važniji standardi bežičnih senzorskih mreža

Najvažniji standard [1] koji se odnosi na WSN je IEEE 802.15.4. Ovo je standard koji definiše funkcionisanje "personalnih bežičnih mreža malog troška održavanja" (low-rate wireless personal area network LR-WPAN). Specificira fizički podsloj (868/915MHz i 2.4 GHz) i MAC podsloj sloja veze. Predstavlja osnovu i za sledeće specifikacije: ZigBee, ISA100.11a, WirelessHART, MiWi, SNAP i Thread . Svaka od ovih specifikacija razvija gornje slojeve komunikacionih modela koji nisu definisani u IEEE 802.15.4 standardu.



Slika 3. IEEE 802.15.4 i ZigBee standard u WSN komunikacionom modelu

Mada se u vezi sa bežičnim senzorskim mrežama nerijetko kao dodatni standard pominje i ZigBee, on je u stvari IEEE 802.15.4 bazirana specifikacija/nadgradnja za paket komunikacionih protokola višeg nivoa u mrežama u kojima se prenose manje količine podataka, manjim brzinama i na manjim udaljenostima (10-100m). Prenos podataka na veće udaljenosti postiže se ekstenzijom mreže tj. dodavanjem novih nodova. Neki standardi kao što su WirelessHART i ISA100.11a karakteristični su za industrijske aplikacije.

3. VRSTE PRIJETNJI I NAPADA NA BEŽIČNE SENZORSKE MREŽE

Bezbjednosni zahtjevi

Bezbjednosni principi [3][4] koji se javljaju u ostalim informacionim sistemima i koji pored ostalih generalno

nastoje da riješe i kriptografske tehnike pronalazimo i kod bežičnih senzorski mreža:

- povjerljivost podataka – Data Confidentiality – u kontekstu WSN znači da samo autorizovani nodovi imaju pristup podacima,
- povjerljivost izvora – Data Authentication – u kontekstu WSN znači da podaci potiču od autorizovanih nodova,
- integritet podataka – Data Integrity – podaci od izvora do odredišta nisu mijenjani od neautorizovanih nodova,
- vremenska validnost podataka – Data Freshness – stare poruke se ne ponavljaju i
- dostupnost – Availability – servisi koje nudi WSN ili pojedinačni nod su dostupni kada god je to potrebno.

Pored ovih principa značajni su i: sinhronizacija vremena, bezbjedno upravljanje nodovima (nodovi bi trebali biti fleksibilini, samoorganizujući, prilagodljivi i korektivni u odnosu na sigurnosne mjere) bezbjedna lokalizacija (očuvanje podataka o lokaciji tokom komunikacije sa susjednim nodovima).

Bezbjednosni izazovi u bežičnim senzorskim mrežama

Bezbjednosni izazovi [5] koji se javljaju u bežičnim senzorskim mrežama su:

- emitujuća priroda bežičnih komunikacija rezultuje time da su ove mreže podložne različitim napadima, od pasivnog prisluškivanja, reemitovanja lažnih poruka do izobličavanja signala,
- lokalizacija na teško dostupnom terenu kao što je šuma ili npr. bojno polje onemogućava kvalitetno fizičko obezbjeđenje mreže,
- ograničenja u procesorskoj i memorijskoj snazi kao i ograničeni energetski resursi,
- potencijalno velik broj nodova i ostalih uređaja u mreži,
- dinamička priroda ovih mreža može izazvati česte promjene u topologiji i autorizaciji ...

Protivnik je osoba ili entitet koji pokušava da naruši rad mreže neautorizovanim pristupom, uskraćivanjem servisa ili nekim drugim napadom ili prijetnjom.

Pasivni protivnik samo nadgleda komunikaciju i prijetnja je povjerljivosti podataka. *Aktivni protivnik* pokušava da briše, dodaje ili mijenja podatke koji se prenose kanalima. Prijetnja je integritetu podataka. *Mote-Class napadač* (mote=bubica; WSN nod veoma malih dimenzija) raspolaže resursima koji su slični resursima koje posjeduju nodovi u WSN. *Laptop-Class napadač* raspolaže moćnijim resursima nego što su to nodovi u mreži – veća procesorska i memorijska snaga, veći energetski resursi, jači komunikacioni resursi i dr. *Insajder* je napadač koji je kompromitovao neke autorizovane dijelove mreže npr. krađom ključeva ili pokretanjem malicioznog koda. *Autsajder* je napadač koji nema neki poseban nivo pristupa mreži.

Vrste prijetnji i napada na WSN

Sigurnosni problemi u bežičnim senzorskim mrežama [6] mogu se klasifikovati u 5 grupa:

- problemi koji se javljaju pri upotrebi kriptografskih tehnika (cryptography)
- upravljanje kriptološkim ključevima (key management)

Ključevi se koriste za obezbjeđivanje komunikacije u simetričnoj i asimetričnoj kriptografiji pri implementaciji različitih šema bezbjednosti. Distribucija ključeva nije tipična za bežične senzorske mreže, a ograničenja u resursima centralizovano upravljanje ključevima čini gotovo nemogućim. Direktna razmjena ključeva između svaka dva noda u WSN nije pogodna za mreže koje su rastuće. Bezbjednosna šema mora koristiti efikasnu i pouzdanu tehniku distribuciju ključeva kako bi se obezbijedila bezbjedna komunikacija među svim čvorovima.

- bezbjedno rutiranje (secure routing)

Protokoli regulišu na koji način nodovi šalju pakete drugim nodovima ili sinkovima. Najveći izazov sastoji se autentifikaciji komunikacije na strani sinka. Kriptografija javnog ključa zbog svojih resursnih zahtjeva je neisplativa u WSN u rješavanju ovih problema. Iz tog razloga uvode se protokoli koji u sebi uključuju i bezbjedno rutiranje i koji ujedno obezbjeđuju integritet podataka, autentikaciju i dostupnost poruka.

- bezbjedna agregacija podataka (secure data aggregation)

Agregacija podataka rješava problem duplih podataka koji se može pojaviti tokom prikupljanja podataka. Ovo je poseban problem u energetski-limitiranim mrežama. Agregatori su osjetljivi na napade kada dođe do injektiranja podmetnutih podataka preko kompromitovanog noda. Bez autentikacije napadač bi lako prevario agregator. Obezbjeđivanje agregacije tako uključuje:

autentikaciju, povjerljivost i integritet podataka kao i saradnju nodova u identifikaciji eventualno kompromitovanih nodova.

- detekcija upada (intrusion detection)

Uskraćivanje usluga (The Denial of Service - DoS) je bilo koji događaj koji umanjuje ili potpuno eliminiše sposobnost mreže da izvrši svoju osnovnu funkciju.

Napadi na fizičkom sloju

Na fizičkom sloju [7] postoje dvije vrste napada:

- "jamming" koji predstavlja ometanje interferencijom sa frekvencijama koje koristi WSN mreža i
- "tampering" koji označava fizičku kompromitaciju nodova.

Rješenja za uklanjanje ovih problema su:

- širenje komunikacionog spektra,
- redovan monitoring izvještaja o jamming-u

Napadi na sloju veze

Na sloju veze najčešći su napadi:

- namjerne kolizije („collision") – izmjena okteta koji se prenose kako bi se poremetili paketi i poremećaji u MAC protokolima,
- iscrpljivanje („exhaustion") – kolizija i poremećaji u MAC paketima rezultuju nepotrebnom retransmisijom paketa koji dovode do iscrpljivanja energetskih resursa,
- nekorektnost („unfairness") – degradacija servisa koja uzrokuje da korisnici real-time MAC protokola promaše rokove

Tehnike kojima se može preduprijediti nastajanje ovih problema su: upotreba kodova za korekciju greške, detekcija kolizije, multipleksiranje dijeljenjem vremena (time-division multiplexing – TDM), ograničavanje brzine prenosa, ...

Napadi na mrežnom sloju

Na mrežnom sloju možemo se susresti sa napadima:

- selektivno prosljeđivanje ("Selective Forwarding") – maliciozni nodovi odbijaju proslijediti poruke i jednostavno ih odbaciju,
- lažni sink ("Sinkhole") – napadač privlači nodove lažiranjem informacija o rutiranju,
- "Sybil" napad – jedan nod predstavlja više identiteta za druge nodove,
- "Wormhole" – napadač tuneliše saobraćaj iz jednog dijela mreže u drugi,
- "HELLO flood" – Laptop-Class napadač emituje informacije takvom transmisionom snagom da uvjerava svaki nod u mreži da mu je susjedni.

Rješenja za navedene probleme mogu se naći u enkripciji sloja veze i autentikaciji, rutiranjem po više putanja, verifikaciji identiteta ili autentikaciji emitovanja.

Napadi na transportnom sloju

Na transportnom sloju javljaju se napadi:

- plavljenje ("flooding") – napadač šalje veliki broj zahtjeva za uspostavljanjem konekcije što dovodi do iscrpljivanja memorije i ostalih resursa,
- desinhronizacija – napadač konstantno šalje poruke zahtjeva za retransmisiju navodno izgubljenih paketa

Ovi problemi se izbjegavaju upotrebom "connectionless" protokola i autentikacijom paketa ključujući i sva kontrolna polja u hederu transportnog protokola.

Preporuke za zaštitu WSN

Generalne preporuke za zaštitu bežičnih senzorskih mreža koje se mogu dati su:

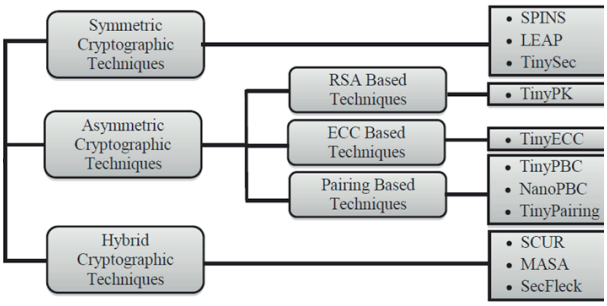
- ukoliko je moguće obezbijediti fizičku bezbjednost mreže,
- kriptografija može obezbijediti enkripciju na sloju veze i mehanizme autentikacije (MAC), ali to nije dovoljno,
- "end-to-end" mehanizmi zaštite nisu dovoljni,
- pažljivo dizajnirati protokole uz poštivanje bezbjednosnih principa i
- razmotriti probleme sa napajanjem kod usvajanja protivmjera.

4. KRIPTOGRAFSKE METODE ZAŠTITE BEŽIČNIH SENZORSKIH MREŽA

Mogućnost upotrebe kripto-algoritama u bežičnim senzorskim mrežama

Kriptografske tehnike su jedan od najčešćih i najkvalitetnijih načina obezbjeđivanja komunikacija pa tako i

komunikacija u bežičnim senzorskim mrežama. Kao i u drugim i ovdje se kriptografske metode zaštite mogu implementirati kroz: simetrične, asimetrične i heš algoritme. S obzirom na ograničenja u resursima, u odnosu na neke druge sisteme koji ih nemaju i koja lako implementiraju ove tehnike, potrebni su i posebni „resursnonezahtijevni“ algoritmi koje je moguće implementirati u praksi [8]. Na sledećoj slici prikazane su kriptografske tehnike, predloženi su neki od asimetričnih algoritama i navedene su realizacije u vidu “light-weight” protokola.



Slika 4. Tehnike i protokoli pogodni za zaštitu WSN

Hibridne tehnike kombinuju simetrične i asimetrične algoritme kako bi se iskoristile sve prednosti i jednog i drugog šifarskog sistema. U nekim od takvih rješenja simetrična kriptografija se koristi kod šifrovanja i autentikacije, a asimetrična za generisanje ključeva.

Primjena simetričnih algoritama

U simetričnim algoritmima koristi se jedan dijeljeni ključ za šifrovanje i dešifrovanje na obe strane komunikacije. Ključ treba biti tajan što je teško obezbijediti u izloženom okruženju kakvo je WSN. Mnoge bezbjednosne šeme za WSN koriste upravo samo simetrične algoritme zbog jednostavne implementacije i manjih hardverskih zahtjeva od drugih kripto-algoritama.

Iz grupe najčešće korištenih simetričnih algoritama (AES, Blowfish, DES, IDEA, MD5, RC4, RC5, SHA-1, SHA-256) algoritmi RC4 i MD5 su se pokazali kao najpogodniji za primjenu u WSN dok je za AES algoritam, na primjer, potrebno relativno veliko vrijeme za izvršavanje jedne AES operacije.

Primjena asimetričnih algoritama

Asimetrična kriptografija bazira se na dva ključa: privatnom i javnom. Javni se koristi za šifrovanje podataka, a privatni za dešifrovanje. Asimetrični kriptografski algoritmi najčešće se realizuju operacijama sa velikim brojevima, a to za posljedicu ima velike zahtjeve u pogledu hardverskih resursa i ovakvi algoritmi nisu baš najpodesniji za implementaciju u WSN.

Najveći broj predloženih rješenja koja koriste asimetrične algoritme zasniva se na upotrebi ECC (Elliptic Curve Cryptography) algoritma ili nekoj njegovoj adaptaciji u WSN okruženju. U odnosu na RSA algoritam ECC algoritam generalno operiše sa ključevima znatno manjih bitskih dužina, a u WSN okruženju ostvaruje manju potrošnju energije i angažovanje procesorskih i memorijskih resursa [9]. Većina rješenja bazirana na ECC algoritmu uključuje dodatni hardver u vidu ECC koprocesora male potrošnje energije. On uključuje i logičku jedinicu za modularnu aritmetiku koja se koristi za izvođenje operacija u odabranom “ECC polju”.

Postoje rješenja koja koriste i neke druge asimetrične algoritme kao što su Rabinova šema ili NtruEncrypt i drugi, ali podrazumijevaju upotrebu dodatnog hardvera za manipulaciju ključevima [10].

Kriptografski radni okviri za WSN

Kriptografski radni okviri (engl. *frameworks*) predstavljaju protokole i algoritme koji se izvršavaju u određenim slojevima sa ciljem uspostavljanja bezbjednog okruženja u bežičnoj senzorskoj mreži. Svaki radni okvir može obuhvatati algoritme za: šifrovanje i dešifrovanje, usaglašavanje ključeva i autentikaciju. Generalno ih možemo podijeliti [8] na okvire za:

- simetričnu kriptografiju (SPINS, LEAP, TinySec),
- asimetričnu kriptografiju (RSA bazirani kao TinyPK, ECC bazirani kao npr. TinyECC, „Pairing“ bazirani kao npr. TinyPBC, NanoPBC, TinyPairing i
- hibridne koji kombinuju simetričnu i asimetričnu kriptografiju (SCUR, MASA, SecFleck)

Framework	*Encryption*	*Cipher*	*Key Agreement*	*Code Requirement*
SPIN	CTR mode	RC5 (Block)	Master Key & Delayed Disclosure	2674B
LEAP	RC5	RC5 (Block)	Pre-deployed (Master Varaible)	ROM: 17.9KB RAM: no. of neighbours
TinySec	CBC mode (Optional)	Cipher independent	Any	RAM: 728B program space: 7146B
TinyPK	RSA	-	PK-RSA	13387B (512 bit key)
TinyECC	ECIES	-	ECDH	20818B (micaz)
TinyPBC	PBC	-	ID-NIKDS	Stack: 2,867B RAM: 368B ROM: 47,948B
NanoPBC	-	-	-	-
TinyPairing	PBC	-	-	RAM: 392B ROM: 21,742B
SCUR	Rabbit	Rabbit (Stream) (128bit)	Pre-Deployed key	-
MASA	-	-	-	-
SecFleck	RSA	RSA (Block) (2048 bit) & XTEA (128 bit)	-	RAM: 52B Program space: 1,082B

Framework	*Authentication*	*Cost (time/energy)*	*Support*
SPIN	CBC-MAC	7.24 ms	SmartDust
LEAP	CBC-MAC	Variable (No. of neighbours)	Mica2
TinySec	CBC-MAC	RC5(C): 0.90ms Skipjack(C): 0.38ms RC5(C, assembly): 0.26ms	Mica, Mica2, & Mica2Dot
TinyPK	CA-signed Diffie-Hellman public value	3.8 s	Mica1, Mica2
TinyECC	ECDSA	20266.47ms / 486.4 mJ (micaz)	Mica2/MicaZ, TelosB/Tmote Sky, BSNV3, & Imote2
TinyPBC	ID-NIKDS	5.45s (pairing computation)	Mica2 & MicaZ
NanoPBC	-	-	MicaZ
TinyPairing	-	21.95 s	MICA family, Telos, eyesIFX, Intel's Imote,
SCUR	-	-	-
MASA	-	-	-
SecFleck	RSA	RSA (s/w): 219,730 μs / 7,030.0 μJ RSA (h/w): 27 μs / 5.4 μJ XTEA (s/w): 18 μs / 0.6 μJ	Fleck sensor node

Slika 5. Kriptografski radni okviri za bežične senzorske mreže

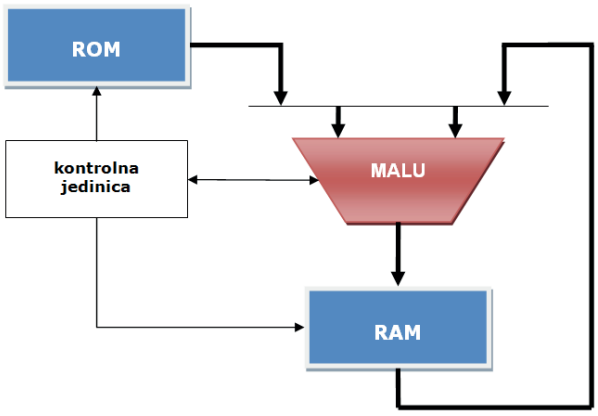
Prethodna tabela sadrži protokole u svakoj od navedenih podgrupa i može biti od koristi prilikom projektovanja bežičnih senzorskih mreža u fazi tokom koje se rješavaju pitanja zaštite podataka. Ova tabela sadrži uporedne podatke za svaki navedeni protokol kao što su: koji algoritmi se koriste za šifrovanje heširanje usaglašavanje ključeva i autentikaciju, kakvi su memorijski zahtjevi koje je neophodno obezbijediti za izvršavanje koda, koji su troškovi u vidu vremena izvršavanja i potrošnje energije i kakva je aplikabilnost na najvažnije familije senzorskih nodova.

5. PRIJEDLOZI MOGUĆIH UNAPREĐENJA MODELA ZAŠTITE BEŽIČNIH SENZORSKIH MREŽA

Na osnovu svega izloženog daćemo dva prijedloga [11] modela za zaštitu bežičnih senzorskih mreža. Poći ćemo od pretpostavke da želimo realizovati vlastite algoritme za šifrovanje, heširanje i usaglašavanje ključeva, te ih implementirati u hardveru, a zatim i u softveru.

Prijedlog 1 – hardverski pristup

Ovaj pristup zasniva se na upotrebi hardvera za obavljanje resursno kritičnih operacija. Kako se većina algoritama izvršava u modularnoj aritmetici naš kripto-hardverski dodatak biće opremljen procesorom koji umjesto aritmetičke logičke jedinice (ALU) ima modularnu aritmetičke logičke jedinice (MALU) sposobnu da obavlja aritmetičke operacije u modularnoj aritmetici.

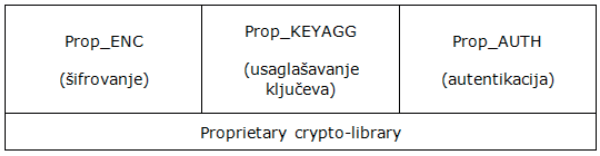


Slika 6. Koprocesor koji realizuje kriptooperacije vlastitog šifarskog sistema

Registre MALU možemo realizovati u npr. programabilnim logičkim mrežama (programmable logic array - PLA). Registre realizujemo tako što najprije postavimo neki matematički izraz koji određuje naš šifarski algoritam, a zatim vršimo programiranje PLA za izvršavanje modularnih operacija. Na primjer, u ECC algoritmu bismo kroz PLA mogli realizovati funkcije $f(z)=z^{163}+z^7+z^6+z^3+1$ ili $f(z)=z^{233}+z^{74}+1$.

Prijedlog 2 – softverski pristup

Drugo rješenje bazira se na kreiranju vlastitih softverskih biblioteka koje bi bile pridodate operativnom sistemu koji pokreće nodove naše bežične senzorske mreže. Ako pretpostavimo da imamo nodove na kojima se izvršava TinyOS onda je potrebno da u nekom od programskih jezika koje podržava operativni sistem (C, C++, Java) napišemo kod za kriptografske operacije šifrovanja, usaglašavanja ključeva i autentifikacije. Tokom pisanju koda treba voditi računa o resursnim ograničenjima koja nameće ciljana platforma.



Slika 7. Struktura vlastite biblioteke za kriptozaštitu WSN

6. ZAKLJUČAK

Bežične senzorske mreže su sve više upotrebi u različitim oblastima. Neke karakteristike njihovih gradivnih elemenata, nodova, kao što su niska potrošnja energije i ograničeni procesorski, memorijski i energetski resursi sa jedne strane omogućavaju njihovu minijaturizaciju što je poželjno, dok sa druge strane smanjuju mogućnost izvršavanja složenih kriptografskih operacija u cilju bolje zaštite podataka. Ovi problemi uslovili su razvoj mnogih inovativnih protokola i tehnika koje nastoje da riješe opisane probleme. Odabir odgovarajućih kriptografskih metoda za senzorske nodove je fundamentalan za pružanje bezbjednih servisa WSN. U ovom radu su opisani: bezbjednosni zahtjevi, vrste napada i prijetnji, načini za primjenu kriptografskih metoda zaštite bežičnih senzorskih mreža kao i kriptografski radni okviri dizajnirani namjenski za bežične senzorske mreže. Data su dva generalna prijedloga za realizaciju vlastitog modela bezbjednosti bežičnih senzorskih mreža.

LITERATURA

[1] K. Sohraby, D. Minoli, T. Znati, "Wireless sensor networks", Technology, Protocols, and Applications John Wiley & Sons, 2007.

[2] M. A. Matin, "Wireless Sensor Networks", Technology and Protocols Intech, 2012.

[3] M. Conti, "Secure wireless sensor networks, threats and solutions", Advances in Information Security, Vol. 65, Springer, 2016.

[4] G. Anuradha, "Wireless sensor network security and analysis" International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 9, 2016.

[5] R. Jadhav, "Security issues and solutions in wireless sensor networks", International Journal of Computer Applications, Volume 162 – No 2, 2017.

[6] G. S. Oreku, T. Pazynyuk, "Security in wireless sensor networks", Springer, 2016.

[7] K. S. Selvam, S. P. Rajagopalan, "Security analysis with respect to wireless sensor network", Review International Journal Of Engineering And Computer Science, Volume 6 Issue 4, 2017.

[8] G. Sharmaa, S. Balaa, A. K. Verma, "Security Frameworks for Wireless Sensor Networks - Review", 2nd International Conference on Communication, Computing and Security, ICCCS-2012, Elsevier, 2012.

[9] S. Ranjitha, D. Prabakar, S. Karthik, "A study on security issues in wireless sensor networks", International Journal of Computer Sciences and Engineering, Volume-3, Issue-9, 2015.

[10] Proceedings, "Cryptographic hardware and embedded systems – CHES 2015", 17th International Workshop Saint-Malo, France, Springer, 2015.

[11] B. Brkić, "Bezbjednosni aspekti bežičnih senzorskih", pristupni rad, Departman za poslediplomske studije i međunarodnu saradnju, Univerzitet Singidunum, 2017.