گزارش پروژه درس نظریه بازی‌ها

بررسی و تحلیل مقاله:

Game theoretic models for detecting network intrusions

تهیه و تنظیم: پرنیان ملک‌زاده

استاد راهنما: دکتر نریمانی

تیر ۱۴۰۴

فهرست مطالب

فصل ۱

چکیده و مقدمه

۱۰۱ چکیده

این مقاله به بررسی مسئله تشخیص نفوذ [۱] در شبکه‌های زیرساخت سیمی با استفاده از ابزارهای نظریه بازی [۲] می‌پردازد. فرآیند تشخیص از طریق نمونه‌برداری [۳] از زیرمجموعه‌ای از بسته‌های ارسالی در خطوط ارتباطی یا واسط‌های مسیریاب [۴] منتخب شبکه انجام می‌شود. با توجه به یک بودجه کلی تخصیص‌داده‌شده برای نمونه‌برداری، چارچوب ارائه‌شده به دنبال توسعه یک استراتژی بهینه برای نمونه‌برداری از بسته‌های شبکه است تا شانس موفقیت یک مهاجم را به طور مؤثری کاهش دهد.

نویسندگان دو سناریوی اصلی را در نظر می‌گیرند:

- **سناریوی اول:** یک مهاجم هوشمند و آگاه، حمله خود را به چندین بسته تقسیم می‌کند تا شانس خود را برای نفوذ موفقیت‌آمیز به یک دامنه هدف افزایش دهد.
- **سناریوی دوم:** چندین مهاجم همکار [۵] حمله را بین خود توزیع کرده و هر یک قطعاتی از حمله را از مسیرهای مختلف به سمت گره هدف ارسال می‌کنند.

فرض کلیدی این است که اگر این بسته‌های حاوی قطعات حمله به صورت مستقل تحلیل شوند، نفوذ قابل تشخیص نخواهد بود. این مقاله برای اولین بار، با استفاده از نظریه بازی، مسئله‌ای را مدل‌سازی می‌کند که در آن حمله بر روی چندین بسته تقسیم شده یا توسط مهاجمان همکار توزیع می‌شود. برای بیان رسمی مسئله از نظریه بازی غیرهمکارانه [۶] استفاده می‌شود که در آن دو بازیکن عبارتند از: (۱) مهاجم هوشمند (یا مهاجمان همکار) و (۲) سیستم تشخیص نفوذ [۷]. هدف نهایی، ارائه یک چارچوب نظریه بازی است که مهاجم را برای انتخاب استراتژی حمله خود و IDS را برای یافتن یک استراتژی نمونه‌برداری بهینه جهت شناسایی بسته‌های مخرب، راهنمایی کند.

---

[۱] Intrusion Detection
[۲] Game Theory
[۳] Sampling
[۴] Router Interfaces
[۵] Cooperative Intruders
[۶] Non-cooperative Game Theory
[۷] Intrusion Detection System (IDS)

۲.۱ مقدمه

شبکه‌های مبتنی بر زیرساخت سیمی، علی‌رغم استفاده از مکانیزم‌های امنیتی مانند دیواره‌های آتش [۸] و تکنیک‌های رمزنگاری، همچنان در برابر انواع مختلفی از نفوذها آسیب‌پذیر هستند. این نفوذها می‌توانند منجر به حملات انکار سرویس [۹] یا تلاش برای نفوذ به شبکه شوند. در چنین شرایطی، سیستم تشخیص نفوذ (IDS) به عنوان یک خط دفاعی ثانویه برای شناسایی این حملات و تولید پاسخ‌های مناسب، ضروری است.

به طور معمول، تشخیص فعالیت‌های غیرعادی از طریق نظارت و تحلیل ترافیک شبکه انجام می‌شود. تحلیل ترافیک می‌تواند بر روی کل ترافیک شبکه یا بخشی از آن (نمونه‌برداری) صورت گیرد. تحلیل کل ترافیک به دلیل نیاز به منابع محاسباتی زیاد (مانند پردازنده و حافظه) بسیار پرهزینه است. از سوی دیگر، نمونه‌برداری هزینه کمتری دارد اما با خطر از دست دادن برخی از نفوذها به دلیل محدودیت بودجه نمونه‌برداری همراه است. بنابراین، یافتن یک استراتژی که بتواند احتمال تشخیص را با استفاده از نمونه‌برداری افزایش دهد، یک چالش بزرگ محسوب می‌شود، به ویژه زمانی که با مهاجمان هوشمندی روبرو هستیم که قادرند یک حمله را به چندین قطعه تقسیم کنند.

نظریه بازی به عنوان یک ابزار قدرتمند ریاضی، برای مدل‌سازی و تحلیل سیستم‌هایی که در آن چندین بازیکن با اهداف متفاوت با یکدیگر رقابت می‌کنند، بسیار مناسب است. تقابل دائمی بین مهاجمان و مدیران امنیتی را می‌توان به عنوان یک بازی غیرهمکارانه مدل‌سازی کرد. در این بازی، بازیکنان عبارتند از مهاجمان و سیستم تشخیص نفوذ. هدف این مقاله استفاده از این چارچوب برای ارائه یک راهکار ریاضی دقیق برای مسئله نمونه‌برداری در سیستم‌های تشخیص نفوذ است.

این پژوهش بر اساس کارهای قبلی، به ویژه مقاله‌ای که در آن مسئله تشخیص نفوذ از طریق نمونه‌برداری بسته با استفاده از نظریه بازی فرمول‌بندی شده بود، بنا شده است. با این حال، کار قبلی تنها حمله‌ای را در نظر گرفته بود که در آن مهاجم از یک بسته برای انجام وظیفه خود استفاده می‌کند. این یک محدودیت بزرگ است، زیرا یک مهاجم حرفه‌ای می‌تواند حمله خود را بر روی چندین بسته تقسیم کرده و هر کدام را از یک مسیر متفاوت ارسال کند. این مقاله با در نظر گرفتن این سناریوی عملی‌تر، به توسعه مدل‌های نظریه بازی برای مقابله با این نوع حملات پیچیده می‌پردازد.

[۸] Firewalls
[۹] Denial of Service (DoS)

فصل ۲

بیان و فرمول‌بندی مسئله

در این فصل، چارچوب کلی مسئله و مفاهیم پایه‌ای که برای مدل‌سازی بازی استفاده می‌شوند، تشریح می‌گردد. ابتدا مدل شبکه و مفروضات آن بیان شده، سپس بازیکنان و اهداف آن‌ها تعریف می‌شوند و در نهایت، استراتژی‌های در دسترس هر بازیکن معرفی می‌گردد.

۱۰۲ مدل شبکه و مفروضات

شبکه به صورت یک گراف جهت‌دار [۱] مدل‌سازی می‌شود که آن را با $G = (N, E)$ نمایش می‌دهیم. در این نمایش:

- N مجموعه گره‌ها (مانند مسیریاب‌ها و کامپیوترها) است.
- E مجموعه یال‌های جهت‌دار (خطوط ارتباطی) است.

فرض می‌شود که شبکه دارای k گره و l خط ارتباطی است. ظرفیت [۲] هر خط $e \in E$ با c_e و میزان ترافیک جاری بر روی آن با f_e نمایش داده می‌شود. برای هر دو گره u و v در شبکه، مجموعه تمام مسیرهای ممکن از u به v با ρ_u^v نشان داده می‌شود.

مفهوم کلیدی دیگری که در این مقاله استفاده می‌شود، **شار بیشینه** [۳] بین دو گره u و v است که با $MF_u^v(f)$ نمایش داده می‌شود. این مقدار، بیشترین حجم داده‌ای است که می‌تواند از u به v با توجه به ظرفیت یال‌ها ارسال شود. بر اساس قضیه شار بیشینه-برش کمینه [۴]، مقدار شار بیشینه بین دو گره برابر با ظرفیت **برش کمینه** [۵] بین آن دو گره است. برش کمینه، مجموعه‌ای از یال‌هاست که حذف آن‌ها ارتباط بین دو گره را قطع می‌کند و مجموع ظرفیت آن‌ها کمترین مقدار ممکن است.

۲۰۲ معرفی بازی‌ها و بازیکنان

این مقاله دو بازی غیرهمکارانه مجموع-صفر [۶] را با اطلاعات کامل [۷] مدل‌سازی می‌کند. بازیکنان در هر دو بازی عبارتند از:

---

[۱] Directed Graph
[۲] Capacity
[۳] Maximum Flow
[۴] Max-Flow Min-Cut Theorem
[۵] Minimum Cut
[۶] Zero-Sum Game
[۷] Complete Information

۱. **مهاجم (یا مهاجمان):** که هدفش ارسال بسته‌های مخرب به سمت هدف بدون شناسایی شدن است.

۲. **سیستم تشخیص نفوذ :(IDS)** که هدفش شناسایی این بسته‌های مخرب با استفاده از نمونه‌برداری است.

۱.۲.۲ بازی اول: مهاجم هوشمند منفرد

در این سناریو، یک مهاجم هوشمند قصد دارد با ارسال n بسته که هر کدام حاوی قطعه‌ای از حمله [۸] هستند، به یک گره هدف t حمله کند. حمله زمانی موفقیت‌آمیز تلقی می‌شود که حداقل $n-m+1$ قطعه از n قطعه بدون شناسایی شدن به مقصد برسند. به عبارت دیگر، IDS برای شناسایی نفوذ، باید حداقل m قطعه از n قطعه را شناسایی کند $(m \leq n)$. مهاجم می‌تواند مسیر ارسال هر قطعه را به صورت مستقل و با هدف کاهش احتمال شناسایی، انتخاب کند.

۲.۲.۲ بازی دوم: مهاجمان همکار

در این سناریو، یک گروه از مهاجمان همکار (Ω) وجود دارند. هر مهاجم $x \in \Omega$ یک قطعه از حمله را به سمت گره هدف t ارسال می‌کند. حمله زمانی موفقیت‌آمیز است که تمام قطعات ارسال‌شده توسط همه مهاجمان بدون شناسایی به مقصد برسند. IDS باید با بودجه نمونه‌برداری خود، ترافیک را به گونه‌ای نمونه‌برداری کند که بتواند این حمله توزیع‌شده را شناسایی نماید.

۳.۲ اهداف و محدودیت‌های بازی

نمونه‌برداری و تحلیل تمام بسته‌های عبوری از یک خط ارتباطی در لحظه، بسیار پرهزینه است. بنابراین، فرض می‌شود که IDS دارای یک بودجه نمونه‌برداری کلی و ثابت برابر با B_s (بسته بر ثانیه) در کل شبکه است. این بودجه می‌تواند به صورت دلخواه بین خطوط مختلف شبکه توزیع شود.

اگر نرخ نمونه‌برداری روی خط e برابر با s_e باشد و ترافیک جاری روی آن f_e باشد، احتمال نمونه‌برداری یک بسته (و در نتیجه یک قطعه مخرب) روی این خط برابر است با:

$$p_e = \frac{s_e}{f_e}$$

محدودیت اصلی IDS، محدودیت بودجه است که به صورت زیر تعریف می‌شود:

$$\sum_{e \in E} s_e \leq B_s$$

با جایگذاری $s_e = f_e p_e$، این محدودیت بر حسب احتمالات نمونه‌برداری به صورت زیر بازنویسی می‌شود:

$$\sum_{e \in E} f_e p_e \leq B_s$$

[۸] a-fragment

مجموعه تمام بردارهای احتمال تشخیص $p = (p_{e_1}, p_{e_2}, \ldots, p_{e_l})$ که در این محدودیت صدق می‌کنند، با U نمایش داده می‌شود.

۴.۲ استراتژی‌های بازیکنان

- **استراتژی مهاجم:** یک استراتژی خالص [۹] برای مهاجم، انتخاب یک مسیر مشخص از مبدأ به مقصد برای ارسال بسته مخرب است. اما در این مدل، مهاجم از یک استراتژی ترکیبی [۱۰] استفاده می‌کند. یعنی مهاجم یک بردار احتمال q بر روی مجموعه مسیرهای ممکن ρ_x^t تعریف می‌کند، به طوری که $\sum_{P \in \rho_x^t} q(P) = ۱$. مهاجم برای ارسال هر بسته، یک مسیر را با احتمال $q(P)$ انتخاب می‌کند.
- **استراتژی IDS:** استراتژی IDS انتخاب نرخ‌های نمونه‌برداری s_e (یا معادل آن، احتمالات تشخیص p_e) برای هر خط e در شبکه است، به گونه‌ای که در محدودیت بودجه B_s باقی بماند. به عبارت دیگر، IDS یک بردار $p \in U$ را انتخاب می‌کند تا احتمال کلی تشخیص را بیشینه سازد.

[۹] Pure Strategy
[۱۰] Mixed Strategy

فصل ۳

سناریوی اول: مهاجم هوشمند با بسته‌های چندگانه

در این فصل، بازی بین IDS و یک مهاجم هوشمند که حمله خود را به n بسته تقسیم می‌کند، به تفصیل فرمول‌بندی و حل می‌شود.

۱۰۳ فرمول‌بندی بازی

ابتدا احتمال اینکه یک بسته (قطعه حمله) در مسیر خود از مبدأ a به مقصد t شناسایی شود را محاسبه می‌کنیم. اگر مهاجم مسیر P را انتخاب کند، بسته شناسایی نمی‌شود اگر در هیچ‌یک از یال‌های $e \in P$ نمونه‌برداری نشود. احتمال این رویداد برابر است با $\prod_{e\in P}(۱ - p_e)$. در نتیجه، احتمال شناسایی شدن بسته در مسیر P برابر است با $۱ - \prod_{e\in P}(۱ - p_e)$

با توجه به اینکه مهاجم مسیرها را با توزیع احتمال q انتخاب می‌کند، احتمال کلی شناسایی یک قطعه حمله، که آن را با α نمایش می‌دهیم، برابر است با میانگین وزنی این احتمالات روی تمام مسیرها:

$$\alpha = \sum_{P\in\rho_a^t} q(P)\left[۱ - \prod_{e\in P}(۱ - p_e)\right] \tag{۱۰۳}$$

حال، IDS برای شناسایی کل نفوذ، باید حداقل m قطعه از n قطعه ارسالی را شناسایی کند. احتمال اینکه دقیقاً i قطعه شناسایی شود (و $n-i$ قطعه شناسایی نشود) از توزیع دوجمله‌ای به دست می‌آید و برابر است با $\binom{n}{i}\alpha^i(۱-\alpha)^{n-i}$. بنابراین، احتمال کلی تشخیص نفوذ (شناسایی حداقل m قطعه) برابر است با:

$$P_{detect} = \sum_{i=m}^{n}\binom{n}{i}\alpha^i(۱-\alpha)^{n-i} \tag{۲۰۳}$$

هدف IDS بیشینه کردن این احتمال و هدف مهاجم کمینه کردن آن است. این مسئله به یک بازی مجموع-صفر منجر می‌شود. بر اساس قضیه مینی‌مکس [۱]، یک نقطه تعادل برای این بازی وجود دارد که در آن:

$$\max_{p\in U}\min_{n,q}\sum_{i=m}^{n}\binom{n}{i}\alpha^i(۱-\alpha)^{n-i} = \min_{n,q}\max_{p\in U}\sum_{i=m}^{n}\binom{n}{i}\alpha^i(۱-\alpha)^{n-i} \tag{۳۰۳}$$

[۱] Minimax Theorem

مقدار مشترک این دو عبارت، مقدار بازی [۲] نامیده می‌شود.

۲.۳ حل بازی

حل مستقیم معادله ۲.۳ از نظر ریاضی بسیار پیچیده است. بنابراین، نویسندگان مسئله را با یک فرض ساده‌کننده حل می‌کنند: آنها حالتی را در نظر می‌گیرند که IDS برای شناسایی نفوذ نیاز به شناسایی **دقیقاً** m قطعه از n قطعه دارد. در این حالت، تابع هدف به $\alpha^m(1-\alpha)^{n-m}$ کاهش می‌یابد (با صرف نظر از ضریب ثابت $\binom{n}{m}$ که در بهینه‌سازی تأثیری ندارد). بازی به شکل زیر ساده می‌شود:

$$\theta = \max_{p\in U}\min_{n,q}\alpha^m(1-\alpha)^{n-m} = \min_{n,q}\max_{p\in U}\alpha^m(1-\alpha)^{n-m} \qquad (۴.۳)$$

برای حل این مسئله، دو گام برداشته می‌شود:

۱. برای یک α ثابت، مقدار بهینه m که تابع هدف را بیشینه می‌کند، پیدا می‌شود.

۲. استراتژی بهینه برای IDS (بردار p) و مهاجم (بردار q) که مقدار α را به نقطه تعادل خود می‌رساند، پیدا می‌شود.

۱.۲.۳ یافتن مقدار بهینه m

برای یافتن مقدار m که عبارت $\Gamma = \alpha^m(1-\alpha)^{n-m}$ را بیشینه می‌کند، از Γ نسبت به m مشتق گرفته و برابر با صفر قرار می‌دهیم (با در نظر گرفتن m به عنوان یک متغیر پیوسته). محاسبات نشان می‌دهد که این عبارت زمانی بیشینه می‌شود که:

$$m = n\alpha$$

تحلیل مشتق دوم نیز تأیید می‌کند که این نقطه یک ماکزیمم است. این نتیجه به این معناست که برای یک احتمال شناسایی α معین، سخت‌ترین سناریو برای مهاجم (و بهترین برای IDS) زمانی رخ می‌دهد که تعداد قطعات مورد نیاز برای شناسایی، متناسب با خود احتمال شناسایی باشد.

۲.۲.۳ بیشینه‌سازی α

اکنون مسئله به پیدا کردن نقطه تعادل برای α تبدیل می‌شود. از دید IDS، هدف بیشینه کردن α است:

$$\max_{p\in U}\alpha = \max_{p\in U}\sum_{P\in\rho_a^t} q(P)\left[1-\prod_{e\in P}(1-p_e)\right]$$

این عبارت معادل است با:

$$1-\min_{p\in U}\sum_{P\in\rho_a^t} q(P)\prod_{e\in P}(1-p_e)$$

[۲] Value of the Game

تابع هدف غیرخطی است. برای ساده‌سازی، نویسندگان فرض می‌کنند که احتمالات نمونه‌برداری p_e به قدر کافی کوچک هستند، به طوری که می‌توان از تقریب $\prod_{e\in P}(۱-p_e) \approx ۱ - \sum_{e\in P} p_e$ استفاده کرد. این فرض زمانی معتبر است که IDS بودجه خود را روی یال‌های برش کمینه متمرکز کند، زیرا در این صورت هر مسیر حداکثر با یکی از این یال‌های نمونه‌برداری شده تلاقی دارد. با این تقریب، مسئله بهینه‌سازی به یک مسئله برنامه‌ریزی خطی [۳] تبدیل می‌شود:

$$\max_{p\in U} \sum_{P\in\rho_a^t} q(P) \sum_{e\in P} p_e \qquad (۵.۳)$$

این یک مسئله min-max است که حل آن به طور مستقیم دشوار است. با استفاده از دوگانگی [۴] در برنامه‌ریزی خطی، می‌توان نشان داد که حل این بازی معادل حل یک مسئله شار بیشینه است.

استراتژی بهینه برای بازیکنان:

- **استراتژی IDS:**

۱. شار بیشینه از گره مهاجم a به گره هدف t را با فرض اینکه ظرفیت هر یال e برابر با ترافیک آن (f_e) است، محاسبه می‌کند $(MF_a^t(f))$.

۲. برش کمینه متناظر با این شار بیشینه را شناسایی می‌کند.

۳. تمام بودجه نمونه‌برداری B_s را فقط به یال‌های موجود در برش کمینه اختصاص می‌دهد. نرخ نمونه‌برداری برای یال e_i در برش کمینه برابر است با: $s_{e_i} = B_s \frac{f_{e_i}}{MF_a^t(f)}$.

- **استراتژی مهاجم:**

۱. شار بیشینه $MF_a^t(f)$ را به جریان‌های منفرد در مسیرهای مختلف تجزیه می‌کند (با استفاده از الگوریتم‌های تجزیه شار [۵]).

۲. اگر m_i میزان شار تخصیص‌یافته به مسیر P_i باشد، مهاجم این مسیر را با احتمال $q(P_i) = \frac{m_i}{MF_a^t(f)}$ برای ارسال بسته‌های خود انتخاب می‌کند.

مقدار بازی (احتمال شناسایی در نقطه تعادل) برابر خواهد بود با: $\theta = \frac{B_s}{MF_a^t(f)}$.

مثال کاربردی

مقاله یک مثال ارائه می‌دهد. فرض کنید A مهاجم و I هدف است و بودجه IDS برابر $B_s = ۱۲$ است.

۱. IDS شار بیشینه از A به I را محاسبه می‌کند که برابر با ۲۹ است.

۲. برش کمینه شامل یال‌های (C,E)، (B,D) و (B,G) است.

۳. IDS نرخ‌های نمونه‌برداری را به صورت زیر تخصیص می‌دهد:

- $s_{CE} = ۱۲ \times \frac{۱۱}{۲۹}$

[۳] Linear Programming
[۴] Duality
[۵] Flow Decomposition

- $s_{BG} = ۱۲ \times \frac{۸}{۲۹}$
- $s_{BD} = ۱۲ \times \frac{۱۰}{۲۹}$

۰۴. مهاجم نیز شار ۲۹ واحدی را به مسیرهای مختلف تجزیه کرده و احتمالات ارسال را متناسب با آن تنظیم می‌کند.

فصل ۴

سناریوی دوم: مهاجمان همکار

در این فصل، بازی به سناریویی گسترش می‌یابد که در آن چندین مهاجم همکار (Ω) به طور همزمان به یک هدف مشترک حمله می‌کنند.

۱۰۴ فرمول‌بندی بازی

در این سناریو، هر مهاجم $x \in \Omega$ یک قطعه از حمله را به سمت هدف t ارسال می‌کند. حمله زمانی موفق است که **همه** قطعات بدون شناسایی به مقصد برسند. بنابراین، IDS برای موفقیت، کافی است حداقل یکی از این قطعات را شناسایی کند.

برای هر مهاجم x، احتمال شناسایی بسته ارسالی او، α_x، مشابه معادله ۱۰۳ تعریف می‌شود:

$$\alpha_x = \sum_{P \in \rho_x^t} q_x(P) \left[۱ - \prod_{e \in P} (۱ - p_e) \right] \tag{۱۰۴}$$

از آنجا که IDS نمی‌داند کدام مهاجم در حال ارسال بسته است، یک رویکرد منطقی برای IDS، بیشینه کردن میانگین احتمال تشخیص بر روی تمام مهاجمان است. این تابع هدف جدید با Φ نمایش داده می‌شود:

$$\Phi = \frac{۱}{|\Omega|} \sum_{x \in \Omega} \alpha_x \tag{۲۰۴}$$

بازی min-max برای این سناریو به صورت زیر تعریف می‌شود:

$$\beta = \max_{p \in U} \min_{q_x \forall x} \Phi = \min_{q_x \forall x} \max_{p \in U} \Phi \tag{۳۰۴}$$

که در آن β مقدار بازی است.

۲۰۴ حل بازی

برای حل این بازی، IDS بودجه کل خود B_s را به طور مساوی بین تمام مهاجمان بالقوه تقسیم می‌کند. بنابراین، برای هر مهاجم $x \in \Omega$، یک بودجه مجازی برابر با $B_s/|\Omega|$ در نظر گرفته می‌شود. با این کار، مسئله به $|\Omega|$ زیربازی مستقل تجزیه می‌شود. هر زیربازی دقیقاً مشابه بازی سناریوی اول است که بین IDS و مهاجم x با بودجه $B_s/|\Omega|$

انجام می‌شود.

استراتژی بهینه برای بازیکنان:

- **استراتژی IDS:**

۱. برای هر مهاجم $x \in \Omega$، شار بیشینه $MF_x^t(f)$ و برش کمینه متناظر $Mincut_x^t$ را پیدا می‌کند.

۲. نرخ نمونه‌برداری نهایی برای هر یال e در شبکه، از مجموع نرخ‌های نمونه‌برداری محاسبه‌شده برای آن یال در تمام زیربازی‌ها به دست می‌آید. اگر یک یال e در برش کمینه چند مهاجم مختلف قرار داشته باشد، بودجه‌های تخصیص‌یافته به آن از طرف هر مهاجم با هم جمع می‌شوند. نرخ نمونه‌برداری برای یال e برابر است با:

$$s_e = \sum_{x \in \Omega, e \in Mincut_x^t} \frac{B_s}{|\Omega|} \frac{f_e}{MF_x^t(f)}$$

- **استراتژی هر مهاجم x:**

۱. شار بیشینه خود به هدف $(MF_x^t(f))$ را به جریان‌های منفرد در مسیرها تجزیه می‌کند.

۲. مسیر P_i را با احتمال $q(P_i) = \frac{m_i}{MF_x^t(f)}$ انتخاب می‌کند.

مقدار بازی برای هر زیربازی x برابر است با $\frac{B_s/|\Omega|}{MF_x^t(f)}$.

مثال کاربردی

مقاله مثالی با دو مهاجم همکار A و E و هدف I ارائه می‌دهد. بودجه کل $B_s = ۶۰$ است، بنابراین بودجه تخصیص‌یافته به هر مهاجم برابر با ۳۰ است.

- $MF_A^I(f) = ۹۹$، $Mincut_A^I = \{(A,B),(D,G),(E,G),(E,F)\}$
- $MF_E^I(f) = ۵۴$، $Mincut_E^I = \{(E,G),(E,F)\}$

نرخ نمونه‌برداری برای هر یال محاسبه می‌شود. به عنوان مثال، برای یال (E,G) که در هر دو برش کمینه وجود دارد:

$$s_{EG} = \left(\frac{۳۰}{۹۹} \times f_{EG}\right) + \left(\frac{۳۰}{۵۴} \times f_{EG}\right)$$

که مقاله مقادیر عددی نهایی را بر اساس جریان‌های روی یال‌ها محاسبه کرده است.

فصل ۵

نتایج عددی و تحلیل

در این بخش، مقاله به ارزیابی عملکرد مدل‌های پیشنهادی در مقایسه با دو رویکرد دیگر می‌پردازد:

۱. **مدل تصادفی** [۱]: بودجه نمونه‌برداری به صورت تصادفی بین یال‌های شبکه توزیع می‌شود.

۲. **مدل یکنواخت** [۲]: بودجه نمونه‌برداری به طور مساوی بین تمام یال‌های شبکه تقسیم می‌شود.

شبیه‌سازی‌ها بر روی گراف شبکه‌ای مشابه آنچه در مقاله شرح داده شده، انجام شده است.

۱۰۵ تحلیل سناریوی اول (مهاجم منفرد)

تأثیر بودجه بر احتمال تشخیص: این تحلیل، احتمال تشخیص را به عنوان تابعی از بودجه نمونه‌برداری (B_s) نشان می‌دهد.

- همانطور که انتظار می‌رود، با افزایش بودجه، احتمال تشخیص برای هر سه مدل افزایش می‌یابد.
- شیب نمودار برای مدل مبتنی بر نظریه بازی به مراتب بیشتر از دو مدل دیگر است. دلیل این امر آن است که این مدل تمام بودجه خود را بر روی یال‌های حیاتی (برش کمینه) متمرکز می‌کند. هر بسته‌ای که از مهاجم به هدف ارسال می‌شود، مجبور است حداقل از یکی از این یال‌ها عبور کند. در نتیجه، منابع بهینه تخصیص داده می‌شوند.
- زمانی که بودجه نمونه‌برداری به مقدار شار بیشینه (در اینجا ۹۹) نزدیک می‌شود، احتمال تشخیص برای مدل بازی به ۱ نزدیک می‌شود. زیرا در این حالت، IDS می‌تواند با نرخی برابر با جریان واقعی روی هر یال برش کمینه نمونه‌برداری کند و عملاً تمام بسته‌های عبوری از این گلوگاه را بررسی نماید.

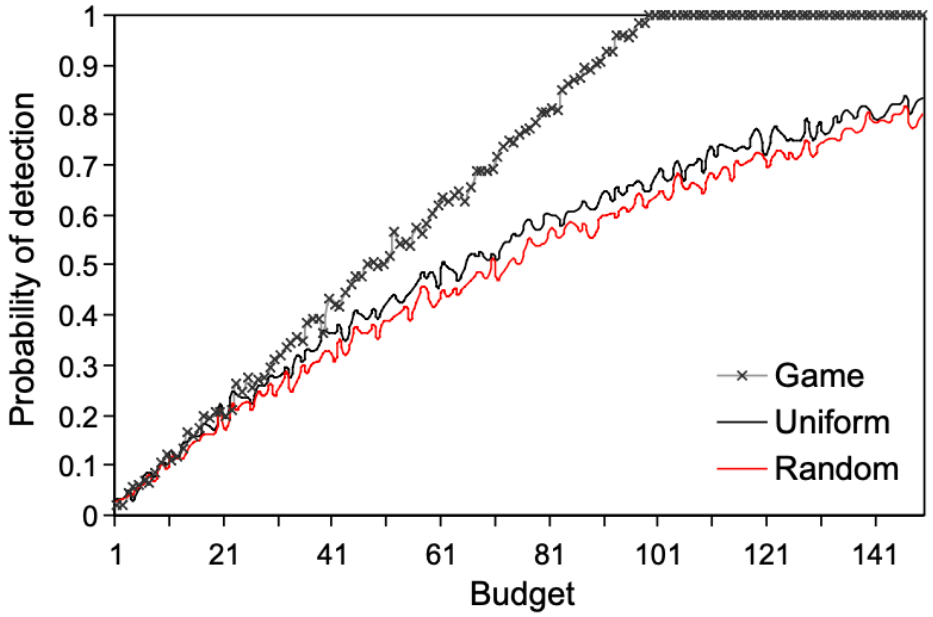
تأثیر تعداد قطعات حمله: این تحلیل، احتمال تشخیص را به عنوان تابعی از تعداد کل قطعات حمله (n) با بودجه ثابت ($B_s = ۶۰$) نشان می‌دهد.

- یک الگوی جالب مشاهده می‌شود: احتمال تشخیص برای تعداد فرد قطعات، کمی کمتر از تعداد زوج بعدی است. این به دلیل فرض مقاله است که برای تشخیص نفوذ، IDS باید "نصف" قطعات را شناسایی کند. برای مثال، اگر $n = ۳$ باشد، IDS به ۲ قطعه نیاز دارد، اما اگر $n = ۴$ باشد، باز هم به ۲ قطعه نیاز دارد. نیاز به یک قطعه اضافی در حالت فرد، احتمال موفقیت IDS را اندکی کاهش می‌دهد.
- در تمام موارد، مدل بازی عملکرد بهتری نسبت به مدل‌های تصادفی و یکنواخت از خود نشان می‌دهد.

---

[۱] Random Sampling

[۲] Uniform Sampling

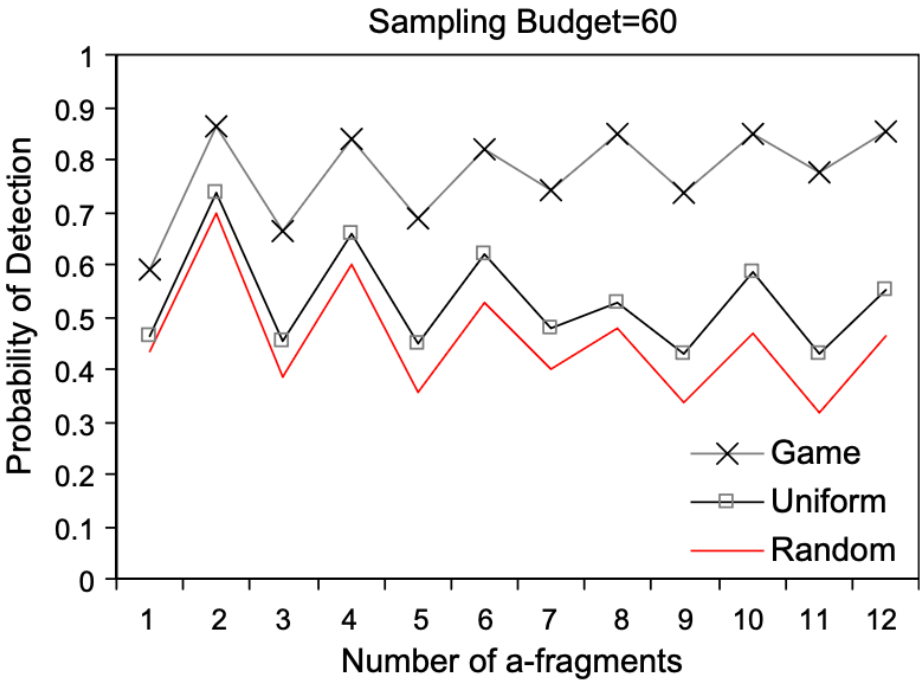


شکل ۱۰۵. نمودار مقایسه احتمال تشخیص بر حسب بودجه نمونه‌برداری (B_s) برای مدل‌های نظریه بازی، تصادفی و یکنواخت

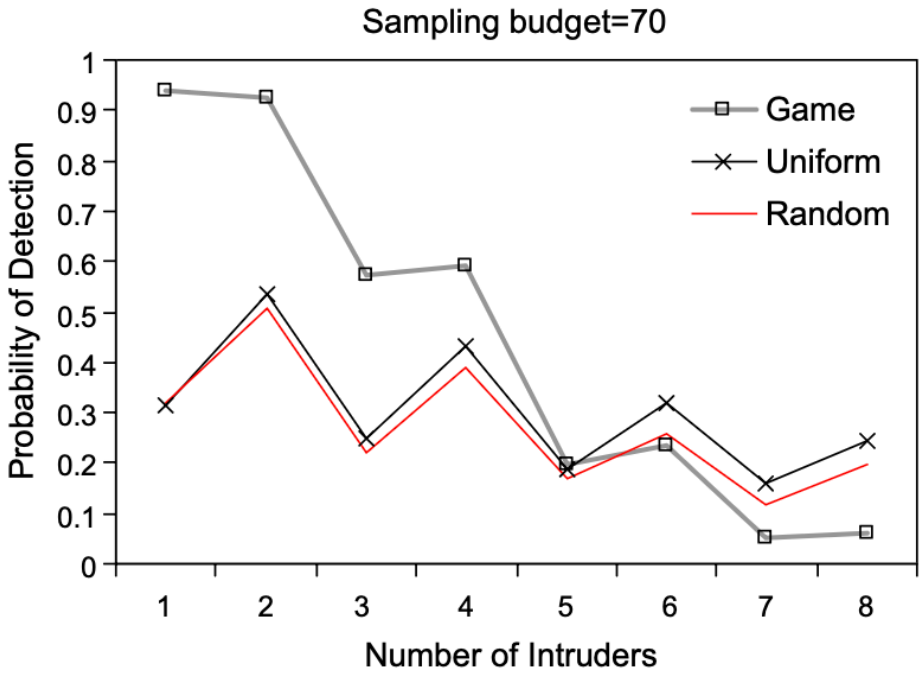
۲۰۵ تحلیل سناریوی دوم (مهاجمان همکار)

تأثیر تعداد مهاجمان: این تحلیل، احتمال تشخیص را به عنوان تابعی از تعداد مهاجمان همکار با بودجه ثابت ($B_s = ۷۰$) نشان می‌دهد.

- با افزایش تعداد مهاجمان، احتمال تشخیص برای هر سه مدل کاهش می‌یابد. برای مدل بازی، این کاهش شدیدتر است.
- دلیل کاهش در مدل بازی این است که بودجه کل (B_s) بین تعداد فزاینده‌ای از مهاجمان تقسیم می‌شود. با افزایش تعداد مهاجمان، بودجه تخصیص‌یافته به هر یک ($B_s/|\Omega|$) کوچک و کوچک‌تر می‌شود که منجر به کاهش نرخ نمونه‌برداری مؤثر برای هر مهاجم می‌گردد.
- یک نتیجه بسیار جالب مشاهده می‌شود: زمانی که تعداد مهاجمان از یک آستانه مشخصی فراتر می‌رود (در اینجا حدود ۵ یا ۶ مهاجم که بیش از ۵۰% گره‌های شبکه است)، عملکرد مدل بازی از مدل‌های یکنواخت و تصادفی بدتر می‌شود.
- دلیل این پدیده این است که با افزایش تعداد مهاجمان، مجموعه یال‌های موجود در "اجتماع برش‌های کمینه" بزرگ و بزرگ‌تر می‌شود تا جایی که تقریباً کل یال‌های شبکه را در بر می‌گیرد. در این نقطه، استراتژی متمرکز کردن بودجه، مزیت خود را از دست می‌دهد و تقسیم شدید بودجه به یک عامل منفی غالب تبدیل می‌شود. در مقابل، مدل‌های یکنواخت و تصادفی که از ابتدا بودجه را در سطح وسیعی توزیع می‌کردند، تحت تأثیر این "رقیق شدن بودجه" قرار نمی‌گیرند.



شکل ۲.۵. نمودار مقایسه احتمال تشخیص بر حسب تعداد قطعات حمله (n) با بودجه ثابت $(B_s = ۶۰)$ برای مدل‌های نظریه بازی، تصادفی و یکنواخت



شکل ۳.۵. نمودار مقایسه احتمال تشخیص بر حسب تعداد مهاجمان همکار با بودجه ثابت $(B_s = ۷۰)$ برای مدل‌های نظریه بازی، تصادفی و یکنواخت

فصل ۶

نتیجه‌گیری

این مقاله با موفقیت از چارچوب نظریه بازی برای توسعه یک استراتژی بهینه نمونه‌برداری بسته‌های شبکه با هدف تشخیص نفوذ استفاده می‌کند. نویسندگان به طور خاص دو سناریوی پیچیده و واقع‌گرایانه را مدل‌سازی کردند که در کارهای قبلی به آنها پرداخته نشده بود: حمله توسط یک مهاجم هوشمند که نفوذ خود را به چندین بسته تقسیم می‌کند، و حمله هماهنگ‌شده توسط گروهی از مهاجمان همکار.

در هر دو سناریو، تقابل بین مهاجم(ها) و سیستم تشخیص نفوذ (IDS) به عنوان یک بازی مجموع-صفر غیرهمکارانه با اطلاعات کامل فرمول‌بندی شد. با حل این بازی‌ها با استفاده از رویکرد مینی‌مکس و بهره‌گیری از مفاهیمی مانند دوگانگی در بهینه‌سازی و قضیه شار بیشینه-برش کمینه، استراتژی‌های بهینه برای هر دو بازیکن به دست آمد.

دستاوردهای کلیدی مقاله عبارتند از:

- **استراتژی بهینه :IDS** به جای توزیع یکنواخت یا تصادفی بودجه نمونه‌برداری، IDS باید منابع خود را بر روی یال‌های موجود در برش(های) کمینه بین مهاجم(ها) و هدف متمرکز کند. این استراتژی تضمین می‌کند که نمونه‌برداری در گلوگاه‌های شبکه انجام می‌شود.
- **استراتژی بهینه مهاجم:** مهاجم باید مسیرهای خود را بر اساس تجزیه شار بیشینه انتخاب کند، یعنی از مسیرهایی با "ظرفیت" بالاتر (که توسط IDS کمتر محافظت می‌شوند) با احتمال بیشتری استفاده کند.
- **تحلیل عملکرد:** نتایج عددی نشان داد که رویکرد مبتنی بر نظریه بازی در اکثر شرایط عملکرد بسیار بهتری نسبت به روش‌های ساده‌تر دارد. همچنین، تحلیل‌ها به درک عمیق‌تری از محدودیت‌های این رویکرد، به ویژه در سناریوی با تعداد بسیار زیاد مهاجمان، منجر شد.

در مجموع، این مقاله یک چارچوب ریاضی منسجم و کارآمد برای تخصیص منابع در سیستم‌های تشخیص نفوذ ارائه می‌دهد و به خوبی نشان می‌دهد که چگونه ابزارهای نظریه بازی می‌توانند برای حل مسائل پیچیده در حوزه امنیت سایبری به کار گرفته شوند.

منابع

[۱] Bhattacharya، P. and Debbabi، M. Assi، C. Mehrandish، M. Otrok، H. theoretic "Game network detecting for models intrusions،" *Computer Communications*، vol. ۳۱، no. ۸، pp. ۱۹۳۴-۱۹۴۴، ۲۰۰۸.