طراحی سیستم تشخیص نفوذ سبک وزن با روش آزمون فرض

چیمن علافی[1*] ، سیروس فتحی‌منش[2]، محمد فتحی[3]
[1]کارشناس ارشد مهندسی برق_مخابرات، دانشگاه کردستان، alafi.chiman@yahoo.com
[2] دکتری آمار، دانشگاه کردستان، s.fathimanech@uok.ac.ir
[3] دکتری مهندسی برق_مخابرات، دانشگاه کردستان، mfathi@uok.ac.ir

چکیده : شبکه اینترنت اشیاء به دلیل کاربردهای وسیعی که دارد، تهدیدات امنیتی زیادی را نیز به همراه دارد. این تهدیدات امنیتی به عنوان عامل مهمی توسعه‌ی اینترنت اشیاء را محدود می‌کند. شبکه اینترنت اشیاء، معمولا به دلیل محدود بودن منابع محاسباتی دستگاه‌ها این شبکه، در معرض حملات سایبری است. یکی از این حملات، حمله Packet flooding است که باعث افزایش نرخ ورود بسته و در نهایت ایجاد ترافیک کاذب در شبکه می‌شود. یکی از راه‌های جلوگیری از حملات استفاده از سیستم‌های تشخیص نفوذ در شبکه است. برای کاهش این دست از حملات ، یک سیستم تشخیص نفوذ سبک وزن برای شناسایی حملات و فیلتر کردن بسته های بیش از نرخ ورود مجاز در شبکه هستند طراحی شده است. این سیستم تشخیص نفوذ سبک وزن به یک مسئله بهینه سازی متکی است که احتمال هشدار کاذب را به حداقل می رساند در حالی که احتمال تشخیص از دست رفته را زیر سطح مطلوب حفظ می کند. با استفاده از یک روش جستجو مشکل حل می شود. نتایج شبیه سازی تأثیر سیستم تشخیص نفوذ پیشنهادی را نشان می دهد .

کلید واژه‌ها: اینترنت اشیاء، تهدیدات امنیتی، سیستم تشخیص نفوذ، سیستم تشخیص نفوذ سبک وزن.

1- مقدمه

اینترنت اشیاء را می‌توان مجموعه‌ای از سنسورها و محرک-های جاسازی شده در اشیاء فیزیکی تعریف کرد؛ این دستگاه‌ها در قالب کاربردی که دارند از طریق شبکه‌های سیمی و بیسیم به اینترنت متصل می‌شوند تا بتوان صرفه نظر از مکان و زمان به اطلاعات این دستگاه‌ها دسترسی داشته و حتی آنها را کنترل و نظارت کرد [۱]. به عبارت دیگر در این شبکه اتصال دستگاه‌های فیزیکی نظیر وسایل نقلیه، لوازم خانگی، گوشی‌های هوشمند و غیره به همدیگر از طریق نرم‌افزارها و حسگرها صورت می‌گیرد. در این شبکه، تمامی دستگاه‌ها قادر هستند که کارهایشان را به‌صورت خودکار انجام دهند. همچنین می‌توانند ضمن اتصال به شبکه جهانی اینترنت با یکدیگر در ارتباط بوده و داده جمع‌آوری شده را به مراکز مورد نظر ارسال کنند. در دنیای سایبری امکان انتقال داده از طریق اینترنت اشیاء بدون نیاز به رابط‌های انسان به انسان یا انسان به کامپیوتر فراهم می‌شود [۲].

همانطور که در شکل ۱ نشان داده شده است معماری اینترنت اشیا را می توان در سه بخش ادراک ، شبکه و کاربرد دسته بندی کرد که هر بخش چالش‌های خاص خود را دارد [۳]. لایه ادراک وظیفه جمع آوری اطلاعات از محیط فیزیکی توسط اشیاء و حسگرهای موجود در این لایه را دارد؛ لایه انتقال با ایفای نقش واسط بین لایه‌های ادراک و اپلیکیشن، مسئولیت انتقال اطلاعات بین این دو لایه‌ها را با نمونه فناوری‌هایی چون 5G ، بر عهده دارد. در آخر لایه اپلیکیشن، یک محیط کاربری ساده‌ای را برای افراد جهت بهره برداری از اطلاعات تولیدشده را ایجاد می‌کند [۴].

شکل ۱: شبکه اینترنت اشیاء [۱۳]

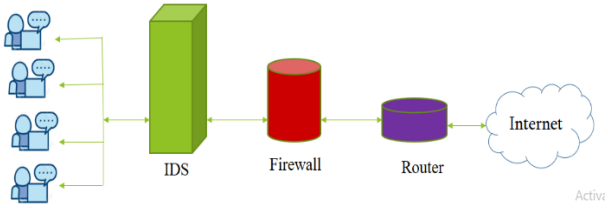
1-2- تهدیدات امنیتی اینترنت اشیاء

امنیت یکی از مهمترین چالش های اینترنت اشیا در برابر حملات مختلف است. چراکه، این دستگاه‌ها در مقابل انواع مختلفی از حملات و نفوذ مهاجم‌ها آسیب پذیر هستند. همانطور که اشاره شد، امروزه اینترنت اشیاء به صورت وسیع در حوزه‌های مختلف زندگی استفاده می‌شود و روزبه‌روز استفاده از آن بیشتر و فراگیرتر خواهد شد؛ با این حال، امنیت اینترنت اشیاء به عنوان یک چالش بزرگ در چنین سیستم‌هایی محسوب می‌شود [۵].

شبکه اینترنت اشیاء امن شده به شبکه‌ای اطلاق می‌شود که در آن اطلاعات مبادله شده توسط شخص ثالث قابل تغییر نباشد (یکپارچگی) ؛ اطلاعات فقط برای افراد مشخص شده در دو طرف ارتباط، قابل فهم و مشخص باشد (محرمانگی) ؛ اطمینان حاصل شود که نهادها یا دستگاه‌های درگیر ارتباط، خودشان باشند و هویت آن دستگاه‌ها توسط دستگاه دیگری جعل نشده باشد (احراز هویت) ؛ سیستم‌ها و دستگاه‌های موردنظر از کار نیفتاده باشند (در دسترس بودن) ؛ نهادها و دستگاه‌ها فقط مجاز به اجرای دستوراتی هستند که مجوز اجرای آنها را دارند (مجوز) [۶].

1-3- سیستم‌های تشخیص نفوذ سبک وزن

سیستم‌های تشخیص نفوذ به ابزار یا مکانیسم‌هایی برای تشخیص حملات وارده بر یک سیستم یا یک شبکه به وسیله آنالیز کردن رفتار در شبکه یا سیستم رامی گویند. علاوه بر امنیت های ایجاد شده در لایه‌های مختلف، استفاده از سیستم تشخیص نفوذ برای جلوگیری از حملات، لازم و ضروری است (شکل ۲). این روش دارای دقت بالا در تشخیص است، مهاجمان را در هنگام شکسته شدن رمز نگاری شناسایی می‌کند و یک نوع دیوار دفاعی دوم محسوب می‌شود. تاکنون سیستم‌های تشخیص نفوذ مختلفی برای شبکه اینترنت اشیاء پیشنهاد شده‌اند که هر کدام فقط می‌توانند تعدادی از حملات را پشتیبانی وبا آنها مقابله کنند که نیاز است این روش‌ها گسترش پیدا کرده تا بتوانند بخش عمده‌ای از حملات را پشتیبانی کرده و به حد بالایی از امنیت برسیم [۷] .



شکل ۲: شبکه امن شده با سیستم تشخیص نفوذ [۱۴]

سیستم‌های تشخیص نفوذی که طراحی شده‌اند همگی در تشخیص نفوذ کارآمد بوده و هستند. همچنین قادر به تشخیص حملات ناشناخته بوده و از سرعت تشخیص بالایی نیز برخوردار است [۸] . اما مشکل اصلی آن، اضافه بار محاسباتی بالاست [۹] . این سیستم‌های تشخیص نفوذ چون به محاسبات با منابع متکی هستند، ممکن است برای گره‌های کم ظرفیت در شبکه‌های اینترنت اشیاء بسیار سنگین باشند. بنابراین نیاز به طراحی یک سیستم تشخیص نفوذ که نیاز به هزینه محاسباتی کم، انرژی مینیمم و حافظه کم در گره‌های شبکه داشته باشد، احساس می-شود. می‌توان سبک وزن را به عنوان کوچک، قدرتمند و به اندازه کافی انعطاف پذیر تعریف کرد که می‌توان از آن به عنوان عنصر دائمی در زیر ساخت امنیت شبکه استفاده کرد. بطور کلی یک سیستم سبک وزن با هدف صرفه جویی در مصرف انرژی و کاهش منابع محاسباتی در نظر گرفته می‌شود [۱۰] .

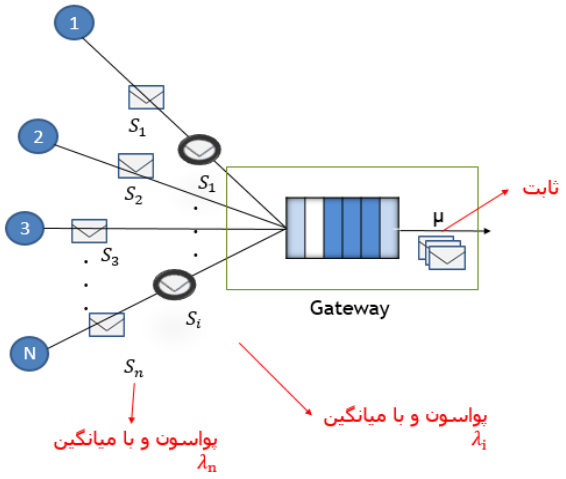
1-4- معرفی آزمون فرض

آزمون فرض نوعی از آمار استنباطی است که به ما این امکان را می‌دهد که بر اساس یک نمونه نماینده درباره کل جمعیت نتیجه بگیریم. در اکثر موارد، مشاهده کل جمعیت برای درک خصوصیات آن غیرممکن است، لذا با کار با یک نمونه مزایای فوق العاده ای را می‌توان کسب کرد. بطور کلی نقش اصلی فرضیه در تحقیقات علمی پیش بینی نتایج آزمایش‌های آینده از فرضیه است [۱۱].
معیار ارزیابی: برای ارزیابی یک آزمون فرض از دو نوع خطای، نوع اول و نوع دوم استفاده می‌شود که در ادامه تشریح می‌گردد.
انواع خطاها: خطای نوع اول (α) : احتمال رد کردن فرض صفر هنگامی که فرض صفر در حقیقت درست است را احتمال خطای نوع اول می‌گوییم. احتمال خطای نوع اول را سطح معنی دار بودن یا سطح معنی داری آزمون می‌گوییم، در آمار خطای نوع اول دارای اهمیت فوق العاده ای است و لذا همواره میزان خطای نوع اول را کنترل می‌کنند. در علم مهندسی این خطا را false alarm یا گزارش اشتباه نیز می‌گویند.
خطای نوع دوم(ß) : عبارت است از احتمال قبول فرض صفر هنگامی که غلط است و باید رد شود. بطورکلی می‌توان گفت، یک آزمون خوب آن است که در آن آلفا و بتا هر دو کوچک باشند و بنابراین به ما شانس بالایی برای اتخاذ تصمیم درست بدهد. در علم مهندسی این خطا را miss detection یا تشخیص از دست رفته می‌گویند [۱۲] .

2- سیستم و مدل حمله

همانطور که اشاره شد؛ شبکه اینترنت اشیاء، معمولا به دلیل محدود بودن منابع محاسباتی دستگاه‌ها، در معرض حملات سایبری است. یکی از این حملات، حمله Packet flooding است که باعث افزایش نرخ ورود بسته و در نهایت ایجاد ترافیک کاذب در شبکه می‌شود. هدف این تحقیق، پیشنهاد یک چارچوب برای شناسایی این دست از حملات در شبکه اینترنت اشیاء است.
شبکه‌ای را در نظر می‌گیریم که شامل مجموعه‌ای از گره‌های ار سال کننده $N=\{n : n=1,2,...,N\}$ در امتداد زمان به صورت

اسلات‌های زمانی $T=\{t : t=1,2,...,T\}$ است (مطابق شکل ۳)؛ به این صورت که در هر اسلات زمانی، هر گره اقدام به ارسال تعدادی بسته نرمال و مخرب می‌کند. تعداد بسته‌های نرمال دریافتی در هر اسلات زمانی توسط گره دروازه را $S_n(t)$ در نظر می‌گیریم که از تابع احتمال پواسن با میانگین λ_n پیروی می‌کند. همچنین تعداد بسته‌های مخرب دریافتی در هر اسلات زمانی توسط گره دروازه را $S_i(t)$ در نظر می‌گیریم که از تابع احتمال پواسن با میانگین λ_i پیروی می‌کند. در این شبکه مخابراتی، جهت بررسی و آنالیز کردن بسته‌های دریافتی یا به عبارت دیگر ترافیک شبکه از یک سیستم تشخیص نفوذ استفاده می‌کنیم. بنابراین می‌توان برای کاهش این دست از حملات یک سیستم تشخیص نفوذ برای شناسایی حملات و فیلتر کردن بسته‌هایی که بیشتر از نرخ ورود مجاز در شبکه هستند، طراحی کرد.



شکل ۳: مدل صف موجود در دروازه اینترنت اشیاء در یک شبکه مخابراتی

2-1- تشخیص حمله

این سیستم تشخیص نفوذ در رویکرد خود و پس از قرارگیری در محل تعیین شده (گره دروازه)، شروع به نظارت تعداد بسته‌های دریافتی می‌کند و در هر اسلات زمانی و بر اساس آستانه تعیین شده توسط مدیر شبکه، تصمیم می‌گیرد که تعداد بسته دریافتی، نرمال یا بیشتر از حد معمول است.

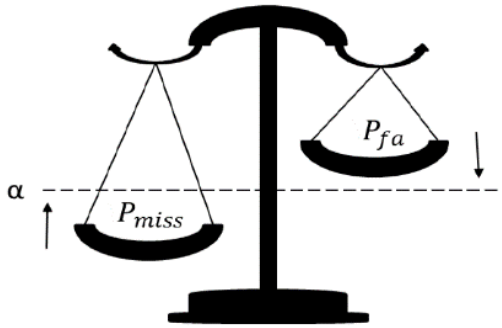
در این راستا دو متغیر m و m_{Th} را تعریف می‌کنیم که به ترتیب بیانگر تعداد بسته‌های دریافتی و مقدار سطح آستانه هستند. بر این اساس، قانون تصمیم‌گیری برای تشخیص حمله را به صورت زیر تعریف می‌کنیم:

$$\begin{cases} H_0 & m \le m_{Th} \\ H_1 & m > m_{Th} \end{cases}$$

که در آن H_0 و H_1 به ترتیب نشان دهنده شرایط نبود حمله و وجود حمله Packet flooding است.

2-2- وظیفه سیستم تشخیص نفوذ

جهت دستیابی به عملکرد بالای شبکه در تشخیص حمله packet flooding، معمولاً مدیر شبکه در تلاش برای فراهم کردن نرخ تشخیص بالا برای این حمله است. به عبارت دیگر، مدیر شبکه به دنبال اعمال مقادیر و پارامترهایی است که نرخ تشخیص را تا حد امکان افزایش دهد؛ اما با افزایش نرخ تشخیص یا به عبارتی کاهش احتمال عدم تشخیص حمله (P_{miss}) توسط سیستم تشخیص نفوذ، احتمال گزارش اشتباه (P_{fa}) افزایش میابد. همانطور که در شکل ۴ نشان داده شده، هنگامی که کفه احتمال عدم تشخیص ترازو به مقدار ماکزیمم خود یعنی مقدار α، از قبل تعیین شده توسط مدیر شبکه، نزدیک می‌شود، کفه احتمال گزارش اشتباه به مقدار کمینه ممکن برای آن α می‌رسد.



شکل ۴: مصالحه بین احتمال اخطار اشتباه و احتمال عدم تشخیص حمله

پس برای حل مسئله فوق و ایجاد یک مصالحه میان این احتمالات، مسئله بهینه سازی زیر پیشنهاد می‌شود:

$$\min_{m_{Th}} P_{fa}$$

$$\text{Subject to} \quad P_{miss} \le \alpha$$

جایی که P_{miss} نشان دهنده احتمال عدم تشخیص حمله است، یعنی حمله بوده و اتفاق افتاده اما سیستم تشخیص نفوذ نتوانست آن را تشخیص دهد. P_{fa} احتمال گزارش اشتباه است، یعنی در واقع هیچ حمله‌ایی اتفاق نیافتاده اما سیستم تشخیص نفوذ اعلام حمله می‌کند. این مسئله نشان می‌دهد که احتمال

اخطار ا شتباه باید کمینه شود. درحالیکه احتمال عدم ت شخیص باید کمتر از مقدار α باشد، یا به عبارت دیگر احتمال تشخیص حمله بزرگتر از α -1 باشد. در حالت نرمال توزیع تعداد بسته‌های دریافتی از تابع توزیع پواسن با متوسط λ_n و در حالت حمله با متوسط λ_i پیروی می‌کند. بر این اساس احتمال عدم تشخیص و احتمال گزارش اشتباه را در قالب روابط زیر بیان می‌کنیم.

$$P_{miss} = P(m < m_{Th} \mid \lambda = \lambda_i) = \sum_{k=0}^{m_{Th}} \frac{e^{-\lambda_i}\lambda_i^k}{k!}$$

$$P_{fa} = P(m > m_{Th} \mid \lambda = \lambda_n) = \sum_{k=m_{Th}+1}^{\infty} \frac{e^{-\lambda_n}\lambda_n^k}{k!}$$

که در اینجا m_{Th}، آستانه به دست آمده بر روی تعداد بسته‌های بیش از حد معمول، باید به گونه‌ایی تعیین شود که شرط $P_{miss} < \alpha$ را ارضا کند. این سطح آستانه توسط یک روش تکرار شونده ودر قالب الگوریتم زیر قابل محاسبه است.

Algorithm: IDS detection threshold

Input P_{miss} . α
Output m_{Th}
1: $0 \leftarrow p_{miss}$
2: $0 \leftarrow m_{Th}$
3: **While** $P_{miss} < \alpha$

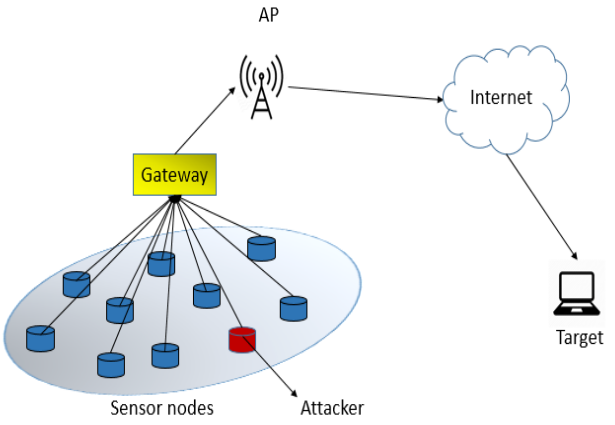
4: $P_{miss} \leftarrow P_{miss} + P(X = m_{Th})$
5: $m_{Th} \leftarrow m_{Th} + 1$

6: End while

این الگوریتم، از رابطه مربوط به P_{miss} جهت محاسبه m_{Th} استفاده می‌کند. به این ترتیب ابتدا کار خود را با مقدار اولیه صفر مربوط به m_{Th} شروع می‌کند. سپس مقدار m_{Th} را با هر بار به روز رسانی P_{miss}، افزایش می‌دهد. تا زمانی‌که رابطه $P_{miss} > \alpha$ نقض شود.

3- نتایج شبیه سازی

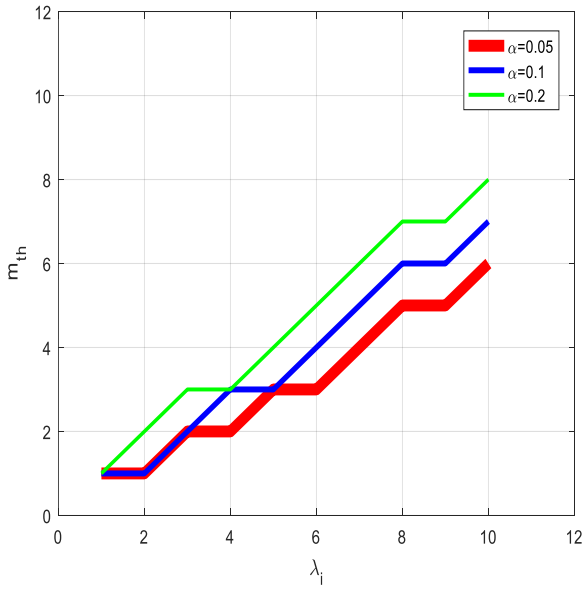
یک شبکه همانند شکل ۵ را در نظر می‌گیریم که در هر اسلات زمانی، گره دروازه تعدادی بسته نرمال با نرخ متوسط λ_n و همچنین تعدادی بسته مخرب با نرخ متوسط λ_i را دریافت می‌کند. شبیه سازی‌ها برای مدت زمان $T=1000$ اسلات زمانی اجرا می‌شوند.



شکل ۵: نمونه ساختار شبکه اینترنت اشیاء با وجود مهاجم درون شبکه‌ای

3-1- تغییرات سطح آستانه برای آلفاهای مختلف

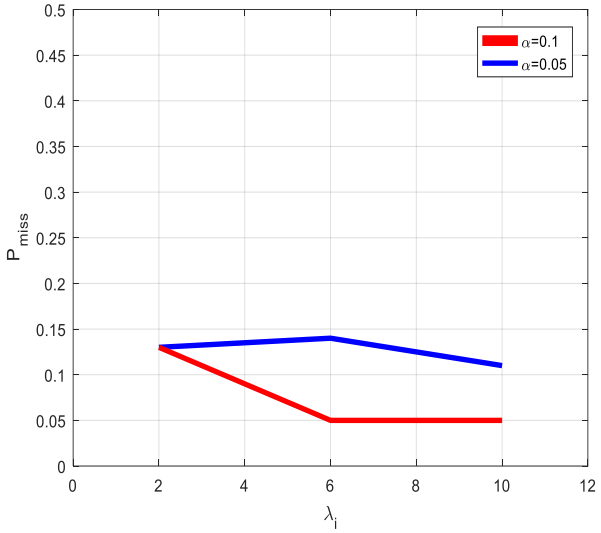
تعیین سطح آستانه با استفاده از قانون تصمیم‌گیری معرفی شده، یکی از پارامترهای مهم این سیستم تشخیص نفوذ به حساب می‌آید. شکل ۶ مقدار سطح آستانه را برای مقادیر مختلف λ_i را به ازای سه مقدار از α نشان می‌دهد. همانطور که مشاهده می‌شود، درواقع هر چه λ_i بیشتر باشد یعنی شرایط حمله شدیدتر باشد، برای داشتن یک P_{miss} محدود باید آستانه تصمیم گیری بیشتر باشد که این امر منجر به کاهش P_{fa} می‌گردد. همچنین هرچه درجه آزادی بیشتر در P_{miss} باشد مقدار آستانه می‌تواند بیشتر باشد.



شکل ۶: تغییرات سطح استانه برای آلفاهای مختلف

3-2- حالت‌های عدم تشخیص حمله بر حسب λ_i

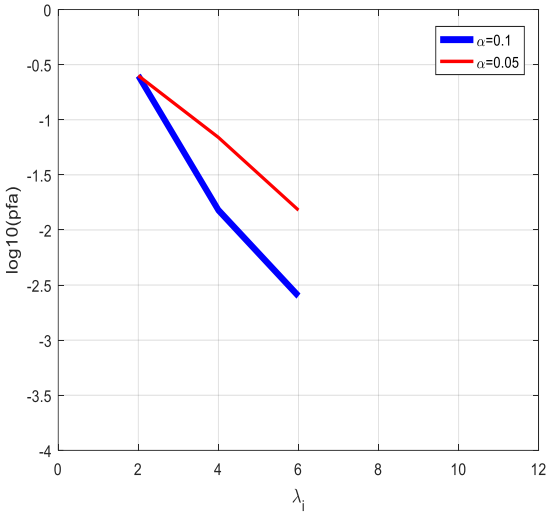
اگر در هر زمان بسته های ورودی کمتر از مقدار آستانه تعیین شده در مرحله قبل باشد، در این حالت سیگنال حمله صفر است. اگر مساوی یا بزرگتر از مقدار آستانه باشد، در این حالت سیگنال حمله یک است. در شکل ۷ تعداد حالت‌های عدم تشخیص حمله یا P_{miss} بر حسب λ_i نشان داده شده است. همانطور که دیده می‌شود مقدار P_{miss} در هر دو حالت به مقدار کران بالا یعنی α همگرا شده است.



شکل ۷: حالت‌های عدم تشخیص حمله بر حسب λ_i

3-3- حالت‌های گزارش اشتباه برحسب λ_i

برای بررسی تغییرات P_{fa} برحسب λ_i ؛ در هر مقدار از λ_i حد آستانه به دست آمده در شکل ۸ را در شبیه سازی اعمال می‌کنیم. بسته‌های دریافتی را با $\lambda_n = 3$ در نظر می‌گیریم. در هر مقدار از λ_i تعداد بسته‌های دریافتی را با حد آستانه مقایسه می‌کنیم و اگر بیشتر بود گزارش اشتباه اعلام می‌گردد. بدین ترتیب منحنی P_{fa} برحسب λ_i در شکل ۷ ترسیم می‌گردد. مشاهده می‌شود که هر چه λ_i بیشتر باشد P_{fa} کمتر می‌شود. هم‌چنین در مقادیر بزرگ α احتمال گزارش اشتباه (P_{fa}) کمتر است.



شکل ۸: حالت‌های گزارش اشتباه برحسب λ_i

جمع بندی

در این مقاله، یک چارچوب تحلیلی در باب تشخیص حمله Packet Flooding برای شبکه‌های اینترنت اشیاء انجام شد. این واقعیت وجود دارد که وجود احتمالات بزرگ حمله، منجر به ایجاد طول صف بزرگتر در شبکه و کاهش چشمگیر عملکرد آن می‌شود. این سیستم تشخیص نفوذ پیشنهادی، برای مقابله با این دست از حملات و جلوگیری از ایجاد ازدحام، اقدام به محدود کردن شبکه با استفاده از فیلتر بسته‌های با نرخ ورود بیش ازحد معمول می‌کند. معیار به حداقل رساندن احتمال عدم تشخیص و احتمال اخطار اشتباه، در قالب یک قاعده تصمیمگیری و با تکیه بر تعداد بسته‌هایی با نرخ ورود بیش ازحد معمول، صورت می‌گیرد. یکی از چالش‌های ما برای رسیدن به این مهم، انتخاب مقدار آستانه است که تابعی از احتمال حمله خواهد بود و توسط مدیر شبکه تعیین می‌شود. این آستانه باید تا حد امکان کوچک تعیین شوند تا بتواند در احتمالات بزرگ حمله، احتمال اخطار اشتباه را مینیمم کند.

مراجع

[1] K. L. Lueth, "IoT Analytices," 2015. [Online]. Available: https://iotanalytics.com/product/whitepaper-iot-basics-getting-started-with-the-internet-of-things/.

[2] Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, and Sean Carlisto de Alvarenga. A survey of intrusion detection in internet of things. *Journal of Network and Computer Applications*, 84:25–37, 2017.

[3] intel team, 2014. [Online]. Available: https://www.intel.com/content/www/us/en/internet-of-things/white-papers/developing-solutions-for-iot.html.

[4] F. Bing, "The research of IOT of agriculture based on three layers architecture," *2016 2nd International Conference on Cloud Computing and Internet of Things (CCIOT)*, pp. 162-165, 2016.

[5] A. Rayes and S. Salam, "Internet of things-from hype to reality: The road to digitization," Internet Things From Hype to Real. Road to Digit, 2016, pp. 1-328.

[6] Agent, R., & Hids, T. (2015). Classification of intrusion detection systems, 118(7), 8887.

[7] Hichem Sedjelmaci, Sidi Mohamed Senouci, and Tarik Taleb. An accurate security game for low-resource IoT devices. *IEEE Transactions on Vehicular Technology*, 66(10):9381–9393, 2017.

[8] Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in
The Internet of Things. Ad Hoc Networks, 11(8), 2661–2674. 2013.

[9] J. L. ,. K. K. C. a. M. A. Anhtuan Le, "A Specification-Based IDS for Detecting Attacks on RPL-Based Network Topology," *information*, vol. 7, no. 2, 2016.

[10] Stolyar, A. L. (2005). Maximizing queuing network utility subject to stability: Greedy primal–dual algorithm. *Queueing Systems, 50*(4), 401–457.

[11] Sedjelmaci, H., Senouci, S. M., & Al-Bahri, M. (2016). A lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology. In *2016 IEEE international conference on communications (ICC)*, 2016.

[12] M Keshtgary, N Rikhtegar, et al. Intrusion detection based on a novel hybrid learning approach. *Journal of AI and Data Mining*, 6(1):157–162, 2018.

[13] Jyoti Deogirikar and Amarsinh Vidhate. Security attacks in IoT: a survey. *In I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017 International Conference on. IEEE*, 2017.

[14] Manal A Abdullah, Bdoor M Alsolami, Hana M Alyahya, and Maha H Alotibi. Intrusion detection of dos attacks in wsns using classification techniuqes. *Journal of Fundamental and Applied Sciences*, 10(4S):298– 303, 2018.