ششمین همایش بین‌المللی افق های نویـن در
مهندسی برق، کامپیوتـر و مکانیک
6th International Conference on the New Horizons in
Electrical Engineering, Computer and Mechanical
www.mhconf.ir

شناسایی و کاهش حملات متقاطع لایه ای مبتنی بر عامل موبایل امن در شبکه بی سیم

محمدجوادحسین پور[۱،*]، صابرصادقی[۲]،مژگان زارعی[۳]، سعیده زردشت[۴]

[۱،*]عضو هیئت علمی و استادیار بخش مهندسی کامپیوتر،دانشگاه آزاد اسلامی واحد استهبان،استهبان،ایران

Email: mj.hosseinpoor@iau.ac.ir

[۲]دانشجوی کارشناسی ارشد مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد استهبان،استهبان،ایران

Email: ssabersadeghii@yahoo.com

[۳] دانشجوی کارشناسی ارشد مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد استهبان،استهبان،ایران

Email: mojhizare@gmail.com

[۴] دانشجوی کارشناسی ارشد مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد استهبان،استهبان،ایران

Email: saeedeh_z60@yahoo.com

چکیده

تهدیدات در شبکه های بی سیم این روزها رایج است و وقتی صحبت از تهدیدات امنیتی می شود عواقب آنها بی شمار است. برخی از رایج ترین تهدیدات امنیتی که شاهد آن هستیم، دستکاری مسیر و پارازیت است. تحقیقات متعددی برای افزایش کارایی این حملات در برابر تقلبی آنها پیشنهاد شده است. تهدیدی که اخیراً پیشنهاد شده و چالش برانگیزترین تهدید است، حمله چند لایه است. اگرچه راه‌حل‌هایی برای حملات تک لایه داریم، اما روش‌های رضایت‌بخش بسیار کمی برای شناسایی و ضدحمله حملات چندلایه وجود دارد. با این به عنوان هدف اصلی برای این مقاله، ما یک چارچوب جدید پیشنهاد کردیم که شبکه بی‌سیم را از حملات متقاطع ایمن می‌کند. این پیشنهاد بر شناسایی و کاهش حمله متمرکز است. اولی مبتنی بر طرح تشخیص یادگیری بیزی است و دومی برای افزایش امنیت و عملکرد شبکه ساخته شده است. پروتکل تشکیل شده بر روی یک چارچوب با حمله لایه ای که از پارازیت استفاده می کند، آزمایش می شود.

کلید واژه ها : شبکه های حسگر بی سیم سیستم تشخیص نفوذ . معماری لایه های متقاطع امنیت WSN

۱. مقدمه

یک سیستم مجموعه ای از وسایل مرتبط با یکدیگر است. در حساب سیستم های شبکه، مکاتبات رادیویی معمولاً وسیله تصمیم گیری است. به هر حال، حتی در داخل زیرمجموعه کنترل‌شده رادیویی، پیشرفت‌های متنوع زیادی برای استفاده در مقیاس‌ها، توپولوژی‌های مختلف و موارد استفاده فوق‌العاده وجود دارد. سیستم‌های شبکه ناهمگن صعود به یک شرایط دسترسی چند رادیویی را ارائه می‌کنند که برای تنظیم بار برای دور نگه داشتن از انسداد سیستم و ارائه مدیریت‌های باورنکردنی برای افزایش استفاده از دارایی رادیویی حیاتی است[۱]. برای این منظور، یک بخش مشترک توان و ظرفیت انتقال داده با محاسبه تقویت QoS با استفاده از تکنیک تقویت قوسی در این روش پیشنهاد شده است.Bolding کانال[1] یک روش نشان داده شده برای افزایش ظرفیت انتقال داده و کاهش تاخیر در سیستم های شبکه است. در سیستم‌های شبکه مرسوم، به عنوان مثال، سیستم‌های سلولی و همسایگی شبکه در کنار سیستم‌های رادیویی ذهنی در حال توسعه ، متصل شده است[۲].CB سیستمی است برای پیوستن به ترتیبی از مستقیم شبکه های غیر پوششی مجاور با هدف نهایی ایجاد یک کانال واحد با ظرفیت انتقال داده بالاتر، و زمانی که دیگر مورد نیاز نیست، می توان این پیوند را برای آزاد کردن کانال های باند محدود تشکیل دهنده تقسیم کرد. CB در مجموع ظرفیت انتقال بیشتری را برای تبادل اطلاعات نسبت به آنچه که از طریق کانال های جداگانه قابل دسترسی است ارائه می دهد. [۳]

یک شبکه Ad-Hoc موبایل[2] مجموعه ای از هاب های قابل حمل (ایستگاه) است که در یک مسیر پرش چندگانه بدون چارچوب ثابت، به عنوان مثال، گذرگاه ها یا ایستگاه های پایه، انتقال می یابد.MANET مؤلفه حفاظتی مشخصی ندارد، بنابراین حملات مخرب بدون شک می توانند به این نوع سیستم برسند.

۲. پژوهش های مرتبط

وقفه در سیستم شبکه، امنیت چارچوب را به خطر می اندازد. جهت‌های هاب‌های متحرک و دروازه‌شکن‌های متحرک به طور کامل مورد بررسی قرار نگرفته‌اند، جایی که اثر بین دو هاب متحرک به هم پیوسته و بین یک حسگر متحرک و یک متحرک متحرک هنوز مشخص نشده است[۶].

پنگ ژائو و همکاران، مکاتبات را در سیستم‌های چند هاپ شبکه گردشی مشخص می‌کنند، محاسبه OR گنجانده شده در زیربخش فوق برنامه‌ریزی شده است تا به روشی انتقال یافته کار کند[۷]. برای شروع، برای هر هاب ni، احتمالات انتقال اتصال برای همه همسایگان به طور متناوب تخمین زده می شود.

Daisuke Mashima و همکاران، ترتیبات امنیتی مختلف را روشن می کند [۸] ، به عنوان مثال، دیوار آتش مدرن، در برابر برنامه نویسی عفونت، چارچوب های تأیید و کنترل دسترسی، برای اطمینان از چارچوب های شبکه هوشمند پیشنهاد شده است. در هر صورت، هنوز قابل تصور است که چارچوب تمرکز کنترل بدخیم شود.

استفاده حیاتی از IoT، ارائه انواع اطلاعات متعدد در میان حسگرها، اگرچه چنین سیستمی در برابر انواع گسترده حملات، به ویژه حملات خودی، به دلیل زیستگاه منظم و انتقال مشکل ساز طبیعی آن درمانده است[۹]. برای محافظت از امنیت، چارچوب‌های مکان وقفه (IDS)به

[1] CB
[2] MANET

طور گسترده در یک WSN برای محافظت در برابر حملات خودی از طریق اجرای ابزارهای مبتنی بر اعتماد مناسب دریافت می‌شوند. با این وجود، در دوره اطلاعات بسیار زیاد، حسگرها ممکن است اطلاعات و اطلاعات بالایی ایجاد کنند که می تواند کفایت محاسبه اعتماد را مختل کند. در اینجا، ما حول این آزمایش متمرکز می‌شویم و روشی را برای ادغام مدیریت اعتماد مبتنی بر بیزی با بازرسی حرکت برای کشف وقفه شبکه تحت یک ساختار پیشرو پیشنهاد می‌کنیم.

حملات پارگی، هر چند ممکن است، در میان مکاتبات شبکه از حسگرها به برآوردگرهای شبکه در لایه دیجیتال در نظر گرفته شوند[۱۰]. برخلاف بررسی‌های تئوری داده‌ها در مورد مکاتبات امن، که اساساً شامل اطمینان از اطلاعات و مدیریت فناوری اطلاعات است، ما بر روی تحقیق در مورد اجرای برآورد مناسب تحت حملات از دیدگاه نظری چارچوب تمرکز خواهیم کرد. یک دشمن انتقام جو در همان زمان یک حمله تزریق اطلاعات نادرست به لایه چارچوب فیزیکی ارسال می کند تا عمداً وضعیت چارچوب را تغییر دهد و حمله چسبنده لایه دیجیتال را برای جلوگیری از کانال های انتقال شبکه در بین حسگرها و برآوردگرهای شبکه ارسال می کند.

در مورد توطئه قاب بندی و چسبندگی ستون توافقی جدید مشترک(JCBJ) برای افزایش امنیت لایه فیزیکی سیستم های شبکه تفسیر و ارسال می شود که در آن هاب منبع با راهنمای هاب های انتقالی مختلف در دید یک شبکه به هدف خود منتقل می کند [۱۱]. هدف این کار شامل موارد منفی است که به طور کلی با هم در نظر گرفته می‌شوند تا یک راه‌حل بهینه‌سازی پیشنهاد شود که تمام الزامات را برآورده کند. از این رو به جای حمله به ویژگی های ضعیف به صورت جداگانه، به لایه های مختلف شبکه حمله می کند. حتی یک تغییر کوچک در این لایه ها می تواند منجر به آسیب جدی به شبکه شود. باز هم پلتفرم های طراحی شده نرم افزاری، دستکاری کدها و حمله به شبکه را برای مهاجمان آسان تر می کند. از این رو تمام حملات ممکن در سطح لایه مانند سیاه چاله، ربودن، حمله بالماسکه، کرم چاله، حمله انکار، حمله مرد در وسط، DDOS و پارازیت باید در نظر گرفته شود. به منظور افزایش تشخیص حمله در لایه MAC، فیزیکی، شبکه و برنامه ما الگوریتم بیزی[1] را پیشنهاد می کنیم. این طرح تشخیص همراه با الگوریتم کاهش ادغام می شود تا به عنوان یک اقدام متقابل برای این حملات چندلایه عمل کند.

۳. تشخیص لایه CROSS برای حمله لایه فیزیکی و لایه مک

در این مقاله روشی برای شناسایی یا شناسایی حملات لایه فیزیکی مانند حملات مسمومیت لایه WNAC و پارازیت ارائه می‌کنیم [۱۲]. الگوریتم تشخیص بیزی با استفاده از توزیع پسینی[2] برای تشخیص این حملات لایه فیزیکی پیشنهاد شده است. در محیطی که حملات چندلایه وجود دارد،در ابتدا این روش اجرا می شود.این روش تمام فعالیت های مخربی را که در شبکه اتفاق می افتد مشاهده و ثبت می کند و بعداً آن را با حملات احتمالی که قبلاً با استفاده از برخی ویژگی ها ثبت شده اند مقایسه می کند. این حملات مخرب تنها زمانی درست اعلام می شوند که باعث ایجاد تغییراتی در فعالیت های شبکه شوند. اما در سناریوی واقعی، این تغییرات فعالیت های شبکه ناچیز است، زیرا آنها کمی با فعالیت های اصلی تفاوت دارند. بنابراین پیشنهاد روشی که از این تغییرات کوچک در فعالیت‌ها غافل نشود و این سناریوها را برای تشخیص حمله در نظر بگیرد، حائز اهمیت است.از این رو در این مورد از الگوریتم یادگیری بیزی استفاده شده است که این تغییرات

[1] Bayesian algorithm
[2] posteriori distribution

کوچک ناشناخته را به عنوان هر متغیر تصادفی در نظر می گیرد. تمام این تغییرات جزئی فعال ثبت می شود و نام متغیری که توزیع واقعی متغیر از آن ساخته می شود، داده می شود. اجازه دهید "W" را یک متغیر تصادفی با توزیع ناشناخته در نظر بگیریم. این W تحت تأثیر متغیرهای محیطی[1] قرار می گیرد اما به طور کلی به عنوان یک ثابت فرض می شود و این متغیرهای محیطی تأثیری بر W ندارند. تمام اتفاقات احتمالی مانند موفقیت یا عدم موفقیت در ارسال و دریافت بسته ها، اختلاف کانال، تاخیر در تحویل پیام و غیره. این رویدادها توزیع متغیر W را تشکیل دهد. فعا
در ارسال و دریافت بسته ها، اختلاف کانال، تاخیر در تحویل پیام و غیره. این رویدادها Qk نامیده می شوند. این فعالیت های ذخیره شده همچنین اطلاعاتی در مورد کیفیت مسیر، SINR یک پیوند، احتمال دسترسی به کانال و غیره می دهد. با توجه به احتمال Qk = qk فقط زمانی اتفاق می افتد که W= w

$$P\{Qk = qk|W = w\} = f(qk; w) \qquad (1)$$

تابع f(qk, w) در معادله (۱) از نظر تئوری با احتمال خطای بیت برای SINR معین قاب بندی شده است. A- توزیع پسینی به شرح زیر است:

$$P\{W = w|\{Qk\} = \{qk\}\} = \frac{P\{\{Qk\} = \{qk\}|W = w\}}{\int_v P\{\{Qk\} = \{qk\}|W = w\}.P\{W = w\}dw}.Pw, \qquad (2)$$

در اینجا PfW = wg توزیع پیشینی W است و وضعیت ایده آل شبکه را در غیاب هرگونه حمله نشان می دهد. این مقدار با استفاده از مدل محو برای استخراج توزیع SINR در یک پیوند در دسترس است. احتمال دسترسی به کانال برای هر گرهی در شبکه ای که CSWNA/CA را اجرا می کند تقریبا یکسان است.

اگرچه مقادیر واقعی مشخص نیست، اما همیشه اطلاعاتی در مورد آن در دسترس است. با کمک توزیع پسینیA داده شده در معادله (۲) مدافع در مورد فعالیت های مخرب آگاه خواهد شد. ما هنوز باید هدف ck را تخمین بزنیم تا بتوانیم حملات احتمالی را که می تواند به لایه های دیگر جدا از فعالیت های حمله انجام دهد، شناسایی کنیم. طبقه‌بندی پیاده‌سازی شده است که هم توزیع پسینی و هم ویژگی‌های حملات را به عنوان ورودی در نظر می‌گیرد. ویژگی ها با متغیر B نشان داده می شوند که دانش پیشینی را تحت یک حمله احتمالی نشان می دهد و طبقه بندی کننده به صورت زیر است:

$$C(P\{W|\{Qk\} = \{qk\}\}, B) \underset{Not\ Attacked}{\overset{Attacked}{\lessgtr}} C_{th}, \qquad (3)$$

در اینجا آستانه ای که باید بر اساس تأثیر ناشی از حمله
مشکوک در یک شبکه تنظیم شود. C_{th} موتور کاهش حمله است که در طول شناسایی حمله اجرا می شود که در معادله (۳) نشان داده شده است. استراتژی حمله می تواند به طور مستقیم بر عملکرد شبکه تأثیر بگذارد و از این رو عامل خطر را افزایش دهد.

[1] environmental variables

$$h(S_k,A_k)=\alpha.E[U(W_k)]-\beta.E[G(W_k)]=\alpha.E[U(g(S_k,A_k))]-\beta.E[G(g(S_k,A_k))], \quad (4)$$

بنابراین موتور کاهش باید در مورد استراتژی S_k به منظور بهینه سازی تبادل عملکرد امنیتی تصمیم بگیرد. بنابراین یک تابع عملکرد امنیتی در معادله تعریف شده است. مثل (۴):

$$\begin{matrix} maximize & h(S_k,A_k) \\ S_k & E[U(W_k)]\le U_{th} \\ Subject & to\, E[G(W_k)]\le G_{th}, \end{matrix} \quad (5)$$

در اینجا E[.]مخفف انتظار یک متغیر تصادفی است.

سودمندی مورد انتظار از عملکرد به عنوان E[U(Wk)] داده شده است و و سودمندی مورد انتظار حمله منفی به عنوان E[G(Wk)]–داده شده است برای امنیت. استراتژی بهینه انتخاب شده توسط موتور کاهش با حل معادله زیر (۵) به دست می آید:

α و β که دو متغیر کنترل هستند، برای به دست آوردن نقطه مبادله مطلوب بین امنیت و عملکرد تنظیم می شوند. مقادیر α و β تنها بر اساس برنامه ای که در سناریو در نظر گرفته می شود متفاوت است. در مورد برنامه های پخش ویدئو، این مقادیر برای عملکرد بالا و برای امنیت پایین در نظر گرفته می شوند. در حالی که در سناریوی حسگر بی سیم نیاز به سطح امنیتی بالایی دارد و می تواند سرعت داده پایین را به خطر بیاندازد.

۳،۱. شبه کد

1. Start the program
2. Input a-priori distribution AP {Ifm1= i} with the node mc 2 Ne

3. While do
4. If(anyone node ma 2 Ne receiver node) && (channel contest) TRUE then
5. If (Channel estimation condition in term nc & mc b) && (Hfncmc; ψe f ϵ Fc) TRUE;
6. for with Hfncmc,nc tends to decides and transmits; end
7. else if (mc selects a Fc'= { fcc Fc : Prfn!=0})
8. do fcϵ Fc' while
9. {Calculate the likelihood in eq(15) suitable for bit reception events;
10. equate with the a-posteriori probability in (17);}
11. while STEP 5 the loop until
12. A-posteriori distribution satisfies convergence condition;
13. The equation (18) holds based on certain number of fc ϵ Fc
14. Process continue until node mc is considered jammed; end
15.else Node mc is considered not jammed;
16. END the for loop
17. END the while loop
18. END

این روش در مورد روش‌های شکل‌دهی خودکار بدنه و محاسبه تنظیم خودکار برای ردیابی پارازیت بزرگ و تضعیف پرچم آن، توضیح می‌دهد [۱۱]. شبه کد در مورد یک مسدود کننده دلخواه بسته های معمولی یا یک پرچم رادیویی ثابت را به صورت بی رویه ارسال می کند. مهاجم با تبادل تصادفی بین حالت استراحت و چسبیدن خود، از نشاط خود صرفه جویی می کند. این سیستم نسبت به انواع هجوم بی وقفه در یک بازه زمانی معین خلوت کمتری خواهد داشت. در هر صورت، سیستم با تخمین کیفیت پرچم و همچنین زمان تشخیص حامل و نسبت انتقال بسته، حمله را در زمان طولانی‌تری شناسایی می‌کند [۱۲].

چسباندن لایه اتصال که از معناشناسی لایه MAC استفاده می کند، نوع درهم آمیزی از حملات چسبندگی گیرنده است. یک پارازیت لایه اتصال نه تنها بین حالت استراحت و پویا سوئیچ می‌کند، بلکه فعالیت‌های خود را به دستورالعمل‌های لایه MAC اعضا در مکاتبات تغییر می‌دهد. در امتداد این خطوط، پارازیت از سرزندگی کل خود به روشی موثر استفاده می کند. همانطور که توسط سیستم نشان داده شده است، زمان شناسایی برای این نوع حمله تقریباً برابر با چسبیدن رادیویی پاسخگو به تاخیر می افتد. پارامترهایی مانند fc، Fc و f اولویتی هستند که از پارامترهای یادگیری بیزی گرفته شده است.

۴. شناسایی لایه برنامه و لایه شبکه

هدف از ارائه این مقاله طراحی یک سیستم تشخیص است که به طور خاص برای شبکه و لایه کاربردی شبکه اعمال می شود. ایده پشت این پیشنهاد استفاده از تشخیص ناهنجاری و سوء استفاده به منظور شناسایی و تجزیه و تحلیل گره های مخرب در شبکه مانند حملات کرم، حملات ویروس و غیره است. برخی از حملات دیگری که در این تحقیق در نظر گرفته شده اند عبارتند از DoS-Denial of Service، جعل، حمله به خطر افتاده، حمله Sybil و غیره. سروری مانند Wireless Node Agent به نام WNA در این روش معرفی شده است که همراه با هر گره برای تشخیص نفوذ ایجاد شده در شبکه کار می کند. سرور WNA عمدتاً مسئول ارسال و مدیریت WNA ها است.ADS موجود در هر گره در این روش برای شناسایی گره های مخرب استفاده می شود [۱۳]. تشخیص سوء استفاده به عنوان تشخیص نفوذ مبتنی بر میزبان در نظر گرفته می شود که برای همه گره های موجود در شبکه شناخته شده است. اکنون هنگامی که WNA ها به شبکه ارسال می شوند، می توانند امضاهای حمله جدیدی را نیز اضافه کنند، در صورتی که نفوذی شناسایی شود و توسط WNA های تجزیه و تحلیل تایید شود. اکنون امضای حمله جدید به سرور WNA ارسال می‌شود و از WNAهای دوره‌ای می‌خواهد تا آن را به تمام گره‌های موجود در شبکه ارسال کنند. برای پیاده سازی تشخیص ناهنجاری در ADS، ابتدا یک نمایه منظم برای هر برنامه کاربردی با کمک داده های ممیزی که در سرور WNA موجود است ایجاد می شود.

این داده های ممیزی از فعالیت های سطح برنامه و فراخوانی های سیستمی هستند که از طریق برنامه های کاربردی فراخوانی می شوند. این فراخوانی های سیستمی برای محاسبه پروفایل های معمولی استفاده می شود. در ابتدا گره هایی با پروفایل های معمولی در شبکه مستقر می شوند. هنگامی که یک برنامه معمولی جدید به دلیل وصله برنامه یا راه اندازی برنامه جدید تشکیل می شود، WNA ها مسئول حمل این به روز رسانی به تمام گره های موجود در شبکه هستند. عامل نظارت و تشخیص اکنون نمایه جدید را با نمایه معمولی با استفاده از فاصله همینگ مقایسه می کند. اگر هر گونه انحرافی ثبت شود، به ADS محلی در مورد آن هشدار می دهد. اگر ناهنجاری تشخیص داده شود، WNA ها از سرور WNA درخواست می کنند تا WNA های تحلیلی را به آن مکان ارسال کند. اگر WNA ها وجود حمله ناهنجاری را تایید کنند، عمل پاسخ اجرا می شود و امضای حمله جدید برای حمله شناسایی شده تولید می شود. هر گره همچنین دارای رکوردی از فعالیت های مرتبط با ADS است که شامل تشخیص ناهنجاری و سوء استفاده است. جدا از WNAهای تشخیص نفوذ، داده های ممیزی و گزارش های ADS را نیز تجزیه و تحلیل کرده و سپس گزارش را برای بررسی بیشتر به سرور WNA ارسال می کند.

۴،۱. سرور WNA سه نوع WNA را ایجاد و ارسال می کند

- WNA[1] های بروزرسانی
- WNA[2]های آنالیز
- WNA[3] های تأیید

[1] UPDATE WNAs
[2] ANALYSIS WNAs
[3] VERIFICATION WNAs

۴،۱،۱. WNA های بروزرسانی

WNA های بروزرسانی مسئول اضافه کردن امضاهای حمله جدید، به روز رسانی پروفایل های معمولی، وصله و نصب برنامه ها و برنامه های کاربردی جدید به تمام گره های موجود در شبکه هستند.

هنگامی که سرور WNA یک امضای حمله جدید دریافت می کند، لازم است که تمام گره های موجود در شبکه آگاه باشند و با این امضای جدید به روز شوند. سرور HenceWNA WNA های به روز رسانی را برای انجام این فعالیت مستقر می کند تا تمام گره ها از تغییرات جدید آگاه شوند. در این سناریو از WNA به روز رسانی مجدد برای به روز رسانی تمام گره ها استفاده می شود.WNA های به روز رسانی نه بر اساس درخواست گره ها، بلکه در صورت نیاز سرور WNA مستقر می شوند. از آنجایی که WNA های به روز رسانی به تمام گره های موجود در شبکه ارسال می شوند، سرور WNA نیازی به ارسال مجدد همان به روز رسانی ها به شبکه ندارد. از این رو از گلوگاه ارتباطی سرور WNA جلوگیری می کند و ترافیک و بار شبکه را کاهش می دهد.

۴،۱،۲. WNA های آنالیز

WNAهای تحلیلی مسئول تجزیه و تحلیل بیشتر رفتار ناهنجاری هستند که توسط گره ها شناسایی می شود. هنگامی که ADS محلی موجود در گره یک ناهنجاری را تشخیص می دهد، ابتدا با امضاهای حمله موجود در پایگاه داده مقایسه می شود. اگر مطابقت نداشته باشد، گزارش ناهنجاری را به سرور WNA ارسال می کند و درخواست استقرار WNA های تحلیلی را می دهد. گزارش ناهنجاری شامل اطلاعات مربوط به گزارش های ADS، مکان ناهنجاری و غیره است. بر اساس این اطلاعات، WNAهای تحلیل مناسب توسط سرور WNA انتخاب شده و به مکان خاص ارسال می شود. تجزیه و تحلیل WNA ها می توانند تحقیقات بهتری نسبت به ADS محلی انجام دهند و در مورد نفوذ ایجاد شده تصمیم گیری کنند. اگر analysisWNAs نفوذ ناهنجاری را نادرست اعلام کند، گزارش را به سرور WNA ارسال می کند و خود را از بین می برد. از طرف دیگر اگر نفوذ درست باشد، WNAها پاسخ نفوذ را با کمک عامل پاسخ موجود در ADS محلی آغاز می کنند. در نهایت یک امضای جدید برای نفوذ شناسایی شده ایجاد می شود و سپس گزارش تشخیص به سرور WNA ارسال می شود و پس از اتمام کار آن WNA های آنالیز خود را از بین می برند. در صورتی که WNA های تجزیه و تحلیل قادر به نتیجه گیری در مورد نفوذ نباشند، یا از سرور WNA درخواست می کند تا WNA های تجزیه و تحلیل مناسب دیگری را بر اساس گزارش تشخیص ارسال شده به سرور ارسال کند یا به گره های همسایه مهاجرت می کند تا بررسی های مربوط به نفوذ را انجام دهد. این بررسی که در گره های همسایه انجام می شود، تشخیص ناهنجاری مبتنی بر شبکه چند نقطه ای[1] نامیده می شود.

۴،۱،۳.WNA های تاییدیه

[1] multi-point

WNAهای تأیید مسئولیت تأیید ADS محلی موجود در هر گره را بر عهده دارند، گزارش های ADS را بررسی کرده و بررسی می کنند که آیا این عوامل ADS در معرض خطر هستند یا خیر. تابع هش تصادفی[1] برای تأیید عوامل محلی ADS استفاده می شود. سرور WNA مسئول ارسال این WNAهای تأیید به صورت دوره ای برای بررسی یکپارچگی عوامل ADS با سرور WNA است.WNA های تأیید از کلید هش برای محاسبه هش روی عامل ADS استفاده می کنند و مقدار را به سرور WNA می فرستند تا تأیید شود.WNA های راستی‌آزمایی همچنین فعالیت غیرعادی یا رویدادهای ناهنجاری را در گزارش‌های ADS بررسی می‌کنند. اگر گره در تست تایید شکست بخورد، WNA های تایید از سرور WNA برای به روز رسانی WNA ها درخواست می کنند یا کل گره را از شبکه خاموش می کند.

۴,۲.احراز هویت و مجوز WNA

به منظور احراز هویت و مجوز نودها و WNA های موجود در شبکه، مفهوم زیرساخت کلید عمومی (PKI) در حال پیاده سازی است. این فرض وجود دارد که یک مرجع گواهی آفلاین قابل اعتماد ((CAوجود دارد که مسئول صدور گواهی برای گره ها و سرور WNA در شبکه است. این گواهینامه ها دارای یک کلید عمومی و شناسه گره مالک هستند.CA همچنین یک کلید خصوصی و عمومی به هر گره می دهد. WNA هایی که توسط سرور WNA مستقر می شوند حاوی اطلاعاتی در مورد گواهی های ارائه شده توسط CA هستند و WNA ها را با کلید خصوصی آن امضا می کنند. هنگامی که WNA ها می خواهند اطلاعات را به سرور WNA برگردانند، یک تابع رمزگذاری اجرا می شود، گزارش را امضا می کند و به سرور WNA می فرستد [۱۴].WNA برنامه رمزگذاری را در تمام گره های شبکه برای امضای دیجیتال توزیع می کند. هنگامی که سرور WNA گزارش تشخیص را دریافت می کند، امضا را برای تأیید صحت گزارش بررسی می کند.

۴,۳. اعزام WNA

سرور WNA سه نوع WNA را ارسال می کند: تجزیه و تحلیل WNA ها، به روز رسانی WNA ها و WNA های تایید.WNA های به روز رسانی فقط در صورت درخواست ارسال می شوند، WNA های تأیید به صورت دوره ای ارسال می شوند و WNA های تجزیه و تحلیل مجدداً در صورت درخواست یا درخواست دریافت شده از گره های شبکه ارسال می شوند. سرور WNA مسئول این WNAها است و تعداد WNAهایی که باید ارسال شوند و زمان گزارش آنها را کنترل می کند. فاصله زمانی ارسال WNAهای تایید به شبکه توسط سرور WNA تعیین می شود. با در نظر گرفتن اندازه شبکه، شرایط شبکه و منطقه تصمیم گیری می شود. این WNAهای تأیید در واقع ADSهای محلی موجود در هر گره موجود در شبکه را تأیید می کنند.یک کلید متقارن در سطح شبکه و PKI در این روش برای حفظ اصالت و محرمانه بودن شبکه پیاده سازی می شوند. این WNAهایی که در شبکه ارسال می شوند، دو نوع گزارش را به سرور WNA تحویل می دهند. گزارش دوره ای و گزارش تشخیص. مورد اول برای جمع آوری داده ها و تحمل خطا و دومی برای شناسایی و گزارش حمله شناسایی شده موجود در شبکه استفاده می شود. اگر سرور WNA هیچ گزارشی از WNAهای ارسال شده دریافت نکرد، WNAهای بیشتری به شبکه ارسال می شوند. گزارش دوره ای شامل اطلاعات مربوط به باتری، نتایج به روز شده/تأیید، اطلاعات ADS و غیره است. گزارش تشخیص شامل اطلاعات

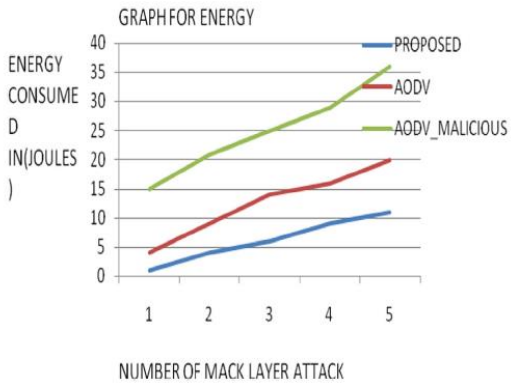
[1] Randomized Hash Function

گره مخرب، گزارش‌های مفید ADS و محل فعالیت مخرب شناسایی‌شده است و از سرور WNA درخواست می‌کند تا WNAهای تحلیلی را برای بررسی بیشتر ارسال کند. هر یک از WNA شامل یک TTL به نام پارامتر timeto-live است که در آن تعبیه شده است. اگر TTL منقضی شود، آن WNA خاص از بین می رود یا از شبکه حذف می شود.

۴،۳،۱. پروتکل WNA-dispatching به شرح زیر خلاصه می شود:

۱)WNAS هایی که توسط سرور WNA به یک شبکه خاص ارسال می شوند حاوی گواهی CertS و رمزگذاری WNAS با کلید متقارن K و با یک کلید خصوصی kS که برای احراز هویت استفاده می شود، خواهد بود. ۲)در صورتی که WNAS یک WNA به روز رسانی باشد، S امضاهای حمله جدید را خواهد داشت. این S همچنین حاوی وصله های برنامه یا هر برنامه جدیدی در صورت به روز رسانی برنامه است که باید به گره ها ارسال شود.۳) در صورتی که این WNAS یک WNA به‌روزرسانی یا یک WNA تأیید باشد، در این سناریوها S WNAS را در مکان تصادفی در شبکه ارسال می‌کند. اگر این WNAS یک WNA تحلیلی باشد، به گره درخواست کننده تخصیص داده می شود.۴) هر یک از WNA دارای یک پارامتر TTL است که مسئول تصمیم گیری در مورد تعداد گره هایی است که WNA می تواند بازدید کند.۵) هر یک از WNA حاوی یک پارامتر TTL است که مسئول ارسال گزارش های دوره ای و گزارش های تشخیص به S است.۶) اگر گواهی TTL یک WNA خاص منقضی شود، WNA خود را از شبکه نابود می کند.

هنگامی که WNA یک گره را تأیید کرد، پس از به‌روزرسانی با گزارش فعلی، به گره بعدی در شبکه منتقل می‌شود. اکنون WNA تجزیه و تحلیل تصمیم خواهد گرفت که آیا به گره بعدی سوئیچ کند یا خود را از شبکه حذف کند. این امکان برای سرور WNA وجود دارد که چندین WNA را در شبکه ارسال کند. در چنین سناریویی، WNAها زمان کمتری برای تجزیه و تحلیل سریع شبکه کامل خواهند داشت. اما در عین حال این امکان نیز وجود دارد که همان گره بتواند توسط چندین WNA بازدید شود و باعث ایجاد سربار در ارتباط بین سرور WNA و گره ها شود. از این رو شناسایی مقدار بهینه برای تصمیم گیری در مورد تعداد WNAهایی که باید ارسال شوند مهم است. (شکل ۱).



شکل۱. نمودار انرژی برای حمله لایه MAC

WNA ها از رویه پرش چندگانه برای سفر از یک گره به گره دیگر، برای ارسال به روز رسانی های منظم و گزارش های تشخیص به سرور WNA استفاده می کند. در طول فرآیند ارسال، گره ها می توانند دادن پیام وجود دارد که توسط گره های همسایه ایجاد می شود. از این رو مسیریابی ایمن برای مدیریت این توزیع به‌روزرسانی منظم و ارسال گزارش‌های تشخیص به سرور WNA پیاده‌سازی می‌شود.

در صورتی که WNA ها توسط گره های مخرب دستگیر شوند، این به روز رسانی های معمولی توسط گره ها دریافت نمی شوند. در طول چنین سناریوهایی، گره ها WNA را برای مدت طولانی تری دریافت نمی کنند، سپس درخواستی به WNA ارسال می شود و درخواست به روز رسانی می کند. در صورتی که گزارش‌های دوره‌ای گم شوند یا ضبط شوند، سرور WNA گزارش‌های دوره‌ای را از WNA دریافت نمی‌کند و از وضعیت WNA و نتایج به‌روزرسانی/تأیید از اطلاعات گزارش‌شده مطلع نخواهد شد. هنگامی که WNA هیچ اطلاعاتی از یک WNA دریافت نکرده است، به دنبال آخرین به روز رسانی دریافت شده می گردد و سپس آن WNA را به عنوان مشکوک علامت گذاری می کند. اکنون سرور WNA یک پیام پرس و جو به این گره مشکوک می فرستد و گزارش های منظم دریافت شده از سرور WNA را درخواست می کند.

اگر WNA هنوز گزارشی دریافت نکرد، WNAهای تحلیلی برای بررسی گره مشکوک ارسال می شوند. اگر حتی این تحلیل WNA هم نتواند گزارش های تشخیص را ارسال کند، WNA های تحلیلی بیشتری برای انجام وظیفه بررسی ارسال می شوند. نفوذ در یک شبکه بی سیم با استفاده از تشخیص سوء استفاده یا با تشخیص ناهنجاری شناسایی می شود. عامل پاسخ موجود در ADS گره در مورد شناسایی اعلامیه می کند. پاسخی که ارائه می شود به عوامل مختلفی مانند نوع نفوذ، میزان آسیب ایجاد شده و نوع برنامه مخرب بستگی دارد. هنگامی که به وجود یک ناهنجاری مشکوک شد، عامل پاسخ از WNA درخواست می کند تا WNA تجزیه و تحلیل را برای افزایش تحقیقات ارسال کند. اگر آسیب توسط عامل پاسخ قابل درمان باشد، سعی می کند گره را دوباره برنامه ریزی کرده و گره را ضد عفونی کند. اگر فراتر از توانایی عامل پاسخ باشد، درخواست به سرور WNA ارسال می شود تا با استفاده از وصله های برنامه مشکل را برطرف کند. گاهی اوقات، عامل پاسخ می‌تواند از شبکه درخواست کند تا گره آسیب‌دیده را دوباره احراز هویت کند یا حتی گره را به طور کامل از شبکه حذف کند.(Table 1)

Table 1 Simulation parameter

PARAMETER	VALUE
Simulator	NS-2.34
Topology	Random
Number of nodes	50,100,150,200
Wifi Data Rate	2 Mbps
Propagation Model	Two Ray Ground
Physical Model	wirelessphy
Antenna model	OmniAntenna
Queue Size	50
Traffic type	CBR,UDP
Mobility Model	Random Way Point
Routing Algorithm	SMACLAD
Packet size	512
Mac protocol	802.11 standard

۵. نتایج شبیه سازی

۵،۱. فرمول برای نمودار

۱) PDR[1] کسر تحویل بسته =بسته دریافتی / ارسال بسته

۲) NRL[2] بار مسیریابی عادی =تعداد بسته های مسیریابی / تعداد بسته های داده دریافتی

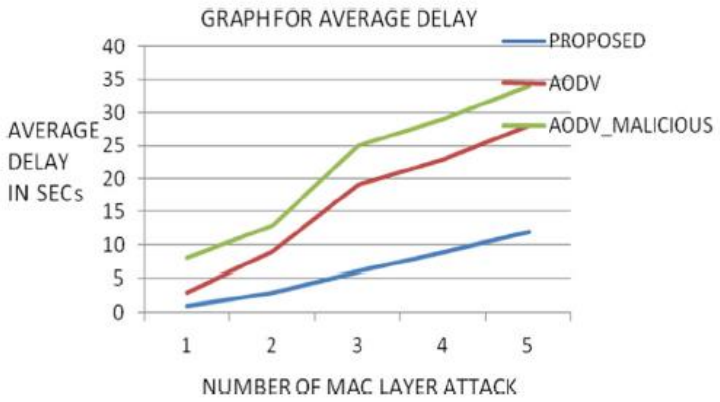
۳) AD[3] میانگین تاخیر سرتاسر = آخرین زمان ارسال بسته / تعداد بسته های دریافتی

۴) میانگین مصرف انرژی= (انرژی اولیه - انرژی نهایی) / تعداد کل گره ها

۵،۲. حمله لایه MAC

شکل ۲ تأخیری را که هنگام انتقال بسته از مبدا به مقصد رخ می دهد نشان می دهد.SMACLAD در مقایسه با AODV_MALICOUS و BLAD حداقل مقدار تاخیر را نشان می دهد.

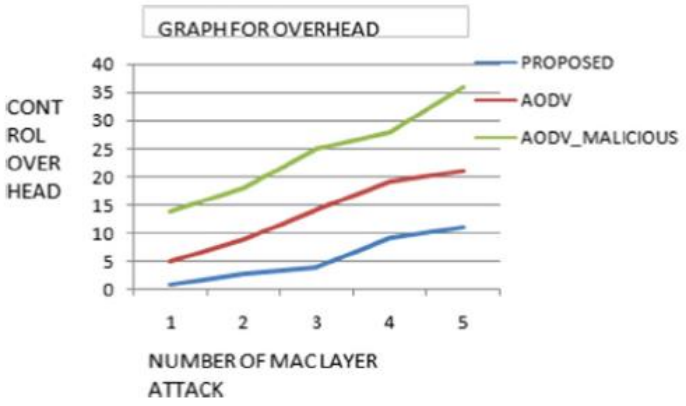
[1] Packet Delivery Fraction
[2] Normalized Routing Load
[3] Average end-to-end Delay



شکل۲. میانگین تاخیر در حمله لایه MAC

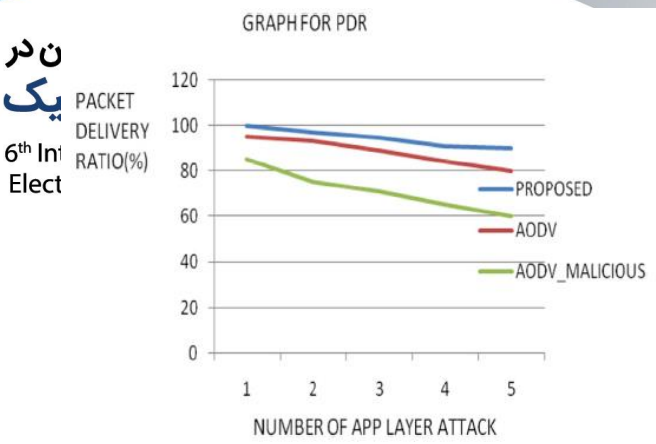
از این رو به نظر می رسد SMACLAD با توجه به جنبه ذکر شده در بالا نیز بهترین است.

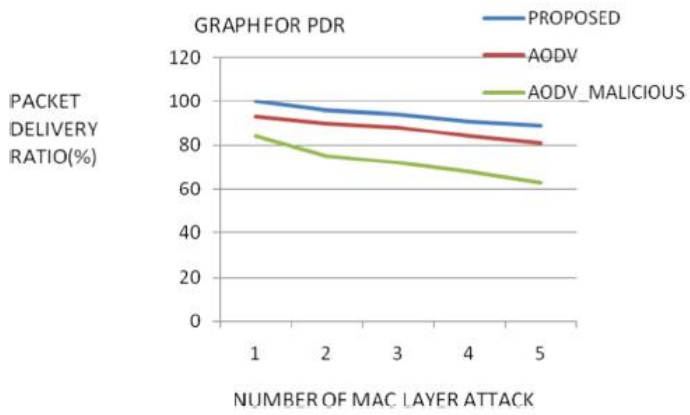
در شکل ۳ نمودار سربار مسیریابی هر سه روش را نشان می دهد. سربار بر اساس تعداد گره‌های مهاجم لایه MAC مانند حمله میانی، حمله سریع و سیاه‌چاله است. با افزایش گره‌های مهاجم و در نتیجه افزایش تعداد بسته‌های کنترلی برای انتخاب کوتاه‌ترین مسیر برای رسیدن به مقصد، تعداد سربارها بالا می‌رود.



شکل۳. نمودار سربار برای حمله لایه MAC

اگرچه BLAD مفهوم چند مسیری را برای انتقال اطلاعات حیاتی پیاده‌سازی می‌کند، اما همچنان پیام‌های کنترلی بالایی تولید می‌کند که منجر به سربار هنگفتی می‌شود.(شکل ۴، ۵ و ۶)





شکل۵. حمله لایه APP برای نمودار PDR

شکل۴. نمودارPDR برای حمله لایه MAC

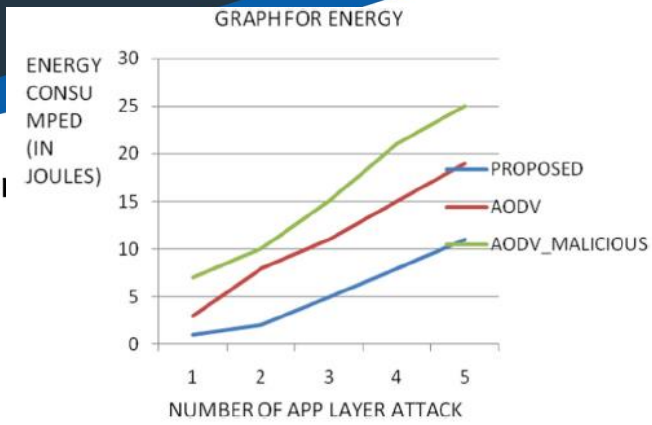
از این رو SMACLAD با تعادل بهینه از قابلیت اطمینان و کارایی و با هزینه های سربار کمتر از بقیه تکنیک ها بهتر عمل می کند.مشاهده می شود که PDR به طور غیر مستقیم با تعداد گره های مهاجم متناسب است. نتایج آزمایش نشان می دهد که SMACLAD تمایل به پایداری دارد و کاهش بسیار جزئی در PDR ثبت شده است که کمتر از ۴٪ است.

۵,۳. لایه برنامه

مشاهده می شود که PDR به طور غیر مستقیم با تعداد گره های مهاجم متناسب است.

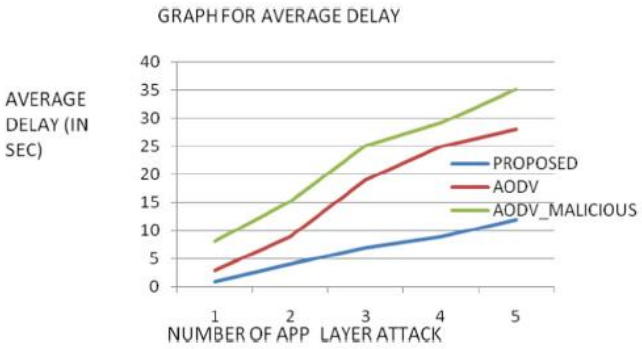
نتایج آزمایش نشان می دهد که SMACLAD تمایل به پایداری دارد و کاهش بسیار جزئی در PDR ثبت شده است که کمتر از ۴٪ است. AODV_MALICIOUS نشان داد که PDR تقریباً ۵۰٪ و BLAD با ۱۲٪ کاهش می یابد. از این رو SMACLAD کارایی خود را در حفظ PDR نشان داده است.

شکل۶ یک نمایش تصویری از انرژی مصرف شده در حین حضور گره های مهاجم است. ثابت شده است که نمونه اولیه SMACLAD بهتر از BLAD و AODV_MALICIOUS است.



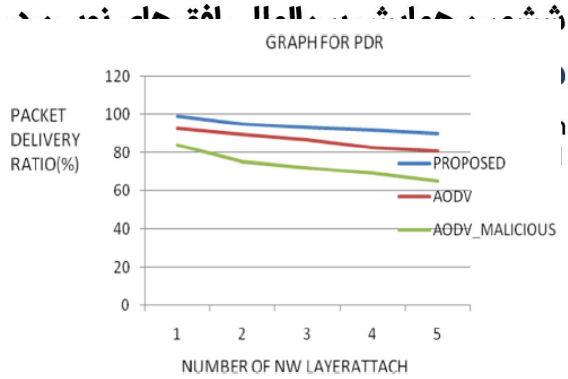
شکل۶. لایه APP حمله با نمودار انرژی

شکل ۷ همانطور که مشاهده می شود نمایشی از میانگین تاخیر است. تاخیر متوسط دوره زمانی است که برای انتقال یک بسته از مبدا به مقصد صرف می شود. خاطرنشان می شود که در AODV_MALCIOUS تأخیر مستقیماً با تعداد گره های مهاجم متناسب است.

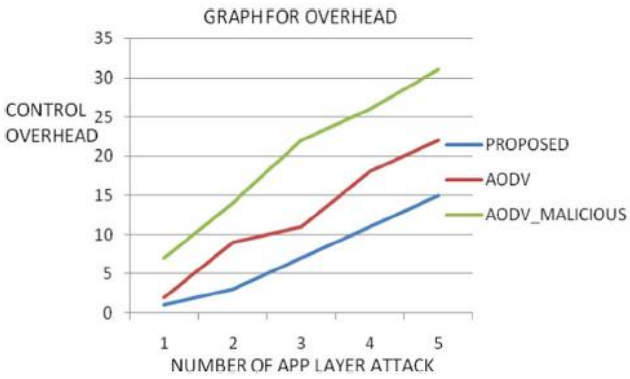


شکل۷. حمله لایه APP با نمودار تاخیر میانگین مرتبط است

شکل ۸ در مورد سربار از نظر گره های مهاجم لایه APP است. برخی از این گره ها عبارتند از حمله عجولانه، سیاهچاله و انسان در حمله میانی. این یک واقعیت شناخته شده است که سربار شبکه با تعداد گره های Attack نسبت مستقیم دارد. با بیشتر شدن تعداد گره‌های حمله، بسته‌های کنترلی افزایش می‌یابد تا کوتاه‌ترین مسیر پیدا شود.



شکل۹. حمله لایه شبکه با نمودار PDR



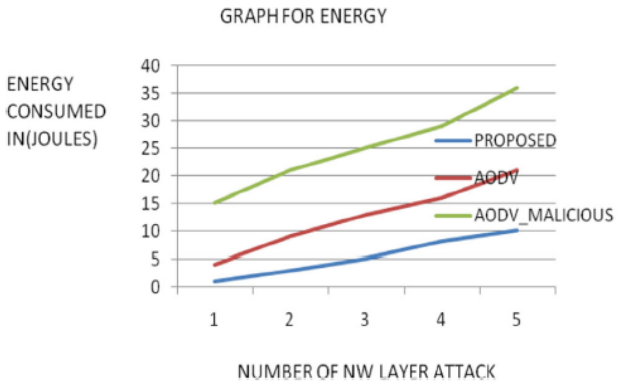
شکل۸. حمله لایه APP در مقابل نمودار سربار

مشاهده می شود که SMACLAD کمترین سربار را نسبت به AODV و BLAD دارد. در مورد BLAD، سیستم چند مسیری برای اطلاعات حیاتی استفاده می شود و این امر با تولید پیام های کنترلی، هزینه های سربار را افزایش می دهد.

۵,۴. حمله لایه شبکه

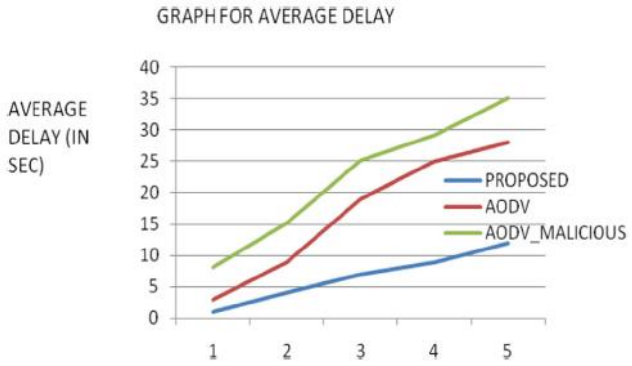
مشاهده می شود که PDR به طور غیر مستقیم با تعداد گره های مهاجم متناسب است. نتایج آزمایش نشان می دهد که SMACLAD تمایل به پایداری دارد و کاهش بسیار جزئی در PDR ثبت شده است که کمتر از ۴٪ است.AODV_MALICIOUS نشان داد که PDR تقریباً ۵۰٪ و BLAD با ۱۲٪ کاهش می یابد. از این رو SMACLAD کارایی خود را در حفظ PDR نشان داده است.

شکل ۱۰ خروجی حاصل از مصرف انرژی را در طول حضور گره های مهاجم نشان می دهد. پروتکل SMACLAD نتایج بهتری نسبت به نمونه اولیه AODV_MALICIOUS و BLAD نشان می دهد.



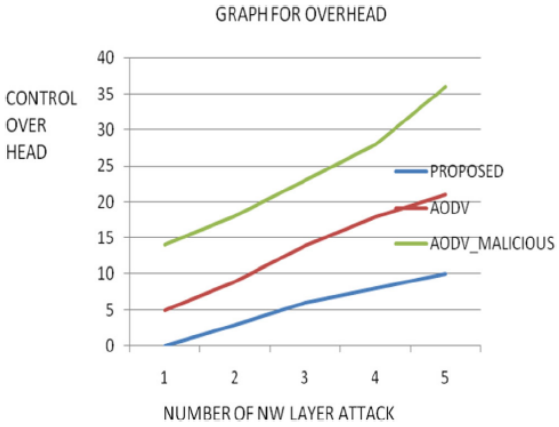
شکل ۱۰. حمله لایه شبکه با نمودار انرژی

شکل ۱۱ میانگین تاخیر را نشان می دهد. تاخیر متوسط دوره زمانی است که برای انتقال یک بسته از مبدا به مقصد صرف می شود. بنابراین مشاهده می شود که SMACLAD کمترین تاخیر را نسبت به AODV_MALICOUS و BLAD ثبت می کند. خاطرنشان می شود که در AODV_MALCIOU تاخیر مستقیماً با تعداد گره های مهاجم متناسب است.



شکل۱۱. نمودار تاخیر لایه شبکه حمله بیش از میانگین

در شکل ۱۲ نمودار سربار مسیریابی هر سه روش را نشان می دهد. سربار بر اساس تعداد گره‌های مهاجم لایه MAC مانند حمله میانی، حمله سریع و سیاه‌چاله است. با افزایش تعداد حملات یا گره های مهاجم، شمارش در سربار افزایش می یابد و در نتیجه باعث افزایش تعداد بسته های کنترلی برای انتخاب کوتاه ترین مسیر به مقصد می شود. اگرچه BLAD مفهوم چند مسیری را برای انتقال اطلاعات حیاتی پیاده‌سازی می‌کند، اما همچنان پیام‌های کنترلی بالایی تولید می‌کند که منجر به سربار هنگفتی می‌شود. از این رو SMACLAD با تعادل بهینه قابلیت اطمینان و کارایی همانطور که در شکل ۹ نشان داده شده است و با هزینه های سربار کمتر، از بقیه تکنیک ها بهتر عمل می کند.



شکل ۱۲. حمله به لایه شبکه با گراف سربار

نتیجه گیری

یک روش بیزی به منظور پیش بینی حملات لایه فیزیکی در یک شبکه و همچنین بازیابی شبکه از حملات لایه MAC، شبکه و لایه برنامه پیشنهاد شده است. یک نمونه اولیه مسیریابی ایمن با پیاده سازی سرور مانند گره بی سیم در یک شبکه بی سیم معرفی می شود. این طرح محله را از نظر فعالیت های مخرب، خودخواهانه و هرگونه رفتار نادرست در شبکه مشاهده و بررسی می کند.هنگامی که چنین فعالیتی شناسایی می شود، کلید را باطل می کند، بنابراین گره های شناسایی شده سقوط می کنند و این گره ها با امضاهای حمله، برنامه ها وصله و نصب برنامه ها، پروفایل های نرمال برنامه، تجزیه و تحلیل و تشخیص بیشتر هر گره به روز رسانی می شوند و یکپارچگی عوامل ADS را آزمایش می کنند، که در هر گره وجود دارد. کل معماری ADS به همراه ساختار شبکه کامل طراحی شده و پروتکل ها با استفاده از WNA تعریف شده اند.

منابع

1. Miao J, Hu Z, Yang K, Wang C, Tian H (2012) Joint Power and Bandwidth Allocation Algorithm with QoS Support in Heterogeneous Wireless Networks. IEEE Communications Letters, 16(4), 1089–7798/12$31.00_c2011 IEEE
2. Raza Bukhari SH, Rehmani MH, Siraj S (2016) A survey of channel bonding for wireless networks and guidelines of channel bonding for futuristic cognitive radio sensor networks. Communications Surveys & Tutorials, https://doi.org/10.1109/COMST.2015. 2504408, IEEE
3. Jie Z, Jiandong L, Qin L, Hua S, Xiaoniu Y (2014) On minimizing delay with probabilistic splitting of traffic flow in heterogeneous wireless networks. Communications System Design, China Communications
4. Zhang Q, Zhang Y-Q (2008) Cross-layer design for qos support in multihop wireless networks. roceedings of the IEEE 96(1), 0018–9219/$25.00 _2007 IEEE
5. Huang H, Gong T, Zhang R, Yang L, Zhang J, Xiao F (2018) Intrusion detection based on k-coverage in mobile sensor networks with empowered intruders. IEEE Trans Veh Technol. https://doi.org/10.1109/TVT.2018.2872848
6. Zhao P, Yang X (2016) Opportunistic routing for bandwidthsensitiven traffic in wireless networks with lossy links. Journal of Communications and Networks 18(5), Digital object identifier.https://doi.org/10.1109/JCN.2016.000109, 1229-2370/16/$10.00 c 2016
7. Mashima D, Gunathilaka P, Chen B (2018) Artificial command delaying for secure substation network control: design and implementation. IEEE Transactions on Smart Grid.https://doi.org/10.1109/TSG.2017.2744802
8. Meng W, Li W, Su C, Zhou J, Lu R (2018) enhancing trust management for wireless intrusion detection via traffic sampling in the era of big data. Received October 1, 2017, accepted October 28, 2017, date of publication November 13, 2017, date of current version March 9, 2018

9. Guan Y, Ge X (2017) Distributed attack detection and secure estimationof networked cyber-physical systems against false data injection attacks and jamming attacks. IEEE Transactions on Signal and Information Processing Over Networks
10. Guo H, Yang Z, Zhang L, Zhu J, Zou Y (2017) Joint cooperative beamforming and jamming for physical-layer security of decodeand- forward relay networks. Received August 11, 2017, accepted September 4, 2017, date of publication September 14, 2017, date of current version October 12, 2017
11. Pan Y, Hou Y, Li M, Gerdes RM, Zeng K, Towfiq MA, Cetiner BA (2017) Message integrity protection over wireless channel: countering signal cancellation via channel randomization. IEEE Transactions on Dependable and Secure Computing. https://doi.org/10.1109/TDSC.2017.2751600
12. Yi C-W (2009) Unified analytic framework based on minimum scan statistics for wireless Ad Hoc and sensor networks. IEEE Transactions on Parallel and Distributed Systems 20(9), 1045–9219/09/$25.00 _ 2009 IEEE
13. Fang D, Qian Y, Hu RQ (2017) Security for 5G Mobile Wireless Networks. Department of Electrical and Computer Engineering, University of Nebraska–Lincoln, Omaha, 2169–3536, IEEE
14. Tian F, Chen X, Liu S, Yuan X, Li D, Zhang X, Yang Z (2018) Secrecy rate optimization in wireless multi-hop full duplex networks. Special Section on Secure Modulations for Future Wireless Communications and Mobile Networks, Digital Object Identifier. https://doi.org/10.1109/Access.2018.2794739