ارائه یک راهبرد دفاعی جدید و کارا برای مقابله با حمله بیزانسی در شبکه‌های حسگر بی‌سیم

مرتضی شریفی[۱]، دانشجوی دکتری؛ محمود محصل فقهی[۲]، استادیار

۱- دانشکده مهندسی برق و کامپیوتر - دانشگاه تبریز - تبریز - ایران - msharifi@tabrizu.ac.ir
۲- دانشکده مهندسی برق و کامپیوتر - دانشگاه تبریز - تبریز - ایران - mohasselfeghhi@tabrizu.ac.ir

چکیده: ویژگی‌ها و محدودیت‌های شبکه‌های حسگر بی‌سیم باعث شده است که امنیت این شبکه‌ها با چالش‌های جدی مواجه باشد. در این مقاله یکی از رایج‌ترین حملات موجود در شبکه‌های حسگری با نام حمله بیزانسی مورد بررسی قرار می‌گیرد. با در نظر گرفتن یک شبکه حسگری با یک مرکز جمع‌آوری داده متحرک، یک روش ادغام داده بهینه پیشنهاد می‌گردد که قادر است معیار نیومن پیرسون را در یک روش خاص از ادغام داده سخت پیاده کند، به این معنی که با ثابت نگه داشتن خطای هشدار غلط، احتمال آشکارسازی را حداکثر کند. با استفاده از تحلیل‌های آماری داده‌ها، در حالت‌های مختلف از تعداد حسگرها و تعداد مهاجمین در شبکه، یک مدل بسته با سرعت قابل‌قبول برای یافتن پارامترهای روش ارائه می‌شود. سپس یک روش شناسایی مهاجمین به‌کار گرفته می‌شود که با استفاده از فاصله همینگ گزارشات هر حسگر با تصمیم نهایی، اقدام به تشخیص مهاجم می‌کند. شبیه‌سازی‌ها بهبود حاصل از اعمال روش پیشنهادی در تصمیم‌گیری و همچنین کارآیی روش تشخیص مهاجمین را نسبت به سایر روش‌های موجود به‌وضوح نمایش می‌دهند.

واژه‌های کلیدی: حمله بیزانسی ، شبکه‌های حسگر بی‌سیم ، معیار نیومن پیرسون، ادغام داده، فاصله همینگ.

A New Efficient Defense Strategy against Byzantine Attack in Wireless Sensor Networks

M. Sharifi[1], PhD Student; M. Mohassel Feghhi[2], Assistant Professor

1- Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran, Email: msharifi@tabrizu.ac.ir
2- Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran, Email: mohasselfeghhi@tabrizu.ac.ir

Abstract: Wireless sensor networks' characteristics and limitations have led to severe challenges in their security. In this paper, one of the most common attacks, named as the Byzantine attack, has been studied. A sensor network with a mobile data fusion center is considered, and an optimized data collecting method is proposed which can apply the Neyman-Pearson criterion in a particular case of hard decision making. It means that keeping the false alarm rate constant, the detection probability is maximized. Using statistical data analysis, a closed model is obtained with an acceptable speed of convergence in a various number of sensors and attackers in the network. Then a novel malicious sensor detection scheme is exploited to identify the attack strength using the Hamming distance between every sensor report and the final decision. The simulation results show the superior performance of applying the proposed method in the decision process and also the proposed attack detection method in comparison with the conventional methods.

Keywords: Byzantine Attack, Wireless Sensor Networks, Neyman-Pearson Criterion, Data Fusion, Hamming Distance.

تاریخ ارسال مقاله: ۱۳۹۸/۰۵/۰۱
تاریخ اصلاح مقاله: ۱۳۹۸/۰۶/۲۱
تاریخ پذیرش مقاله: ۱۳۹۸/۰۶/۲۶
نام نویسنده مسئول: محمود محصل فقهی
نشانی نویسنده مسئول: ایران - تبریز - بلوار ۲۹ بهمن - دانشگاه تبریز - دانشکده مهندسی برق و کامپیوتر - گروه مهندسی مخابرات.

۱- مقدمه

پیشرفت‌های اخیر فن‌آوری امکان استقرار تعداد زیادی از حسگرها را در یک شبکه حسگر بی‌سیم فراهم کرده است تا به‌طور مداوم یک منطقه را برای برآورد، کشف یا ردیابی قابل‌اطمینان از یک رویداد تحت نظر داشته باشند. این شبکه‌ها اغلب به صورت توزیع شده در خصوص حضور یا عدم حضور هدف تصمیم می‌گیرند. در تشخیص توزیع شده، هر حسگر به جای ارسال داده‌های خام خود، داده‌های کمی را به مرکز جمع‌آوری داده ارسال می‌کند تا میزان مصرف انرژی و پهنای باند را به حداقل رساند. مرکز با توجه به داده‌های جمع‌آوری‌شده از حسگرها، تصمیم نهایی را درباره هدف اتخاذ می‌کند. یکی از جدی‌ترین تهدیدات امنیتی در این شبکه‌ها، حمله بیزانسی[۱] است [۲،۱]. در مفاهیم شبکه، مفهوم بیزانسی به گره‌هایی از شبکه اطلاق می‌شود که رفتار غیرعادی از خود بروز می‌دهند[۳]. این تعریف به‌طور ویژه به دو رفتار خاص اشاره می‌کند، رفتار بداندیشانه[۲] و رفتار خرابی[۳] [۴]. در رفتار خرابی ممکن است یک حسگر به دلیل پایان یافتن منبع انرژی یا یک ساختار غلط برنامه‌ای، به‌صورت ناصحیح عمل کند و اطلاعات غلط به مرکز ارسال نماید ولی در رفتار بداندیشانه و تهاجمی، ارسال اطلاعات غلط به‌صورت عمدی می‌باشد و ممکن است نشانه سرقت یک حسگر توسط دشمن و دسترسی به اطلاعات امنیتی آن باشد.

مسئله رسیدن به یک تصمیم نهائی در شبکه‌های حسگری بی‌سیم با حضور تعدادی حسگر مخرب در شبکه، از زوایای مختلفی مورد بررسی قرار گرفته است. در [۵] برای مقابله با خرابی بیزانسی در شبکه‌های توزیع‌شده یک روش افزایشی بازگشتی پیشنهاد شده است. بدین‌ترتیب که مرکز داده تعدادی از گره‌ها را برای تصمیم انتخاب می‌کند و تا زمانی که به یک سطح از اطمینان نرسیده است شروع به افزایش تعداد گره‌های همه‌پرسی شده می‌کند. در مقاله [۶] همه‌پرسی در دو سطح برای شبکه‌های حسگری خوشه‌بندی شده بدین صورت برگزار می‌شود که ابتدا هر سرخوشه از حسگرهای درون آن خوشه همه پرسی می‌کند و به یک تصمیم نهائی می‌رسد. سپس مرکز همه‌پرسی را در یک سطح بالاتر و در بین سرخوشه‌ها انجام می‌دهد. در این مقاله برای هر حسگر در خوشه یک وزن در نظر گرفته می‌شود که این فاکتور وزن از طریق همبستگی موجود در نتایج حسگر با نتایج همسایه‌های آن تخصیص داده می شود. در مقاله [۸،۷] برای شناسائی حسگرهای بیزانسی از یک سطح اعتماد برای هر حسگر استفاده می‌کنند. این سطح اعتماد برای هر حسگر از وزن اختصاصی آن بدست می‌آید که به وسیله یک مفهوم تئوری اطلاعاتی به‌نام فاصله همگرایی KL[۴] بدست می‌آید. در مقالات [۱۰،۹] از آزمون فرض باینری برای تشخیص تصمیم نهایی استفاده می‌کنند. مثلا در [۹] فرض می‌شود در یک شبکه توزیع شده، در طی جمع‌آوری داده، حسگرهای مهاجم از وضعیت فرضیه درست داده همواره اطلاع دارند، لذا توسط فرآیند پرکردن‌آب[۵]، یک فاصله توزیعی مناسب برای مهاجمین به‌دست می‌آید که در این فاصله، آزمون فرض قادر به تمییز مهاجم نخواهد بود. در [۱۰] با توجه به گزارشات هر حسگر یک مجموعه ممکن از مهاجمین فرض می‌شود، سپس زمانی که استراتژی حمله مهاجمین معلوم باشد و نسبت مهاجمین در شبکه تغییر نکند، روی تمام مجموعه‌های ممکن از مهاجمین جستجو انجام می‌شود تا مجموعه‌ای که بیشترین احتمال را دارد، بدست آید.

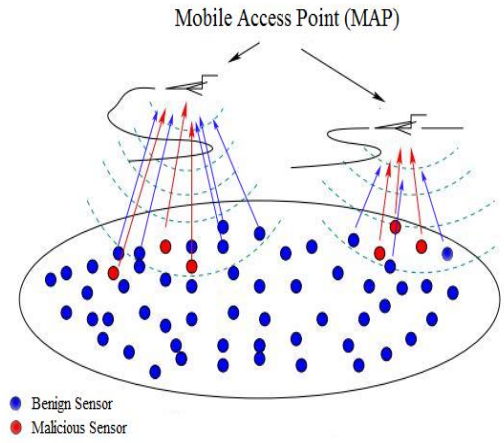
حمله بیزانسی یک حمله درون‌شبکه‌ای محسوب می‌شود و لذا مقابله با آن همواره جزو چالش‌هایی است که در طراحی لایه فیزیکی و یا مسیریابی شبکه از سناریوهای مشارکتی استفاده شده است [۱۱]. برای مثال در شبکه‌های بی‌سیم چندگانه که مسیریابی به‌طور مشارکتی و با اجماع گره‌های نزدیک صورت می‌گیرد [۱۲] یا در شبکه‌های هوشمند انرژی که تخمین وضعیت شبکه با رای‌گیری از گره‌های شبکه به‌دست می‌آید [۱۳]. در اغلب این مقالات، دو هدف اصلی دنبال می‌گردد: ابتدا نحوه تصمیم‌گیری در حضور کاربران بیزانسی باید طوری انتخاب گردد که اثر تخریبی آن دسته از کاربران بیزانسی که در تصمیم مشارکت کرده‌اند به کمترین میزان کاهش پیدا کند و هدف دوم شناسایی و علامت‌گذاری کاربری است که عملکرد مشکوک دارد. در شبکه‌های رادیوشناختی نیز برای سنجش طیفی و تشخیص طیف خالی معمولاً از روش‌های مشارکتی استفاده می‌شود که در آن یک مرکز داده اطلاعات طیفی را از کاربران ثانویه جمع‌آوری نموده و در خصوص حضور یا عدم حضور کاربر اولیه تصمیم‌گیری می‌کند. در این شبکه‌ها نیز حمله بیزانسی یکی از اصلی‌ترین مشکلاتی است که در منابع متعدد به آن پرداخته شده است [۱۴]. در این شبکه‌ها حمله بیزانسی به‌نام حمله تحریف اطلاعات طیف سنجی[۶] شناخته می شود. در مقاله [۱۵] یک روش مقابله با این حمله ارائه شده است که مبتنی بر تخمین پارامترهای حمله توسط کاربران می‌باشد. با تخمین احتمالات حمله کاربران مخرب، تعداد کاربران لازم برای همه‌پرسی در روش Q از M طوری تعیین می‌شود که تابع هزینه را کمینه کند. مقاله [۱۶] اثر حمله بیزانسی در شبکه‌های حسگر بی‌سیم مبتنی بر ارسال بسته‌ای داده را بررسی می‌کند. در این مقاله نویسندگان فرض می‌کنند که یک بسته داده شناسه همواره در بین کاربران در حال تبادل است و لذا هر کاربر تاریخچه ارسال خود را در این بسته درج می‌کند. مرکز داده در هر لحظه می‌تواند با طراحی یک الگوریتم مناسب تاریخچه تمام کاربران را بررسی و گره بیزانسی را کشف کند. در مقاله [۱۷] کران خطاهای روش Q از M در آزمون فرض باینری به‌دست آمده است. نویسندگان در این مقاله کران پایین خطا را بهینگی و کران بالا را حد امنیت شبکه می‌نامند و در ادامه حالت‌های مختلف مصالحه بین دو کران بالا و پایین خطا را برای پیدا کردن بهترین پارامتر تصمیم‌گیری نشان می‌دهند.

در این مقاله، ابتدا یک الگوریتم بهینه برای نحوه ادغام داده‌ها در حضور مهاجمین بیزانسی در روش انتخاب Q از M مطرح می‌کنیم. در الگوریتم ارائه شده، هدف اصلی بیان یک مدل تصمیم است که بتوان معیار نیومن-پیرسون را در روش ادغام داده سخت پیاده سازی کرد. به

این معنی که با ثابت نگه دا شتن میزان احتمال خطای ه شدار غلط در یک حد معین، بتوان به بی شینه احتمال آ شکار سازی ر سید. این روش در ادبیات آشکارسازی سیگنال‌ها به روش نرخ ثابت هشدار غلط[۷] مشهور است. در این مقاله، روش مذکور برای ادغام داده سخت با حضور تعدادی گره بیزانسی پیاده می‌شود. در ادامه نیز برای شناسایی مهاجمین از روش بی شینه فا صله گزار شات حسگرها ا ستفاده می شود. در نهایت نیز شبیه‌سازی‌های عددی در حالت‌های مختلف انجام می‌شود تا کارآیی الگوریتم پیشنهادی نسبت به روش‌های متداول ارزیابی گردد.

۲- مدل شبکه

برای سادگی م سئله از یک مدل معماری خاص مرکزی در شبکه‌های حسگری بی‌سیم استفاده می‌کنیم [۱۸]. در این معماری یک مرکز جمع‌آوری داده متحرک (MAP[۸]) وجود دارد که می‌تواند نتایج سنجش محیطی را در یک مسیر مستقیم، از یک سری حسگرهای انتخاب شده یا کل شبکه دریافت کند (شکل ۱). بنابراین در مدل ارائه شده م شکل م سیریابی نخواهیم دا شت. همچنین با م سئله محو شدگی یا اثر سایه مواجه نیستیم و مرکز جمع‌آوری داده می‌تواند مرکزی باشد که محدودیت مصرف توان نداشته باشد.



شکل ۱. توپولوژی شبکه حسگر بی‌سیم مفروض.

فرض می‌کنیم N حسگر با توان محدود به‌صورت یکنواخت در محیط پخش شده‌اند و یک MAP طوری شبکه را جاروب می‌کند که توانایی مخابره با تمام حسگرها را دارد. هر حسگر نتیجه سنجش محلی خود را کوانتیزه کرده و در یک بیت (بیت ۱ به معنی حضور هدف یا H_1 و بیت ۰ به معنی عدم حضور هدف یا H_0) به MAP اعلام می کند و سپس با اعمال روش ادغام داده‌ای، ت صمیم نهائی در خ صوص هدف اتخاذ می‌شود. درادغام داده‌ها روش‌های مختلفی ذکر می‌شود مثل روش‌های منطقی OR یا AND و یا روش اکثریت. یکی از پرکاربردترین روش‌های ادغام داده‌ای، روش انتخاب گزاره در ست به شرط گزارش Q بیت از بین M بیت (Q-out-of-M) است [۱۹]، که می‌تواند توازن مناسبی بین احتمال خطای کلی هشدار غلط[۹] (Q_{Fa}) و خطای عدم آشکارسازی[۱۰] (Q_m) برقرار کند. در این روش هدف یافتن تعداد مطلوب M گره از N گره کل شبکه می‌با شد که نتیجه گزارش آنها در ت صمیم م شارکت داده شود. حال اگر Q از این M گره، گزارش ح ضور هدف را داده باشند، نتیجه نهائی H_1 است و در غیر اینصورت H_0. به مقادیر بهینه M و Q پارامترهای روش می‌گویند.

با فرض حضور k حسگر مهاجم در شبکه، درصد حسگرهای مخرب به کل حسگرها را $\alpha = k/N$ می‌گیریم که فرض می‌کنیم این مقدار برای MAP معلوم است. فرض کنیم P_0 احتمال حمله مهاجم باشد، یعنی یک حسگر مهاجم با این احتمال، اطلاعاتی مخالف نتایج سنجش محیطی خود را به مرکز ارسال کند. در یک بازه همه‌پرسی فرض بر آن است که همه حسگرهای مهاجم احتمال حمله یکسانی دارند. استراتژی حمله حسگرهای مخرب در دو کلاس طبقه‌بندی می‌شود[۲۰]:

حمله استاتیکی: در این مدل م هاجم با احت مال حم له دلخواه $0 \le P_0 \le 1$ ن تایج غلط ارسال می‌ک ند. بدترین حا لت برای مرکز وضعیتی است که در آن $P_0 = 1$ یعنی مهاجم همواره هدف را حاضر اعلام می‌کند که به این نوع حمله Always Attack می‌گویند و در این حالت میزان احتمال خطای Q_{Fa} زیاد خواهد شد. حالت خاص دیگر این است که مهاجم همواره اقدام به ارسال صفر کند و باعث ایجاد خطای Q_m بالا برای کل سیستم شود. به این نوع حمله Always Free می‌گویند.

حمله دینامیکی: در این مدل مهاجم احتمال حمله خود را پس از یک یا چند قالب سنجش عوض می‌کند. در این حالت مقدار P_0، میانگین احتمالات حمله در طول کل قالب‌های حمله خواهد بود.

اگر فرض کنیم هر حسگر سالم دارای احتمالات هشدار غلط P_{Fa} و عدم آشکارسازی P_m باشد و هر حسگر مهاجم دارای $\tilde{P}_{Fa}$ و $\tilde{P}_m$ باشد و این احتمالات در کل شبکه یک‌سان با شد، آنگاه احتمال حمله در دو وضعیت محیطی H_0 و H_1 متفاوت خواهد بود. در یک حسگر مهاجم احتمالات کلی حمله منجر به هشدار غلط $P_{a,Fa}$ و حمله منجر به عدم آشکارسازی $P_{a,m}$ به‌صورت زیر خواهد بود:

$$\begin{aligned} H_0 &: P_{a,Fa} = P_0(1-\tilde{P}_{Fa}) + (1-P_0)\tilde{P}_{Fa} \\ H_1 &: P_{a,m} = P_0(1-\tilde{P}_m) + (1-P_0)\tilde{P}_m \end{aligned} \qquad (۱)$$

حال می‌توان یک احتمال کلی حمله برای یک ح سگر مهاجم را به صورت زیر تعریف کرد:

$$P_a = P(H_0)P_{a,Fa} + P(H_1)P_{a,m} \qquad (۲)$$

که در آن $P(H_0)$ و $P(H_1)$ احتمال وضعیت محیطی در حالتهای H_0 و H_1 می‌باشد. اگر در حالت خاصی مهاجم، خود هیچ خطایی در آشکارسازی نداشته باشد ($\tilde{P}_{Fa} = \tilde{P}_m = 0$) آنگاه طبیعی است که داشته باشیم: $P_a = P_{a,Fa} = P_{a,m} = P_0$

۳- ادغام بهینه در حضور مهاجمین بیزانسی

در یک شبکه با فرض این‌که هیچ خطایی درکانال بین حسگرها و MAP وجود ندارد و در نظر گرفتن مهاجمین بیزانسی که با استراتژی حمله Always Attack سعی در تخریب عملکرد شبکه دارند و همچنین با فرض اینکه حسگرهای مهاجم خطایی در شناسایی وضعیت محیطی ندارند، روابط احتمالات Q_{Fa} و Q_d برای تصمیم نهایی به‌صورت زیر به‌دست می‌آید[۱۹]:

$$Q_{Fa}=\sum_{d=\max\{0,m+k-N\}}^{k} P_{k,N-k}^{d,m-d}\sum_{i=0}^{d}\binom{d}{i}P_a^i(1-P_a)^{d-i} \times \sum_{j=\max\{0,q-i\}}^{m-d}\binom{m-d}{j}P_{Fa}^j(1-P_{Fa})^{m-d-j} \quad (۳)$$

$$Q_d=\sum_{d=\max\{0,m+k-N\}}^{k} P_{k,N-k}^{d,m-d}\sum_{i=0}^{d}\binom{d}{i}P_a^i(1-P_a)^{d-i} \times \sum_{j=\max\{0,q-i\}}^{m-d}\binom{m-d}{j}P_d^j(1-P_d)^{m-d-j} \quad (۴)$$

واضح است که در این حالت داریم: $Q_m=1-Q_d$.

در روابط فوق مقدار $P_{k,N-k}^{d,m-d}$ میزان احتمال همه‌پرسی از m حسگر است که در آن d حسگر مهاجم و m-d حسگر سالم وجود دارد به‌طوری که این احتمال برابر است با:

$$P_{k,N-k}^{d,m-d}=\frac{\binom{k}{d}\binom{N-k}{m-d}}{\binom{N}{m}} \quad (۵)$$

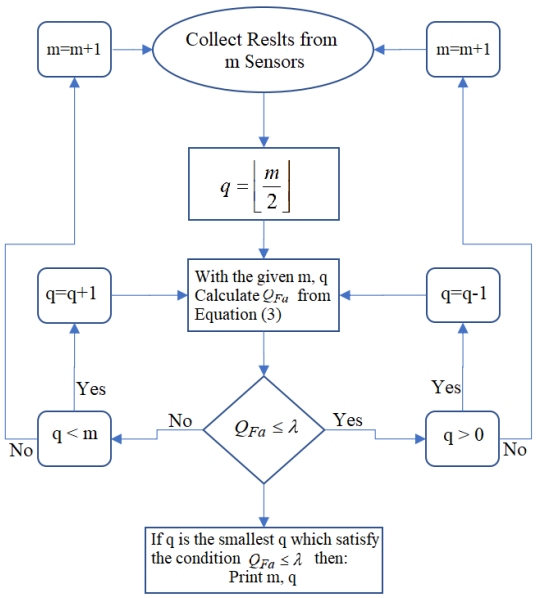
۳-۱- الگوریتم تصمیم بهینه

در معیار نیومن پیرسون سعی بر این است که با استفاده از احتمالات آشکارسازی و هشدار غلط یک روش تصمیم‌مناسب در یک آزمون فرض انتخاب گردد. برای این منظور با اعمال محدودیت روی خطای هشدار غلط و ثابت نگه داشتن آن در یک حد مشخص، میزان آشکارسازی بیشینه می‌گردد. اگر فرض کنیم در مدل شبکه موردنظر مقدار q در روش q-out-of-m حد آستانه تصمیم بین دو وضعیت H_0 و H_1 باشد، هدف محاسبه مقدار q ای است که در معیار نیومن پیرسون شرط $Q_{Fa}\le\lambda$ را رعایت کرده و بیشینه Q_d را تولید کند. واضح است که با انتخاب یک q بالا مثل روش منطقی AND، میزان Q_{Fa} پایینی حاصل خواهد شد ولی این بهبود در ازای کاهش میزان Q_d حاصل شده است. همچنین انتخاب یک q پایین مثل روش منطقی OR، Q_{Fa} زیادی در ازای بهبود Q_d تولید می‌کند.

در ادامه الگوریتمی پیشنهاد می‌شود که قادر است در ازای افزایش بار محاسباتی این مصالحه بین دو احتمال خطا را ایجاد کند. با توجه به روابط ۳ و ۴، الگوریتم بهینه زیر این امکان را فراهم می‌سازد تا با اعمال شرط $Q_{Fa}\le\lambda$، q ای که بیشینه Q_d را می‌دهد به‌دست آید. هر حسگر با توجه به شرایط محیطی یک بیت داده در خصوص وضعیت هدف تعیین می‌کند. MAP از m حسگر، اطلاعات سنجش محیطی را جمع‌آوری می‌کند. با قرار دادن $q=\lfloor m/2\rfloor$ میزان Q_{Fa} از رابطه ۳ محاسبه می‌شود که در آن علامت $\lfloor x\rfloor$ بیان‌گر جزءصحیح x است. اگر $Q_{Fa}\le\lambda$ باشد، آن‌گاه $q_{new}=q-1$ و مجدداً میزان Q_{Fa} از رابطه (۳) با q جدید محاسبه می‌شود. در غیر این‌صورت اگر $Q_{Fa}\ge\lambda$ باشد، آنگاه $q_{new}=q+1$ و مشابه مرحله قبل میزان Q_{Fa} با q جدید محاسبه می‌شود. تکرار تا زمانی ادامه دارد که کوچکترین q ای که شرط را برآورده می‌کند به‌دست آید. این الگوریتم تضمین می‌کند که q به‌دست‌آمده بیشترین Q_d را به‌همراه داشته باشد، در عین این‌که Q_{Fa} در مرز شرط حفظ گردد. فلوچارت مربوط به این الگوریتم در شکل ۲ نمایش داده شده است.

۳-۲- فرم بسته تصمیم بهینه

مقدار q ای که از الگوریتم بهینه بخش قبل به‌دست می‌آید نتیجه‌ای از میزان خطاهای محلی هر حسگر است. لذا در محیط‌هایی که شرایط



شکل ۲. الگوریتم پیشنهادی برای جستجوی پارامتر q مطلوب.

هدف با سرعت تغییر می‌کند، مقادیر این خطاها نیز تغییرات سریعی خواهد داشت و استفاده از الگوریتم جستجوی گام‌به‌گام فوق، تاخیر قابل توجهی را در روند کار MAP ایجاد خواهد کرد. در ادامه یک روش برای محاسبه q ارائه می‌شود که قادر است در ازای افزایش ناچیز از مقادیر خطا هدف الگوریتم را در یک فرم بسته برآورده کند. فرض می‌کنیم هر دوره تناوب از سنجش در شبکه مستقل از قبل و بعد آن باشد، آنگاه گزارش حسگر iام را $u_i\in\{0,1\}, i=1,\ldots,m$ می‌نامیم. حال اگر حسگر موردنظر یک حسگر سالم باشد، در زمانی که در وضعیت محیطی H_1 هستیم u_i یک متغیر تصادفی برنولی با پارامتر $(w=P_d, f=1-P_d)$ می‌باشد که در آن w و f احتمال پیروزی و شکست توزیع گسسته برنولی

می‌باشند. اگر وضعیت محیطی H_0 بر شبکه حاکم باشد، u_i متغیر تصادفی برنولی با پارامتر ($w=1-P_{Fa}, f=P_{Fa}$) است. در صورتی که حسگر iام مهاجم باشد، آنگاه اگر در وضعیت H_1 باشیم u_i متغیر تصادفی برنولی با پارامتر ($w=1-P_a, f=P_a$)و اگر در وضعیت H_0 باشیم u_i یک متغیر تصادفی برنولی با پارامتر ($w=P_a, f=1-P_a$) است. در MAP آماره تصمیم q-out-of-m، به‌صورت زیر تشکیل می‌شود:

$$U=\sum_{i=1}^{m}u_i \underset{H_0}{\overset{H_1}{\gtrless}} q \qquad (۶)$$

در واقع متغیر تصادفی U نشان‌دهنده تعداد حسگرهایی خواهد بود که به MAP بیت ۱ را گزارش کرده‌اند. با توجه به این‌که m متغیر تصادفی برنولی مستقل با هم جمع شده و U را تشکیل داده‌اند و با فرض m بزرگ، می‌توان طبق قضیه حد مرکزی U را نرمال فرض کرد[۲۱]. پس U در حالت H_1 دارای توزیع $U\sim N(\mu_1,V_1)$ و در حالت H_0 دارای توزیع $U\sim N(\mu_0,V_0)$ خواهد بود. زمانی که تعداد حسگرهای شبکه کم باشد این تقریب با خطای اندکی قابل‌قبول خواهد بود.

در هر تناوب سنجش ما با مجموع m-d حسگر سالم و d حسگر مهاجم رو به رو هستیم، به‌عبارتی با m-d متغیر تصادفی برنولی با میانگین P_d و واریانس $P_d(1-P_d)$ و d متغیر تصادفی برنولی با میانگین P_a و واریانس $P_a(1-P_a)$. لذا در حالت H_1 داریم:

$$\begin{aligned}\mu_1&=(m-d)P_d+d(1-P_a)\\&=m\left[\left(1-\frac{d}{m}\right)P_d+\frac{d}{m}(1-P_a)\right]\\V_1&=(m-d)P_d(1-P_d)+d(1-P_a)P_a\\&=m\left[\left(1-\frac{d}{m}\right)P_d(1-P_d)+\frac{d}{m}(1-P_a)P_a\right]\end{aligned} \qquad (۷)$$

و در حالت H_0 نیز داریم:

$$\begin{aligned}\mu_0&=(m-d)P_{Fa}+dP_a\\&=m\left[\left(1-\frac{d}{m}\right)P_{Fa}+\frac{d}{m}P_a\right]\\V_0&=(m-d)P_{Fa}(1-P_{Fa})+d(1-P_a)P_a\\&=m\left[\left(1-\frac{d}{m}\right)P_{Fa}(1-P_{Fa})+\frac{d}{m}(1-P_a)P_a\right]\end{aligned} \qquad (۸)$$

اگر نسبت تعداد مهاجمین در هر تناوب از سنجش برابر با نسبت کل مهاجمین در شبکه باشد (یا به‌طور معادل در هر تناوب از همه حسگرها همه‌پرسی صورت گیرد $m=N$)، آنگاه می‌توان گفت $\frac{d}{m}=\alpha$. با محاسبه توزیع U در هر دو حالت H_1 و H_0 می‌توان خطای نهایی Q_{Fa} را در MAP به‌صورت زیر نوشت:

$$Q_{Fa}=\Pr\{U\geq q\,|\,H_0\}=\int_q^{\infty}f_{u|H_0}(u)du \qquad (۹)$$

از طرفی می‌دانیم که $f_{u|H_0}(u)=N(\mu_0,V_0)$ و چون بیشینه q برابر m است، حاصل انتگرال فوق به‌صورت زیر خواهد بود:

$$Q_{Fa}=Q\left(\frac{q-\mu_0}{\sqrt{V_0}}\right)-Q\left(\frac{m-\mu_0}{\sqrt{V_0}}\right) \qquad (۱۰)$$

که در آن $Q(x)=\int_x^{\infty}\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}dx$ می‌باشد. به‌همین‌ترتیب می‌توان برای میزان احتمال Q_d نیز نوشت:

$$Q_d=Q\left(\frac{q-\mu_1}{\sqrt{V_1}}\right)-Q\left(\frac{m-\mu_1}{\sqrt{V_1}}\right) \qquad (۱۱)$$

با توجه به این‌که مقادیر خطاهای محلی حسگرها در حدود چند صدم فرض می‌شود و داریم $0\leq\frac{d}{m}=\alpha\leq 1$، آنگاه می‌توان بخش دوم از سمت راست معادلات ۱۰ و ۱۱ را برابر با صفر گرفت و روابط فوق را به‌صورت زیر بازنویسی کرد:

$$\begin{cases}Q_{Fa}=Q\left(\frac{q-\mu_0}{\sqrt{V_0}}\right)\\Q_d=Q\left(\frac{q-\mu_1}{\sqrt{V_1}}\right)\end{cases} \qquad (۱۲)$$

حال اگر محدودیت $Q_{Fa}\leq\lambda$ را اعمال کنیم مقدار q بهینه به‌دست خواهد آمد:

$$q\leq\sqrt{V_0}Q^{-1}(\lambda)+\mu_0 \qquad (۱۳)$$

این مقدار q بهینه شرط فوق را برآورده می‌کند و به‌عبارتی کران پایین برای q خواهد بود. ولی برای این‌که بیشینه آ شکار سازی حا صل شود هم‌زمان باید بنویسیم:

$$q=\left\lfloor\begin{matrix}\sqrt{m[(1-\alpha)P_d(1-P_d)+\alpha(1-P_a)P_a]}\cdot Q^{-1}(\lambda)\\+m[(1-\alpha)P_d+\alpha(1-P_a)]\end{matrix}\right\rfloor \qquad (۱۴)$$

رهیافت فوق برای محاسبه q و اتخاذ تصمیم نهایی در مرکز با استفاده از روش q-out-of-m تضمین می‌کند که علاوه بر رعایت شرط $Q_{Fa}\leq\lambda$ میزان احتمال آشکارسازی نیز بیشینه خواهد شد. از طرفی این رهیافت، مشکل بار محاسباتی زیاد، ناشی از الگوریتم بهینه بخش قبل را نیز برطرف می‌کند.

۴- شناسایی مهاجمین بیزانسی

در حوزه داده‌کاوی از تحلیل خوشه‌بندی برای کلاس‌بندی نمونه‌ها استفاده می‌شود. این نوع از تحلیل بر اساس یک سنجه مشابهت متغیرها یا نمونه‌ها را در کلاس‌های مختلف قرار می‌دهد. از آنجایی‌که روش تعیین حسگرهای مهاجم نیز به‌نوعی مثل تحلیل خوشه‌بندی خواهد بود و حسگرها را به دو دسته سالم و مهاجم تقسیم خواهد کرد، لذا از این روش استفاده می‌کنیم و سنجه مقایسه را به‌دلیل دودویی بودن نتایج سنجش محیطی حسگرها، فاصله همینگ انتخاب می‌کنیم. فرض کنید

دو بردار باینری x_i و x_j به‌طول T موجود است. فاصله همینگ این دو بردار به‌صورت زیر محاسبه می‌شود[۲۲]:

$$D_{x_i x_j} = \left(\frac{\#\left(x_i \neq x_j\right)}{T} \right) \quad (۱۵)$$

در طی T تناوب از سنجش محیط، بردار گزارشات همه حسگرها به صورت زیر در MAP تشکیل می‌شود:

$$X^i = \left\{ x_1^i, x_2^i, ..., x_T^i \right\}$$
$$x_t^i \in \{0,1\},\ t = 1,2,...,T\ \ i = 1,2,...,N \quad (۱۶)$$

بردار دیگری نیز از نتیجه تصمیم نهایی MAP تشکیل شده و با Y نمایش داده می‌شود. عناصر بردار Y با استفاده از روش q-out-of-m بهینه، مطابق آن‌چه در بخش قبل گفته شد، به‌دست آمده است. MAP فاصله همینگ بین X^i ها و Y را محاسبه کرده و در یک جدول ذخیره می‌کند.

$$D^i = \left(\frac{\neq \left(X^i \neq Y\right)}{T} \right) \quad (۱۷)$$

با مقایسه اندازه فواصل به‌دست آمده با یک سطح آستانه از قبل تعیین شده می‌توان حسگرهای مهاجم را شناسایی کرد. اگر فقط از یک سطح آستانه استفاده شود این امکان وجود دارد که یک مهاجم با حمله در چند دور سنجش و ارسال صحیح در بقیه موارد، شناسایی نشود. لذا برای مقایسه، از دو سطح آستانه پایین و بالا استفاده می‌شود به‌نحوی‌که اگر فاصله D^i از سطح آستانه بزرگتر $D^{\max}$، بیشتر باشد یا از سطح آستانه کوچکتر $D^{\min}$، کمتر باشد، حسگرiام به عنوان مهاجم بیزانسی تلقی شده و نتایج ارسالی آن از فرآیند تصمیم‌گیری خارج خواهد شد. دو حد آستانه $D^{\max}$ و $D^{\min}$ به‌صورت زیر محاسبه می‌شود:

$$D^{\max} = \frac{1}{N(N-1)} \sum_{i=1}^{N} D^i + \frac{\delta_P}{T} \quad (۱۸)$$

$$D^{\min} = \frac{1}{N(N-1)} \sum_{i=1}^{N} D^i - \frac{\delta_P}{T} \quad (۱۹)$$

که در آن δ_P تخمینی از واریانس فاصله کل حسگرها است. پس از شناسایی حسگرهای مهاجم می‌توان نتایج آن‌ها را از تصمیم MAP خارج ساخت و مجدداً پارامترهای m و q جدید را طبق آن‌چه در بخش قبل گفته شد، محاسبه کرد. با اتخاذ روش حذف مهاجمین، مقدار Q_d بهبود خواهد یافت.

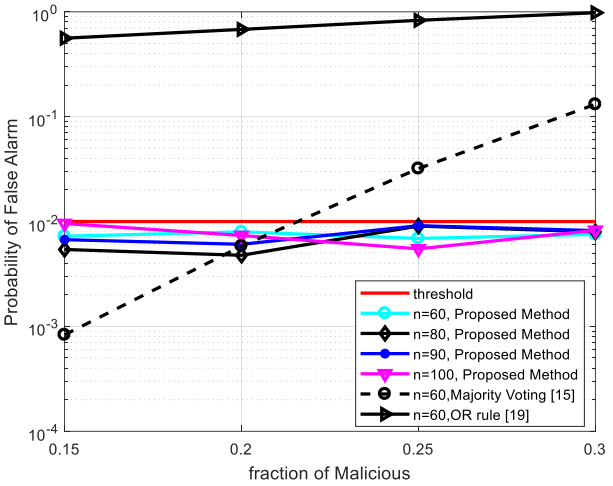
۵- شبیه‌سازی نتایج

در این بخش برای ارزیابی عملکرد الگوریتم تصمیم بهینه پیشنهادی در بخش ۳ و روش شناسایی مهاجمین در بخش ۴ از شبیه‌سازی عددی استفاده می‌شود. برای این منظور فرض می‌شود هر حسگر سالم دارای خطاهای محلی به میزان $P_{Fa} = 0.1$ و $P_m = 0.225$ باشد. شبکه را همگن و احتمالات فوق را برای همه حسگرها یکسان فرض می‌کنیم.

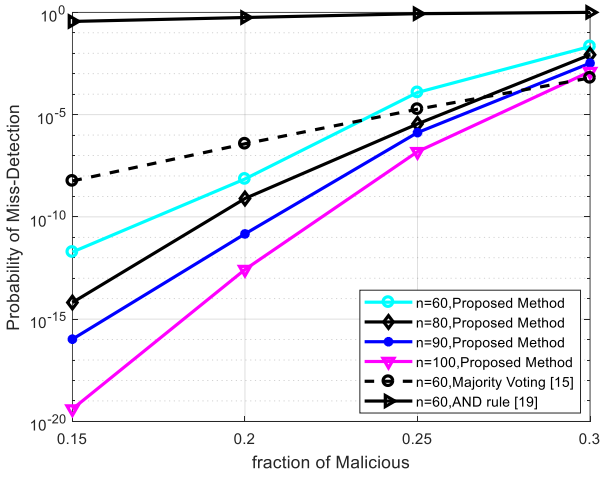
استراتژی حمله را برای مهاجمین در بدترین وضعیت یعنی $P_a = P_0 = 1$ فرض می‌کنیم. با این فرض خطاهای بدست آمده حد بالای خطا خواهند بود. شکل ۳ و ۴ به‌ترتیب احتمال خطای هشدار غلط Q_{Fa} و عدم آشکارسازی صحیح Q_m به‌دست آمده برای تصمیم MAP به‌روش الگوریتم بهینه q-out-of-m مطرح شده در بخش ۳-۱، را به ازای افزایش نسبت مهاجمین (α) نشان می‌دهند. محدودیت اعمالی برای خطای Q_{Fa} به مقدار $\lambda = 0.01$ خواهد بود.

همان‌طوری‌که از شکل ۴ مشخص است با افزایش تعداد مهاجمین حاضر در شبکه، آشکارسازی شبکه تخریب می‌گردد. این تخریب برای شبکه‌هایی با تعداد حسگر کم بیشتر خواهد بود. پس لازم است در زمان‌هایی که نسبت مهاجمین (α)، بزرگ است از تعداد زیادی حسگر اطلاعات جمع شود. شکل ۳ نشان می‌دهد که الگوریتم پیشنهادی میزان خطای Q_{Fa} را در طول فرآیند تصمیم‌گیری به ازای همه نسبت‌های α در حد تعیین‌شده نگه‌داشته‌است. برای مقایسه، نتایج برای روش‌های تصمیم‌گیری منطقی نیز رسم شده است. مثلاً در شکل ۳ ، خطای هشدار غلط روش OR بیشینه می‌باشد به این معنی که با حضور تعدادی مهاجم این روش کارایی خود را از دست می‌دهد. همین موضوع برای روش AND در شکل ۴ در خصوص احتمال آشکارسازی صادق است. در هر دو شکل روش همه‌پرسی اکثریت نیز شبیه‌سازی شده است که اغلب نتیجه‌ای بهتر از روش‌های منطقی قبلی دارد. در هر دو شکل به‌وضوح مشخص است که الگوریتم معرفی‌شده از روش‌های قبلی عمل‌کرد بهتری دارد. در واقع دو روش قبلی به‌دلیل عدم فرض مهاجم و با حضور حتی تعداد کمی مهاجم، کارآیی خود را از دست می‌دهند.

در شکل ۵ به‌جای استفاده از الگوریتم گام‌به‌گام، مقدار عددی q با استفاده از رابطه ۱۴ محاسبه می‌شود. نسبت مهاجمین نیز $\alpha = 0.15$ فرض می‌شود. همان‌طوری‌که قبلاً هم عنوان شد، استفاده از رابطه ۱۴ برای محاسبه q بار محاسباتی تصمیم را کاهش خواهد داد. با استفاده از روش مطرح شده در بخش ۴ در طی فرآیند سنجش اقدام به شناسایی مهاجمین می‌شود. برای یک شبکه با تعداد $N = 30$ حسگر که تعداد $k = 8$ مهاجم در بین آن‌ها وجود دارد، روند شناسایی در شکل ۶ رسم شده است. برای این‌که عمل‌کرد روش شناسایی مهاجمین، مطرح شده در بخش ۴ ارزیابی شود، لازم است تا یک پارامتر برای صحت شناسایی تعریف کنیم. این پارامتر باید دقت روش را نشان دهد. با تعریف نسبت $w_d = \frac{N_m}{k}$ که در آن N_m تعداد حسگرهایی است که به‌درستی توسط روش پیشنهادی مهاجم معرفی شده‌اند و k نیز تعداد کل مهاجمین در شبکه است، قادر خواهیم بود دقت مذکور را اندازه‌گیری کنیم. اندازه پارامتر w_d در طی تناوب‌های مختلف از سنجش در شکل ۶ رسم شده است.

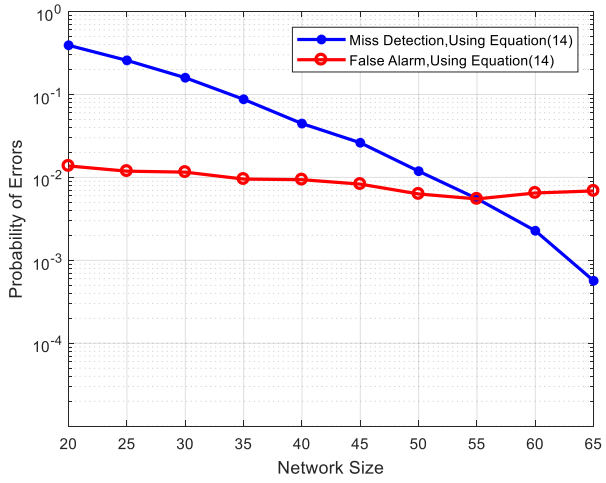


شکل ۳. احتمال هشدار غلط در تصمیم نهایی MAP به ازای افزایش نسبت مهاجمین به کل حسگرهای شبکه.

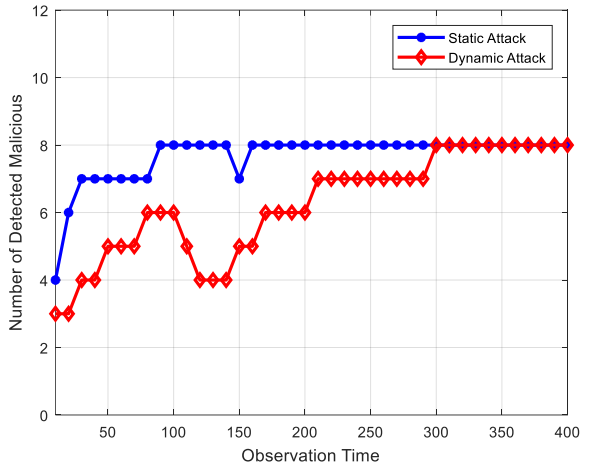


شکل ۴. احتمال عدم آشکارسازی در تصمیم نهایی MAP به ازای افزایش نسبت مهاجمین به کل حسگرهای شبکه.

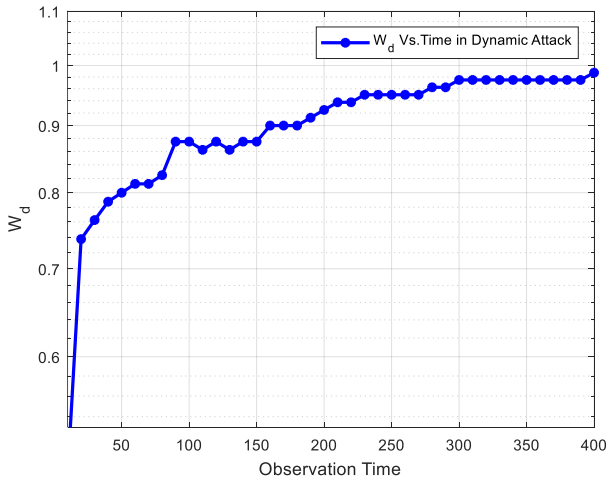
چنانچه از شکل‌های ۶ و ۷ استنباط می‌شود، با این‌که در حمله استاتیکی پس از حدود ۲۰۰ تناوب سنجش تعداد مهاجمین به‌درستی اعلام شده است، اما به‌علت این‌که در این زمان هنوز دقت عمل‌کرد روش کامل نشده است، حدس می‌زنیم که تعدادی از حسگرهای سالم دچار خطای سنجش شده و توسط MAP به‌عنوان مهاجم معرفی شده‌اند. این میزان از زمان لازم برای شناسایی در حمله دینامیکی تا ۳۰۰ افزایش پیدا می‌کند. لذا اگر بخواهیم یک کران پایین برای پایداری نتایج اعلام کنیم، باید از W_d استفاده گردد. برای مثال در حمله دینامیکی برای کامل شدن روند شناسایی مهاجمین و رسیدن W_d به مقدار ۱ حداقل $T = 350$ تناوب لازم است. در کل، این دو شکل نشان می‌دهد که شناسایی یک مهاجم بیزانسی که از یک احتمال حمله ثابت استفاده نمی‌کند، برای شبکه بسیار مشکل است.



شکل ۵. احتمال آشکارسازی و هشدار غلط در تصمیم نهایی MAP به ازای محاسبه q از رابطه (۱۴).



شکل ۶. روند شناسایی تعداد مهاجمین در طی تناوب‌های مختلف.



شکل ۷. تغییرات فاکتور صحت شناسایی مهاجمین در حمله دینامیکی

۶- نتیجه گیری

در این مقاله، با در نظر گرفتن یک شبکه حسگری با یک مرکز جمع‌آوری داده متحرک، یک الگوریتم بهینه تصمیم پیشنهاد گردید

که قادر است خطای نهایی تشخیص را حداقل کند. به‌دلیل ممانعت از ایجاد تاخیر و با استفاده از تحلیل‌های آماری داده‌ها، یک مدل بسته ارائه شد به‌طوری‌که در هر حالتی از شبکه و با تغییر پارامترهای محیط با افزایش ناچیزی در میزان خطای شناسایی با سرعت قابل قبولی پارامترهای روش را به‌دست می‌دهد. سپس روش شناسایی مهاجمین را که از فاصله گزارشات حسگرها با نتایج تصمیم نهایی استفاده می‌کرد، تشریح شد. یکی از مسائل مهم در مقابله با حمله بیزانسی، تشخیص راهبرد حمله یک مهاجم است. راهبرد حمله روند تغییر احتمال حمله در طول زمان را نشان می‌دهد. یک مرکز با تخمین میزان احتمال حمله قادر خواهد بود اثر تزریق اطلاعات ناصحیح در شبکه را کاهش دهد یا این‌که برای گام بعدی از حسگرهایی با میزان احتمال حمله کمتر برای جمع‌آوری اطلاعات استفاده کند. به‌عنوان یک پیشنهاد برای ادامه این کار، تحقیق برای یافتن یک روش برای استفاده از نتایج حسگرهای مخرب در تصمیم‌گیری در شبکه است. در مقالات مختلف نشان داده شده است که با افزایش تعداد حسگرهای مخرب کارآیی الگوریتم‌های پیشنهادی برای مقابله با حمله بیزانسی به شدت کاهش می‌یابد. لذا اگر نقش این حسگرها در تحلیل داده ها عوض شود، اولاً میزان تاثیر حمله کاهش می‌یابد و ثانیاً میزان سربار کمی به شبکه تحمیل خواهد شد.

مراجع

[1] C. Chong and S. P. Kumar, "Sensor networks: evolution, opportunities, and challenges," *in Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247-1256, Aug. 2003.

[2] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and countermeasures" *In Proc. Of First IEEE International Workshop on Sensor Network Protocols and Applications*, May 2003.

[3] L. Lamport, R. Shostak, M. Pease, "The Byzantine Generals Problem", *ACM Trans. Programming Languages and Systems*, vol. 4, no. 3, pp. 382-401, Jul. 1982.

[4] Y. Wang, G. Attebury and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *in IEEE Communications Surveys & Tutorials*, vol. 8, no. 2, pp. 2-23, Second Quarter 2006.

[5] Y. Brun, G. Edwards, J. Y. Bang, and N. Medvidovic, "Smart redundancy for distributed computation," *in 31st International Conference on Distributed Computing Systems (ICDCS)*, pp. 665 -676, Jun. 2011.

[6] P. Sridhar, A. Madni, and M. Jamshidi, "Hierarchical aggregation and intelligent monitoring and control in fault-tolerant wireless sensor net-works," *IEEE Systems Journal*, vol. 1, no. 1, pp. 38-54, Sep. 2007.

[7] F. Liu, X. Cheng and D. Chen, "Insider attacker detection in wireless sensor networks," *in Proc. of IEEE Conference on Computer Commu-nications (Infocom)*, 2007.

[8] W. Zhang, S. K. Das and Y. Liu, "A Trust Based Framework for Secure Data Aggregation in Wireless Sensor Networks," *3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks*, Reston, VA, pp. 60-69, 2006.

[9] S. Marano, V. Matta, "Distributed detection in the presence of byzantine attacks," *IEEE Transactions on Signal Processing*, vol. 57, no. 1, pp. 16-29, Jan. 2009.

[10] E. Soltanmohammadi, M. Orooji, and M. N. Pour, "Decentralized Hypothesis Testing in Wireless Sensor Networks in the Presence of Misbehaving Nodes", *IEEE Transaction on Information Forensics and Security*, vol. 8, no. 1, Jan. 2013.

[11] A. Vempaty, L. Tong, and P. K. Varshney, "Distributed inference with Byzantine data," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 65-75, Sep. 2013.

[12] R. Curtmola and C. Nita-Rotaru, "BSMR: Byzantine-resilient secure multicast routing in multihop wireless networks," *IEEE Transactions on Mobile Computing*, vol. 8, no. 4, pp. 445-459, Apr. 2009.

[13] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 3, pp. 717-729, Mar. 2014.

[14] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, J. Wang, "Byzantine attack and defense in cognitive radio networks: A survey", *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1342-1363, Apr. 2015.

[15] A. A. Sharifi and M. J. Musevi Niya, "Defense Against SSDF Attack in Cognitive Radio Networks: Attack-Aware Collaborative Spectrum Sensing Approach," *in IEEE Communications Letters*, vol. 20, no. 1, pp. 93-96, Jan. 2016.

[16] N. Choudhary, P. Dabas, "An Enhanced Mechanism to Detect and Prevent Byzantine Attack in Wireless Network based on CBDS," *in Journal of Network Communications and Emerging Technologies*, vol. 7, no. 7, pp. 25-28, Jul. 2017.

[17] X. Ren, J. Yan and Y. Mo, "Binary Hypothesis Testing With Byzantine Sensors: Fundamental Tradeoff Between Security and Efficiency," *in IEEE Transactions on Signal Processing*, vol. 66, no. 6, pp. 1454-1468, Mar. 2018.

[18] G. Mergen, Z. Qing, and L. Tong, "Sensor networks with mobile access: Energy and capacity considerations," *IEEE Transactions on Communications*, vol. 54, no. 11, pp. 2033-2044, Nov. 2006.

[19] H. Wang, L. Lightfoot, and T. Li, "On PHY-layer security of cognitive radio: Collaborative sensing under malicious attacks," *44th Annual Conference on Information Sciences and Systems (CISS)*, pp. 1-6, Mar. 2010.

[20] M. Abdelhakim, L. E. Lightfoot, J. Ren and T. Li, "Distributed Detection in Mobile Access Wireless Sensor Network Under Byzantine Attacks," *IEEE Transactions on parallel and Distributed system*, vol. 13, pp. 1045-9219. Apr. 2013.

[21] P. K. Varshney, *Distributed detection and data fusion*, Springer-Verlag, 1997.

[22] P. Tan, M. Steinbach, and V. Kumar, *Introduction to Data Mining*, Addison Wesley, 2006.

زیرنویس‌ها

[1] Byzantine Attack
[2] Malicious Behavior
[3] Malfunction
[4] Kullback–Leibler divergence
[5] Water-Filling
[6] Spectrum Sensing Data Falsification Attack
[7] Constant False Alarm Rate (CFAR)
[8] Mobile Access Point
[9] False Alarm Error
[10] Miss Detection Error