Pregled sigurnosnih pretnji i mehanizama prevencije i zaštite u bežičnim senzorskim mrežama s primenom u preciznoj poljoprivredi

Nemanja Radosavljević, Đorđe Babić
Katedra za računarsko inženjerstvo, Računarski fakultet
Beograd, Srbija
nradosavljevic@raf.rs, djbabic@raf.rs

Sažetak – **U radu su prikazani aktuelni problemi bezbednosti prenosa podataka sa aspekta precizne poljoprivrede i ograničavajući faktori koje sa sobom donosi tehnologija bežičnih senzorskih mreža. Da bi se ovi problemi rešili ili predupredili, detaljno smo predstavili različite tipove napada u bežičnim senzorskim mrežama, kao i mehanizme detekcije, prevencije i odbrane od pomenutih napada.**

Ključne reči – bežične senzorske mreže; precizna poljoprivreda; bezbednost podataka; detekcija napada; mehanizmi zaštite.

I. UVOD

Poslednjih godina primetan je nagli razvoj tehnologija u korišćenju bežičnih senzorskih mreža (WSN – Wireless Sensor Networks), i to u sasvim različitim oblastima, kao što su vojna industrija, medicina, sport, privreda uopšte, a naročito u poljoprivredi, što je i predmet pažnje ovog rada. WSN se u poljoprivredi koriste za posmatranje različitih ekoloških pojava na velikoj površini, što se postiže korišćenjem uređaja koji se nazivaju senzorski čvorovi. Bežične senzorske mreže sastoje se od senzorskih čvorova, procesora i radio-frekventnih (RF) modula i imaju baterijsko napajanje. Način komunikacije senzorskih čvorova zavisi prvenstveno od samog sklopa datog čvora, kao i od topologije na kojoj je zasnovana WSN [1].

Čvorovi koji se koriste u preciznoj poljoprivredi (PP) mogu biti veoma kompleksni, kao u slučaju kada prate lokaciju ili analiziraju slike, ali mogu da budu i sasvim jednostavni, kada prate promene temperature, pritiska, vlažnosti, ph vrednosti, nivoa vode i nekih drugih pokazatelja. Svi ovi senzorski čvorovi omogućavaju nam da precizno pratimo razne promene parametara koji su od značaja za posmatrano područje. Primena tehnologije WSN za prikupljanje, čuvanje i obradu podataka pruža nam mogućnosti da konstantno unapređujemo poljoprivredu, a samim tim i prinose [2].

Prilikom primene WSN u poljoprivredi srećemo se sa sledećim problemima koje je potrebno rešiti; to su [3]: izrada optimalnih nacrta raspoređivanja čvorova, određivanje perioda merenja, izbor protokola za rutiranje, energetska efikasnost, način prenosa podataka, skalabilnost, stepen tolerancije na greške, kao i bezbednost prenosa i tačnost podataka [1].

Da bi se jedna WSN smatrala bezbednom, neophodno je obezbediti dostupnost, poverljivost, integritet i autentikaciju podataka koji se prenose kroz mrežu. U ovom radu razmatramo probleme bezbednosti prenosa podataka i predlažemo moguća rešenja za navedene tipove napada.

II. PROBLEMI BEZBEDNOSTI U PRECIZNOJ POLJOPRIVREDI

Bežične senzorske mreže koje se primenjuju u preciznoj poljoprivredi imaju nekoliko karakteristika koje ih čine podložnim različitim napadima [4]. Da bi WSN mogle da se koriste u različitim aplikacijama, neophodni su jednostavni protokoli za upravljanje topologijom, bezbednošću i komunikacijom, koje razmatramo dalje u radu. Važno je naglasiti da je bezbednost WSN-a pitanje kojem je potrebno posvetiti najveću pažnju bez obzira na područje primene [5]. Ograničavajući faktori arhitekture WSN u PP su: i) senzorski čvorovi u bežičnim senzorskim mrežama imaju ograničenu memoriju, energiju, sposobnost računanja, propusni opseg i opseg komunikacije; ii) *ad hoc* raspoređivanje čvorova u senzorskoj mreži olakšava napadačima da pokrenu različite vrste napada, koji se kreću od aktivnog ometanja do pasivnog prisluškivanja; iii) WSN topologija je dinamična i nedostaje joj fiksna infrastruktura, zbog čega je neprekidan nadzor mreže otežan; iv) snažni sigurnosni protokoli mogu degradirati performanse pošto troše više resursa na senzorskim čvorovima pa se mora uspostaviti kompromis između performansi i bezbednosti; v) u bežičnim mrežama svako može da učestvuje ili prati kanale komunikacije s radio-konfiguracijom na istoj frekvenciji, što ih čini podložnim napadima.

III. SIGURNOSNI CILJEVI U WSN S PRIMENOM U PP

Da bismo zaštitili bežične prenose od različitih vrsta napada, potrebno je ispuniti dva osnovna zahteva u bežičnim senzorskim mrežama: bezbednost i potreba preživljavanja (*survivality requirements*) senzorske mreže. Sigurnosni ciljevi koji se odnose na bezbednost sistema PP su [4]: i) poverljivost – kod poverljivosti najveća opasnost jeste postojanje kompromitovanih čvorova, jer napadač može da eksploatiše ove čvorove da bi ukrao važne podatke kao što su kriptografski ključevi; ii) autentikacija – svaka bazna stanica i senzorski čvor

moraju biti sposobni da ustanove da li im paket šalje napadački ili legitimni čvor; iii) integritet podataka – ukoliko se koriste podaci čiji je integritet narušen, to može da dovede do nesagledivih posledica, pa se precizna poljoprivreda u velikoj meri oslanja na integritet informacija koje se prenose kroz mrežu; iv) upravljanje bezbednošću – od posebne važnosti u PP jeste kontrola bazne stanice.

Zahtevi za preživljavanje WSN u PP odnose se na njihovu pouzdanost, dostupnost i energetsku efikasnost. Ovi zahtevi za preživljavanje senzorskih mreža opisani su u nastavku [4]. Energetska efikasnost je posebno važna jer u arhitekturi sistema u preciznoj poljoprivredi datoj na Sl 1. senzorski čvorovi imaju baterijsko napajanje ograničene energije.

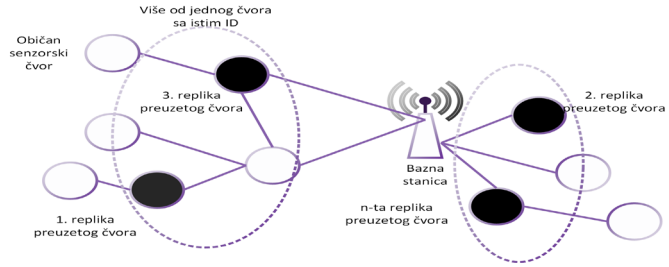
IV. Istaknuti napadi i mehanizmi odbrane u WSN za preciznu poljoprivredu

U delu rada koji sledi dat je opis karakterističnih napada i mehanizama detekcije, prevencije i zaštite u bežičnim senzorskim mrežama.

A. *Napad hvatanja čvora*

Bežične senzorske mreže podložne su napadu hvatanja čvora (NC –Node capture) ukoliko čvorovi nisu raspoređeni tako da budu pod nadzorom. Kada protivnik uhvati senzorske čvorove, on može da pokrene različite vrste napada kroz taj kompromitovani čvor. Napadač uzima informacije o tajnim ključevima iz ugroženog čvora i širi (plasira) u WSN veliki broj replika (lažnih čvorova) koje imaju isti ID i tajni ključ kao originalni čvor. NC napad može da napravi veliku štetu u energetskoj efikasnosti susednih čvorova, ali i samoj distribuciji netačnih informacija sa tog čvora koje mogu da dovedu do donošenja nekih pogrešnih odluka [6].

Princip zaštite prikazan je na Sl 1. i počiva na tome da se u WSN za preciznu poljoprivredu lokacije senzorskih čvorova ne menjaju nakon implementacije, kao i da svaki senzorski čvor može da identifikuje izvore svih poruka od svojih suseda. Primena WSN u arhitekturi PP u ovom radu zasnovana je na činjenici da znamo poziciju i gustinu postavljenih senzora, a za ovaj tip napada napadač mora fizički da uzme senzor; možemo se pozvati na svojstvo ovog pristupa koje se zasniva na broju senzorskih čvorova koji mogu biti fizički uhvaćeni u određenoj regiji jer ako se poveća broj uhvaćenih senzora, povećava se i verovatnoća da se otkrije napadač. Pored ovoga, neophodno je određeno vreme za preuzimanje čvorova i za njihovo ponovno vraćanje u mrežu. U statičkim mrežama senzora kao što je naša čvor se smatra kompromitovanim ukoliko se isti ID ponavlja na više od jedne lokacije.



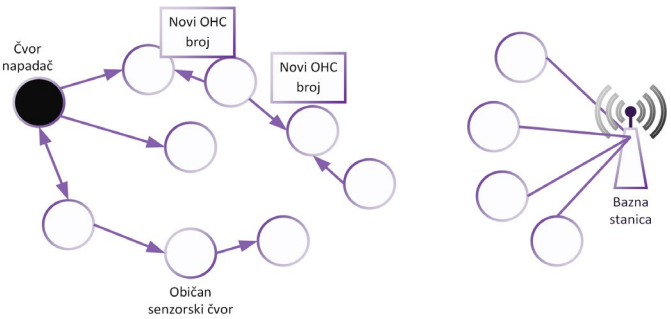
Slika 1. Shematski prikaz napada hvatanja čvora

B. *Napad odbijanja sna (DoS)*

Glavna meta napada odbijanja sna je baterijsko napajanje i iscrpljivanje resursa senzorskog čvora, koji su ograničeni. Ovaj napad pričinjava poteškoće zato što zamena senzora često nije nimalo jednostavna, već komplikovana ili skupa, a to isto odnosi se i na zamenu ili dopunjavanje baterijskog napajanja. Ukoliko WSN podlegne ovom napadu i ne uspemo da ga zaustavimo, to automatski znači da je time smanjen životni vek mreže.

Čvorovi su ugroženi uprkos tome što se autentičnost potvrđuje upotrebom *hash* algoritama i simetričnih ključeva. Zlonamerni čvor koji pristupa simetričnim ključevima može pristupiti i informacijama koje pripadaju baznoj stanici. Ukoliko dođe do kompromitovanja podataka koji se tiču bazne stanice, onda je i cela WSN kompromitovana. Najkritičnija tačka za arhitekturu bežične senzorne mreže u PP je bazna stanica, tako da svi podaci koji joj pripadaju moraju da budu maksimalno zaštićeni, tj. ne smeju da budu poznati nijednom drugom čvoru u mreži jer je to jedini način da budemo sigurni da bazna stanica nije kompromitovana.

U PP najučestaliji je takozvani permanentni DoS (PDoS) napad [7], gde neprijatelj iz daljine preplavljuje senzorske čvorove tako što šalje lažne pakete ili ponavlja pakete koji su već preneseni kroz mrežu. Na Sl. 2 predloženo je rešenje pomoću One-way Hash Chains (OHC) kako bi se zaštitila komunikacija s kraja na kraj od PDoS-a. Svaki čvor je konfigurisan pomoću OHC-a, tako što srednjim čvorovima omogućuje otkrivanje PDoS-a i sprečava širenje ponovljenih ili lažnih paketa. Ovde svaki paket uključuje novi OHC broj. Samo ako je OHC broj novi, srednji čvor predaje paket. Upotreba OHC broja sprečava neprijatelja da preplavi put ponovljenim paketima.



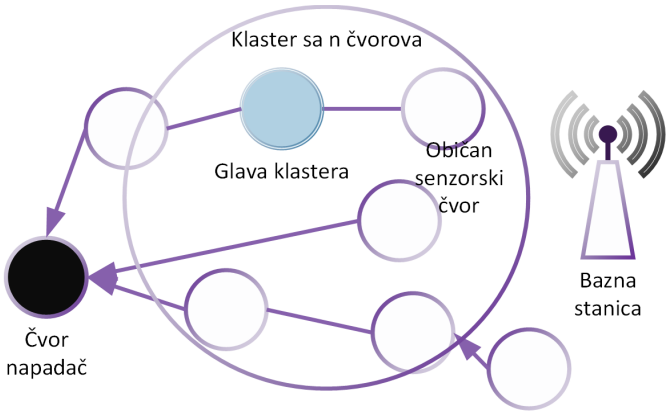
Slika 2. Shematski prikaz napada odbijanja sna

C. *Napad preplavljivanja pozdravnim porukama*

Napad preplavljivanja pozdravnim (HELLO) porukama je opasnost od poplava porukama koje se koriste za otkrivanje suseda. Napadač velikom snagom prenosa šalje ili odgovara na HELLO pakete tako da ga veliki broj čvorova u mreži vidi kao susedni čvor. Napadač emituje pakete tako velikom snagom da ga veliki broj čvorova u mreži bira kao roditeljski čvor. Kašnjenje se povećava jer se sve poruke prenose preko čvora napadača. Na ovaj način deo mreže koji je pod napadom stiče utisak da je napadač bazna stanica i može da preuzme potpunu

kontolu nad čvorovima i da u potpunosti odseče deo mreže od ostatka WSN [8].

Jedan od najboljih mehanizama zaštite od ovog napada koji je prikazan na Sl. 3, između ostalog, počiva na velikoj energetskoj efikasnosti – to je Low Energy Adaptive Clustering Hierarchy (LEACH). Prema podacima koji se mogu naći u literaturi [9], ovaj mehanizam zaštite zasnovan je na podeli WSN na klastere. Na osnovu određivanja praga za broj čvorova koji pripadaju svakom od klastera određuje se glava (*head*) za svaki od klastera i na taj način pokreće mehanizam zaštite od ove vrste napada WSN u PP. Algoritam zaštite funkcioniše po principu detekcije glave klastera čiji je broj članova iznad praga koji je određen za svaki od klastera i na taj način se detektuje da li postoji uljez u mreži; međutim, potvrda da je zlonamerni čvor definitivno prisutan u mreži izvodi se na osnovu jačine primljenog signala i udaljenosti.



Slika 3. Shematski prikaz napada preplavljivanja pozdravnim porukama

D. *Napad ometanja*

Kod ove vrste napada uređaj koji izvodi ometanje emituje signale radio-frekvencija koji su za čvorove senzora beskorisni ili neželjeni podaci. Ovaj signal može da podseća na mrežni protok ili može biti beli šum. Čin namernog usmeravanja elektromagnetne energije prema komunikacionom sistemu naziva se ometanje, i služi da bi prekinuo prenos signala [10]. Napadi bežičnih senzorskih mreža koji se „igraju“ radio-frekvencijama čvorova nazivaju se ometanje [5].

Izdvajamo tri vrste napada ometanja:

• Napadač cilja na jednu frekvenciju (*spot jamming*) koju žrtva koristi trošeći mnogo snage da bi nadglasala originalni signal.

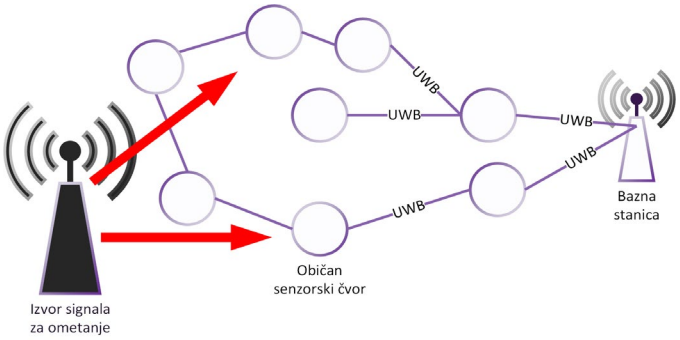
• Napadač velikom brzinom menja različite frekvencije (*sweep jamming*) i na taj način svaku od njih na kratko ometa signalom pune snage.

• Napadač u isto vreme ometa više frekvencija (*barrage jamming*). Kako raste opseg ometanih frekvencija, tako se smanjuje moć ometanja na prethodnu frekvenciju.

Postoji nekoliko protivmera koje se koriste za sprečavanje ometanja, kao što su Frequency Hopping Spread Spectrum [11], Direct Sequence Spread Spectrum, Ultra Wide Band Spectrum, Antenna Polarization, Directional Transmission koje se opisane u radu koji je naveden u literaturi [4]. Neke od navedenih metoda su računski zahtevne, kao što je Direct Sequence Spread Spectrum, ili nisu nimalo energetski efikasne, kao Frequency Hopping Spread Spectrum, jer zahtevaju konstantnu promenu frekvencija, kao i Antenna Polarization i Directional Transmission jer su im potrebne suviše kompleksne antene za primenu u PP.

Mehanizam zaštite koji privlači našu pažnju prikazali smo na Sl. 4, a to je upotreba Ultra Wide band (UWB) tehnike modulacije koja je zasnovana na emitovanju kratkih impulsa na veoma velikom frekvencijskom opsegu [12]. Ovo otežava prenošenje ili presretanje signala koji se prenosi i čini ga otpornim na efekte izazvane rasejanjem i refleksijom signala. Postoje istraživanja u kojima je predstavljen raspored senzorskih čvorova koji zahteva malo energije [13].

UWB takođe garantuje produženo trajanje baterije i preciznu lokalizaciju.



Slika 4. Shematski prikaz napada ometanja

E. *Napad ponovnog prosleđivanja poruka*

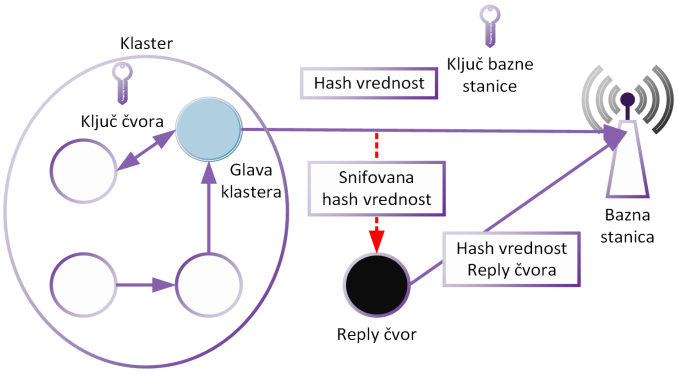
Napad ponovnog prosleđivanja poruka jedan je od podtipova napada odbijanja spavanja. Primena WSN u PP je ranjiva i podložna ovom tipu napada koji se zasniva na prisluškivanju saobraćaja u mreži i njegovom ponovnom slanju kroz mrežu. Ako se na neki način ne branimo od ove vrste napada, saobraćaj koji napadač generiše smatraće se regularnim saobraćajem za ovu mrežu pa će čvorovi pokušati da ga prenesu do odredišta. Na ovaj način generiše se velika količina nekorisnog saobraćaja u mreži i tako se iscrpljuje napajanje svakog čvora ponaosob. Napad je zasnovan na principu da protivnik presreće podatke i da ih ponovo šalje [14].

Dobre rezultate u zaštiti od ovog napada dao je mehanizam zaštite na mreži koja je 100x100 metara i ima 100 čvorova koji su nasumično raspoređeni [14]. Primena ovog modela u PP može lako da se skalira na veće površine, kao i na površine različitih proporcija a da ne ugrozi mehanizam zaštite. Polazimo od toga da nisu definisani klasteri, kao i da su heterogeni uslovi u mreži, te da nemaju svi čvorovi istu početnu energiju. Svaki čvor ima dva tajna (privatna) ključa. Jedan od ključeva koristi se za komunikaciju između čvorova. Drugi ključ koristi se za komunikaciju s baznom stanicom, i to tek kada čvor preuzme ulogu glave klastera (*cluster head*).

Da bismo napadača odvratili od pristupa mreži, autentifikaciju treba izvršiti između glave klastera i čvorova koji treba da se pridruže mreži kao što smo prikazali na Sl. 5.

Svaki čvor proverava autentičnost glave klastera (*cluster head*) pre nego što pošalje zahtev za pridruživanje mreži.

Autentičnost čvorova koji zahtevaju pridruživanje klasteru verifikuje se od strane glave klastera pre nego što oni postanu članovi tog klastera. Određeni čvor je glava klastera u jednom ciklusu. Izbor čvora koji treba da postane glava klastera u novom ciklusu vrši se pre kraja trenutnog ciklusa. Čvor koji je izabran za novu glavu kalastera mora da se verifikuje na baznoj stanici preko postojeće glave klastera. Posle toga bazna stanica obaveštava čvorove o tome koji su čvorovi izabrani da budu glave klastera u sledećem ciklusu.



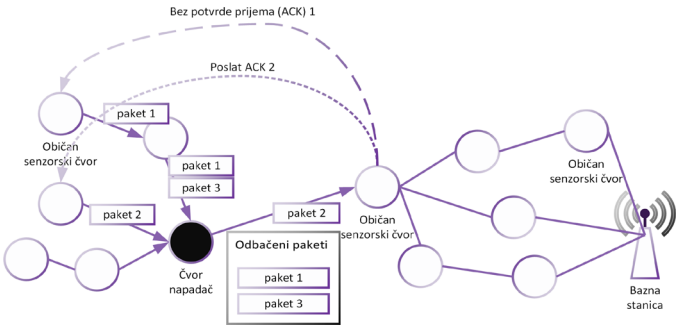
Slika 5. Shematski prikaz napada ponovnog prosleđivanja poruka

F. *Napad selektivnog prosleđivanja*

To je napad na sloju prenosa podataka u kojem zlonamerni čvor odbija neke legitimne pakete i odbacuje ih. Selektivno prosleđivanje može se implementirati na dva različita načina u odnosu na pakete koji se odbijaju. Prvo, odbacivanjem paketa određenog tipa i, drugo, odbacivanjem paketa određenog porekla ili namene za određene čvorove [4].

Mehanizam zaštite koji je pogodan za primenu u PP jeste detekcija korišćenjem priznanja (Detection Using Acknowledgments – DUA) zbog relativno malog opterećenja za resurse kojima čvorovi raspolažu i prikazan je na Sl. 6, za razliku od ostalih mehanizama koji daju podjednako dobre rezultate, ali su zahtevni u pogledu iscrpljivanja baterijskog napajanja čvorova.

DUA predstavlja multihop šemu priznanja koja pokreće alarm, na osnovu odgovora iz drugih čvorova. Čvorovi koji se nalaze na ruti prosleđivanja imaju mogućnost da primete zlonamerni čvor unutar mreže. Srednji čvorovi prilikom otkrivanja zlonamernog čvora putem multihopa šalju poruku sa alarmom baznoj stanici. DUA se sastoji od tri paketa za detekciju napada koji su nazvani paket priznanja, paket izveštaja i paket alarma. Postoje dva postupka detekcije: i) nizvodno koji označava da se prenos podataka vrši iz izvora čvorišta prema baznoj stanici; ii) uzvodno koji označava prenos podataka od bazne stanice prema izvornom čvoru [15].



Slika 6. Shematski prikaz napada selektivnog prosleđivanja

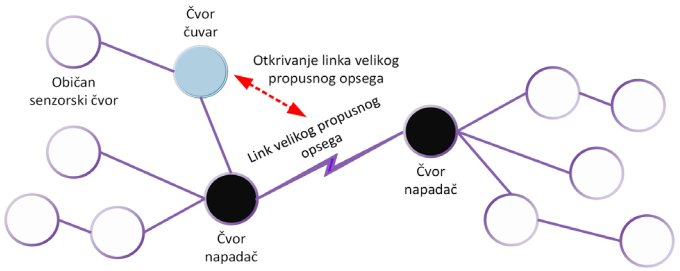
G. *Napad crvotočine (Wormhole)*

U ovom napadu neprijatelji putem tunela šalju paket kroz snop ili van snopa kanala između dve udaljene lokacije. Takvi vormhol (*wormhole)* tuneli udaljenim čvorovima stvaraju iluziju da su oni mnogo bliži jedan drugome nego što zapravo jesu [16]. Protivnik može sakupljati mrežni protok i manipulisati njime jer wormhol može proći i privući ogromnu količinu protoka. Napadač ne poseduje validan mrežni identitet, on je autsajder koji može da prosledi komunikacijski tok duž ormhola a da nema direktan uvid u sadržaj paketa. Koristeći takve veze sa vormholovima, protivnik može pokrenuti obrnuti inženjering protokola, čovek-u-sredini (*man in the middle*) napad, prekidanje šifara itd. [4].

Kao najpogodniji mehanizam odbrane za primenu na otvorenom polju pokazuje se mehanizam koji ne zahteva nikakva dodatna hardverska rešenja, kao ni potrebu da se unapred znaju lokacije čvorova. Rešenje prikazano na Sl. 7 objedinjuje u sebi već dva dobro poznata principa – to je princip zasnovan na kombinaciji *Liteworp* koncepta i koncepta abnormalno visokih frekvencija na vormhol kanalu.

Liteworp koncept polazi od pretpostavke da topologija mreže pre samog inicijalnog pokretanja nije pod *wormhole* napadom. Svaki čvor u fazi raspoređivanja zajedno sa svoja dva suseda prisluškuje nesusedne čvorove, koji biraju čvorove čuvare, te ukoliko se naruši taj poredak, oni detektuju da je došlo do napada [17]. Ovaj koncept je posebno značajan za primenu bežičnih senzorskih mreža u PP.

Koncept abnormalnih frekvencija zasnovan je na osobini *wormhole* veza koje imaju veliku učestalost. To je način da se razlikuje *wormhole* veza u odnosu na normalne veze [18].

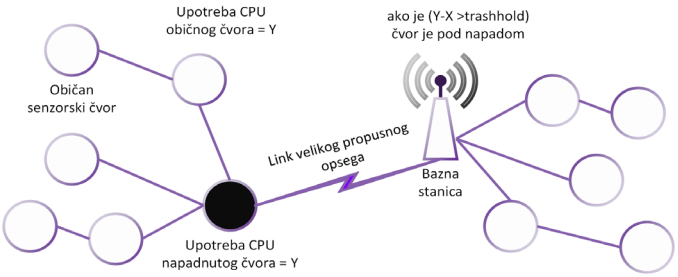


Slika 7. Shematski prikaz *womhole* napada

H. *Sinkhol napad*

U sinkhol napadu kompromitovani čvor izgleda posebno privlačno za okolne čvorove u skladu sa algoritmom rutiranja u napadnutoj mreži. Kompromitovani čvor privlači okolne čvorove lažnim informacijama o rutiranju, a zatim menja podatke koji prolaze. Svojim selektivnim prosleđivanjem ili neprosleđivanjem određenih poruka sprečava pristupnu tačku (*gateway*) da dobije potpunu i tačnu informaciju, što dovodi do problema u procesu analize i obrade podataka [4].

Jedna od karakteristika koja je uočena za čvor koji je pod ovim napadom jeste povećanje opterećenja procesora, pa kao najadekvatniji predlog za detekciju ovog napada može poslužiti tehnika za izračunavanje razlike korišćenja CPU-a za svaki čvor praćenjem korišćenja procesora u fiksnom vremenskom intervalu. Korišćenjem ove razlike, bazna stanica određuje da li je čvor legitiman ili zlonameran [19]. Ovaj mehanizam zaštite prikazali smo na Sl. 8.



Slika 8. Shematski prikaz sinkhol napada

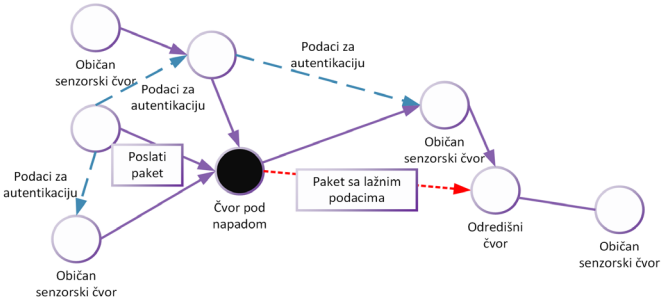
I. *Napad lažnog predstavljanja*

Ovaj napad zasnovan je na ugrožavanju autentičnosti izvorišnog čvora. Napad nije moguće izvesti ukoliko dva čvora koja komuniciraju nisu jedan drugom u dometu, a da bi mogli da komuniciraju međusobno, neophodno je da se komunikacija obavlja posredno, preko drugih čvorova koji se nalaze između njih.

Napadi oponašanja koji su od ključne važnosti za primenu na otvorenom prostoru sprovode se ili tako što zlonamerni čvor preuzme ID izvorišnog čvora iz paketa koje prosleđuje iz relejnih paketa podataka ili pak tako što zlonamerni čvor šalje lažne podatke odredišnom čvoru, a u tim podacima je i prethodno ukradeni ID izvorišnog čvora [20].

Da bi se odbranili od ovog napada, svi čvorovi WSN moraju da budu uvereni da su paketi autentični. Na Sl. 9 prikazan je metod koji daje dobre rezultate i koji zadovoljava sve kriterijume na kojima se zasniva arhitektura sistema posmatranog u ovom radu. Metod počiva na više ruta. Za registraciju *hash* vrednosti ID-jeva susednih čvorova na izvorišnom čvoru koristi se Bloom filter. Ovaj metod je nazvan autentični identitet Bloom filter (AIBF) i koristi se da obezbedi raštrkan prenos podataka za autentifikaciju paketa legitimnog izvorišnog čvora.

Pored toga, u predloženoj metodi koristi se Source-initiated tree-based Routing (SRIDR) [21]. SRIDR se bazira na metodi rutiranja ID-ja zasnovanog na stablu i za svaki čvor je kreirana tabela rutiranja. Ovaj metod se sastoji od tri postupka: prenosa autentičnog identiteta, korišćenja autentičnog identiteta za otkrivanje falsifikata i otkrivanja napada lažnog predstavljanja.



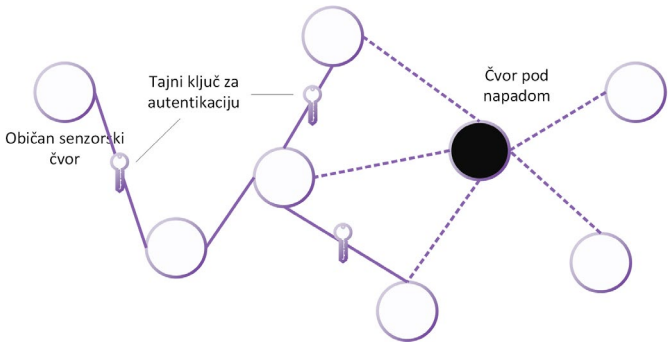
Slika 9. Shematski prikaz napada lažnog predstavljanja

J. *Sybil napad*

Kod bežičnih senzorskih mreža karakteristično je da sibil (*sybil*) napad iscrpljuje resurse i da predstavlja ozbiljnu pretnju protokolima rutiranja. U ovom napadu napadač preuzima identitet čvorova u sistemu i lažno se predstavlja drugim legitimnim čvorovima u sistemu. Takvi čvorovi nazivaju se sibil čvorovima. Sibil čvorovi šalju veliki broj zahteva za pridruživanje pristupnoj tački, koristeći nasumične MAC vrednosti. Jednom kada sibil čvor zauzme kanale za pristup ili asocijativne slotove, onda je legitimnim klijentima pristup onemogućen [4].

Protivnici imaju potencijalno više resursa kao što su procesorska snaga, jačina primopredajnika ili izvor napajanja, a ovi faktori su od presudnog značaja za sistem koji je zasnovan na baterijskom napajanju, na velikom području kao što su njive i polja.

Pristup zaštite prikazan na Sl. 10 koncipiran je na tehnikama autentifikacije tajnim ključem. Nekoliko ključnih tehnika upravljanja predloženo je na osnovu deljenja ključnih delova za verifikaciju u senzorskim mrežama [22]. Kako bi se smanjila potreba za sistemskim zahtevima za šifrovanje, najpogodnije je koristiti informacije o lokaciji senzorskih čvorova na fizičkom sloju.



Slika 10. Shematski prikaz *sybil* napada

V. ZAKLJUČAK

U ovom radu predstavljen je pregled bezbednosnih pretnji u WSN sa upotrebom u preciznoj poljoprivredi. Posebna pažnje usmerena je na bezbednost prenosa podataka u bežičnim senzorskim mrežama, kao i na algoritme i mehanizme koji

obezbeđuju adekvatnu zaštitu od karakterističnih napada u bežičnim senzorskim mrežama.

Zaključeno je da ovi mehanizmi koji su sublimirani u jedan rad, a koji su detaljno objašnjeni i grafički prikazani, u potpunosti mogu da obezbede sve aspekte bezbednosti kao što su poverljivost, autentifikacija i integritet.

ZAHVALNICA

Ovaj rad podržalo je Ministarstvo prosvete, nauke, i tehnološkog razvoja Republike Srbije, u okviru projekta tehnološkog razvoja TR32023 – „Optimizacija performansi energetski efikasnih računarskih i komunikacionih sistema“.

LITERATURA

[1] H. M. Jawad, R. Nordin, S. K. Gharghan, A. M. Jawad and M. Ismail, “Energy-Efficient Wireless Sensor Networks for Precision Agriculture: A Review.”, Sensors, Vol. 17. 1781, doi:10.3390/s17081781, 2017.

[2] I. Jawhar., “A framework for using unmanned aerial vehicles for data collection in linear wireless sensor networks.”, Journal of Intelligent & Robotic Systems, Vol. 74. 437–453, 2014.

[3] T. Ojha, S. Misra and N. S. Raghuwanshi, “Wireless sensor networks for agriculture: The state-of-the-art in practice and future challenges.”, Computers and Electronics in Agriculture, Vol. 118. 66–84, 2015.

[4] B. Bhushan and G. Sahoo, “Recent Advances in Attacks, Technical Challenges, Vulnerabilities and Their Countermeasures in Wireless Sensor Networks.”, Wireless Pers Commun, Springer Science+Business Media, doi: 10.1007/s11277-017-4962-0, 2017.

[5] E. Shi and A. Perrig, “Designing secure sensor networks.”, Wireless Communications Magazine, 11(6), 38–43, 2004.

[6] S. Pavaimalar and G. ShenbagaMoorthy, “Detection of node capture attacks in wireless sensor networks.”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 1, ISSN: 2278 – 1323, 2013.

[7] J. Deng, R. Han and S. Mishra, “Defending against path-based DoS attacks in wireless sensor networks.”, In Proceedings of 3rd ACM workshop on security of ad hoc and sensor networks (SASN’05), Alexandria, VA, 2005.

[8] R. Singh, J. Singh and Dr. Ravinder, “Hello flood attack countermeasures in wireless sensor networks.”, International Journal of Computer Science and Mobile Applications, Vol.4 Issue. 5, pg. 1-9, ISSN: 2321-8363, 2015.

[9] Y. Shen, S. Liu and Z. Zhang, “Detection of Hello Flood Attack Caused by MaliciousCluster Heads on LEACH Protocol.”, International Journal of Advancements in Computing Technology (IJACT)) Volume 7, Number 2, 2015.

[10] D. L. Adamy and D. Adamy, “EW 102: A second course in electronic warfare.”. Norwood, MA:Artech House Publishers, 2015.

[11] R. L. Pickholtz, D. L. Schilling and L. B. Milstein, “Theory of spread spectrum communications.”, 1982.

[12] http://en.wikipedia.org/wiki/Ultrawideband., UWB-wikipedia.

[13] I. Oppermann, L. Stoica, A. Rabbachin, Z. Shelby and J. Haapola, “UWB wireless sensor networks: UWEN-a practical example.”, IEEE Communications Magazine, 42(12), 27–32, 2004.

[14] V. C. Manju and M. Sasikumar, “Mitigation Of Replay Attack In Wireless Sensor Network.”, Int. J. on Information Technology, Vol. 5, 2014.

[15] B. Yu and B. Xiao, “Detecting selective forwarding attacks in wireless sensor networks.”, IPDPS 2006 - 20th In Parallel and distributed processing symposium, p. 8, 2006.

[16] Ž. Gavrić and D. Simić, “Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks.” Ingeniería e Investigación, 38(1), 130-138, doi: 10.15446/ing.investig.v38n1.65453, 2018.

[17] I. Khalil, S. Bagchi and N. B. Shroff, “Liteworp: A light-weight countermeasure for the wormhole attack in multi-hop wireless networks.” In Proceedings of DSN, pp. 612–621, 2005.

[18] N. Song, L. Qian and X. Li, “Wormhole attack detection in wireless ad hoc networks: A statistical analysis approach.”, In Proceedings of IEEE IPDPS, 2005.

[19] C. Chen, M. Song and G. Hsieh, “Intrusion detection of sinkhole attacks in large-scale wireless sensor networks.”, In IEEE international conference on wireless communications, networking and information security (WCNIS), pp. 711–716, 2010.

[20] N. Tanabe, E. Kohno and Y. Kakuda, “An Impersonation Attack Detection Method Using Bloom Filters and Dispersed Data Transmission forWireless Sensor Networks.”, 2012 IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, 2012.

[21] T. Okazaki, E. Kohno and Y. Kakuda, “Improvement of assurance for wireless sensor networks using packet detouring and dispersed data transmission.” in Proc. 2011 IEEE International Conference on Internet of Things and Cyber, Physical and Social Computing (iThings/CPSCom 2011), pp. 144–151, 2011.

[22] H. Chan, A. Perrig and D. Song, “Random key predistribution schemes for sensor networks.”, In Proceedings of IEEE symposium on security and privacy, pp. 197–213., 2003.

ABSTRACT

With the increasing global concern for the security and privacy of data, and the question of their transfer through various types of networks. The issue of security is particularly important for wireless sensor networks because of their architecture. These are composed of a plurality of small sensors. These sensors collect and transmit data. In wireless sensor networks only a few nodes act as base stations. This paper presents the basic problems related to security threats in precision agriculture in wireless sensor networks and mechanisms that are used to prevent them.

ANALYSIS OF SECURITY THREATS, PREVENTION AND PROTECTION MECHANISMS IN WIRELESS SENSOR NETWORKS IN PRECISION AGRICULTURE

Nemanja Radosavljević, Đorđe Babić