Sigurna detekcija i praćenje objekata u kompromitovanoj bežičnoj senzorskoj mreži

Milan Stanojević,Aleksandar Jevremović,Igor Vujčić
Tehnički fakultet/Elektrotehnika i računarstvo
Univerzitet Singidunum
Beograd, Republika Srbija
milan.stanojevic.16@singimail.rs
ajevremovic@singidunum.ac.rs
ivujcic@singidunum.ac.rs

Petar Spalević,Nenad Stanojević
Fakultet tehničkih nauka
Univerzitet u Prištini-Kosovska Mitrovica
Kosovska Mitrovica, Republika Srbija
petar.spalevic@pr.ac.rs
nenad.stanojevic@pr.ac.rs

Sažetak—**Tokom dugogodišnjeg razvoja i primene bežičnih senzorskih mreža, napravljen je ogroman napredak na polju istraživanja i unapređenja bezbednosti bežičnih senzorskih mreža, naročito imajući u vidu njihova nepremostiva ograničenja. Jedna od važnih primena bežičnih senzorskih mreža jeste bezbednosna zaštita, a u okviru nje primena funkcije praćenja objekata u nadgledanoj zoni (senzorskom polju). Izvršavanje ove funkcije zavisi od sposobnosti mreže da izvrši efikasnu detekciju objekta koji se kreće i da tu informaciju pošalje, kako bi se obezbedila pravovremena reakcija. Sigurna detekcija i praćenje objekata još više predstavlja imperativ kada je bežična senzorska mreža primenjena u zaštiti kritičnih misija, u udaljenoj i neprijateljskoj sredini. U jednom takvom okruženju je naročito važno da senzorski čvorovi sačuvaju svoju pouzdanost i integritet podataka. Upad u celovitost mreže i izmena podataka dobijenih merenjem i opažanjem senzora, ima za rezultat slanje lažnih i pogrešnih informacija o kretanju objekta, što u konačnom može dovesti do katastrofalnih posledica. U ovom radu predstavljen je bezbedan i pouzdan protokol za praćenje objekata, koji uzima u obzir istovremeno i bezbednost i praćenje objekata, čime obezbeđuje pouzdanost podataka u bežičnoj senzorskoj mreži čak i u prisustvu kompromitovanih senzorskih čvorova.**

Ključne reči-praćenje objekata; zaštita kritičnih misija; pouzdano praćenje; bežične senzorske mreže

I. UVOD

Bežične senzorske mreže (skr. BSM) postavljaju jedinstvene sigurnosne izazove upravo zbog svojih inherentnih ograničenja u komunikaciji i računarskoj snazi. One predstavljaju skup prostorno distribuiranih autonomnih senzorskih čvorova (skr. SČ) sa kojima se vrši detekcija pojava i mere njene vrednosti. Zbog svojih osobina samoorganizovanja čvorova bez centralnog upravljanja, samoizlečenja, dinamičkog prilagođavanja stanju u mreži, cene implementacije i brzine postavljanja, predstavljaju atraktivno rešenje za mnoge aplikacije. Međutim, način njihovog raspoređivanja čini ih naročito ranjivim na razne napade. Bežične senzorske mreže se postavljaju u slučajevima gde imaju fizičku interakciju sa okolinom, ljudima i drugim objektima, zbog čega postaju naročito ranjivi na sigurnosne pretnje. Upotreba BSM u misijama zaštite kritičnih infrastruktura [1] podrazumeva gust raspored SČ u negostoljubivom okruženju, što može imati za posledicu napade na senzorske čvorove.

Sa godinama se cena koštanja BSM smanjila nasuprot unapređenju i povećanju njenih mogućnosti, resursa i performansi. Pa ipak ograničenja senzorskih čvorova su ostala ista naspram zahteva i količine dobijenih podataka u uslovima ograničene memorije, male energije, ograničenih računarskih mogućnosti i komunikacionih sposobnosti. Upravo su to njene ranjivosti na upad, presretanje, modifikaciju i fabrikaciju podataka dobijenih senzorima. Zato se u negostoljubivim uslovima ne mogu primeniti tradicionalne tehnike za ispunjenje bezbednosnih ciljeva poverljivosti, integriteta, pouzdanosti i dostupnosti podataka.

Detekcija i praćenje objekata u bežičnim senzorskim mrežama u funkciji zaštite kritičnih infrastruktura, je jedna od veoma važnih karakteristika BSM u kritičnim misijama. Kao jedna od kritičnih misija gde se BSM koriste za zaštitu kritične infrastrukture je nadzor granice neke države, nadzor objekta od vitalnog značaja za društvo ili generalno nadgledanje stanja nekog geografskog prostora.

Iako je objavljeno puno radova na temu algoritama za detekciju i praćenje objekata, pri čemu su se razmatrali različiti aspekti upotrebe istih u svetlu očuvanja energije, protoka podataka i komunikacionog opterećenja SČ, veoma se malo radova bavilo sigurnošću detekcije i praćenja objekata u nadgledanoj zoni. Imajući u vidu da se ne postavlja pitanje da li će, već kada će i kako će biti izvršen napad na BSM, potrebno je uspostaviti efikasan mehanizam za detektovanje inficiranih i kompromitovanih čvorova. Kao dodatna neophodnost u tako kompleksnoj situaciji se nameće da BSM i dalje ostane energetski efikasna, bez obzira na prisustvo kompromitovani SČ. Takođe se potencira i razmatranje efikasnost primene algoritma za praćenje u uslovima ograničenih hardverskih i kompjuterskih resursa.

Rad je organizovan prema sledećem: u Poglavlju II je data analiza neophodnih karakteristika sistema, u Poglavlju III su date hipotetičke osnove modela za sigurno detektovanje i praćenje objekata u BSM i problemi u detekciji i praćenju, u Poglavlju IV je dat pregled algoritama i protokola zasnovan na sigurnom i pouzdanom predviđanju na osnovu pouzdanih SČ. Poglavlje V daje bitne zaključke za rad i razvoj budućih BSM.

II. ANALIZA NEOPHODNIH KARAKTERISTIKA SISTEMA

A. Analiza postojećih algoritama za detektovanje i praćenje objekata

Pregledom dosadašnjih algoritama za detekciju i praćenje objekata u BSM, uočavamo tradicionalne i savremene pristupe. Kod tradicionalnih algoritama, prisutna je zahtevna i složena digitalna obrada signala, zbog čega su algoritmi centralizovani na jednom mestu. Upravo zbog toga bi primena tradicionalnih algoritama bila teško primenljiva u BSM zbog potrebe SČ za velikim hardverskim resursima i prisutnim ograničenjima SČzbog raspoložive energije. Zbog toga savremeni pristup u algoritmima za detekciju i pozicioniranje uzima u obzir očuvanje energetske efikasnosti SČ i BSM u celini, protok podataka i opterećenje komunikacionih kanala. Upravo svaka specifična primena BSM povlači jedinstven dizajn algoritma, pa tako primena BSM u zaštiti kritičnih infrastruktura nezaobilazno podrazumeva razmatranje pouzdanog i sigurnog izvršavanja algoritma. Algoritam treba da ispuni osnovne sigurnosne ciljeve, kojima se garantuje sigurno detektovanje i praćenje objekata u BSM i to:

- poverljivost (tajnost) podataka,
- integritet (celovitost/originalnost) podataka,
- autentičnost (poreklo) podataka i
- dostupnost (mogućnost korišćenja) resursa BSM svim SČ.

Osnovni sigurnosni cilj u BSM je zaštiti samu bežičnu senzorsku mrežu, senzorske čvorove i komunikaciju između čvorova. Analogno sigurnosnim klasama u računarskim sistemima [2], u BSM su takođe usvojene klase [3]. Ove klase pretnji su:

- prekid komunikacije SČ,
- presretanje podataka SČ (neovlašćen pristup SČ ili podacima),
- modifikacija podataka SČ ili samog SČ (potpun pristup SČ i podacima i njihova izmena) i
- fabrikovanje podataka (ubacivanje lažnih podataka u BSM).

Zbog toga je neophodno da BSM poseduje minimalni sigurnosni okvir, kako bi se efikasno suprotstavila ovakvim napadima.

U dosadašnjim razmatranjima [4],[5],[6] izbor adekvatnog algoritma je uslovljen energetskom efikasnošću mreže u celini. Da bi detektovanje i praćenje objekta bilo precizno potrebno je da bude aktivno što višeSČ, međutim to ima za posledicu brz utrošak raspoložive energije. Zato se pravi kompromis između energetske efikasnosti i broja aktivnih čvorova. Ovakvi aktivacioni algoritmi za detektovanje i praćenje imaju nekoliko metoda za aktiviranje SČ i to:

a) potpuna aktivacija, gde su svo vreme aktivni svi SČ dok ne potroše svu energiju. Ovakav metod nije energetski efikasan, ali je sigurnosno pouzdan, jer su svi SČ aktivni celo vreme i bilo kakvo neadekvatno ponašanje čvora mogu da detektuju ostali čvorovi u BSM.

b) nasumična aktivacija, gde je svaki čvor nasumično aktivan sa određenom verovatnoćom. Ovaj metod nije sigurnosno pouzdan zbog moguće kompromitacije čvora u stanju mirovanja i kasnijeg falsifikovanja podataka o kretanju objekta,

c) selektivna aktivacija, je takav algoritam gde se izbor sledećeg čvora ili grupe čvorava za aktivaciju zasniva na tome koji je od čvorova najbliži sledećem predviđenom položaju objekta, i u skladu sa tim se aktivira SČ u mod praćenja. Sa sigurnosnog aspekta propusti su isti kao kod nasumične aktivacije SČ.

*d) ciklična (**eng.** duty cycled) aktivacija, je takav algoritam koji podrazumeva da se određeni delovi BSM uključuju i isključuju u određenim trenucima vremena (ciklusima). Sigurnosni rizik ovakvog algoritma leži u mogućnosti da se kroz SČ distribuira komanda za uključenje/isključenje što može imati za posledicu isključenja dela ili cele BSM, a što uljez može iskoristiti.*

S druge strane hijerarhijski algoritmiza detekciju i praćenje objekata u mreži naglasak daju na što efikasnije prikupljanje podataka o objektu, a samim tim i energetski efikasnijim metodama. U okviru ove grupe algoritama izdvojili su se:

a) algoritmi sa metodom detektovanja i praćenja objekata zasnovan na stablu BSM [7][8][9][10][11], gde se čvor koji je detektovao objekat uvek postavlja za prvi čvor (eng. root node) i najbliži je samom objektu. Kako se objekat kreće kroz mrežu tako se ova uloga čvora predaje sledećem, a pojedini SČ postaju delovi stabla, dok drugi bivaju izbačeni.U analizi ovakvih algortama se izdvajaju: Skalabilno praćenje uz pomoć mrežnih senzora (eng. Scalable Tracking Using Networked Sensors - STUN), Kolaboracija na bazi dinamičkog konvojskog stabla (eng. Dynamic Convoy Tree-based Collaboration - DCTC), Optimizovana komunikacija i organizacija (eng. Optimized Communication & Organization - OCO) i Stablo za izbegavanje odstupanja (eng.Deviation Avoidance Tree-DAT).

b) algoritmi sa metodom detektovanja i praćenja objekata zasnovan na klasteru, gde se čvor koji je prvi detektovao objekat postavlja za vođu klastera-VK (eng. cluster head). U okviru ove grupe algoritama izdvajaju se sledeći tipovi: algoritmi statičkog klasterovanja i algoritmi dinamičkog klasterovanja[12][13][14][15].

c) Hibridni algoritmi za detektovanje i praćenje objekata, gde se kombinuju više metoda za detektovanje i praćenje, kao npr. prediktivno distribuirano praćenje (eng.

Distributed Predictive Tracking - DPT), dinamičko klasterovanje za akustično praćenje (eng. Dynamic Clustering for Acoustic Tracking - DCAT), hijerarhijska prediktivna strategija (eng. Hierarchical prediction strategy - HPS)[16][17][18].

Uporednom analizom dosad navedenih algoritama dolazi se do zaključka da njihove performanse sa stanovišta detektovanja i praćenja objekata mogu dati zadovoljavajuće rezultate, ali se ni jedan od algoritamanije pokazao dovoljno sigurnim čak i kada je i jedan čvor kompromitovan, jer pogrešni podaci mogu dovesti do pogrešnih odluka. Ni jedan od algoritama ne uzima u obzir da u slučaju malicioznog napada mreža neće moći da izvesti o tačnoj poziciji objekta u nadgledanoj zoni.U slučajevima kada BSM detektuje i prati objekte u kritičnim misijama, odsustvo sigurnosnog mehanizma u algoritmu za praćenje, može biti fatalno po samo ispunjenje misije. U tom slučaju, logična je upotreba neke vrste zaštite, međutim, olaka upotreba kriptografskih funkcija mogu dovesti do bitnih umanjenja performansi same BSM, kao što je povećanje vreme odziva senzorskih čvorova ili smanjenje energetske efikasnosti same mreže.

B. Bitne pretpostavke za model sigurne BSM

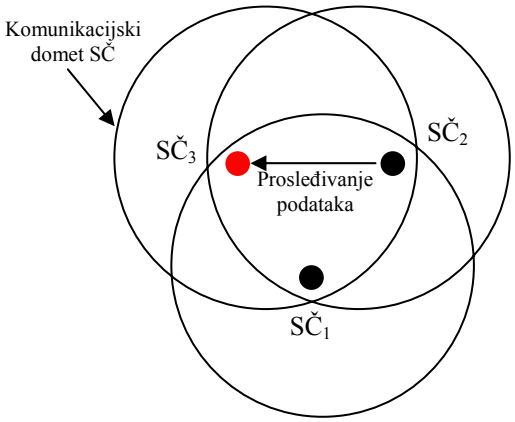
Pretpostavka je da će sistem koristiti veliki broj senzorskih čvorova, raspoređenih na udaljenom mestu, kako bi se izvršilo nadgledanje željenog prostora.Čvorovi su uniformno raspoređeni i u dovoljnom broju kako bi garantovali i obezbedili redundantnu pokrivenost nadgledane zone uz neophodnost poznavanja lokacije svakog senzorskog čvora. Pretpostavka je da jeukupan broj senzorskih čvorova u BSM (Ns) mnogo veći od broja malicioznih čvorova (Nc). Kako bi se omogućila zaštita senzorskih čvorova od kompromitacije, potrebno ih je opremiti osnovnim kriptografskim algoritmom kroz koji će susedni čvorovi da razmenjuju ključeve po unapred distribuiranoj šemi. Cilj je obezbediti proces detektovanja i praćenja objekta, pri čemu je potrebno obratiti pažnju na napade protiv integriteta i tačnosti podataka. S tim u vezi, se ne razmatra kriptovanje poruke, već se svaka poruka obeležava porukom integriteta, kao dokaz ne izmenjenosti poruke. Na takav način se SČ ne opterećuje računskim funkcijama, ne troši se dodatna energija i ne povećava se njegov vremenski odziv. Na ovakav način se želi obezbediti siguran proces detektovanja i praćenja objekata i zaštita SČ od napada na integritet, tačnost i ispravnost poruka.

III. MODEL SIGURNOG DETEKTOVANJA I PRAĆENJA OBJEKATA U BSM

Osnovni zahtev sigurne BSM je da kompromitovani čvorovi i napadači ne utiču na proces donošenja odluke ili da to čine sa veoma malom efikasnošću. Osnovna pretpostavka je da kompromitovani SČ u slučaju da se nađu na trajektoriji kretanja objekta, neće poslati podatke o objektu koji je ušao u nadgledani prostor vođi klastera (VK). Od ovakvog napada se VK može odbraniti, ako mu drugi SČ u blizini kompromitovanog SČ pošalju poruku o detektovanom objektu.

Međutim situacija je mnogo ozbiljnija ako je kompromitovan SČ zapravo VK. To se može desiti ako je u okviru određenog klastera kompromitovano više SČ, pa se prilikom smene VK drugim SČ radi pravilne uštede energije, za VK izabere upravo kompromitovani SČ. U tom slučaju kompromitovani VK može izbaciti iz rada veliki deo senzorskog polja jedne BSM. Ovakav VK može sprovesti više vrsta napada i to:da ne pošalje poruke buđenja SČ, čime bi deo mreže u blizini uljeza ostao ne aktiviran, a on ne detektovan; da ne probudi grupu senzora u blizini uljeza, već sasvim neku udaljenu grupu senzora, čime bi uljez izbegao detektovanje; da VK poruku o detektovanom uljezu zadrži ili ne prosledi baznoj stanici (BS).

Jedan od metoda da se efekti kompromitovanih čvorova ublaže jeste da se oni detektuju, a nakon toga i izoluju iz mreže. Osnovna ideja bi bila da se izvrši procena poverenja SČ koristeći model reputacije koji utvrđuje pouzdanost nekog čvora posmatrajući broj njegovih dobrih i loših postupaka. Procenu pouzdanosti jednog čvora utvrđuju susedni čvorovi međusobno posmatrajući i procenjujući stepen njegove pozdanosti. Kao elemente procene SČ posmatraju kako susedni čvor detektuje i usmerava (eng. routing) tako dobijene podatke. Ako u BSM postoje kompromitovani SČ, oni će selektovano ili pogrešno prosleđivati podatke, menjajući odredišnu adresu. Takvo pogrešno ponašanje detektuju susedni SČ i uz pomoćmehanizamazadetekcijuupadainadzora, gdečvorovisenzoraodržavajubafernedavnoposlatihpaketa podatkaiupoređivanjemsvakogslučajnogpaketasapaketom ubaferudabisevidelodalipostojipodudaranje[19]. Primerposmatračaje prikazannaslici1.



Slika 1. Ako kompromitovani čvor $SČ_3$ ne predaje pakete podataka $SČ_2$ pravilno, $SČ_1$ detektuje nepravilno ponašanje $SČ_3$

Raspored SČ u nadgledanoj zoni treba da bude takav da se susedni čvorovi svojim senzorskim poljima detekcije preklapaju, zbog čega su podaci o registrovanim pojavama povezani. Na takav način se uz pomoć gustog rasporeda čvorova može registrovati napada lažnim podacima.

Za potrebe detektovanja i usmeravanja, svaki SČ snima dobre i loše aktivnosti susednih čvorova u tabelu pod nazivom tabela ugleda (ili reputaciona tabela). Ova tabela se razmenjuje među SČ, kako bi se koristila kao informacija iz druge ruke u procesu evaluacije poverenja SČ, kao i u izboru SČ za VK. Tabela I. predstavlja tabelu ugleda gde čvor ocenjuje svoje čvorove susede. Ugled usmeravanja koristi se za odabir

pouzdanog pravca do bazne stanice, dok se ugled detektovanja koristi kako bi se povećala pouzdanost agregiranih podataka.Vrednosti senzorskih aktivnosti su u tabeli kvantifikovane uz pomoć beta reputacionog sistemaili Bajesove formule[19]. Upravo je Bajesova formulacija uspešno mogla da detektuje pogrešno ponašanje senzorskih čvorova i da na osnovu njenih vrednosti se iskaže poverenje nekom SČ.

TABELA I. TABELA UGLEDA SENZORSKOG ČVORA A SA 3 SUSEDNA ČVORA

$RepTab_A$	*Detekcija*	*Usmeravanje*
$Sused_A^1$		
$Sused_A^2$		
$Sused_A^3$		

Verovatnoća binarnih događaja može biti iskazana beta raspodelom koja je indeksirana sa dva parametra α i β. Beta raspodela $f(p|\alpha,\beta)$ može se izraziti koristeći gama funkcijuΓkao:

$$f(p|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)+\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1} \quad (1)$$

gde je $0 \le p \le 1$, $\alpha > 0$, $\beta > 0$.Vrednost očekivane verovatnoće beta raspodele je data formulom

$$E(p) = \frac{\alpha}{(\alpha+\beta)} \quad (2)$$

Beta funkcija se eksploatiše u BSM za zadatke detektovanja objekata tako što se uzima da su njegovi konačni ishodi dvojaki, „ispravan“ i „lažan“ [19]. Ako pretpostavimo da je *r* uočen broj „ispravnih“ objekata i *s* uočen broj „lažnih“ objekata od strane SČ. Beta funkcija uzima ceo broj detektovanih „ispravnih“ i „lažnih“ objekata u prošlosti , kako bi predvideo učestanost detektovanja „ispravnih“ objekata od strane tog SČ u budućnosti postavljanjem:

$$\alpha = r + 1 \;\; \beta = s + 1, gde\ je\ r, s \ge 0 \quad (3)$$

Promenljiva*p* predstavlja verovatnoću detektovanja „ispravnih“ objekata i$f(p|\alpha,\beta)$predstavlja verovatnoću da *p* ima specifičnu vrednost. Vrednost očekivane verovatnoće je data$E(p)$, koja se predstavlja kao najverovatnijavrednost *p*. Stim u vezi pouzdanost SČ može biti predviđena u budućnosti uz pomoć *funkcije beta raspodele*svih njegovih prethodnih akcija, sve dok se te akcije predstavljaju u binarnom formatu.

IV. PROTOKOL ZA DETEKTOVANJE I PRAĆENJE ZASNOVANO NA SIGURNOM I POUZDANOM PREDVIĐANJU

Ovaj protokol treba da obezbedi da je svaki SČ nadgledan od njegovog suseda, koga još zovemo i posmatrač, kako bi se obezbedilo detektovanje i praćenje zasnovana na sigurnom i pouzdanom predviđanju. U prilog tome ide i činjenica da svaki SČ posmatra svoje susedne čvorove, kad god su oni budni. Nakon što se mreža postavi, VK i njegovi nadgledani čvorovi se biraju slučajno. Kada je mreža pokrenuta i kada je klasterovanje mreže završeno, predloženi protokol započinje svoju funkciju kroz tri faze:

1. *Nadgledanje. Svaki SČ kontinuirano vrši nadgledanje svih svojih susednih čvorova i VK i na osnovu tih podataka popunjava tabelu ugleda.*
2. *Izbor vođe klastera. Periodično SČ međusobno razmenjuju tabele ugleda i preračunavaju vrednosti poverenja za svoje komšije. Na osnovu tih vrednosti poverenja i preostale energije čvora bira se novi vođa klastera.*
3. *Detektovanje i praćenje objekata. Svaki vođa klastera je odgovoran za detektovanje objekta u svom senzorskom polju i za buđenje odgovarajućih SČ za praćenje.*

Kada je objekat detektovan od strane VK, on budi SČ u njegovoj blizini. Da bi se predupredili problemi uzrokovani kompromitovanim SČ, bira se T broj suseda od strane VK i postavljaju se za „posmatrače“. Osnovni koraci u algoritmu nadgledanja i izboraVK prikazani su u Tabeli II [20].

TABELA II. ALGORITAM ZA NADZOR I IZBOR ČVOROVA U VOĐE KLASTERA

Ulaz	Grupa senzorskih čvorova
Izlaz	Vođa klastera sa najvećom reputacijom i energijom
Korak 1	Inicijalno se VK biraju slučajno
Korak 2	VK formiraju svoj klaster šaljući poruke ADV
Korak 3	Aktivni SČ nadgledaju svoje susede i snimaju način opažanja objekata u tabelu ugleda
Korak 4	Kada istekne period života kao VK, on odašilje poruku da se započne nov izbor VK
Korak 5	SČ unutar klastera razmenjuju tabele ugleda i izračunavaju ugled za svoje komšije
Korak 6	Svaki SČ šalje svoje tabele ugleda zajedno sa trenutnim stanjem energije VK
Korak 7	VK pravi vrste SČ u skladu sa kombinacijom najviših nivoa energije i nivoa ugleda
Korak 8	Čvor koji ima najviše nominovane vrednosti je novi VK, a čvorovi sa drugim i trećim nivoom nominovanih vrednosti su novi „posmatrači“

Prilikom svake selekcije VK i T čvorova „posmatrača“ algoritam dodeljuje indekse susednim čvorovima kako bi rangirao kombinaciju njihovih vrednosti ugleda i nivoa energije. Na osnovu ovih indeksa se preračunava T broj čvorova „posmatrača“. Aritmetička sredinaugleda i preostale energije se zove nominacijska vrednost. Vođe klastera izračunavaju i rangiraju SČ prema najvišim nominacijskim vrednostima. Nominacijska vrednost NV se izračunava kao

$$NV = \left[\frac{(z\times\upsilon)+(t\times\varepsilon)}{2}\right] \quad (4)$$

gde je $\boldsymbol{\upsilon}$ vrednost ugleda sa vrednostima $0 \le \upsilon \le 1$, $\boldsymbol{\varepsilon}$je preostala energija SČ izražena u džulima (J), a **z** i **t** koeficijenti čije vrednosti mogu biti između 1 i 2. Pre izračunavanja NV,vrednosti $\boldsymbol{\upsilon}$ i $\boldsymbol{\varepsilon}$ moraju biti normalizovane. Ako primena BSM zahteva veću sigurnost, tada je vrednost koeficijenta**z** i **t** bliža 2, u suprotnom je bliža 1. Takođe, ako se BSM se koristi u kritičnim misijama, onda vrednost ugleda mora imati veće vrednosti na početku (od 0,5 do 1), nasuprot

tome ako je zahtev da BSM ima duži životni vek, onda energetski nivo mora da ima veće vrednosti. Način da se što više umanji štetan uticaj kompromitovanih SČ jeste da se u izbor vođe klastera i „posmatrača“ uključi što veći broj susednih čvorova.

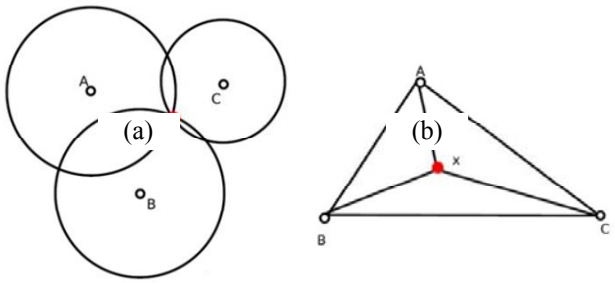
Detektovanje i praćenje objekata zavisi od rada VK. Naime, VK mora da detektuje ulazak objekta u nadgledanu zonu i da na osnovu njegovih očitanih i proračunatih parametara odredi njegovu lokaciju, brzinu i trajektoriju, čime stiče uslov da izvrši buđenje adekvatne grupe SČ. Takođe, kada je objekat detektovan od strane VK, određuje se T broj „posmatrača“ koji se nalaze u neposrednoj blizini objekta i koji će pratiti njegovo kretanje u nadgledanoj zoni.U tabeli III. je dat algoritam za detektovanje i praćenje objekta.

Kad god je objekat detektovan, na osnovu udaljenosti SČ od objekta, tri najbliža SČ se određuju da nadgledaju kretanje objekta u svakom trenutku.Ovi čvorovi koriste algoritam

TABELA III. ALGORITAM ZA DETEKTOVANJE I PRAĆENJE OBJEKTA

Ulaz	Pozicija detektovanog objekta
Izlaz	Odgovarajuća grupa probuđenih SČ
Korak 1	Formira sa zona nadgledanja, „posmatrači“nadgledaju ponašanje VK i zonu nadzora zajedno sa VK
Korak 2	VK detektuje objekat
Korak 3	VK budi T senzorskih čvorova najbližih objektu
Korak 4	SČ nadgleda objekat i informiše VK o brzini i pravcu objekta
Korak 5	VK aktivira trilateralni algoritam i izračunava koordinate objekta
Korak 6	Kako se objekat kreće VK budi druge SČ, služeći se predviđanjem buduće pozicije objekta
Korak 7	Kada objekat napušta zonu jednog VK, tada VK predviđa sledeću poziciju objekta i šalje poruku upozorenja VK najbližem predviđenoj poziciji.

trilateracije da bi izračunali x i y koordinate objekta, kao što je prikazano na slici 2a. Ovi senzori se u toku kretanja objekta menjaju. Proces izbora svaka tri nova SČ se neprekidno obavlja na osnovu lokacije objekta u različitim vremenskim



Slika 2. Tehnike pozicioniranja (a) trilateracija, (b) triangulacija

momentima [21]. Pored algoritma trilateracije moguće je koristiti i algoritam triangulacijekao na slici 2b, gde se na osnovu dolaznog ugla signala sa sva tri SČ i uz pomoć jednostavne geometrijske veze može izračunati pozicija objekta.

Procena performansi datog protokola se vrši simulacijom [20]. Uz pomoć simulacionog softvera TISA (eng. **T**arget in **S**ensing **A**rea **T**est) je moguće odrediti koji su objekti detektovani, kao i koji VK i „posmatrači“ su ih detektovali. TISA se primenjuje na sve pripadnike klastera i tokom celog procesa se podaci o detektovanim „ispravnim“ i „lažnim“ objektima snimaju. Ako u toku simulacije VK ne detektuje objekat, a neki od „posmatrača“ to učine, oni obaveste VK i šalju poziciju objekta. Ako je neki objekat detektovan od strane kompromitovanog VK, člana klastera ili nekog drugog SČ u mreži, TISA pretpostavlja da je objekat ostao nedetektovan. U toku testiranja se određuje i životni vek BSM, koji se definiše brojem realizovanih upita do vremena kada je došlo do prvog otkaza SČ usled nedostatka energije.

Na osnovu dosad prikupljenih podataka, protokol zasnovan na sigurnom i pouzdanom predviđanju dao je znatno poboljšanje u pogledu broja tačnih i sigurnih detekcija u nadgledanoj zoni. Slučaj kada su kompromitovani SČ rasuti nasumično po čitavoj BSM pokazuje da je mreža bez protokolazasnovanomna sigurnom i pouzdanom predviđanju ranjivija nego što je to u slučaju mreže sa protokolom. Njegov doprinos je i u tome što on sprečava da kompromitovani SČ postane VK, usled čega se sprečava da podatak o detektovanom objektu bude „ispušten“ ili izmenjen. Kako broj kompromitovanih čvorova u mreži bez protokola predviđanja raste, tako broj detekcija objekata opada, a u BSM sa protokolom za detekciju i praćenje objekata na bazi sigurnog i pouzdanog predviđanja učinak detekcije i praćenje objekata je stabilan. Rezultati simulacija pokazuju i da u slučajevima kada je napad pokrenut sa oboda ili iz određenog dela senzorskog polja, protokol značajno ublažava efekte napada i održava nivo detekcije na stabilnom nivou.

Preciznost praćenja je takođe bila predmet simulacije za BSM sa i bez protokola zasnovanom na sigurnom i pouzdanom predviđanju, gde je u uslovima ravnomernog rasta broja kompromitovanih SČ mreža uspevala da zadrži relativno stabilnu tačnost.

Proces neprekidne evaluacije svakog senzorskog čvora u određenom periodu vremena povećava sigurnost i pouzdanost mreže. U ovakvom protokolu, sigurnost detekcije i praćenja objekta je proces koji se obezbeđuje uz pomoć pouzdanih izvora informacija.

Visoka sigurnost i niži overhed(**eng.** overhead)su dva cilja koja svaki upravljačkiprotokol BSM želi da postigne, iako je to veoma teško. Protokol za detekciju i praćenje objekata zasnovanom na sigurnom i pouzdanom predviđanju pravi veliki računarski i komunikacijski overhed , mada sa druge strane on značajno pomaže da VK ili „posmatrači“ne postanu kompromitovani čvorovi. Pored toga, protokol omogućava bolju energetsku efikasnost BSM sa protokolom nego bez njega, što u konačnom ima za posledicu duži životni vek BSM.

V. ZAKLJUČAK

Bežične senzorske mreže su postale neizostavan deo sadašnjih i budućih aplikacija. U nedostatku adekvatne bezbednosne zaštite, BSM postaju ranjive na mnoge napade. Nemogućnost primene fizičke zaštite SČ od fizičkog

tamperovanja, jer ista značajno poskupljuje cenu BSM, ne daje puno mogućnosti da jednu takvu mrežu učini bezbednosno prihvatljivom za razne aplikacije. Iako se problem bezbednosti BSM razmatra kroz mnoge radove, u njima je fokus dat na problemu sigurnosti prikupljenih podataka, gde se razmatra autentičnost i ispravnost podataka.

U ovom radu je predstavljen jedan drugačiji pristup, tj. razmatralo se poverenje i integritet senzorskih čvorova i vođe klastera pre svega. Ako isključimo mogućnost da je SČ i VK kompromitovan i da se tom prilikom ne postavlja pitanje njegovog integriteta kao izvora podataka, funkcionisanje BSM u neprijateljskom i kompromitovanom okruženju je značajno olakšano. Uspostavljanjem poverenja među čvorovima čini da mehanizmi dodatne zaštite podataka i bezbednosti čvorova budu suvišni i opterećujući za računarski osiromašen hardver SČ i njegovu energetsku efikasnost. Smanjujući broj angažovanih procesa, algoritama i mehanizama za bezbednost BSM, smanjuje se vreme trajanja procesa, vreme odziva i ubrzava proces donošenja odluke, što za posledicu ima sistem sa bržim, preciznijim i tačnijim procesom detekcije i praćenja objekata u nadgledanoj zoni kritične misije. Sam koncept ugleda i poverenja SČ je jedan od efikasnih načina prevazilaženja nedostatka kriptografskih funkcija u hardverski ograničenim mrežama i unapređenja rada BSM.

LITERATURA

[1] M. Stanojević , P. Spalević , I. Milovanović , S. Stanojčić, "The use of secure wireless sensor networks to control and protect critical infrastructure" Proceedings of 52nd International Scientific Conference On Information, Communication And Energy Systems and Technologies, pp. 253–256, 2017.

(b)

[2] C.P. Fleeger, „Security in computing" 3rd edition, Prentice-Hall Inc.,New York, 2003.

[3] T.Zia, A. Zomaya, „Security issue in wireless sensor network", International Conference on Systems and Networks Communications, pp. 40, IEEE , 2006.

[4] S. Bhatti, J. Xu. "Survey of target tracking protocols using wireless sensor network", Proceedings of Fifth International Conference on Wireless and Mobile Communications (ICWMC), pp. 110-115, 2009.

[5] M. Fayyaz, "Classification of object tracking techniques in wireless sensor networks", Wireless Sensor Network, Vol. 3, No. 4, pp. 121-124, 2011.

[6] J.Li, Y. Zhou, "Target Tracking in Wireless Sensor Networks", Wireless Sensor Networks: Application-Centric Design, Yen Kheng Tan (Ed.), ISBN: 978-953-307-321-7, InTech , 2010, Available from: http://www.intechopen.com/books/wireless-sensor-networks-application-centric-design/target-tracking-inwireless-sensor-networks

[7] H. T. Kung, D. Vlah, "Efficient Location Tracking Using Sensor Networks", Proceedings of 2003 IEEE Wireless Communications and Networking Conference

[8] W. Zhang, G. Cao, "DCTC: Dynamic Convoy Tree-Based Collaboration for Target Tracking in Sensor Networks", Published in the IEEE Transactions on Wireless Communications, 2004

[9] S.P.M. Tran, "OCO: Optimized Communication & Organization for Target Tracking in Wireless Sensor Networks", Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference, 2006

[10] S. P. M. Tran, T. A. Yang, "Evaluations of Target Tracking in Wireless Sensor Networks", SIGCSE'06, 2006, Houston, Texas, USA.

[11] C.Y. Lin, W.C. Peng, Y.C. Tseng, "Efficient In-Network Moving Object Tracking in Wireless Sensor Networks", Mobile Computing, IEEE, Volume:5, Issue:8,2006

[12] K. A.Darabkh, S. S. Ismail, M. Al-Shurman, I. F. Jafar, E. Alkhader, M. F.Al-Mistarihi, „Performance evaluation of selective and adaptive heads clustering algorithms over wireless sensor networks", Journal of Network and Computer Applications, Vol. 35, Iss. 6, pp. 2068-2080, 2012.

[13] J. Teng, H. Snoussi, C. Richard, „Prediction-based cluster management for target tracking in wireless sensor networks", Wireless Communications and Mobile Computing, Vol. 12, Iss. 9, pp. 797-812, 2012.

[14] W.P. Chen, „Dynamic Clustering for Acoustic Target Tracking in Wireless Sensor Networks", IEEE Transactions on Mobile Computing, Volume: 3, Issue: 3, pp. 258 - 271, 2004.

[15] K. Huang, H. Wang, W. Wang, Y. Wang, „A Dynamic tracking mechanism for mobile target in wireless sensor networks", Proceedings of 2012 IEEE International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), New Taipei, pp. 822-826, 2012.

[16] Z. Wang, W. Lou, Z. Wang, J. Ma and H. Chen, "A Hybrid Cluster-Based target tracking protocol for wireless sensor networks", International Journal of Distributed Sensor Networks, 16 pages, Volume 2013.

[17] H. Yang and B. Sikdar, "A Protocol for Tracking Mobile Targets using Sensor Networks", Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE, 2003.

[18] Z. Wang, H. Li, X. Shen, X. Sun, "Tracking and Predicting Moving Targets in Hierarchical Sensor Networks", Networking, Sensing and Control, 2008.

[19] S. Ozdemir, „Functional reputation based data aggregation for wireless sensor networks", Proc. Int. Conf. Wireless and Mobile Computing, Avignon, France, pp. 592-597, 2008.

[20] A. Oracevic, S. Akbas, S. Ozdemir, M. Kos, "Secure Target Detection and Tracking in Mission Critical Wireless Sensor Networks", Anti-counterfeiting Security and Identification (ASID) 8th International IEEE Conference on, 2014

[21] Y.C. Tseng, S.P. Kuo, H.W. Lee, C.F. Huang, „Location Tracking in a Wireless Sensor Network by Mobile Agents and Its Data Fusion Strategies", Information Processing in Sensor Networks, pp. 625-641 Springer, Berlin, (2003).

ABSTRACT

Long time development and implementation of wireless sensor networks enabled huge progress to be made in the fields of their security through research and designer techniques especially when it comes to their perpetual limitations. One important field of the wireless sensor networks deployment is security protection including functions of detecting and keeping track of a target in the area of surveillance (e.g. sensor field). Performance of the functions relies on the network capability to effectively detect moving target sending the information further thus providing timely response. Accurate detection and following the target is of particular imperative when the wireless sensor network is deployed in distance and behind the enemy lines to protect crucial missions. It is very important for the sensor nods to maintain the data accuracy and integrity in such an environment. Violation of the network integrity and modification of data observed and gathered by the sensor measurements result in false, inaccurate data on target movements with its potential disastrous effects. This article covers safe and sound protocol for keeping track of targets observed in a secure way providing data accuracy in wireless sensor network even where compromised sensor nods are present.

SECURE DETECTION AND TRACKING OBJECTS IN A COMPROMISED WIRELESS SENSOR NETWORK

Milan Stanojević, Petar Spalević,Aleksandar Jevremović, Nenad Stanojević,Igor Vujčić