یک الگوریتم مقابله با حمله ارسال انتخابی در شبکه‌های حسگر بی‌سیم با استفاده از اتوماتاهای یادگیر

مجتبی جمشیدی[1]، مهدی اثنی‌عشری[2]، محمد رضا میبدی[3]

[1] دانشکده برق، رایانه و فناوری اطلاعات، دانشگاه آزاد اسلامی، واحد قزوین، قزوین، ایران jamshidi.mojtaba@gmail.com
[2] دانشکده کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران، ایران esnaashari@aut.ac.ir
[3] دانشکده کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران، ایران mmeybodi@aut.ac.ir

چکیده

در این مقاله یک الگوریتم کاملاً توزیعی، پویا، سبک وزن و هوشمند مبتنی بر اتوماتای یادگیر در جهت مقابله با حمله ارسال انتخابی در شبکه‌های حسگر بی‌سیم پیشنهاد شده است. در این الگوریتم از مکانیزم شنود به همراه مدل اتوماتای یادگیر جهت انتخاب مسیر ایمن ارسال بسته‌ها در پروتکل‌های مسیریابی چندگامه استفاده می‌شود. هر گره مجهز به یک اتوماتای یادگیر است که وظیفه آن انتخاب گره بعدی(گره بالادستی) برای ارسال داده‌ها به سمت ایستگاه پایه و نظارت بر عملکرد آن است. شبیه‌سازی الگوریتم پیشنهادی توسط شبیه‌ساز J-SIM صورت گرفته و نتایج شبیه‌سازی‌ها، در قالب معیارهای نرخ تحویل بسته‌ها، نرخ ساقط شدن بسته‌ها توسط گره‌های بدخواه و متوسط انرژی باقی‌مانده گره‌ها، حاکی از برتر بودن روش پیشنهادی نسبت به الگوریتم پایه که فاقد هرگونه الگوریتم امنیتی مقابله با حمله ارسال انتخابی است، الگوریتم مبتنی بر تصدیق چندگامه، الگوریتم مبتنی بر چند جریان داده‌ای و الگوریتم چند مسیره می‌باشد.

کلمات کلیدی

شبکه‌های حسگر، امنیت، حمله ارسال انتخابی، اتوماتای یادگیر

۱- مقدمه

به دلیل کاربرد روز افزون شبکه‌های حسگر در زمینه‌های نظامی(نظیر نظارت مرزها، تشخیص حضور یا حرکت وسایل جنگی یا نیروهای دشمن)، همچنین با توجه به ماهیت انتقال بی‌سیم و چندگامه داده‌ها، محدودیت‌ها(انرژی، ارتباطات، حافظه، قدرت محاسباتی)، عدم مراقبت از گره‌ها در محیط و ... برقراری امنیت در این شبکه‌ها امری بسیار مهم و حیاتی است[1].

حمله ارسال انتخابی[1] یکی از حمله‌های لایه شبکه است که اولین بار در [2] مطرح شد. در این حمله گره بدخواه اقدام به ساقط[2] کردن برخی از بسته‌های دریافتی می‌کند. اگر گره بدخواه تمام بسته‌های دریافتی را ساقط کند، تشخیص آن راحت است، ولی اگر فقط برخی از بسته‌های دریافتی را ساقط کند، تشخیص آن مشکل و چالش‌زا خواهد بود[3,4].

یک رویکرد ممکن جهت کاهش اثرات حمله ارسال انتخابی، استفاده از پروتکل‌های مبتنی بر تصدیق چندگامه[3] [5,6] می‌باشد. در این روش، اگر یک گره میانی از گره‌های بالا-دست یا پایین-دست خود بدرفتاری ببیند، یک پیغام هشدار تولید کرده و آن را به گره منبع[4] یا ایستگاه پایه[5] تحویل می‌دهد. سپس گره منبع و ایستگاه پایه با استفاده از یک سیستم تشخیص نفوذ[6] خیلی پیچیده تصمیم‌گیری کرده و عکس‌العمل مناسب را بروز می‌دهند. به‌طور کلی، معایب این الگوریتم‌ها تأخیر و سربار زیاد محاسباتی، عدم کارایی(گره‌های حسگر باید تلاش زیادی جهت شناسایی حمله ارسال انتخابی انجام دهند)، مشکل امنیتی، عدم مقیاس پذیری، عکس العمل کند، مصرف انرژی بالا و متکی بودن به پروتکل‌های مسیریابی و انتقال خاص می‌باشند [7,8].

در این مقاله، یک الگوریتم مقاوم، پویا، کاملاً توزیعی، سبک وزن و هوشمند ارائه می‌شود که می‌تواند گره‌های بدخواه در حمله ارسال انتخابی را از مسیرهای داده‌ای به طور موثری کنار بزند. روش پیشنهادی از مکانیزم شنود به همراه مدل اتوماتای یادگیر جهت انتخاب مسیرهای ایمن ارسال بسته‌ها در پروتکل‌های مسیریابی چندگامه استفاده می‌کند.

ادامه این مقاله به صورت زیر سازماندهی شده است. در بخش ۲ کارهای گذشته و اتوماتاهای یادگیر در بخش ۳ شرح داده می‌شوند. مدل سیستم و فرضیات در بخش ۴ آمده است. در بخش ۵ الگوریتم پیشنهادی شرح داده می‌شود. نتایج شبیه‌سازی و نتیجه‌گیری نیز به ترتیب در بخش‌های ۶ و ۷ آمده است.

۲- کارهای گذشته

همان‌طور که گفته شد حمله ارسال انتخابی برای اولین بار در [2] مطرح شد و اولین راه‌کار جهت مقابله با این حمله، استفاده از پروتکل-های مسیریابی چندمسیره بیان شد. در این روش بسته‌ها از طریق n مسیر کاملاً مجزا از مبدا به سمت مقصد مسیردهی می‌شوند. معایب این راه‌کار: پایین بودن امنیت، عدم تشخیص گره بدخواه و افزایش انرژی مصرفی و سربار ارتباطات است. در [3] یک پروتکل دیگر ارائه شده است که در آن با توجه به پاسخ‌های دریافتی از گره‌های میانی، از یک الگوریتم تصدیق چندگامه استفاده می‌کند تا پیغام‌های هشدار را در سطح شبکه منتشر کند. در [4] یک تکنیک دیگر برای شناسایی گره‌های بدخواه در حمله ارسال انتخابی ارائه شده که در حقیقت بهبود یافته تکنیک [3] می‌باشد. در [9] یک الگوریتم تشخیص نفوذ متمرکز، مبتنی بر ماشین‌های برداری تقویتی[۷] و تکنیک پنجره لغزان[۸] برای مقابله با حمله چاله سیاه[۹] و ارسال انتخابی مطرح شده است. در [10] یک پروتکل دیگر جهت مقابله با حمله ارسال انتخابی ارائه شده که مبتنی بر توپولوژی‌های چند جریان داده‌ای (MDT[۱۰]) می‌باشد. ایده اصلی MDT، تقسیم گره‌های حسگر به چند گروه یا جریان داده‌ای کاملاً مجزا می‌باشد. به طوری‌که، داده‌های حس شده توسط گره‌های منبع از طریق این جریان‌های داده‌ای مجزا به سمت ایستگاه پایه فرستاده شوند. در [11] یک الگوریتم تحویل داده قابل اطمینان مبتنی بر منطق فازی ارائه شده است که در واقع شکل بهبود یافته تکنیک مسیریابی چند مسیره [2] می‌باشد. در [12] یک الگوریتم سبک وزن دیگر ارائه شده که در آن فقط از اطلاعات همسایه‌ها جهت شناسایی حمله ارسال انتخابی استفاده می‌شود. در [13] یک الگوریتم دیگر برای مقابله با حمله ارسال انتخابی ارائه شده که از مدل شبکه حسگر ناهمگن جهت شناسایی حمله ارسال انتخابی استفاده می‌شود. این الگوریتم فقط در شبکه‌های حسگر مبتنی بر کلاستر عمل می‌کند. در [14] یک روش دیگر برای مقابله با حمله ارسالی انتخابی مطرح شده که در آن از یک رویکرد مبتنی بر چندجمله‌ای استفاده می‌شود. ایده اصلی این است که داده‌های حس شده به چند قطعه تقسیم می‌شوند و این قطعات از طریق مسیرهای مجزا به سمت ایستگاه پایه فرستاده می‌شوند. در [15] نیز یک الگوریتم مبتنی بر نظارت ترافیک جهت شناسایی حمله ارسال انتخابی مطرح شده است. در این رویکرد از گره-های EM[۱۱] جهت شنود و نظارت همه ترافیک شبکه استفاده می‌شود. در [16] نیز یک الگوریتم مبتنی بر آزمون مش ترتیبی[۱۲] جهت تشخیص حمله ارسال انتخابی در شبکه‌های حسگر مطرح شده است. ماهیت این الگوریتم متمرکز بوده و برای شبکه‌های مبتنی بر کلاستر کار می‌کند. در [17] یک الگوریتم تدافعی سبک وزن ارائه شده که از گره‌های همسایه به عنوان گره‌های مانیتور کننده(نظارتی) استفاده می‌کند.

۳- اتوماتای یادگیر

یک اتوماتای یادگیر *[18,19,20]* یک ماشین با حالات محدود است که می‌تواند تعداد محدودی عمل را انجام دهد. هر عمل انتخاب شده، توسط یک محیط تصادفی ارزیابی شده و پاسخی به اتوماتای یادگیر داده می‌شود. اتوماتای یادگیر از این پاسخ استفاده نموده و عمل خود را برای مرحله بعد انتخاب می‌کند. در طی این فرآیند، اتوماتای یادگیر یاد می‌گیرد که چگونه بهترین عمل را از بین اعمال مجاز خود انتخاب کند. شکل (۱) ارتباط بین اتوماتای یادگیر و محیط را نشان می‌دهد.

محیط را می‌توان توسط سه‌تایی $E \equiv \{\alpha, \beta, c\}$ نشان داد که در آن $\alpha \equiv \{\alpha_1, \alpha_2, ..., \alpha_r\}$ مجموعه ورودی‌های محیط، $\beta \equiv \{\beta_1, \beta_2, ..., \beta_m\}$ مجموعه خروجی‌های محیط و $c \equiv \{c_1, c_2, ..., c_r\}$ مجموعه احتمال‌های جریمه می‌باشند. ورودی محیط یکی از r عمل انتخاب شده اتوماتا است. خروجی (پاسخ) محیط به هر عمل i توسط β_i مشخص می‌شود. اگر β_i یک پاسخ دودویی باشد، محیط مدلP[۱۳] نامیده می‌شود. در چنین محیطی $\beta_i(n) = 1$ بعنوان پاسخ نامطلوب یا شکست و $\beta_i(n) = 0$ به عنوان پاسخ مطلوب یا موفقیت در نظر گرفته می‌شوند. به این ترتیب اتوماتای یادگیر تصادفی را می‌توان با چهارتایی $LA \equiv \{\alpha, \beta, p, T\}$ نشان داد که $\alpha \equiv \{\alpha_1, \alpha_2, ..., \alpha_r\}$ مجموعه عمل-های اتوماتا (r تعداد عمل‌های اتوماتا)، $\beta \equiv \{\beta_1, \beta_2, ..., \beta_r\}$ مجموعه ورودی‌های اتوماتا، $p \equiv \{p_1, p_2, ..., p_r\}$ بردار احتمال عمل‌های اتوماتا و $T \equiv p(n+1) = T[\alpha(n), \beta(n), p(n)]$ الگوریتم یادگیری می‌باشد.



شکل (۱) اتوماتای یادگیر تصادفی[18]

اتوماتای یادگیر با عمل‌های متغیر: در بعضی از کاربردها نیاز به اتوماتایی با تعداد عمل متغیر می‌باشد[21]. این اتوماتا در لحظه n عمل خود را فقط از یک زیر مجموعه غیر تهی ($V(n)$) از عمل‌ها که عمل-های فعال نامیده می‌شوند، انتخاب می‌کند. انتخاب مجموعه $V(n)$ توسط یک عامل خارجی و بصورت تصادفی انجام می‌شود. نحوه فعالیت این اتوماتا بصورت زیر است. برای انتخاب یک عمل در زمان n، ابتدا مجموع احتمال عمل‌های فعال خود ($K(n)$) را محاسبه می‌کند و سپس بردار $p(n)$ را مطابق رابطه ۱ محاسبه می‌کند. آن‌گاه اتوماتا یک عمل از مجموعه عمل‌های فعال خود را بصورت تصادفی و مطابق بردار احتمال $p(n)$ انتخاب کرده و بر محیط اعمال می‌کند. اگر عمل انتخاب شده α_i باشد، پس از دریافت پاسخ محیط، اتوماتا بردار احتمال $p(n)$ عمل‌های خود در صورت دریافت پاداش(a میزان پاداش) بر اساس رابطه ۲ و در صورت دریافت جریمه(b میزان جریمه) طبق رابطه ۳ به-روز می‌کند(در محیط مدلP)[21].

$$p_i(n) = prob[\alpha(n) = \alpha_i \mid V(n) \text{ is set of active actions}, \alpha_i \in V(n)] = \frac{p_i(n)}{K(n)} \qquad (۱)$$

الف- پاسخ مطلوب از محیط

$$\begin{aligned} p_i(n+1) &= p_i(n) + a.(1 - p_i(n)) \quad \alpha(n) = \alpha_i \\ p_i(n+1) &= p_j(n) + a.p_i(n) \quad \alpha(n) = \alpha_i,\ \forall j\ \ j \neq i \end{aligned} \qquad (۲)$$

ب- پاسخ نامطلوب از محیط

$$\begin{aligned} p_i(n+1) &= (1-b).p_i(n) \quad \alpha(n) = \alpha \\ p_i(n+1) &= \frac{b}{r-1} + (1-b)p_j(n) \quad \alpha(n) = \alpha_i,\ \forall j\ \ j \neq i \end{aligned} \qquad (۳)$$

سپس اتوماتا بردار احتمال عمل‌ها $p(n)$ را با استفاده از بردار $p(n+1)$ و بصورت زیر به‌روز می‌کند:

$$\begin{aligned} p_j(n+1) &= p_j(n+1).K(n) \quad \text{for all j}, \alpha_j \in V(n) \\ p_j(n+1) &= p_j(n) \quad \text{for all j}, \alpha_j \notin V(n) \end{aligned} \qquad (۴)$$

۴- مدل سیستم و فرضیات

گره‌های حسگر به دو دسته‌ی گره‌های منبع (*SN*) و گره‌های میانی (*FN*) تقسیم می‌شوند. فرض می‌شود که گره‌ها شناسه‌های یکتا دارند. محیط عملیاتی مورد نظر، یک محیط دوبعدی مربع شکل می‌باشد که گره‌های منبع به طور مشخص و گره‌های میانی به طور تصادفی در این محیط پراکنده می‌شوند. تمام گره‌ها، همگن و دارای برد رادیویی ثابت (برابر r) هستند. هم‌چنین، فرض می‌شود که گره‌ها با یکدیگر از طریق کانال رادیویی بی‌سیم مخابره و از انتشار به شیوه همه-جهته[۱۴] استفاده می‌کنند. لینک‌های ارتباطی دوطرفه هستند. گره‌های منبع داده‌های حس شده خود را با کمک گره‌های میانی و از طریق یک مسیر چندگامه به تنها گره ایستگاه پایه در شبکه تحویل می‌دهند. در این‌جا فرض می‌شود که دشمن می‌تواند گره‌های نرمال در شبکه را ضبط و از آنها به عنوان گره‌های بدخواه در شبکه استفاده نماید. هم‌چنین، امکان تزریق گره‌های بدخواه خارجی به داخل شبکه نیز برای دشمن وجود دارد. فرض می‌شود که گره‌های بدخواه با همدیگر همکاری ندارند. به علاوه، هیچ محدودیتی در نرخ ساقط کردن بسته‌ها برای گره‌های بدخواه در نظر گرفته نمی‌شود. از پروتکل برپایی کلید LEAP [22] جهت برپایی کلیدها بین گره‌ها در شبکه بهره گرفته می‌شود.

۵- الگوریتم پیشنهادی

الگوریتم پیشنهادی می‌تواند بر روی هر یک از الگوریتم‌های مسیریابی چندگامه اجرا گردد. در این‌جا، صرفاً به عنوان نمونه، از یک درخت مسیریابی چندگامه مبتنی بر کوتاه‌ترین مسیر استفاده شده است که ایستگاه پایه به عنوان ریشه این درخت در نظر گرفته می‌شود. الگوریتم پیشنهادی از ۳ فاز تشکیل شده است. فاز اول، ساخت درخت مسیریابی و تعیین سطح گره‌ها در درخت مسیریابی، فاز دوم، پیکربندی اتوماتاهای یادگیر و فاز سوم، ارسال داده‌ها به همراه انتخاب مسیرهای ایمن است.

۵-۱- فاز اول: تعیین سطح گره‌ها

در الگوریتم پیشنهادی، از یک بسته تولید مسیر که قالب آن در شکل (۲-الف) آمده است، جهت ساخت درخت مسیریابی و تعیین مسیرهای ممکن از گره‌های حسگر به ایستگاه پایه استفاده می‌شود. بسته تولید مسیر دارای دو فیلد *NodeID* و *HopCount* می‌باشد که به ترتیب دربرگیرنده شناسه گره و حداقل فاصله گره تا ایستگاه پایه برحسب گام می‌باشند. هم‌چنین، هر گره حسگر در حافظه خود یک جدول مسیریابی دو ستونه مطابق شکل (۲- ب) دارد که در ستون *NodeID* شناسه هر گره همسایه خود و در ستون *NodeLevel* شماره سطح آن گره همسایه در درخت مسیریابی را ذخیره می‌کند. به‌علاوه، هر گره حسگر در حافظه خود نیز یک فیلد دیگر به نام *MinHopCount* دارد که بیان‌گر حداقل فاصله گره تا ایستگاه پایه برحسب گام، یا به عبارت دیگر مشخص کننده سطح گره در درخت مسیریابی است. هر گره حسگر پس از دریافت بسته‌های تولید مسیر از همسایه‌های خود، مقدار فیلد *MinHopCount* را از رابطه زیر محاسبه می‌کند.

$$MinHopCount=min(NodeLevel) + 1 \qquad (۵)$$

پس از گسترش گره‌ها در محیط، ایستگاه پایه به عنوان ریشه درخت مسیریابی (تنها گره سطح صفر که شناسه آن هم 0 می‌باشد)، یک بسته تولید مسیر با مقدار *<NodeID=0, HopCount=0>* تولید و آن را در همسایگی خود منتشر می‌کند. در حالت ایده‌آل و بدون در نظر گرفتن نویزهای احتمالی، تمام گره‌های حسگر v_i که در برد رادیویی ایستگاه پایه قرار گرفته باشند، به عنوان گره‌های سطح ۱ درخت مسیریابی، این بسته تولید مسیر را دریافت می‌کنند. هر یک از گره‌های سطح ۱ درخت، با دریافت این بسته، در جدول مسیریابی خود یک سطر اضافه می‌کنند به طوری‌که در فیلد *NodeID* شناسه گره ایستگاه پایه (یعنی عدد 0) و در فیلد *NodeLevel* عدد 0 را قرار می‌دهند. سپس هر یک از این گره‌های همسایه ایستگاه پایه، یعنی v_i ها، یک بسته تولید مسیر جدید ایجاد می‌کنند، به طوری که فیلد *NodeID* آن با شناسه‌ی خود گره v_i و فیلد *HopCount* آن با مقدار *MinHopCount* (که در این‌جا، طبق فرمول (۵)، برای همه v_iها برابر ۱ است) مقداردهی می‌شود، و سپس این بسته تولید مسیر خود را منتشر می‌کنند تا به دست همسایه‌های سطح بعدی برسد. این روند ادامه می‌یابد تا بسته تولید مسیر به همه گره‌های دسترس‌پذیر در شبکه برسد.

(الف) بسته تولید مسیر	
NodeID	**HopCount**

(ب) جدول مسیریابی	
NodeID	**NodeLevel**

شکل(۲): (الف) قالب بسته‌های تولید مسیر و (ب) جدول مسیریابی گره‌ها

۵-۲- فاز دوم: پیکربندی اتوماتای یادگیر

در الگوریتم پیشنهادی، هر گره حسگر مجهز به یک اتوماتای یادگیر با عمل متغیر است. در این فاز، هر گره در جدول مسیریابی خود، گره‌های همسایه‌ای که مقدار *NodeLevel* آن‌ها از *MinHopCount* خودش کوچکتر باشد (یعنی همسایه‌های سطح بالاتر) را در لیستی به نام *SelectionSet* قرار می‌دهد. این لیست در واقع همان لیست

مجموعه عمل‌های ممکن برای اتوماتای یادگیر است. در آغاز، همه عمل‌های اتوماتا فعال (یعنی، $V(k)=SelectionSet$) و دارای احتمال یکسانی می‌باشند که از رابطه زیر محاسبه می‌شود:

$$P_i = \frac{1}{r} \qquad (۶)$$

r تعداد اعضای $SelectionSet$ می‌باشد ,

سپس، اتوماتای یادگیر هر گره حسگر u، به طور تصادفی یکی از عمل‌های خود را انتخاب می‌کند. عمل انتخاب شده در واقع همان گره همسایه‌ای است که جهت ارسال بسته‌ها به سمت ایستگاه پایه انتخاب می‌شود و در فاز بعدی گره u بسته‌های خود و یا بسته‌های دریافتی را از طریق این گره همسایه به سمت ایستگاه پایه جلو می‌برد. در ادامه به گره همسایه انتخاب شده توسط اتوماتای یادگیر اصطلاحاً "گام-بعدی" می‌گوییم.

۵-۳- فاز سوم: ارسال داده‌ها و انتخاب مسیرهای ایمن

پس از پایان فاز دوم که خیلی کوتاه می‌باشد، الگوریتم وارد فاز سوم می‌شود که در آن گره‌ها اقدام به ارسال داده‌های خود می‌کنند. هر گره منبع پس از تولید گزارش، آن را به گام بعدی خود ارسال می‌کند تا بسته به صورت چندگامه به دست ایستگاه پایه برسد. گره‌های حسگر بسته‌های گزارشی را با کلید کلاستری خود رمزگزاری می‌کنند تا عمل شنود امکان پذیر شود [32].

هر گره حسگر u هنگام ارسال بسته‌های خود به گام بعدی، مثلاً گره v، با دوره تناوب $T_{OverHear}$ (دوره تناوب شنود و یا به عبارت ساده‌تر، ۱ بسته از هر $T_{OverHear}$ بسته ارسالی)، بسته‌های ارسالی را در بافر خود ذخیره کرده و کانال را شنود می‌کند تا مشخص گردد گره v آن بسته را ارسال می‌کند یا خیر. گره u پس از گذشت زمان T_{wait} با توجه به نتیجه شنود (ارسال بسته توسط گره v یا عدم ارسال بسته توسط گره v) به دو صورت عمل می‌کند. در صورت ارسال بسته، اتوماتای یادگیر به عمل متناظر با همین گره v طبق فرمول (۲) پاداش می‌دهد و گره v هم‌چنان به عنوان گام بعدی گره u در ارسال‌های بعدی مورد استفاده قرار خواهد گرفت. در غیر این‌صورت، اتوماتای یادگیر عمل متناظر با گره v را طبق فرمول (۳) جریمه نموده، گره v را موقتاً از لیست عمل‌های فعال اتوماتا خارج می‌کند (یعنی، $V(k)=SelectionSet-\{v\}$) و سپس از بین عمل‌های فعال خود یک گره دیگر، مثلاً w، را مطابق فرمول (۱) به عنوان گام بعدی انتخاب نموده، بسته ساقط شده را مجدداً از طریق گام بعدی جدید، یعنی w، ارسال می‌کند و سپس v را مجدداً به $SelectionSet$ اضافه می‌کند.

از این‌رو، اتوماتاهای یادگیر با کمترین سربار ممکن، مانع از انتخاب گره‌های بدخواه به عنوان گام بعدی گره‌های نرمال می‌شوند. نکته خیلی مهم در این الگوریتم این است که هیچ گره‌ای به عنوان گره بدخواه علامت زده نمی‌شود و هیچ پیغامی مبنی بر شناسایی گره بدخواه در شبکه منتشر نمی‌شود، بلکه فقط اتوماتاهای یادگیر احتمال آن‌ها را در بردار احتمالات عمل‌های اتوماتا کاهش می‌دهند تا به ندرت یا هیچ وقت به عنوان گام بعدی در درخت مسیریابی انتخاب نشوند.

به این ترتیب اتوماتاهای یادگیر با گذشت زمان و به‌صورت کاملاً توزیعی و پویا مسیرهای ایمن جهت ارسال بسته‌ها به سمت ایستگاه پایه را یاد می‌گیرند و گره‌های بدخواه را از مسیرهای جریان داده‌ای کنار می‌زنند.

۶- نتایج شبیه سازی

به منظور ارزیابی عملکرد الگوریتم پیشنهادی چند آزمایش انجام گرفته و نتایج حاصل از این الگوریتم با نتایج به دست آمده از الگوریتم‌های ذکر شده در جدول (۱) مقایسه شده است. برای انجام شبیه‌سازی‌ها از شبیه‌ساز J-SIM [23] استفاده شده است. در این شبیه‌سازی‌ها، ۳۰۰ گره حسگر به طور تصادفی در یک محیط ۱۰۰ × ۱۰۰ مترمربع پراکنده می‌شوند. از این تعداد، ۲۰ گره به عنوان گره‌های منبع در نظر گرفته شده‌اند که در شبیه‌سازی‌ها از نظر مکانی ثابت (در لبه‌های مرزی محیط عملیاتی) می‌باشند. گره ایستگاه پایه به طور ثابت در مختصات (۵۰،۳۰) قرار می‌گیرد. همه گره‌ها برد رادیویی ثابت و برابر با ۱۰ متر دارند. گره‌های بدخواه نیز به طور تصادفی از بین دیگر گره‌ها، یعنی گره‌های غیر از گره ایستگاه پایه و گره‌های منبع انتخاب می‌شوند. در تمام آزمایش‌ها (بجز آزمایش ۳) احتمال ساقط شدن بسته‌ها توسط گره بدخواه برابر با ۰/۵ می‌باشد، از پروتکل $CSMA$ در لایه MAC برای پیاده سازی الگوریتم‌ها استفاده شده است. در همه شبیه‌سازی‌ها، گره‌های منبع در هر ۵ واحد زمانی یک بسته تولید و ارسال می‌کنند. هر یک از شبیه‌سازی‌ها به مدت ۱۰۰۰۰ واحد زمانی اجرا شده و نتیجه هر آزمایش، از میانگین ۱۰ اجرا بر روی ۱۰ توپولوژی مختلف شبکه به دست آمده است.

جدول (۱) پروتکل‌های مورد مقایسه با الگوریتم پیشنهادی

نام الگوریتم	پارامترهای امنیتی
Single Path Forwarding	-
Multi-Path [2]	تعداد مسیرهای مجزا n=5
MDT [10]	تعداد جریان‌های داده‌ای n=2
ACK-based [5]	$ACK_{span}=2, TTL=4, t=1$

معیارهای زیر جهت ارزیابی و مقایسه الگوریتم‌ها مورد استفاده قرار گرفته‌اند:

نرخ تحویل بسته: درصدی از بسته‌های تولید شده توسط گره‌های منبع که به دست ایستگاه پایه می‌رسند.

نرخ ساقط شدن بسته‌ها توسط گره‌های بدخواه: درصدی از بسته‌ها که توسط گره‌های بدخواه ساقط می‌شوند و به دست ایستگاه پایه نمی‌رسند. توجه شد که در محاسبه این معیار، صرفاً بسته‌هایی که توسط گره‌های بدخواه ساقط می‌شوند در نظر گرفته می‌شوند. یعنی بسته‌هایی که به دلیل خطای کانال و یا تصادم بسته‌ها ساقط می‌شوند لحاظ نخواهد شد.

متوسط انرژی باقی‌مانده گره‌ها: این معیار متوسط انرژی باقی‌مانده کل گره‌های سطح شبکه در طول زمان را بیان می‌کند.

۶-۱- آزمایش ۱

در این آزمایش، نرخ تحویل بسته‌ها در حالتی‌که تعداد گره‌های بدخواه در شبکه ۰، ۱۰، ۲۰،...۱۰۰ باشد را در الگوریتم پیشنهادی و چهار الگوریتم دیگر مورد ارزیابی قرار داده و نتایج بدست آمده را در شکل (۳) نشان داده‌ایم. همان‌طور که از نتایج شبیه‌سازی آشکار است، نرخ تحویل بسته‌ها در الگوریتم پیشنهادی بالاتر از الگوریتم‌های دیگر می‌باشد. چراکه، الگوریتم پیشنهادی به‌طور توزیعی و هوشمند عمل کرده و به محض مشاهده عمل بدخواهانه توسط هر گره، سریعاً آن‌را از مسیرهای جریان داده‌ای کنار می‌زند.

۶-۲- آزمایش ۲

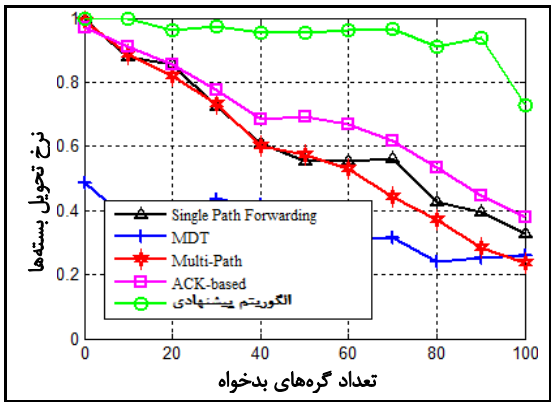
در این آزمایش، که شکل (۴) نتایج آن را نشان می‌دهد، نرخ ساقط شدن بسته‌ها توسط گره‌های بدخواه، در حالتی‌که تعداد گره‌های بدخواه در شبکه ۰، ۱۰، ۲۰،...۱۰۰باشد، در الگوریتم پیشنهادی و چهار الگوریتم دیگر مورد ارزیابی قرار گرفته است. همان‌طور که در این شکل دیده می‌شود، نرخ ساقط شدن بسته‌ها در الگوریتم پیشنهادی بسیار کمتر از دیگر الگوریتم‌ها می‌باشد. چراکه در الگوریتم پیشنهادی، پس از مشاهده عمل بدخواهانه (ساقط شدن بسته‌ها) از سوی گره‌های بدخواه، این عمل سریعاً تشخیص داده شده و این گره‌های بدخواه از مسیرهای جریان داده‌ای کنار زده می‌شوند و بسته ساقط شده مجدداً از مسیر دیگری به سمت ایستگاه پایه هدایت می‌شود. ولی در الگوریتم‌های MDT و Multi-Path رفتار بدخواهانه (ساقط شدن بسته‌ها) گره‌های بدخواه تشخیص داده نمی‌شود. هم‌چنین، در الگوریتم ACK-based عمل تشخیص گره‌های بدخواه فقط توسط ایستگاه پایه و گره‌های منبع صورت می‌گیرد، از این‌رو، الگوریتم فاقد عکس‌العمل سریع بوده و بسته‌های زیادی ساقط می‌شوند.

۶-۳- آزمایش ۳

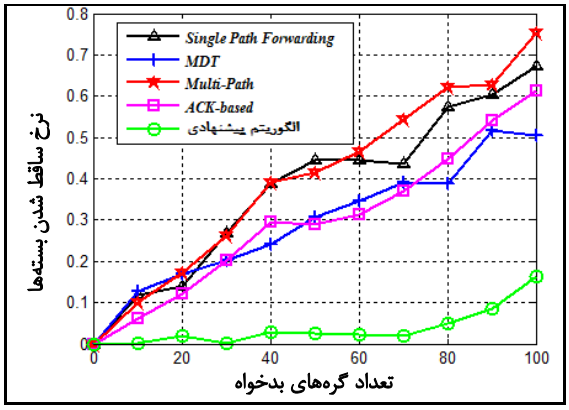
در این آزمایش میزان تأثیر احتمال ساقط شدن بسته‌ها توسط گره‌های بدخواه (*DropProbability*) بر کارایی الگوریتم پیشنهادی مورد ارزیابی قرار گرفته است. بدین منظور، تعداد گره‌های بدخواه برابر با ۵۰ عدد در نظر گرفته شده است. *DropProbability* از ۰ تا ۱ تغییر داده شده و نتیجه آزمایش در قالب نرخ ساقط شدن بسته‌ها توسط گره‌های بدخواه در شکل (۵) به تصویر کشیده شده است. همان‌طور که از نتیجه آزمایش معلوم است، نرخ *DropProbability* تأثیر چندانی بر کارایی الگوریتم پیشنهادی ندارد، چرا که در الگوریتم پیشنهادی با تنظیم پارامتر $T_{overHear}$=1 می‌توان ساقط شدن حتی یک بسته را نیز تشخیص داد.

۶-۴- آزمایش ۴

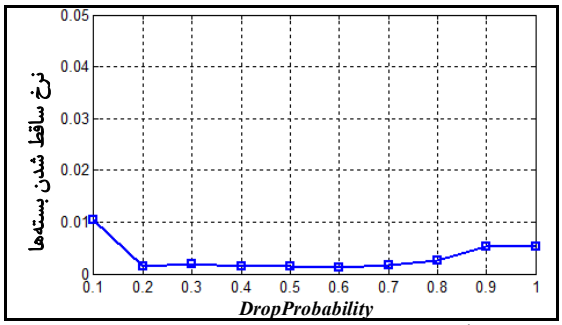
در این آزمایش، متوسط انرژی باقی‌مانده گره‌ها در طول حیات شبکه، در صورت استفاده از الگوریتم پیشنهادی و چهار الگوریتم دیگر مورد مقایسه قرار گرفته است. در این آزمایش، ۵۰ گره بدخواه به طور تصادفی انتخاب شده‌اند. انرژی اولیه تمام گره‌های حسگر 5 ژول در نظر گرفته شده است. شکل (۶) نتیجه این آزمایش را نشان می‌دهد. همان‌طور که از نتیجه این آزمایش معلوم است، متوسط انرژی باقی‌مانده گره‌ها در صورت استفاده از الگوریتم پیشنهادی کمتر از الگوریتم پایه و بیشتر از دیگر الگوریتم‌ها می‌باشد



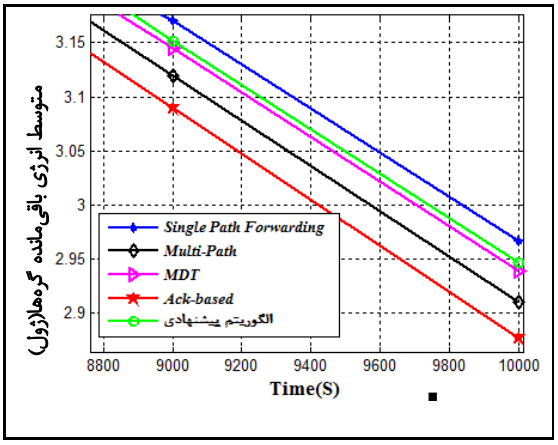
شکل(۳) نرخ تحویل بسته‌ها در الگوریتم پیشنهادی ($T_{overHear}$=1, *a=b=0.0001*) و الگوریتم‌های دیگر.



شکل (۴) نرخ ساقط شدن بسته‌ها در الگوریتم پیشنهادی(*a=0.001*, $T_{overHear}$=1 *b=0.00001*) و الگوریتم‌های دیگر



شکل (۵) تأثیر پارامتر *DropProbability* بر نرخ ساقط شدن بسته‌ها توسط گره‌های بدخواه در الگوریتم پیشنهادی



شکل (۶)انرژی مصرفی الگوریتم پیشنهادی در مقایسه با دیگر الگوریتم‌ها

۷- نتیجه گیری

در این مقاله یک الگوریتم کاملاً توزیعی، پویا، سبک وزن و هوشمند مبتنی بر اتوماتاهای یادگیر جهت مقابله با حمله ارسال انتخابی در شبکه‌های حسگر بی‌سیم ارائه گردید. الگوریتم پیشنهادی، از مکانیزم شنود به همراه مدل اتوماتای یادگیر جهت انتخاب مسیر ایمن ارسال بسته‌ها در پروتکل‌های مسیریابی چندگامه استفاده می‌کند تا گره‌های بدخواه در حمله ارسال انتخابی را از مسیرهای داده‌ای کنار زند. با شبیه‌سازی پروتکل پیشنهادی و انجام آزمایش‌های مختلف، مشخص شد که الگوریتم پیشنهادی در مقایسه با الگوریتم‌های مشابه از نقطه نظر نرخ تحویل بسته‌ها، نرخ ساقط شدن بسته‌ها توسط گره‌های بدخواه و انرژی مصرفی کارآمدتر می‌باشد.

منابع

[1] Akyildiz I. F., Su W., Sankarasubramaniam Y. and Cayircl E., "***A survey on sensor networks***", in: Proceedings of the IEEE Communication Magazine, Vol. 40, pp. 102-114, August 2002.

[2] Karlof C. And Wagner D., "***Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures***", in: Proceedings of the Ad Hoc Networks, pp. 299-302, 2003.

[3] Sharma K. and et al., "***A Comparative Study of Various Security Approaches Used in Wireless Sensor Networks***", in: Proceedings of the International Journal of Advanced Science and Technology, Vol. 17, April, 2010.

[4] Mohammadi S., Atani R. E. and Jadidoleslamy H., "***A Comparison of Link Layer Attacks on Wireless Sensor Networks***", in: Proceedings of the Journal of Information Security, pp. 69-84, April 2011.

[5] Yu B. and Xiao B., "***Detecting selective forwarding attacks in wireless sensor networks***", In: Proceedings of the Second International Workshop on Security in Systems and Networks (IPDPS Workshop), pp. 1-8, April 2006.

[6] Xiao B., Yu B. and Gao C., "***CHEMAS: identify suspect nodes in selective forwarding attacks***", In: Proceedings Of the Journal of Parallel and Distributed Computing, Vol. 67, No. 11, pp. 1218-1230., June 2007.

[7] Bysani L. K. and Turuk A. K., "***A Survey On Selective Forwarding Attack in Wireless Sensor Networks***", In: Proceedings of the International Conference on Device and Communications (ICDeCom), Mesra, india, February 2011.

[8] Kkan W. Z., Xiang Y. and Aalsalem M. Y., "***Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks***", In: Proceedings of the I.J. Computer Network and Information Security, p. 1-10, February 2011.

[9] Kaplantzis S., Shilton A, Mani N. and Sekercioglu Y., "***Detecting selective forwarding attacks in wireless sensor networks using support vector machines***", in: Proceedings of the IEEE 3rd International Conference Intelligent Sensors, Sensor Networks and Information(ISSNIP), pp. 335 –340, December 2007.

[10] Sun H.-M., Chen C.-M. and Hsiao Y.-C., "***An efficient countermeasure to the selective forwarding attack in wireless sensor networks***", in: Proceedings of the IEEE TENCON 2007, pp. 1-4, October 2007.

[11] Lee H. Y. and Cho T. H., "***Fuzzy-based reliable data delivery for countering selective forwarding in sensor networks***", in: Proceedings of the Ubiquitous Intelligence and Computing, pp. 535-544 ,Hong Kong, China, Springer-Verlag, pp. 535-544, 2007.

[12] Hai T. H. and Huh E.-N., "***Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor Knowledge***", In: Proceedings of the Seventh IEEE International Symposium on Network Computing and Applications, pp.325-331, 2008.

[13] Brown J.and Du X., "***Detection of selective forwarding attacks in heterogeneous sensor networks***", in: Proceedings of the IEEE International Conferece on Communications, pp. 1583-1587, May 2008.

[14] Lei X., Yong-jun H., Yong P. and Yue-Fei Z., "***A Polynomialbased Countermeasure to Selective Forwarding Attacks in Sensor Networks***", In: Proceedings of the International Conference on Communications and Mobile Computing, pp.455-459, 2009.

[15] Tumrongwittayapak C. and Varakulsiripunth R., "***Detecting Sinkhole Attack And Selective Forwarding Attack In Wireless Sensor Networks***", in: Proceedings of the 7th International Conference on Information, Communications and Signal Processing (ICICS 2009), pp. 1-5, December 2009.

[16] Li G., Liu X. and Wang C., "***A Sequential Mesh Test based Selective Forwarding Attack Detection Scheme in Wireless Sensor Networks***", in: Proceedings of the International Conference on Networking, Sensing and Control (ICNSC), pp. 554-558, April 2010.

[17] Xin-sheng W., Yong-zhao Z., Shu-ming X. and Liangmin W., "***Lightweight defense scheme against Selective forwarding attacks in wireless sensor***

networks", in: Proceedings of the IEEE International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC '09), pp. 226-232, October 2009.

[18] Narendra K. S. and Thathachar M. A. L., "***Learning automata: An introduction***", in: Proceedings of the Prentice Hall, 1989.

[19] Narendra K. S. and Thathachar M. A. L., "***Learning automata a survey***", in: Proceedings of the IEEE Transactions on Systems, Man and Cybernetics, Vol. 4, no. 4, July 1974.

[20] Lakshmivarahan S. and Thathachar M. A. L., "***Absolutely expedient learning algorithms for stochastic automata***", in: Proceedings of the IEEE Transactions on Systems, Man and Cybernetics, Vol. 6, pp. 281-286, 1973.

[21] Thathachar M. A. L. and Bhaskar R. H., "***Learning automata with changing number of actions***", in: Proceedings of the IEEE Transactions on Systems, Man and Cybernetics, Vol. 17, no. 6, November 1987.

[22] Zhu S., Setia S. and Jajodia S., "***LEAP, Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks***", in: Proceedings of the 10th ACM Conference on Computer and Communications Security (Ccs '03), Washington D.C., October 2003.

[23] J-Sim Simulator, http://www.j-sim.org

زیرنویس‌ها

[1] Selective Forwarding Attack
[2] Drop
[3] Multi-hop Acknowledgment schema
[4] Source Node
[5] Base Station
[6] Intrusion Detection System
[7] Support Vector Machines
[8] Sliding Window
[9] Black hole
[10] Multi-DataFlow Topology
[11] Eavesdropper and Monitor
[12] Sequential Mesh Test Based
[13] P-Model
[14] Omni-directional