همایش ملی مهندسی رایانه و مدیریت فناوری اطلاعات
National Conference On Computer Engineering & Information Technology Management

شناسایی گره‌های کپی در شبکه‌های حسگر بی‌سیم متحرک به کمک اتوماتاهای یادگیر و گره‌های نگهبان

سمیرا عباسی[1]، محمد علی منتظری[2]، محمدرضا خیام باشی[3]

[1] دانشکده کامپیوتر، دانشگاه آزاد اسلامی واحد نجف آباد، نجف آباد، ایران *samiraabasi@sco.iaun.ac.ir*

[2] دانشکده برق و کامپیوتر، دانشگاه صنعتی اصفهان، اصفهان، ایران *montazeri@cc.iut.ac.ir*

[3] گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه اصفهان، اصفهان، ایران *M.R.khayyambashi@eng.ui.ac.ir*

چکیده

با توجه به گسترش روزافزون شبکه‌های حسگر بی‌سیم در زمینه‌های نظامی، محیط زیست، خدمات شهری و اکتشافات، برقرای امنیت در این شبکه‌های امری مهم است. یکی از حمله‌های خطرناک شناخته شده علیه این شبکه‌ها، حمله تکرار گره (یا گره کپی) است. در این حمله، دشمن یک (یا چند) گره نرمال درون شبکه را ضبط کرده، مواد قفل‌گذاری درون آن را استخراج نموده و کپی‌هایی از آن تولید و در شبکه منتشر می‌کند. این گره‌های کپی تحت کنترل دشمن می‌باشد و از آن‌جا که دارای مواد قفل‌گذاری معتبر هستند لذا می‌توانند به راحتی با دیگر گره‌های شبکه کلید مشترک برپا کنند و به مخابره بپردازند. در این مقاله، یک الگوریتم جدید، هوشمند و سبک‌وزن به کمک اتوماتاهای یادگیر جهت شناسایی گره‌های کپی در شبکه‌های حسگر متحرک ارائه می‌شود. الگوریتم پیشنهادی توسط شبیه‌ساز JSIM پیاده‌سازی گردیده و با انجام یک‌سری آزمایش‌ها کارایی آن در قالب معیارهای احتمال تشخیص گره‌های کپی و احتمال تشخیص غلط ارزیابی شده است. نتایج آزمایش‌ها نشان داد، الگوریتم پیشنهادی قادر به شناسایی ۱۰۰٪ گره‌های کپی است.

کلمات کلیدی

شبکه‌های حسگر بی‌سیم، اتوماتاهای یادگیر، گره‌های کپی، گره‌های نگهبان

۱- مقدمه

یک شبکه حسگر بی‌سیم از مجموعه‌ای از گره‌های حسگر تشکیل شده است که با همکاری یکدیگر امکان نظارت بر محیط را فراهم می‌آورند. این نوع شبکه‌ها کاربردهای متنوعی در بخش‌های نظامی، صنعت، بهداشت و علوم دیگر دارند و بیشتر برای مطالعه محیط‌هایی مناسب هستند که امکان حضور انسان در آن محیط پرهزینه و یا خطرناک می‌باشد. در هر مأموریت، گره‌های بسیار زیادی (صدها و یا هزاران گره) در محیط عملیاتی مورد نظر پراکنده می‌شوند و معمولاً پس از گسترش گره‌ها در محیط و یا پایان مأموریت، امکان جمع‌آوری و استفاده مجدد از گره‌ها نیست، بنابر این هزینه تمام شده برای هر گره حسگر باید پایین باشد. با توجه به اندازه بسیار کوچک و نیز هزینه پایین تمام شده برای گره‌ها، محدودیت‌های بسیاری از نظر ظرفیت حافظه، توان محاسباتی، برد رادیویی و میزان انرژی و ... متوجه گره‌های حسگر خواهد بود. با توجه به این محدودیت‌ها، هم‌چنین با توجه به گسترش بدون مراقبت گره‌های حسگر، ماهیت بی‌سیم ارتباطات و نیز کاربرد روز افزون این نوع شبکه‌ها در دامنه‌های نظامی، برقراری امنیت در شبکه‌های حسگر بی‌سیم امری بسیار مهم و چالش‌زا می‌باشد که توجه بسیاری از محققان را به خود جلب کرده است[1] [2] [3] [4].

یکی از حمله‌های خطرناک در شبکه‌های حسگر بی‌سیم حمله تکرار گره[1] یا گره کپی[2] است. با توجه به گسترش بدون مراقبت گره‌ها در محیط عملیاتی، دشمن می‌تواند یک (یا چند) گره قانونی درون شبکه را ضبط و اطلاعات مهم از جمله مواد قفل‌گذاری[3] داخل آن را استخراج کند و با استفاده از این مواد قفل‌گذاری، گره‌های تکراری (یا گره‌های کپی) ایجاد کند. گره‌های کپی دقیقاً حاوی مشخصات و اطلاعات (از جمله شناسه، مواد قفل‌گذاری و ...) گره قانونی ضبط شده می‌باشند، از این‌رو، قابلیت برپایی کلید با دیگر گره‌های قانونی شبکه را

دارد. دشمن سپس می‌تواند این گره‌های کپی را در شبکه پخش کند و حمله‌های مختلفی را راه‌اندازی کند. چراکه از طرفی این گره‌های کپی توسط دشمن کنترل می‌شوند و از طرف دیگر، دارای شناسه و مواد قفل‌گذاری می‌باشند که به آن‌ها اجازه می‌دهد شبیه گره‌های مجاز در شبکه به نظر آیند. بنابراین، پروتکل‌هایی که برای ارتباطات ایمن شبکه‌های حسگر استفاده می‌شوند، این اجازه را به گره‌های کپی می‌دهند تا کلیدهای جفتی با دیگر گره‌ها و ایستگاه پایه برقرار کنند. دشمن می‌تواند از این موقعیت درون شبکه‌ای به روش‌های مختلف بهره‌برداری کند. برای مثال، دشمن می‌تواند به سادگی بخش اعظمی از ترافیک شبکه که از طریق گره‌های کپی عبور می‌کند را نظارت کند، با تزریق داده‌های تحریف شده عملیات نظارتی حسگرها را خراب کند و پروتکل‌های رایج شبکه‌های حسگر از جمله کلاستربندی و تجمع داده‌ها را مختل کند[5] [6].

تاکنون الگوریتم‌های زیادی نظیر [15-7] جهت مقابله با حمله گره‌های کپی در شبکه‌های حسگر ثابت مطرح شده است. ولی این الگوریتم‌ها در شبکه‌های حسگر متحرک قابل بکارگیری نیستند، چراکه اکثر این الگوریتم‌ها یا متکی بر تعیین مکان گره‌ها و ارسال ادعاهای مکانی به گره‌های شاهد یا مکان‌های خاص در شبکه هستند، یا مختص توپولوژی‌های خاص (نظیر، گرید) می‌باشند. هم‌چنین در [30-16] نیز الگوریتم‌هایی جهت مقابله با حمله گره‌های کپی در شبکه‌های حسگر متحرک ارائه شده است که به‌طور کلی دارای معایبی نظیر سربار ارتباطی و حافظه بالا، عدم مقیاس‌پذیری، فرایند پیچیده تشخیص گره‌های کپی، نیاز به تعیین مکان گره‌ها و استفاده از کلیدهای عمومی و امضاهای دیجیتال می‌باشند. در بخش بعدی به شرح ایده اصلی این الگوریتم‌ها و معایب هر یک پرداخته می‌شود.

در این مقاله، یک الگوریتم جدید، هوشمند و سبک وزن مبتنی بر اتوماتاهای یادگیر و گره‌های نگهبان[۴] جهت شناسایی گره‌های کپی در شبکه‌های حسگر متحرک پیشنهاد می‌گردد، به‌طوری که معایب الگوریتم‌های موجود را برطرف کند. الگوریتم پیشنهادی نیاز به تعیین مکان گره‌ها، انتشار پیغام‌های ادعای مکانی، کلیدهای عمومی (و امضای دیجیتال) و فرایندهای پیچیده تشخیص گره‌های کپی ندارد.

ادامه این مقاله بدین ترتیب سازماندهی می‌شود. در بخش ۲، کارهای گذشته و در بخش ۳، اتوماتاهای یادگیر آمده است. مدل سیستم و فرضیات در بخش ۴ آمده است. در بخش ۵ الگوریتم پیشنهادی شرح داده می‌شود. ارزیابی کارایی و نتایج شبیه‌سازی در بخش ۶ ارائه شده است. بخش آخر نیز به نتیجه‌گیری می‌پردازد.

۲- کارهای گذشته

ایده اصلی الگوریتم ارائه شده در [16] به این صورت است که اگر گره حسگر u در یک T_1 گره دیگری نظیر v را ملاقات کرده باشد و گره u در همان زمان یک عدد تصادفی r را برای v ارسال می‌کند. سپس هنگامی‌که گره‌های u و v مجدداً همدیگر را در زمان T_2 ملاقات کنند، گره u از گره v درخواست عدد تصادفی را می‌کند که در زمان T_1 برای آن ارسال کرده بود و انتظار دارد گره v همان عدد r را برایش ارسال کند. اگر گره v تکراری نباشد همان عدد r را برای گره u برگشت داده می‌شود ولی اگر v تکراری باشد ممکن است عدد تصادفی دیگری برگشت داده شود. **معایب این الگوریتم عبارتند از**: سربار ارتباطات بالا، کند بودن فرایند تشخیص گره‌های تکراری است.

ایده اصلی الگوریتم ارائه شده در [17] برگرفته از این حقیقت است که یک گره متحرک ضبط نشده نباید هرگز در سرعتی بیش از حداکثر سرعت سیستم پیکربندی شده حرکت کند. **معایب این الگوریتم عبارتند از**: متمرکز بودن، نیاز به همگام‌سازی، استفاده از کلیدهای عمومی(که برای گره‌های حسگر پرهزینه می‌باشند) و وجود این فرض مشکل که گره‌ها قابلیت تعیین مکان خود و وارسی مکان اعلان شده همسایه‌های خود را دارد(به‌طور کلی تعیین مکان گره‌های حسگر در شبکه‌های حسگر متحرک عمل پرهزینه و مشکلی می‌باشد).

ایده اصلی الگوریتم [19] برگرفته از این ملاحظه است که برای یک شبکه بدون گره تکراری، در یک دوره زمانی مشخص با طول T، تعداد دفعات رویارویی گره u با یک گره خاص v به احتمال زیاد باید محدود باشد. برای یک شبکه با دو گره تکراری v، تعداد دفعات رویارویی گره u با گره v در یک دوره زمانی با طول T باید بزرگتر از یک آستانه باشد. بر طبق این ملاحظه، هر گره قابلیت شناسایی گره‌های تکراری را دارد. **معایب این الگوریتم عبارتند از**: هزینه ارتباطات بالا(هر گره باید به‌طور پریودیک شناسه خود و همسایه‌هایش را منتشر کند)، حداقل و حداکثر سرعت گره‌ها از پیش تعیین شده می‌باشد، هر گره باید از مکان خود آگاه باشد و نیاز به کلیدهای عمومی و امضای دیجیتال دارد.

ایده اصلی الگوریتم ارائه شده در [20] بر این اساس است که کل شبکه به سکتورهایی تقسیم می‌شود و هر سکتور یک گره مرکزی دارد که از روش‌هایی نظیر تشخیص شناسه، تشخیص همسایه‌های تکراری و آرایه‌ی ردیابی (ذخیره مکان‌های گره‌ها) استفاده می‌کند تا گره‌های حسگر را شناسایی کند. **معایب این الگوریتم عبارتند از**: نیمه متمرکز بودن، پیاده‌سازی مشکل(سکتوربندی شبکه)، فرایند پیچیده تشخیص گره تکراری، هزینه ارتباطات بالا در گره‌های مرکزی.

ایده اصلی الگوریتم [21]، استفاده از پروتکل پیش‌توزیع کلید جفتی مبتنی بر چندجمله‌ای و فیلترهای شمارشی Bloom می‌باشد تا تضمین شود که گره‌های کپی هرگز نمی‌توانند نزدیک شناسه‌های واقعی‌شان قرار بگیرند و تعداد کلیدهای جفتی برپا شده توسط هر گره را جمع‌آوری کند. گره‌های کپی با بررسی این‌که آیا تعداد کلیدهای جفتی برپا شده توسط آن‌ها از مقدار آستانه بیشتر است شناسایی شوند. **معایب این الگوریتم عبارتند از**: متمرکز بودن، عدم مقیاس‌پذیری طولانی بودن فرایند تشخیص و باطل‌سازی گره‌های تکراری.

ایده اصلی الگوریتم [22]، SHD، مبادله لیست همسایه‌ها میان گره‌های متحرک و انتخاب گره‌های شاهد برای عمل تشخیص است.

به‌طور کلی، فرآیند تشخیص SHD، مبتنی بر ارسال پیغام < *ID, neighbor_list* > به گره‌های در محدوده رادیویی خود در زمان شروع اجرای پروتکل و سپس استفاده از متدهای پرسش و پاسخ است.

همچنین، در [28] یک الگوریتم دیگر جهت شناسایی گره‌های تکراری در شبکه‌های حسگر متحرک مطرح شده است که از یک تصدیق هویت مبتنی بر نشانه جهت تشخیص گره‌های کپی استفاده می‌کند. در [29] نیز یک الگوریتم دیگر ارائه شده است که فقط از ارتباطات تک‌گامه و تحرک گره جهت شناسایی گره‌های تکراری در شبکه‌های حسگر متحرک استفاده می‌کند. در [30] نیز یک الگوریتم جهت شناسایی گره‌های کپی در شبکه‌های ادهاک ارائه شده است.

۳- اتوماتاهای یادگیر

یک اتوماتای یادگیر[31] [32] [33] 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.

شکل (۱) اتوماتای یادگیر تصادفی[31]

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 مدل P[۵] 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 عمل‌های 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 $T \equiv p(k+1) = T[\alpha(k), \beta(k), p(k)]$ الگوریتم یادگیری می‌باشد. اگر اتوماتای یادگیر در تکرار kام، یک عمل خود مانند α_i را انتخاب کند، تغییر احتمال عمل‌ها بصورت زیر خواهد بود(a پارامتر پاداش و b پارامتر جریمه می‌باشند):

الف- پاسخ مطلوب از محیط

$$p_i(k+1) = p_i(k) + a[1 - p_i(k)]$$
$$p_j(k+1) = (1-a)p_j(k) \qquad \forall j, \ j \neq i \qquad (۱)$$

ب- پاسخ نامطلوب از محیط

$$p_i(k+1) = (1-b)p_i(k)$$
$$p_j(k+1) = \frac{b}{r-1} + (1-b)p_j(k) \qquad \forall j, \ j \neq i \qquad (۲)$$

۴- فرضیات سیستم و مدل حمله

شبکه حسگر حاوی دو مجموعه گره‌های حسگر معمولی (SN[۶]) و گره‌های نگهبان (WN[۷]) می‌باشد که به‌طور تصادفی در یک محیط دوبعدی پراکنده می‌شوند. تعداد گره‌های حسگر معمولی، $\eta = |SN|$ و تعداد گره‌های نگهبان، $\varpi = |WN|$ است. تعداد گره‌های نگهبان خیلی کمتر از تعداد حسگرهای معمولی است ($\varpi << \eta$). تعداد کل گره‌های شبکه را با n نشان می‌دهیم که در الگوریتم پیشنهادی از $n = \varpi + \eta$ بدست می‌آید. گره‌های حسگر معمولی، SN، مأموریت شبکه (نظیر جمع‌آوری اطلاعات، ارسال داده‌ها به سمت ایستگاه پایه و ...) را انجام می‌دهند و گره‌های نگهبان، WN، وظیفه شناسایی گره‌های کپی را بر عهده دارند. هر گره یک شناسه یکتا دارد و از موقعیت مکانی خود آگاه نیست. برد رادیویی تمام گره‌ها، یکسان است. تمام گره‌ها متحرک می‌باشند و در طول حیات شبکه مطابق مدل‌های تحرک، نظیر Random waypoint در محیط عملیاتی مورد نظر حرکت می‌کنند. گره‌ها با یکدیگر از طریق کانال رادیویی بی‌سیم مخابره و از انتشار به شیوه همه-جهته[۸] استفاده می‌کنند. گره‌های حسگر معمولی(SN) در برابر مداخله مقاوم نیستند و دشمن در صورت ضبط یک گره می‌تواند به اطلاعات محرمانه آن دسترسی داشته باشد و آن را برنامه ریزی مجدد کند. ولی فرض می‌شود گره‌های نگهبان در برابر مداخله مقاوم بوده و در صورت ضبط توسط دشمن، قابل کدگشایی و برنامه‌ریزی مجدد نمی‌باشند. همچنین، با توجه به متحرک بودن گره‌های حسگر در محیط عملیاتی، گره‌ها می‌بایست به‌طور پریودیک (مثلاً بعد از هر t واحد زمانی یا پس از این‌که به یک مکان جدید در شبکه می‌رسند) یک پیغام "Hello"، درخواست مسیر، ارسال داده، زنده بودن[۹] و ... از خود منتشر کنند[30]. این عمل درواقع یکی از نیازمندی‌های شبکه‌های حسگر متحرک است تا هر گره بتواند در هر لحظه از زمان همسایه‌های جاری خود را شناسایی کرده، در صورت نیاز با آن‌ها کلیدهای امنیتی برپا کند، با هم مخابره کنند و جدول مسیریابی خود را ایجاد کند. البته در این‌جا، گره‌های نگهبان از ارسال پریودیک این‌گونه پیغام‌ها خودداری می‌کنند تا حضورشان از دید دیگر گره‌ها مخفی بماند. چراکه این گره‌های نگهبان وظیفه شناسایی گره‌های بدخواه دشمن (گره‌های کپی) را دارند.

همچنین فرض می‌شود شبکه حسگر در یک محیط خصمانه گسترش می‌یابد، بنابر این، شبکه ناامن بوده و دشمن می‌تواند گره‌هایی را ضبط کند و کپی‌هایی از این گره‌های ضبط شده را ایجاد و سپس در شبکه تزریق کند. همچنین فرض می‌شود هر گره کپی نیز در هر دوره

زمانی t، یک پیغام "Hello"، درخواست مسیر، ارسال داده یا زنده بودن منتشر می‌کند. فرض آخر این است که گره‌های کپی هم‌چون گره‌های معمولی در طول حیات شبکه، در محیط عملیاتی مورد نظر متحرک می‌باشند.

۵- الگوریتم پیشنهادی

ایده اصلی الگوریتم پیشنهادی، بکارگیری اتوماتاهای یادگیر و استفاده از پیغام‌های "Hello" (و درخواست مسیر، ارسال داده یا زنده بودن) منتشر شده توسط گره‌ها جهت شناسایی گره‌های کپی در شبکه‌های حسگر متحرک است. همان‌طور که گفته شد، در الگوریتم پیشنهادی علاوه بر گره‌های حسگر معمولی، تعدادی گره نگهبان در شبکه وجود دارد که ترافیک شبکه را نظارت کرده و گره‌های کپی را شناسایی می‌کنند. اتوماتاهای یادگیر بر روی این گره‌های نگهبان سوار می‌شوند. از دلایل موثر بودن اتوماتاهای یادگیر می‌توان به هوشمندی، سبک‌وزن و غیر قطعی بودن اشاره کرد که مناسب شبکه‌های حسگر بی‌سیم است.

الگوریتم پیشنهادی از ۳ فاز تشکیل شده است. در **فاز اول**، اتوماتاهای یادگیر پیکربندی می‌شوند. در **فاز دوم**، هر گره نگهبان با نظارت بر ترافیک شبکه، اتوماتای یادگیر خود را بروزرسانی می‌کند. این فاز به‌طور پریودیک در فاصله‌های زمانی t اجرا می‌گردد. در هر دوره زمان t، گره‌ها یک مقصد تصادفی برای خود انتخاب نموده و پس از رسیدن به مقصد در آنجا ساکن می‌مانند و شروع به ارسال پیغام‌های "Hello"، داده‌ای، درخواست مسیر و... می‌کنند. این فاز، ψ مرتبه (دور) اجرا می‌گردد. به عبارت دیگر، ψ دور عمل نظارت بر ترافیک شبکه، توسط گره‌های نگهبان صورت می‌گیرد. در **فاز سوم**، گره‌های کپی شناسایی می‌شوند. در ادامه به شرح جزئیات این ۳ فاز می‌پردازیم:

۵-۱- فاز اول (پیکربندی اتوماتاهای یادگیر)

قبل از گسترش گره‌ها در محیط عملیاتی، اتوماتاهای یادگیر بر روی گره‌های نگهبان بار می‌شوند و با فرض این‌که تعداد گره‌های حسگر معمولی η باشد، بردار عمل (A_vector) و بردار احتمالات (P_vector) عمل‌های اتوماتاهای یادگیر به صورت رابطه (۳) تنظیم می‌شوند:

$$A\_vector = [1,2,\ldots,\eta]$$
$$P\_vector = [\frac{1}{\eta},\frac{1}{\eta},\ldots,\frac{1}{\eta}] \quad (۳)$$

درواقع هر گره حسگر معمولی، بیان‌گر یک عمل ($action$) اتوماتای یادگیر است. سپس هر اتوماتای یادگیر به‌طور تصادفی یک عمل (α_i) را انتخاب می‌کند. این عمل انتخاب شده توسط اتوماتای یادگیر موجود در گره نگهبان v در واقع گره‌ای است که v انتظار دارد در دور بعدی نظارت بر ترافیک (در این‌جا، دور اول از فاز دوم) آن را در همسایگی خود مشاهده کند. پس از انجام این مرحله، یعنی پیکربندی اتوماتاهای یادگیر موجود در گره‌های نگهبان، گره‌ها به‌طور تصادفی در محیط گسترش می‌یابند.

۵-۲- فاز دوم (نظارت بر ترافیک)

هر گره پس از ساکن شدن در یک مکان از محیط عملیاتی، یک پیغام "Hello" منتشر می‌کند تا خود را به همسایه‌هایش معرفی نماید و در صورت نیاز اقدام به ارسال پیغام‌های درخواست مسیر، داده‌ای یا زنده بودن می‌کند. این سبب می‌شود هر گره نگهبان آگاه شود که چه گره‌هایی در حال حاظر (یا دور فعلی از فاز دوم) همسایه آن هستند. پس از گذشت t واحد زمانی یا به عبارت دیگر، پس از پایان دور فعلی، اتوماتای یادگیر هر گره نگهبان v پاسخی (مثبت یا منفی) از محیط دریافت می‌کند. اگر عمل (یا همان گره) انتخاب شده، یعنی α_i، در همسایگی گره نگهبان v ظاهر شده باشد، این به منزله پاسخ مثبت از محیط است و چنانچه عمل α_i در همسایگی گره نگهبان v ظاهر نشده باشد، این به منزله پاسخ منفی از محیط است. اگر اتوماتای یادگیر پاسخ مثبت از محیط دریافت کند، به عمل α_i مطابق رابطه (۱) پاداش داده و همین عمل α_i را برای دور بعدی انتخاب می‌کند. ولی اگر پاسخ منفی از محیط دریافت کند، ابتدا عمل α_i را مطابق رابطه (۲) جریمه نموده، سپس یک عمل را از مجموعه عمل‌های خود (A_vector) به‌طور تصادفی برحسب بردار P_vector انتخاب می‌کند. این عملیات به‌طور همزمان توسط تمام گره‌های نگهبان انجام می‌گیرد. به این ترتیب، پس از گذشت یک برهه زمانی t، دور اول از اجرای فاز دوم الگوریتم پیشنهادی خاتمه می‌یابد. سپس گره‌ها یک مقصد تصادفی جدید برای خود انتخاب و شروع به حرکت به سوی مقصد می‌کنند. به این ترتیب، دور بعدی از فاز دوم آغاز می‌شود.

همان‌طور که گفته شد، فاز دوم، ψ دور اجرا می‌گردد. از آن‌جا که در حمله تکرار گره، دشمن یک گره را ضبط و چندین کپی از آن را در شبکه منتشر می‌کند لذا به تعداد دفعات بیشتری نسبت به گره‌های غیرکپی در همسایگی گره‌های نگهبان ظاهر می‌شوند که این سبب می‌شود اتوماتاهای یادگیر احتمال عمل متناظر با این گره کپی را در بردار احتمالات (P_vector) افزایش دهند تا به مقدار 1 نزدیک شود.

۵-۳- فاز سوم (شناسایی گره‌های کپی)

پس از پایان اجرای فاز دوم الگوریتم پیشنهادی، هر گره نگهبان باید تصمیم بگیرد که آیا گره‌ی کپی‌ای شناسایی کرده است یا خیر. اگر هیچ گره کپی‌ای در شبکه وجود نداشته باشد، در این صورت با توجه به مدل تصافی حرکت گره‌ها، تعداد دفعات حضور همه گره‌ها در همسایگی گره نگهبان v تقریباً برابر خواهد بود که این سبب می‌شود مقدار احتمال‌ها در بردار P_vector تقریباً باهم برابر باشند. ولی اگر دشمن یک گره u را ضبط نموده و چندین کپی از آن در شبکه تزریق کرده باشد، در این صورت، تعداد دفعات ظاهر شدن گره با شناسه u در همسایگی گره نگهبان v بیشتر از سایر گره‌ها خواهد بود. این سبب می‌شود مقدار احتمال عمل متناظر با گره u در بردار P_vector

اتوماتای یادگیر گره نگهبان v به مراتب بیشتر از مقدار احتمال عمل‌های متناظر با سایر گره‌ها باشد. بنابر این، هر گره نگهبان باید با توجه به بردار احتمالات عمل‌های (P_vector) اتوماتای یادگیر خود اقدام به شناسایی گره‌های کپی کند. در اینجا یک روال ساده جهت شناسایی گره‌های کپی، بر اساس بردار P_vector پیشنهاد می‌شود:

ابتدا بردار P_vector به صورت نزولی مرتب می‌شود. سپس، بردار P_vector را از ابتدا پیمایش نموده و چنانچه احتمال عمل iام با عمل $i+1$ بیشتر از مقدار میانگین (یعنی $\frac{1}{\eta}$) باشد، عمل متناظر با $P\_vector[i]$، یعنی $A\_vector[i]$ را به عنوان گره بدخواه کپی علامت می‌زنیم. ولی اگر شرط مورد نظر برای عنصر iام برقرار نباشد، عمل پیمایش شکسته شده و عناصر بزرگتر از i دیگر بررسی نمی‌شوند. چراکه عمل‌های متناظر با گره‌های کپی، میزان احتمال‌شان در بردار احتمال عمل‌های اتوماتا خیلی بیشتر از احتمال دیگر عمل‌ها خواهد شد. از این‌رو، تفاضل مقدار احتمال عمل‌های متناظر با گره‌های کپی نسبت به عمل‌های متناظر با دیگر گره‌ها غیرکپی بیشتر از مقدار میانگین بردار P_vector خواهد شد (بسته به تعداد دورهای اجرای فاز دوم و تعداد کپی‌ها).

۶- نتایج شبیه‌سازی

الگوریتم پیشنهادی توسط نرم‌افزار شبیه‌ساز JSIM پیاده‌سازی گردیده و با انجام یک‌سری آزمایش‌ها، کارایی آن در قالب معیارهای احتمال تشخیص و احتمال تشخیص غلط ارزیابی شده است.

احتمال تشخیص (P_s): این معیار هم‌چون مرجع [12] به صورت زیر محاسبه می‌شود:

$$P_s = \frac{\#successful\ \text{detection}\ times}{\#repeat\ times}$$

یعنی، تعداد اجراهای منجر به تشخیص موفق بر تعداد کل اجراها. البته باید توجه شود که هر اجرای الگوریتم پیشنهادی و برخی الگوریتم‌های دیگر نظیر XED، RED و LSM از ψ دور تکرار الگوریتم تشکیل شده است.

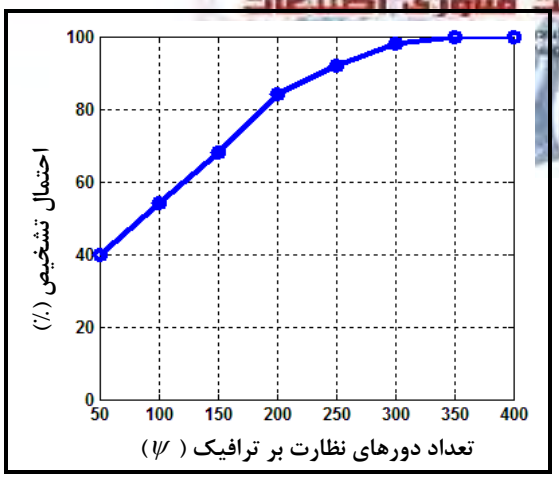
احتمال تشخیص غلط: درصدی از گره‌های غیرکپی است که به اشتباه توسط الگوریتم امنیتی مد نظر به عنوان گره‌های کپی تشخیص داده می‌شوند.

در اجرای شبیه‌سازی‌ها، فرض می‌شود شبکه حاوی n گره حسگر است که به‌طور تصادفی در یک ناحیه دوبعدی ۱۰۰×۱۰۰ متر مربع پراکنده شده‌اند. دشمن M گره قانونی را ضبط نموده و از روی هرکدام R گره کپی ایجاد می‌کند. به عبارت دیگر، محیط عملیاتی حاوی $R\times M$ گره بدخواه می‌باشد. هم‌چنین، تعداد گره‌های نگهبان ϖ در نظر گرفته شده است. پارامترهای پاداش و جریمه اتوماتاهای یادگیر با مقادیر $a=0.01,\ b=0.001$ تنظیم شده است. برد رادیویی تمام گره‌ها نیز 20 متر درنظر گرفته شده است. به منظور اطمینان از اعتبار نتایج، هر شبیه‌سازی ۱۰۰ بار تکرار شده و نتیجه نهایی از میانگین نتایج این ۱۰۰ تکرار بدست آمده است.

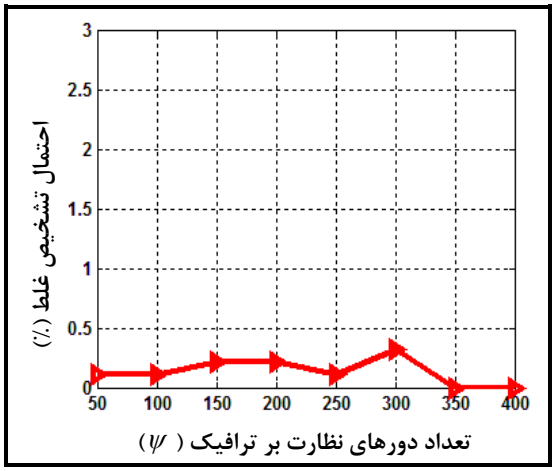
آزمایش ۱: در این آزمایش پارامترهای $\varpi=10,\ M=5,\ R=10,\ n=100$ تنظیم شده و احتمال تشخیص و احتمال تشخیص غلط گره‌های کپی در الگوریتم پیشنهادی، به ازای $\psi=50,\ldots,400$، ارزیابی گردیده است. شکل‌های (۲) و (۳) نتایج این آزمایش را به ترتیب در قالب معیارهای احتمال تشخیص و احتمال تشخیص غلط نشان می‌دهد. نتایج این آزمایش در شکل (۲) نشان داد، احتمال تشخیص گره‌های کپی به ازای $\psi=200$ برابر ۸۴٪، به ازای $\psi=300$ برابر ۹۸٪ و به ازای $\psi\geq 350$ برابر ۱۰۰٪ است. هم‌چنین، نتایج این آزمایش در شکل (۳) نشان داد، احتمال تشخیص غلط الگوریتم پیشنهادی به ازای $\psi<350$ کمتر از ۰٫۵٪ و به ازای $\psi\geq 350$ برابر ۰٪ است. دلیل این نتایج واضح است. هرچه تعداد دورهای نظارت بر ترافیک (یعنی تعداد دورهای فاز دوم) افزایش یابد، گره‌های نگهبان دفعات بیشتری گره‌های کپی را در همسایگی خود ملاقات می‌کنند که این سبب می‌شود احتمال عمل‌های متناظر با این گره‌های کپی به سمت 1 و احتمال سایر عمل‌ها (گره‌های غیرکپی) به سمت 0 میل کند. در نتیجه، فاز سوم الگوریتم پیشنهادی، با دقت بیشتری گره‌های کپی را از گره‌های غیرکپی تمیز می‌کند. بنابر این، افزایش پارامتر ψ سبب می‌شود احتمال تشخیص به سمت ۱۰۰٪ و احتمال تشخیص غلط به سمت ۰٪ میل کند.

آزمایش ۲: هدف این آزمایش، ارزیابی تأثیر تعداد گره‌ها، n، بر کارایی الگوریتم پیشنهادی است. در این آزمایش پارامترهای $\varpi=10,\ M=5,\ R=10,\ \psi=350$ تنظیم شده و احتمال تشخیص و احتمال تشخیص غلط گره‌های کپی در الگوریتم پیشنهادی، به ازای $n=100,200,300$، ارزیابی گردیده و نتایج حاصل در جدول (۱) آمده است. نتایج این آزمایش نشان داد، با افزایش تعداد گره‌ها در شبکه، احتمال تشخیص گره‌های کپی کاهش و احتمال تشخیص غلط افزایش می‌یابد. دلیل این نتیجه این است که هرچه تعداد گره‌ها، n، در شبکه افزایش یابد به نسبت آن تعداد عمل‌های اتوماتاهای یادگیر نیز افزایش می‌یابد. از طرفی، هرچه تعداد عمل‌های اتوماتای یادگیر افزایش یابد، سرعت همگرایی اتوماتای یادگیر کندتر می‌شود. به عنوان مثال، زمانی که ۱۰۰ گره در شبکه وجود داشته باشد احتمال تشخیص و احتمال تشخیص غلط الگوریتم پیشنهادی به ترتیب ۱۰۰٪ و ۰٪ می‌شود. ولی زمانی که ۳۰۰ گره در شبکه وجود داشته باشد احتمال تشخیص و احتمال تشخیص غلط الگوریتم پیشنهادی به ترتیب ۹۲٪ و ۱٫۴٪ است. البته اگر تعداد دورهای فاز دوم، یعنی ψرا افزایش دهیم ($\psi>350$) احتمال تشخیص گره‌های کپی بیشتر از ۹۲٪ می‌شود و به سمت ۱۰۰٪ میل

می‌کند و احتمال تشخیص غلط کمتر از ۱٫۴٪ و به سمت ۰٪ میل می‌کند.



شکل (۲) تأثیر پارامتر ψ بر احتمال تشخیص الگوریتم پیشنهادی



شکل (۳) تأثیر پارامتر ψ بر احتمال تشخیص غلط الگوریتم پیشنهادی

جدول (۱) تأثیر پارامتر n بر احتمال تشخیص و احتمال تشخیص غلط الگوریتم پیشنهادی

	n=100	n=200	n=300
احتمال تشخیص	100%	96%	92%
احتمال تشخیص غلط	0%	0.9%	1.4%

آزمایش ۳: هدف این آزمایش، ارزیابی تأثیر تعداد کپی‌های منتشر شده از هر گره، یعنی R، بر کارایی الگوریتم الگوریتم پیشنهادی است. در این آزمایش پارامترهای $n=100,\ \psi=300\ \ M=5\ \ \varpi=10,$ تنظیم شده و احتمال تشخیص و احتمال تشخیص غلط گره‌های کپی در الگوریتم پیشنهادی، به ازای $R=5,10,15$، ارزیابی گردیده است. جدول (۲) نتایج حاصل از این آزمایش را نشان می‌دهد. نتیجه این آزمایش نشان می‌دهد به ازای افزایش پارامتر R، احتمال تشخیص گره‌های کپی نیز افزایش می‌یابد. در ادامه، دلیل این نتیجه را با یک نکته مهم شرح می‌دهیم:

دشمن به دو صورت می‌تواند با راه‌اندازی حمله گره‌های کپی، عملکرد شبکه را مختل کند. شیوه اول این است که دشمن تعداد زیادی گره قانونی درون شبکه را ضبط کرده و از روی هر کدام فقط تعداد اندکی (مثلاً ۲ یا ۳) گره کپی ایجاد و در شبکه منتشر کند. در این حالت، الگوریتم‌های امنیتی به سختی و حتی ممکن است قادر به شناسایی گره‌های کپی نباشند. ولی پیش گرفتن این روش برای دشمن سخت و زمان‌بر است. چراکه باید گره‌های زیادی را ضبط، کدگشایی، برنامه‌ریزی مجدد و کنترل کند. شیوه دوم این است که دشمن تعداد گره‌های اندکی را ضبط کند ولی تعداد کپی‌های زیادی (مثلاً ۱۰ کپی) از هر گره ضبط شده در شبکه منتشر کند. پیش گرفتن این شیوه، برای دشمن ساده و امکان‌پذیر است. ولی الگوریتم‌هایی امنیتی در این حالت ممکن است سریع‌تر و دقیق‌تر اقدام به شناسایی گره‌های کپی کنند. نتیجه این آزماش نیز نشان داد الگوریتم پیشنهادی به ازای Rهای بزرگتر، سریع‌تر گره‌های کپی را شناسایی می‌کند. چراکه اگر تعداد کپی‌های زیادی از یک گره خاص، نظیر u، در شبکه موجود باشد، گره‌های نگهبان تعداد دفعات بیشتری این گره u را ملاقات می‌کنند و در نتیجه احتمال متناظر با عمل این گره u در اتوماتاهای یادگیر سریعتر افزایش می‌یابد و به سمت 1 میل می‌کند. هم‌چنین، نتایج این آزمایش نشان داد، تغییر در پارامتر R، تأثیر چندانی بر معیار احتمال تشخیص غلط الگوریتم پیشنهادی ندارد.

جدول (۲) تأثیر پارامتر R بر احتمال تشخیص و احتمال تشخیص غلط الگوریتم پیشنهادی

	R=5	R=10	R=15
احتمال تشخیص	70%	100%	100%
احتمال تشخیص غلط	1%	1.3%	1.2%

۷- نتیجه‌گیری

در این مقاله، یک الگوریتم جدید، هوشمند و سبک‌وزن به کمک اتوماتاهای یادگیر جهت شناسایی گره‌های کپی در شبکه‌های حسگر متحرک ارائه گردید. در الگوریتم پیشنهادی علاوه بر گره‌های حسگر معمولی، تعدادی گره نگهبان در شبکه وجود دارد که ترافیک شبکه را نظارت کرده و گره‌های کپی را شناسایی می‌کنند. اتوماتاهای یادگیر بر روی این گره‌های نگهبان سوار می‌شوند. از دلایل موثر بودن اتوماتاهای یادگیر می‌توان به هوشمندی، سبک‌وزن و غیر قطعی بودن اشاره کرد که مناسب شبکه‌های حسگر بی‌سیم است. الگوریتم پیشنهادی توسط شبیه‌ساز JSIM پیاده‌سازی گردید و نتایج آزمایش‌ها نشان داد، الگوریتم پیشنهادی قادر به شناسایی ۱۰۰٪ گره‌های کپی می‌باشد.

یکی از معایب الگوریتم پیشنهادی، سرعت کم در همگرایی اتوماتاهای یادگیر است (به خصوص هنگام زیاد شدن تعداد گره‌ها در

شبکه) به‌کارگیری اتوماتاهای یادگیر سلولی می‌تواند یک راه‌کار موثر جهت برطرف نمودن این مشکل باشد که در کار بعدی خود به آن می‌پردازیم.

مراجع

[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] Yick J., Mukherjee B. and Ghosal D., "***Wireless sensor network survey***", in: Proceedings of the Computer Networks 52, pp. 2292–2330, 2008.

[3] Walters J.P., Liang Z., Shi W. and Chaudhary V., "***Wireless Sensor Network Security: A Survey***", in: proceedings of the Distributed, Grid, and Pervasive Computing, Vol. 1, Issue 2, CRC Press, pp. 1-50, 2007.

[4] Goldsmith A.J. and Wicker S.B., "***Design challenges for energy-constrained ad hoc wireless networks***", in: Proceedings of the IEEE Wireless Commuications, pp. 8–27, August 2002.

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

[6] Padmavathi G. and shanmugapriya D., "***A survey of attacks, security mechanisms and Challenges in Wireless sensor networks***", in: Proceedings of the International Journal of Computer Science And Information Security (IJCSIS), Vol. 4, No. 1 & 2, August 2009.

[7] Parno B., Perrig A., and Gligor V. D., "***Distributed Detection of Node Replication Attacks in Sensor Networks***", in: Proceedings of the IEEE Symposium on Security and Privacy, 2005.

[8] Conti M., Pietro R. D., Mancini L. V., and Mei A., "***Distributed Detection of Clone Attacks in Wireless Sensor Networks***", in: Proceedings of the IEEE TRANSACTIONS ON DEPEDABLE AND SECURE COMPUTING, 2010.

[9] Choi H., Zhu S., and Porta T. F. La, "***SET: Detecting Node Clones in Sensor Networks***", in: Proceedings of the SecureComm '07, pp. 341–350, 2007.

[10] Zhu B., Addada V. G. K., Setia S., Jajodia S., and Roy S., "***Efficient Distributed Detection of Node Replication Attacks in Sensor Networks***", in: Proceedings of the Annual Computer Security Applications Conference (ACSAC), December 2007.

[11] Conti M., Pietro R. D., and Mancini L. V., "***A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks***", In: Proceedings of the ACM MobiHoc, September 2007.

[12] Zeng Y., Cao J., Zhang S., Guo S., and Xie L., "***Random-Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks***", In: Proceedings of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 28, NO. 5, JUNE 2010.

[13] Yu C.-M., Lu C.-S., Kuo S.-Y., "***CSI: Compressed Sensing-Based Clone Identification in Sensor Networks***", in: Proceedings of the 8th IEEE International Workshop on Sensor Networks and Systems for Pervasive Computing, 19 March 2012.

[14] C. KIM, SHIN S., PARK C. and et al.,"***A Resilient and Efficient Replication Attack Detection Schema for Wireless Sensor Network***", in: Proceedings of the IEICE TRANS. INF. & SYST., VOL. E92-D, NO. 7, JULY 2009.

[15] Bekara C. and Laurent-Maknavicius M., "***A new protocol for securing wireless sensor networks against nodes replication attacks***", in: Proceedings of the: Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications WIMOB '0, Washington, DC, USA, 2007.

[16] Yu C. M., Lu C. S., and Kuo S. Y., "***Mobile Sensor Network Resilient Against Node Replication Attacks***" In: Proceedings of the IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), June 2008.

[17] Ho J.-W., Wright M., and Das S., "***Fast detection of replica node attacks in mobile sensor networks using sequential analysis***", In: Proceedings of the IEEE INFOCOM, pp. 1773 – 1781, 2009.

[18] Ho J.-W., Wright M., and Das S., "***Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks Using Sequential Hypothesis Testing***", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 6, JUNE 2011.

[19] Yu C.-M., Lu C.-S., and Kuo S.-Y., "***Efficient and Distributed Detection of Node Replication Attacks in Mobile Sensor Networks***" , In: Proceedings of the IEEE Vehicular Technology Conf. Fall (VTC Fall), Sept. 2009.

[20] Gowtham B., Sharmila S., "***Location Traced Hybrid Detection of Node Replication Attack in Mobile Wireless Sensor Network***", In: Proceedings of the Special Issue of International Journal of Computer Applications (0975 – 8887) on Information Processing and Remote Computing – IPRC, August 2012.

[21] Deng XM, Xiong Y., "***A new protocol for the detection of node replication attacks in mobile wireless sensor networks***", In: Proceedings of the Journal of Computer Science and Technology 26(4),pp. 732-743, July 2011.

[22] Yxainaxniga Y. and et al," ***Single Hop Detection of Node Clone Attacks in Mobile Wireless Sensor Networks***", In: Proceedings of the International Workshop on Information and Electronics Engineering (IWIEE), Vol.29, pp. 2798–2803, 2012.

[23] Deng X., Xiong Y., and Chen D., "***Mobility-assisted Detection of the Replication Attacks in Mobile Wireless Sensor Networks***", In: Proceedings of the 6th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2010

[24] Wang L.-M. et al," ***Patrol Detection for Replica Attacks on Wireless Sensor Networks***", Sensors 2011, 11, 2496-2504; doi:10.3390/s110302496

[25] Xing K. an Cheng X., "***From Time Domain to Space Domain: Detecting Replica Attacks in Mobile Ad Hoc Networks***", In: Proceedings of the IEEE INFOCOM, 2010.

[26] Unnikrishnan D. and et al.,"***Detecting Mobile Replica Node Attacks in Wireless Sensor Networks Using Sequential Probability Ratio Test***", in: Proceedings of the 13th International Conference on Distributed Computing and Networking (ICDCN), Hong Kong, China, January 3-6, 2012.

[27] Lakabhasanee S., Ramesh S.,"***Fast and Efficient Distributed Detection of Mobile Node Replica Attacks in Wireless Sensor Network Test***", in: Proceedings of the Journal of Computer Applications ISSN: 0974 – 1925, Volume-5, Issue EICA2012-5, February 10, 2012.

[28] Zhu W. T., Zhou J., Robert H. Bao D. F., "***Detecting node replication attacks in mobile sensor networks: theory and approaches***", in: Proceedings of the Security and Communication Networks Volume 5, Issue 5, pages 496–507, May 2012.

[29] Conti M., Pietro R. D. and Spognardi A., "***Wireless Sensor Replica Detection in Mobile Environments***", in: Proceedings of the ICDCN, pp. 249-264, 2012.

[30] Piro C., Shields C. and Levine B. N. , "***Detecting the Sybil Attack in Mobile Ad hoc Networks***", in: Proceedings of the *Securecomm and Workshops*, pp 1-11, 2006.

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

[32] 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.

[33] 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.

زیرنویس‌ها

[۱] node replication attack

[۲] Replica node

[۳] keying materials

[۴] Observer Nodes

[۵] P-Model

[۶] Sensor Nodes

[۷] Watchdog Nodes

[۸] Omni-directional

[۹] Keep alive message