مروری بر عملیات جمینگ در شبکه‌های هوشمند

محمدرضا گوهره‌یی
کارشناسی ارشد، مهندسی مخابرات رمز، دانشگاه صنعتی مالک اشتر، تهران، ایران
Goharei@rcdat.ir

چکیده

در این مقاله یکی از مهم‌ترین چالش‌ها در شبکه‌های هوشمند انرژی به‌نام منع سرویس برای پیام‌های زمان بحرانی بیان می‌شود. بر همین اساس انواع ساختارهای مخابراتی برای انتقال داده در شبکه‌های هوشمند انرژی، انواع فناوری‌های مخابراتی پیشنهاد شده، انواع جمینگ‌ها، انواع پیام‌های انتقالی درشبکه معرفی می‌شود. همچنین مبتنی بر نوع فناوری مخابراتی و جمینگ، حالات مختلف جمینگ در شبکه مورد بررسی قرار می‌گیرد که برای بیان مسئله جمینگ از تئوری حل مسئله ورشکستگی قمارباز استفاده می‌شود. در ادامه خواهیم دید که برای برطرف کردن این آسیب پذیری ،کمترین نرخ پیام نامعتبر برای بدترین حالت ممکن در جمینگ محاسبه می‌شود و برای انطباق این مسئله در دنیای واقعی با استفاده از تکنیک TACT حداقل بار ترافیکی ابهام درشبکه ارائه می‌شود.

واژگان کلیدی: جمینگ، شبکه هوشمند، هماهنگ واکنشی، قمار باز، نرخ پیام نامعتبر، TACT

۱- مقدمه

امروزه فناوری شبکه‌های بیسیم بسیار مورد استفاده قرار گرفته است برای مثال می‌توان به کاربرد این فناوری در شبکه‌های هوشمند انرژی اشاره کرد. استفاده از این فناوری در شبکه‌های هوشمند انرژی باعث ایجاد یک بستر یکپارچه از زیرساخت‌های قدرت با فناوری اطلاعات شده که این امر باعث توسعه سریع شبکه‌های هوشمند انرژی و تسهیل تبادل اطاعات بین بخش‌های مختلف شبکه شده است [1]. اگر چه استفاده از این فناوری بسیار راه‌گشا است ولی به نوبه خوددارای آسیب‌پذیری‌هایی است که می‌تواند امینت کلی شبکه را به خطر بیندازد برای مثال می‌توان به حملات جمینگ در لینک‌های رادیویی اشاره کرد [2]. با استفاده از حملات جمینگ مهاجم قادر است برخی از پیام‌های تبادلی بین اعضای شبکه راتخریب کند و مانع رسیدن پیام به گیرنده شود . به‌عبارت دیگر نوعی از حملات منع سرویس در لینک‌های رادیویی ایجاد می شود [3].

این آسیب زمانی باعث تهدید شبکه می‌شود که مهاجم قصد داشته باشد، پیام‌های زمان بحرانی را مورد تخریب قرار دهد. پیام‌های زمان بحرانی به پیام‌های گفته می‌شود در یک بازهٔ زمانی مشخص دارای اعتبار هستند درصورتی‌که این پیام خارج از بازه زمانی مدنظر به گیرنده برسد دیگر دارای اعتبار نیست و به‌عنوان پیام نامعتبر در نظر گرفته می‌شود. به‌طورمعمول این پیام‌ها برای ارسال داده‌های حساس به زمان شبکه استفاده می‌شود [4].

۲- بیان مسئله جمینگ در مخابرات بی‌سیم

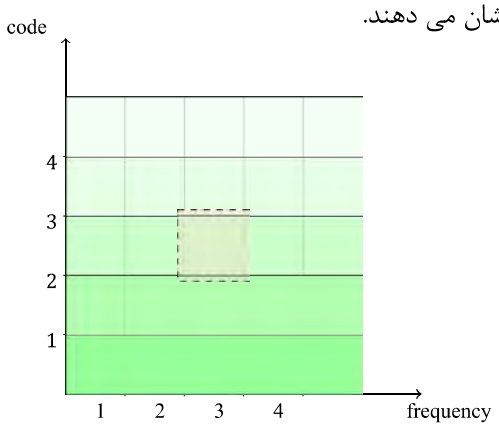
اما برای پاسخ به این سؤال که مهاجم چگونه می‌تواند عملیات جمینگ را انجام دهد، ابتدا لازم است، ساختار مخابراتی مورد نظر در شبکه هوشمند انرژی مورد بررسی قرار گیرد [5]،[6].

- **مخابرات[1] FHSS:** در این فناوری فرستنده و گیرنده در یک استخر کانالو کد قرار دارند.
- **مخابرات[2] DHSS:** در این فناوری فرستنده چندین داده اصلی را با دنبالهٔ شبه‌تصادفی ضرب می‌کنند، گیرنده از یک هم‌بستگی با دنباله یکسان برای بازیابی پیام اصلی استفاده می‌کنند.

به‌دلیل ویژگی‌های بیان‌شده می‌توان از مخابرات FHSS را برای پست‌های محلی در نظر گرفت [7] چرا که در این نوع از مخابرات به‌دلیل تعداد زیاد کانال‌های کد فرکانس دارای هزینه زیادی است؛ اما از همین ویژگی می‌توان برای کاهش هزینه تأخیر پیام‌ها استفاده کرد.

[1] Frequency hopping spread spectrum
[2] Direct sequence spread spectrum

همان‌طور که در شکل (۱) نشان داده شده است در این نوع مخابرات خطوط ارتباطی توسط دو پارامتر فرکانس و کد به بخش‌های مختلف می‌شود که بربخش دوتایی آن را یک کانال مجزا تشکیل می‌دهد. به‌عبارت دیگر در این خطوط ارتباطی به تعداد N_fN_c کانال وجود دارد که N_f تعداد فرکانس هاو N_c تعداد کدهای موجود برای این خطوط ارتباطی را نشان می دهند.



(شکل-۱): تقسیم‌بندی کانال کد-فرکانس

همچنین می‌توان دو حالت برای هریک از فناوری‌های مخابراتی در نظر گرفت[8]،[9]:

- **مخابرات هماهنگ:** در این نوع مخابرات، فرستنده و گیرنده دارای یک راز مشترک هستند و هریک قبل از برقراری ارتباط می‌داند طرف مقابل خود در کدام کانال کد فرکانس است؛ به‌عبارت دیگر در این نوع مخابرات طرفین همگام هستند.
- **مخابرات ناهماهنگ:** برخلاف نوع قبلی در این نوع از مخابرات طرفین از قبل نمی‌دانند که طرف مقابل خود در کدام کانال کد فرکانس هستند؛ برهمین اساس یک مرحلهٔ تعیین کانال قبل از برقراری ارتباط دارند؛ به عبارت دیگر در این نوع مخابرات طرفین ناهمگام هستند؛ اما برای بهره‌وری شبکه از حالت ترکیبی استفاده می‌شود. به عبارت دیگر برای شروع ارتباط از مخابرات هماهنگ استفاده می‌شود تا طرفین بتوانند یک ارتباط اولیه را مبتنی بر راز مشترک بین خودشان تشکیل دهند. پس از برقراری این ارتباط، طرفین سعی می‌کنند برای ادامه ارتباط خود بر روی راز جدید توافق کنند و مبتنی بر راز مشترک جدید ادامه ارتباط خود را مبتنی بر روش غیر هماهنگ ادامه می‌دهند. همچنین می‌توان عملیات جمینگ را به دو نوع تقسیم‌بندی کرد که عبارتند از [4]،[8]،[5]،[9]:
- **جمینگ غیر واکنشی:** در این نوع جمر عملیات اختلال رادیویی براساس استراتژی ازقبل‌تعریف‌شده ارسال می‌کند. به عبارت دیگر در این نوع، جمر هیچ اطلاعاتی از کانال هدف ندارد و فقط براساس برنامه‌ریزی ازپیش‌تعریف‌شده عمل می‌کند.
- **جمینگ واکنشی:** در این نوع جمر عملیات اختلال رادیویی بر اساس عملکرد شبکه انجام می‌شود. به‌عبارت دیگر جمر زمانی فعالیتی بر روی کانال مد نظر حس کند، سیگنال اختلال را ارسال می‌کند. در این نوع از جمرها عملیات جمینگ شامل دو بخش است که عبارتند از:
  - بخش حس کانال هدف که به‌عنوان عملیات پیش‌جمینگ درنظر گرفته می‌شود. در این مرحله کانال مورد نظر حس و انتخاب می‌شود.
  - بخش جمینگ که در این بخش پس از تعیین کانال هدف سیگنال جمینگ بر روی کانال مد نظر ارسال می‌شود.

همچنین می‌توان پیام‌های ارسالی توسط گره‌های شبکه را به دو بخش تقسیم کرد که عبارتند از [4]،[10]:

- **پیام‌های زمان بحرانی:** پیام‌هایی که زمان اعتبار آنها محدود است و باید بازه زمان از تولید تا دریافت پیام کمتر از زمان سطح آستانه باشد در غیر این صورت پیام نامعتبر در نظر گرفته می‌شود. بر همین اساس این پیام‌ها را نباید میان‌گیر[۲] کرد.
- **پیام‌های زمان غیر بحرانی:** پیام‌هایی که زمان اعتبار آنها محدود نیست و فقط لازم است پس از ارسال توسط فرستنده نیز توسط گیرنده دریافت شود.

در شبکه‌های هوشمند از پیام‌های زمان بحرانی برای پیام‌های مانیتورینگ، کنترل و حفاظت تجهیزات الکترونیکی بر روی زیرساخت‌های فیزیکی استفاه می‌شود. باتوجه به حساسیت این پیام‌ها نیازمندی‌هایی برای آنها وجود دارد که عبارتند از [10]،[11]:

- باید دارای بیشترین اولویت در پردازش باشند؛
- فرآیند پردازش باید به‌صورت ساده و با کمترین سربار مخابراتی باشد؛
- باید از صف و بافرکردن آنها اجتناب شود.

طبق تعریف‌های انجام‌شده می‌توان دسته‌بندی جدیدی مبتنی بر نوع جمینگو مخابرات تعریف کرد که عملیات جمینگ را بر روی پیام‌های زمان بحرانی را انجام می‌دهد، این تقسیم‌بندی به‌صورت زیر است [12]:

- هماهنگ- غیر واکنشی
- هماهنگ- واکنشی
- غیرهماهنگ- واکنشی
- غیرهماهنگ- غیر واکنشی

برای بیان عملیات جمینگ لازم است آشکارسازی حملات جمینگ در برابر شبکه‌های بی‌سیم زمان بحرانی مدل‌سازی کرد. در ادامه پارامتر به نام نرخ پیام نامعتبر برای کمیت‌سازی عملکرد کاربردهای زمان بحرانی معرفی می‌شود. طبق بررسی‌های انجام‌شده نشان داده شده که رفتار جمر برای تخریب پیام‌های زمان بحرانی همانند رفتار یک قمارباز برای برنده‌شدن در بازی قمار است. برهمین اساس در ادامه رفتار یک قمارباز در بازی قمار مورد بررسی و همچنین این رفتار با عملکرد یک جمر مورد انطباق قرار می‌گیرد [13].

۳-مسئله ورشکستگی قمار باز

فرض کنیم یک قمارباز قصد دارد با دارایی اولیه خود وارد بازی قمار شود و درنهایت بتواند مقدار پول مدنظر خود را از بازی‌هایی شده به‌دست آورد. قمارباز برای رسیدن به هدفش باید به چند نکتهٔ زیر توجه کند [14]،[15]:

- هرکس برای ورود به بازی قمار نیازمند یک سرمایه اولیه است که بتواند در بازی شرکت کند.
- اگر در هر مرحله از بازی برنده شود، بر اساس قوانین بازی مقدار مشخصی جایزه دریافت می‌کند. این مقدار جایزه براساس قوانین، قابل تغییر است.
- اگر در مرحله‌ای از بازی بازنده شود، باید براساس قوانین بازی مقداری از سرمایه خود را از دست بدهد. این مقدار براساس قوانین قابل تغییر است.
- بازی برای قمارباز در دو حالت به پایان می‌رسد.

۱ . قمار باز به هدف اصلی خود برسد و تمامی سرمایه‌ها را جمع‌آوری کند. در این صورت قمارباز برنده شناخته می‌شود.

۲ . قمارباز تمامی سرمایه خود را از دست بدهد و دیگر سرمایه‌ای برای ادامه بازی نداشته باشد. در این صورت از بازی اخراج می‌شود و به‌عنوان بازنده شناخته می‌شود.

- در بازی امکان هیچ‌گونه تقلبی وجود ندارد و فقط باید براساس قوانین، بازی انجام شود.

حال برای شناخت بهتر مسئله یک بازی قمار را مبتنی بر معادلات ریاضی مدل می‌کنیم:

فرض کنیم قمارباز با سرمایه اولیهٔ یک دلار وارد بازی شود؛ البته الزامی برای داشتن یک دلار نیست. امکان دارد با i دلار بازی را شروع کند، تنها قیدی موجود این است که $0 < i < N$ یک باشد، چرا که هدف قمارباز رسیدن به مقدار N دلار است. احتمال آنکه در هر مرحله برنده شود p و احتمال شکست آن q=1-p است. فرض کنیم میزان دارایی قمارباز در هر مرحله به‌صورت زیر است:

$$R_n = \delta_1 + \ldots + \delta_n, \qquad R_0 = i,$$

این رابطه بیان می‌کند که دارایی اولیه قمارباز i دلار است و در هر مرحله درصورت برد یک دلار به دارایی‌اش اضافه و درصورت باخت یک دلار از دارایی نخست کاسته می‌شود. در جایی که δ_n به‌صورت یک دنباله i.i.d (مستقل و توزیع یکسان) از مقادیرتصادفی به‌گونه‌ای که

$$P(\delta = 1) = p, \qquad P(\delta = -1) = q = 1 - p$$

همچنین شرایط توقف بازی را به‌صورت زیر می‌توان نشان داد:

$$R_n = 0, \quad R_n = N$$

پس نخستین زمان چنین رخدادی را به‌صورت زیر می‌توان مدل کرد:

$$\tau_i = min\{n \geq 0 : R_n \in \{0, N\} | R_0 = i\}$$

این رابطه نشان می‌دهد، که زمانی قمارباز متوقف می‌شود که دارای سرمایه اولیه $R_0 = i$ باشد. برای مشخص‌شدن نوع برد و یا باخت می‌توان چنین بیان کرد، اگر $R_{\tau_i} = N$ قمارباز برنده و اگر $R_{\tau_i} = 0$ قمارباز بازنده شده است؛ پس می‌توان احتمال پیروزی قمارباز با سرمایه اولیه $R_0 = i$ را به‌صورت زیر نشان داد:

$$\begin{cases} P_i = P(R_{\pi_i} = N), & 1 \leq i \leq N-1 \\ P_0 = 0, & P_N = 1 \end{cases} \qquad (۱)$$

ایده اصلی این کار مبتنی بر بازی نخست قمارباز است که دو حالت برای او ممکن است؛ یا برنده می‌شود و سرمایه‌اش افزایش می‌یابد $\tau_i = 1$ یا بازی را واگذار می‌کند و سرمایه‌اش کاهش می‌یابد $\tau_i = -1$ با این توصیف می‌توان روند بازی را با رابطه زیر بیان کرد.

$$P_i = pP_{i+1} + qP_{i-1} \qquad (۲)$$

این رابطه چنین توصیف می‌شود که:

- اگر $\tau_i = 1$ پس سرمایه قمارباز در کل افزایش می‌یابد؛ به‌گونه‌ای که می‌توان بیان کرد $R_1 = i+1$ و به‌وسیله خاصیت مارکوف می‌توان بیان کرد که قمارباز با احتمال P_{i+1} برنده خواهد شد.
- اگر $\tau_i = -1$ پس سرمایه قمارباز در کل کاهش می‌یابد؛ به‌گونه‌ای که می‌توان بیان کرد $R_1 = i-1$ و به‌وسیله خاصیت مارکوف می‌توان بیان کرد که قمارباز با احتمال P_{i-1} برنده خواهد شد.

حال می‌توان رابطه بالا را به‌صورت زیر بازنویسی کرد:

$$\begin{cases} p+q=1 \\ P_i = pP_{i+1} + qP_{i-1} \end{cases} \Rightarrow (p+q)P_i = aP_{i+1} + qP_{i-1} \quad (۳)$$

پس:

$$P_{i+1} - P_i = \frac{q}{p}(P_i - P_{i-1}) \quad (۴)$$

اگر داشته باشیم $i=1$ آنگاه:

$$\begin{cases} P_2 - P_1 = \frac{q}{p}(P_1 - P_0) \\ P_0 = 0 \end{cases} \Rightarrow P_2 - P_1 = \frac{q}{p}(P_1) \quad (۵)$$

اگر داشته باشیم $i=2$ آنگاه:

$$\begin{cases} P_3 - P_2 = \frac{q}{p}(P_2 - P_1) \Rightarrow \\ P_3 - P_2 = (\frac{q}{p})^2(P_1) \end{cases} \quad (۶)$$

پس می توان نتیجه گرفت که:

$$P_{i+1} - P_i = (\frac{q}{p})^i P_1, \quad 0 < i < N \Rightarrow \quad (۷)$$

$$\begin{cases} P_{i+1} - P_1 = \sum_{k=1}^{i}(P_{k+1} - P_k) = \sum_{k=1}^{i}(\frac{q}{p})^k P_1 \Rightarrow \\ P_{i+1} = P_1 \sum_{i}^{k=0}(\frac{q}{p})^k \end{cases} \quad (۸)$$

پس خواهیم داشت که:

$$P_{i+1} = \begin{cases} P_1 \frac{1-(\frac{q}{p})^{(i+1)}}{1-(\frac{q}{p})} & if \quad p \neq q \\ P_1(i+1) & if \quad p = q = 0.5 \end{cases} \quad (۹)$$

چون داریم $PN=1$ آنگاه:

$$1 = P_N = \begin{cases} P_1 \frac{1-(\frac{q}{p})^N}{1-(\frac{q}{p})} & if \quad p \neq q \\ P_1 N & if \quad p = q = 0.5 \end{cases} \quad (۱۰)$$

$$P_1 = \begin{cases} \frac{1-(\frac{q}{p})}{1-(\frac{q}{p})^N} & if \quad p \neq q \\ \frac{1}{N} & if \quad p = q = 0.5 \end{cases} \quad (۱۱)$$

پس خواهیم داشت:

$$P_i = \begin{cases} \frac{1-(\frac{q}{p})^i}{1-(\frac{q}{p})^N} & if \quad p \neq q \\ \frac{i}{N} & if \quad p = q = 0.5 \end{cases} \quad (۱۲)$$

طبق روابط بیان‌شده برای ادامه بازی دو حالت ایجاد می‌شود:

- اگر احتمال پیروزی $p>۰٫۵$ آنگاه داریم $1 > \frac{q}{pq}$ پس در طولانی مدت:
- اگر احتمال پیروزی $p<۰٫۵$ آنگاه داریم $1 < \frac{q}{pq}$ پس در طولانی مدت:

$$\lim_{N\to\infty} P_i = 0, \quad p \leq 0.5$$

۴- انطباق جمینگ به بازی قمار

همان‌طور که در بخش‌های قبل بیان شد، بهترین تعریف برای عملکرد جمر استفاده از مسئله شکست قمار باز است که در بخش قبل به‌صورت کامل بیان شد؛ حال در این بخش قصد داریم نگاشت مسئله شکست قمارباز به عملکرد جمر توضیح دهیم [13].

فرض کنید قمارباز دارای سرمایه اولیه d_0است، در مرحله nام دو حالت وجود دارد:

۱. با احتمال P_a برنده می‌شود و به مقدار d_n دلار به سرمایه او اضافه می‌شود. این اتفاق را با رخداد A می‌توان نشان داد؛ به‌عبارت دیگر داریم:

$$1_A = \begin{cases} 1 & if \quad A\ occurs \\ 0 & if \quad otherwise \end{cases} \quad (۱۳)$$

۲ . بااحتمال q=1-p بازنده می‌شود و به مقدار

$$\frac{p_a}{1-p_a} E(d_n)$$

سرمایه از دست می‌دهد. این اتفاق با رخداد A^c به‌صورت زیر نشان داده می‌شود:

$$1_{A^c} = \begin{cases} 1 & if \quad A^c \ occurs \\ 0 & if \quad otherwise \end{cases} \qquad (۱۴)$$

پس می‌توان میزان دارایی قمارباز را در مرحله nام به‌صورت زیر نشان داد:

$$X_0 = d_0, \qquad X_n = X_{n-1} + \zeta_n \quad (n \in N) \qquad (۱۵)$$

در این فرمول مقدار ζ_n میزان پاداش قمارباز در مرحله n است که می‌توان به‌صورت زیر تعریف کرد:

$$\zeta_n = d_n 1_A - \frac{p_a}{1-p_a} E(d_n) 1_{A^c} \qquad (۱۶)$$

طبق لم ارائه‌شده در [13] فرآیند $\{X_n\}$ مارتینگل است. به‌عبارت دیگر برای این فرآیند سه شرط مارتینگل صدق می‌کند؛ این شروط عبارتند از:

۱ . فرآیند $\{X_n\}$ وابسته به فیلتر $\{F_n\}$ و X_n قابل اندازه‌گیری با F_n باشد؛

۲ . برای هر $n \in N$ داشته باشیم $E|\zeta i| > \infty$؛

۳ . همواره $E(X_n \mid F_{n-1}) = X_{n-1}$

پس می‌توان گفت پول قمارباز دارای ساختار مارتینگل است. حال می‌توان مفهوم جدیدی را به نام نرخ پیام نامعتبر مطرح کرد. درواقع این نرخ برابر است با احتمال شکست قمارباز در بازی قمار است.

برهمین اساس برای فهم بهتر مسئله، دو فرآیند زیر تعریف می‌شود که نتیجهٔ حاصله نرخ پیام نامعتبر را بیان می‌کند [16].

۱. فرض کنیم فرآیند n_1 بیان‌کنندهٔ کوچک‌ترین کران بالای حالت زیر است:

$$n_1 = inf\{X_n < X_{n-1}\} \qquad n \in N \qquad (۱۷)$$

درواقع این فرآیند تنها زمانی رخ می‌دهد که $\zeta_n > 0$ که بیان‌کننده این است که در مرحلهٔ nام بازی رخداد A^c اتفاق بیافتد. به‌عبارت دیگر n_1 کمینه زمانی است که قمارباز پول از دست می‌دهد.

۲ . فرض کنیم فرآیند n_2 بیان‌کننده کوچک‌ترین کران بالای حالت زیر است:

$$n_2 = inf\{X_n < \delta\} \qquad n \in N \qquad (۱۸)$$

در واقع این فرآیند زمانی رخ می‌دهد که میزان دارایی قمارباز بیشتر از سطح آستانه یا هدفش از انجام بازی باشد. به‌عبارت دیگر n_2 کمینه زمانی است که قمارباز به هدفش می‌رسد.

۳ . فرض کنیم $\{n_1 > n\}$ آنگاه خواهیم داشت:

$$\{n_1 > n_2\} \Rightarrow \{X_n < X_{n-1}\} \qquad (۱۹)$$

از این فرآیند می‌توان دریافت که :

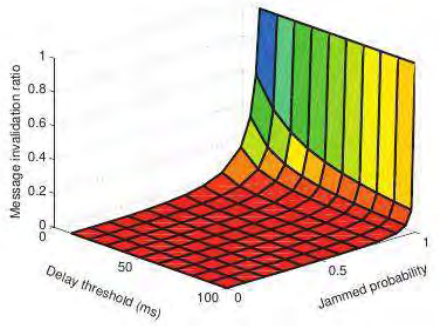
- رخداد باختن قمارباز هرگز قبل از پیروزی او رخ نمی‌دهد.
- همچنین قمارباز تا رسیدن به هدفش هیچ‌یک از بازی‌ها را از دست نمی‌دهد.

۴ . بر همین اساس می‌توان نرخ پیام نامعتبر را به‌صورت زیر تعریف کرد:

$$\begin{cases} r = P(n_1 > n_2) \Rightarrow n_{stop} = min(n_1, n_2) \\ X_{n_{stop}} = X_{n_1 1\{n_1 < n_2\}} + X_{n_2 1\{n_1 > n_2\}} \end{cases} \qquad (۲۰)$$

در اینجا X_{n1} میزان پول قمارباز پس از نخستین باخت، X_{n1-1} میزان پول قمارباز قبل از نخستین باخت است. اگر فرض کنیم نگاشت بین قمارباز و جمر به‌صورت زیر باشد، آنگاه داریم که:

- قمارباز = جمر
- هدف قمارباز (بردن تمامی بازی‌ها و رسیدن به دارایی مد نظر=) انجام عمیات جمینگ و جمر تمامی بسته‌ها
- شکست قمارباز (ازدست‌دادن دست‌کم یک بازی)= ناتوانی درجمینگ حداقل یک بسته و دریافت سالم آن توسط گیرنده پس می‌توان پارامترهای زیر را تعریف کرد:
- $D_s \leq \delta$ میزان تأخیر انتهابه‌انتها از یک پیام تحویل داده‌شده موفق کوچک‌تر مساوی با سطح آستانه تأخیر پیام
- $D_u > \delta$ تأخیر تحویل پیام ناموفق بیشتر از سطح آستانه تأخیر پیام
- $c = E(d_i)$ میانگین تأخیر لایه MAC



(شکل-۲): نمودار تغییرات نرخ

پیام نامعتبر برای زمان بحرانی در جمینگ واکنشی پس می‌توان رابطه (۱۵) را به‌صورت زیر بازنویسی کرد:

$$\begin{cases} X_{n_1} = X_{n_1-1} - \frac{p_a E(d_{n_1})}{1-p_a} = D_s - \frac{p_a c}{1-p_a} \\ X_{n_2} = D_u \end{cases} \quad (۲۱)$$

از آنجا که $\{X_n\}$ مارتینگل است و زمان توقف n_{stop} محدودشده به‌میزان سطح آستانه است پس با استفاده از تئوری Doob's optional sampling می‌توان زمان توقف فرآیند ماتینگل $\{X_n\}$ را به‌صورت زیر نوشت [14]:

$$\begin{cases} E(X_{n_{stop}}) = E(X_0) \Rightarrow \\ E(X_{n_{stop}}) = E(X_{n_1})P(n_1 < n_2) + E(X_{n_2})P(n_1 > n_2) \\ = (1-r)(E(D_s) - \frac{p_a c}{1-p_a}) + rE(D_u) \\ = E(X_0) = E(d_0) \\ r = \frac{E(D_s) - \frac{c}{1-p_c}}{E(D_s) - \frac{p_c c}{1-p_a} - E(D_u)} \end{cases} \quad (۲۲)$$

با فرض اینکه

$$\begin{cases} \frac{1}{1-p_a} = 1 + \frac{p_a}{1-p_a} \\ c = E(d_i) \le E(d_s) \Rightarrow \\ r \le \frac{p^{Nmac} c}{(1-p^{Nmac})(\delta - c) + p^{Nmac} c} \end{cases} \quad (۲۳)$$

همان‌طورکه در شکل (۲) نشان داده شده است، تغییرات نرخ پیام خطا نسبت به احتمال تخریب پیام دارای دو شیب بالارونده کند و تند است که بیان‌گر این مسئله است که در pهای کوچک تأثیر خاصی بر روی نرخ پیام نامعتبر ندارد؛ ولی هرچه این احتمال بیشتر، نرخ پیام نامعتبر بیشتر می‌شود.

۴-۱- جمینگ در شبکه هوشمند انرژی

با توجه به توضیحات داده‌شده حالا می‌توان عملیات جمینگ را برای هریک از نوع مخابرات‌های هماهنگ و ناهماهنگ بیان کرد. فرض کنیم زمان سطح آستانه برای پیام‌های زمان بحرانی δ و میزان تأخیر در هر مرحله ارسال پیام d_i باشد و مجموع تأخیرها نیز D در نظر گرفته شود.

$$D = \sum_{i=1}^{k} d_i \quad (۲۴)$$

از آنجا که تعداد گره‌های یک شبکه محلی در یک استخر کانال قرار دارند، باید در بررسی میزان نرخ پیام‌های نامعتبر علاوه‌بر تأثیر جمر میزان تداخل پیام گره‌ها را درنظر گرفت. در حالت کلی فرآیند جمینگ به‌صورت یک فرآیند تجدیدپذیر مارکوف است [12]. درواقع یک فرآیند تجدیدپذیر است که از ویژگی زنجیره مارکوف پیروی می‌کند. برای فهم بهتر این مسئله هریک از فرآیندهای تجدیدپذیر، زنجیره مارکوف و سایر فرآیندهایی همچون پواسون، مارکوف در ادامه توضیح داده خواهد شد.

بر همین اساس فرآیند جمینگ را به‌صورت زیر می‌توان نشان داد:

$$((F,C),X) = \{F_k, C_k, X_k | k = 1, 2, ...\} \quad (۲۵)$$

به‌گونه‌ای که X_k بازهٔ تجدیدپذیر جمینگ در حالت k که می‌خواهد کانال فرکانس کد (F_k,C_k) را هدف قرار دهد. همچنین پارامتر s نشان‌دهنده تعداد کانال‌های جمر است به عبارت دیگر این پارامتر نشان می‌دهد جمر می‌تواند هم‌زمان s کانال را به‌صورت هم‌زمان مورد حمله قرار دهد.

همان‌طور که بیان شد پارامتر نرخ پیام نامعتبر بیان‌کننده احتمالی است که پیام تخریب شود که این تخریب یا به‌وسیله تصادم سیگنال گره‌ها یا به‌وسیله حمله جمر رخ می‌دهد؛ اما در هر دو صورت مجموعه تأخیرهای رخ‌داده باید از سطح آستانه بیشتر باشد، به‌عبارت دیگر می‌توان بیان کرد که:

$$r = P(D > \delta) \quad (۲۶)$$

همچنین می‌دانیم که نرخ پیام‌های زمان بحرانی λ_j در گره‌های شبکه هوشمند ثابت است بر همین اساس پارامتر زیر را تعریف می‌کنیم:

$$\gamma_k = \sum_{j=1, j\neq k}^{m} \lambda_j \qquad (۲۷)$$

اگر فرض کنیم زمان T_l بازه ارسال پیام و δ زمان سطح آستانه تأخیر پیام باشد، آن‌گاه پارامتر زیر بیان‌گر تعداد ارسال‌های ممکن را نشان می‌دهد:

$$\lfloor \frac{\delta}{T_l} \rfloor \qquad (۲۸)$$

همان‌طورکه بیان شد، احتمال پیام نامعتبر ناشی از تصادم پیام گره‌ها و عملیات جمینگ است، پس نرخ پیام نامعتبر را به‌صورت زیر می‌توان نوشت:

$$r = P(D > \delta) = P(\cap_{i=1}^{\frac{\delta}{T_l}} (J_i \cup C_i)) \qquad (۲۹)$$

که C_i بیان‌گر تصادم پیام ها و J_i بیانگر عملیات جمینگ است.

قبل از بیان نرخ پیام نامعتبر برای مخابرات و جمرهای گوناگون نیز احتمالرخداد تصادم را مورد بررسی قرار می دهیم [13]،[12].

۴-۲- احتمال تصادم

اگر فرض کنیم ρ احتمال پیام نامعتبر باشد، پس $(1-\rho)$ احتمال پیام معتبر بیان می‌کند. برای آن که یک تصادم موفق برای گره یک رخ دهد لازم است گره دیگری تلاش کند در بازهٔ $[-(1-\rho)T_l,(1-\rho)T_l]$ در همان کانال پیامی ارسال کند.

از آنجا که تعدا کل گره‌ها mتا و نرخ ترافیک گره‌ها ثابت، پس به تعداد:

$$2(1-\rho)T_l \sum_{j=2}^{m} \lambda_j$$

تصادم بین سایر گره‌ها با گره یک ممکن است [12]. از آنجا که در استخر کانال به تعداد N_f فرکانس و به تعداد N_c کد وجود دارد و کانال کد فرکانس به صورتی کنواخت اختصاص داده می‌شود پس احتمال تصادم برای گره یک به‌صورت زیر محاسبه می‌شود:

$$P(C_1) = 1 - (1 - \frac{1}{N_f N_c})^{2(1-\rho)T_l\gamma_1} \qquad (۳۰)$$

پس برای گره iام داریم:

$$P(C_i) = 1 - (1 - \frac{1}{N_f N_c})^{2(1-\rho)T_l\gamma_i} \qquad (۳۱)$$

۴-۳- جمینگ غیر واکنشی هماهنگ

در این نوع جمینگ از مخابرات نوع هماهنگ استفاده می‌شود و جمر از نوع غیرواکنشی است، پس نرخ پیام نامعتبر به‌صورت زیر است [12]:

$$r = P(D_k > \delta) \leq [1-(1-\frac{1}{N_f N_c})^{2(1-\rho)T_l\gamma_k}(1-\frac{(1-\rho)s}{\rho N_f N_c})]^{\frac{\delta}{T_l}} \qquad (۳۲)$$

همان‌طورکه بیان شد، نرخ پیام نامعتبر از دو بخش تصادم و جمینگ تشکیل شده است، در فرمول ۳۱ می‌بینید که احتمال تصادم برابر است با

$$(1 - \frac{1}{N_f N_c})^{2T_l(1-\rho)\gamma_k}$$

و احتمال جمر برابر است با

$$(1 - \frac{(1-\rho)s}{\rho N \ N_c})$$

که در این بخش مورد بررسی قرار می‌گیرد.

اگر فرض کنیم پارامتر X_l بیان‌گر بازهٔ زمان فرآیند تجدیدپذیر جمینگ باشد، پس فرآیند تجدیدپذیر زیر را خواهیم داشت که بیان‌کننده بزرگ‌ترین کران پایین برای بازه پیام جمر شده است؛ چون برای جمینگ موفق باید بازه انتقال پیام‌های جمر از بازه پیام‌های ارسال موفق کمتر باشد.

$$N_i = \sup_{n\in N}\{\sum_{l=1}^{n} X_l < (1-\rho)T_l\}, \qquad N = \{0,1,2,...\} \qquad (۳۳)$$

فرض کنیم B_l رخداد lامین بازه با طول X_l بر روی کانال (i,j) پس اگر $X_1,...X_{N_i}$ بازه‌های جمینگ در خلال iامین ارسال باشد، در نتیجه برای داشتن یک جمینگ موفق روی کانال (i,j) باید بازه جمینگ از زمان پیام نامعتبر ρT_l بیشتر باشد، پس می‌توان داشت:

$$\begin{cases} B_l = \{u_i \in F_l, v_i \in C_l\} \\ P(J_j|u_i,v_i) = P(\sum_{l=1}^{N_i} X_l 1_{B_l} \geq \rho T_l) \end{cases} \qquad (۳۴)$$

طبق ویژگی عمومی جمینگ که یک فرآیند مارکوف تجدیدپذیر است، با استفاده از خاصیت مارکوف می‌توان نوشت:

$$\begin{cases} P(X \geq a) \leq \frac{E(x)}{a} \\ P(J_i|u_i, v_i) \leq E(\frac{\sum_{l=1}^{N_i} X_l 1_{B_l}}{\rho T_l}) \frac{E(N_i)E(X_l)P(B_l)}{\rho T_l} \end{cases} \quad (۳۵)$$

با توجه به خاصیت فرآیندهای تجدیدپذیر خواهیم داشت:

$$E(N_i) = (\frac{(1-\rho)T_l}{E(X_l)})$$

از طرفی $P(B_l)$ بیان‌گر احتمال تصادم جمر با گره‌های شبکه است و چون s نشان‌دهندهٔ کانال‌های هم‌زمان جمر است، پس داریم که:

$$P(B_l) = \frac{s}{N_f N_c}$$

پس با جای‌گذاری در رابطه ۳۵ خواهیم داشت:

$$\begin{cases} P(J_i) \leq (\frac{(1-\rho)T_l}{E(X_l)}) E(X_l) \frac{s}{N_f N_c} \frac{1}{\rho T_l} \Rightarrow \\ P(J_i) \leq \frac{(1-\rho)s}{\rho N_f N_c} \end{cases} \quad (۳۶)$$

پس احتمال جمینگ در مخابرات هماهنگ غیر واکنشی اثبات شد.

۴-۴- جمینگ واکنشی هماهنگ

تفاوت این نوع جمینگ با جمینگ غیر واکنشی هماهنگ در این است که بازه تجدیدپذیر جمینگ X_l در غیرواکنشی هماهنگ از پیش تعریف شده بود؛ ولی در این نوع مبتنی بر عملکرد شبکه است؛ به عبارت دیگر در این نوع داریم:

$$X_l = \tau + S_l 1_A \quad (۳۷)$$

که τ زمان حس‌کردن کانال توسط جمر است، این مقدار می‌تواند بسیار ناچیز باشد؛ چون وابسته به فناوری ساخت جمر است. مقدار S_l بازهٔ جمینگ و 1_A تابع رخداد جمینگ است. برای بیشینه‌کردن آسیب به شبکه توسط جمر واکنشی باید بازه جمینگ برابر $S_l = \rho T_l$ باشد. برهمین اساس نرخ پیام نامعتبر برای این نوع جمینگ به‌صورت زیر محاسبه می‌شود [12]:

$$\begin{cases} r = P(D_k > \delta) \leq \\ [1 - (1 - \frac{1}{N_f N_c})^{2(1-\rho)T_l \gamma_k} (1 - \frac{sT_l}{\frac{\tau N_f N_c}{1-\rho} + \rho T_l^2 \gamma_k})]^{\frac{\delta}{T_l}} \end{cases} \quad (۳۸)$$

همان‌طورکه مشاهده می‌شود، قسمت تصادم با غیرواکنشی هماهنگ یکسان است و فقط قسمت جمر متفاوت است که در این قسمت به این مطلب می‌پردازیم:

فرض کنیم iامین ارسال پیام در زمان 0 شروع شده است؛ پس فرآیند تجدیدپذیر $N_i(t)$ کوچک‌ترین کران بالا مجموعه زمان‌هایی در نظر می‌گیرم که بازهٔ جمینگ از زمان مد نظر کمتر باشد؛ پس داریم:

$$N_i(t) = \sup_{n \in N} \{\sum_{l=1}^{n} X_l < t\}, \qquad N = \{0, 1, 2, ...\} \quad (۳۹)$$

به‌منظور اختلال موفق در iامین کانال J_i، جمر واکنشی باید دست‌کم یکبار در بازهٔ $[0,(1-\rho)T_l - \tau]$ به کانال (u_i, v_i) مراجعه کند.

$$\begin{cases} P(J_i|u_i, v_i) = P(\sum_{l=1}^{N_i((1-\rho)T_l - \tau)} 1_{B_l} \geq 1) \Rightarrow \\ P(J_i) \leq E(\sum_{l=1}^{N_i((1-\rho)T_l - \tau)} 1_{B_l}) \Rightarrow \\ P(J_i) \leq E(N_i[(1-\rho)T_l - \tau]) P(B_l) \end{cases} \quad (۴۰)$$

طبق خاصیت فرآیند تجدیدپذیر داریم که:

$$\lim_{t \to \infty} \frac{E(N_i(t))}{t} = \frac{1}{E(X_l)} \quad (۴۱)$$

از طرفی داریم:

$$\begin{cases} X_l = \tau + S_l 1_A \\ E(X_l) = \tau + \rho T_l P(A) \end{cases} \quad (۴۲)$$

و $P(A)$ احتمال اینکه کانال مشغول حس شود:

$$P(A) = (1 - \frac{1}{N_f N_c})^{2T_l(1-\rho)\gamma_k} \quad (۴۳)$$

از طرفی چون $\tau \ll T_l$ و بازه تجدیدپذیر $E(X_l \ll T_l)$ پس داریم که:

(۴۴)

$$\begin{cases} 40, 41 \Rightarrow E(N_i((1-\rho)T_l - \tau)) \simeq \frac{(1-\rho)T_l - \tau}{E(X_l)}, 42 \simeq \\ \frac{(1-\rho)T_l}{E(X_l)} = \\ \begin{cases} \frac{(1-\rho)T_l}{\tau + \rho T_l - \rho T_l (1 - \frac{1}{(N_f N_c)^{(1-\rho)T_l \gamma_1}})} \\ (1-x)^a \simeq 1 - ax \end{cases} \Rightarrow \simeq \frac{(1-\rho)T_l}{\tau + \frac{\rho(1-\rho)T_l^2 \gamma_1}{N_f N_c}} \end{cases}$$

پس داریم که:

$$P(J_j) \leq \frac{(1-\rho)sT_l}{\tau N_f N_c + \rho(1-\rho)T_l^2 \gamma_1} \quad (۴۵)$$

بدین ترتیب بخش جمر در جمینگ واکنشی هماهنگ هم اثبات شد.

۴-۵- جمینگ غیر واکنشی غیر هماهنگ

تفاوت این جمینگ با جمینگ غیر واکنشی هماهنگ فقط در بخش نوع مخابرات است که در این نوع مخابرات گره‌ها ابتدا باید یکدیگر را پیدا و بعد با هم ارتباط برقرار کنند برهمین اساس با احتمال $\frac{1}{N_f N_c}$ گره‌ها یکدیگر را پیدا می‌کنند. فرض کنیم $P(J_i)$ احتمال جمینگ و $P(C_i)$ احتمال تصادم باشد؛ پس $(1-P(J_i))$احتمال عدم جمینگ و $(1-P(C_i))$ احتمال عدم تصادم است؛ از طرفی طبق این فرض و فرمول ۳۲ می‌توان نوشت:

$$r = P(D_k > \delta) \leq [1-(1-P(C_i))^{2T_l(1-\rho)\gamma_k}(1-P(J_i))]^{\frac{\delta}{T_l}} \quad (۴۶)$$

پس اگر پارامتر ψ به‌عنوان احتمال ارسال پیام سالم بدانیم پس داریم:

$$r = P(D_k > \delta) \leq [1-\psi]^{\frac{\delta}{T_l}} \quad (۴۷)$$

از آنجا که در این جمینگ گره‌ها با احتمال $\frac{1}{N_f N_c}$ گره‌ها یکدیگر را پیدا می‌کنند، پس داریم که:

$$r = P(D_k > \delta) \leq [1-\psi\frac{1}{N_f N_c}]^{\frac{\delta}{T_l}} \quad (۴۸)$$

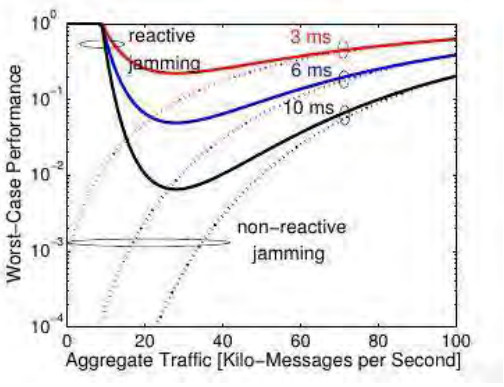
از آنجا که تفاوت این جمینگ با جمینگ غیر واکنشی هماهنگ فقط در بخش نوع مخابرات است؛ پس داریم [12]:

$$\begin{cases} r = P(D_k > \delta) \leq [1-(1-\frac{1}{N_f N_c})^{2T_l(1-\rho)\gamma_k}\frac{1}{N_f N_c} \\ (1-\frac{(1-\rho)s}{\rho N_f N_c})]^{\frac{\delta}{T_l}} \end{cases} \quad (۴۹)$$

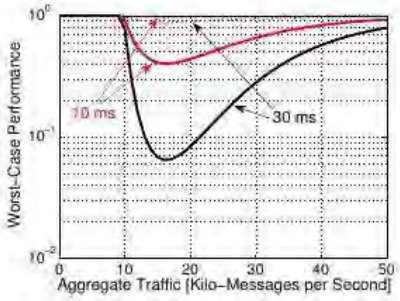
۴-۶- جمینگ واکنشی غیر هماهنگ

تفاوت این جمینگ با جمینگ واکنشی هماهنگ فقط در بخش نوع مخابرات است و طبق توضیحات داده‌شده در بخش قبل داریم که [12]:

$$\begin{cases} r = P(D_k > \delta) \leq [1-(1-\frac{1}{N_f N_c})^{2T_l(1-\rho)\gamma_k}\frac{1}{N_f N_c} \\ (1-\frac{sT_l}{\frac{\tau N_f N_c}{1-\rho}+\rho T_l^2\gamma_k})]^{\frac{\delta}{T_l}} \end{cases} \quad (۵۰)$$



(شکل-۳): تابع U برای مخابرات هماهنگ



(شکل-۴): تابع U برای مخابرات غیرهماهنگ

۴-۷-کمترین نرخ پیام نامعتبر

همان‌طورکه در فرمول‌های نرخ پیام نامعتبر برای جمینگ‌های مختلف دیده می‌شود، تنها عامل قابل تغییر توسط گره‌ها در این نرخ، مجموعه نرخ ترافیک سایرگره‌ها یعنی γ_k است. اگر فرمول‌های نرخ پیام نامعتبر مبتنی بر این متغیر بنویسیم با فرض اینکه مقادیر ثابت $0 < A_i > 1$ و $B_0 \geq 1$ آنگاه خواهیم داشت که:

$$\begin{cases} r = P(D_k > \delta) \leq [1-(A_1)^{\gamma_k}A_2]^{B_0} \\ r = P(D_k > \delta) \leq [1-(A_1)^{\gamma_k}\frac{A_3}{A_4+\gamma_k}]^{B_0} \end{cases} \quad (۵۱)$$

همان‌طورکه در شکل‌های (۳) و (۴) می‌بینید، تغییرات نرخ پیام نامعتبر نسبت بهγ_k به‌صورت یک تابع U شکل است. با توجه به اینکه این تابع دارای نقطه اکسترمم است، پس می‌توان مقدار کمینه این نرخ را نسبت به γ_k به‌دست آورد، آنگاه میزان γ_kبهینه که بیان‌کنندهٔ نرخ ترافیک بهینه گره‌ها و بار بهینه به‌دست می‌آید. از آنجا که بدترین نرخ پیام نامعتبر در جمر واکنشی است، پس محاسبات بار بهینه فقط برای این نوع جمر در نظر گرفته می‌شود.

با توجه به به‌دست‌آوردن نقاط اکسترمم می‌توان میزان γ_k بهینه برای جمینگ واکنشی هماهنگ به‌صورت زیر

به‌دست آورد. در ادامه ثابت می‌کنیم که این γ_kبرای جمینگ واکنشی غیرهماهنگ هم صدق می‌کند:

(۵۲)

$$\begin{cases} \gamma_k^* = \frac{1}{\rho(1-\rho)(T_l)^2}\left(\frac{c_1c_2-\sqrt{c_1^2c_2^2-4c_1c_2}\rho T_l}{2c_1} - \tau N_f N_c\right) \\ c_1 = 2\ln(1-\frac{1}{N_f N_c}) \\ c_2 = (1-\rho)T_l \end{cases}$$

از نکات مهم مقدار γ_k* این است که مستقل از سطح آستانه تاخیر δ است؛ پس تمامی تأخیر پیام‌ها با سطح آستانه متفاوت در بار ترافیکی بهینه می‌توانند کمینه شوند [12].

کمترین نرخ پیام برای جمینگ واکنشی غیرهماهنگ: اگر فرمول‌های نرخ پیام‌های نامعتبر برای جمینگ‌های واکنشی هماهنگ و واکنشی غیرهماهنگ را به‌صورت ساده‌شده مبتنی بر متغییر γ_k بنویسیم، آنگاه خواهیم دید:

$$\begin{cases} r = P(D_k > \delta) \le [1-(1-\frac{1}{N_f N_c})^{2T_l(1-\rho)\gamma_k} \\ \qquad (1-\frac{sT_l}{\frac{\tau N_f N_c}{1-\rho}+\rho T_l^2\gamma_k})]^{\frac{\delta}{T_l}} \\ r = P(D_k > \delta) \le [1-(1-\frac{1}{N_f N_c})^{2T_l(1-\rho)\gamma_k}\frac{1}{N_f N_c} \\ \qquad (1-\frac{sT_l}{\frac{\tau N_f N_c}{1-\rho}+\rho T_l^2\gamma_k})]^{\frac{\delta}{T_l}} \end{cases} \quad (۵۳)$$

پس با ساده‌سازی و معادل‌سازی داریک که:

$$\begin{cases} r = P(D_k > \delta) \le [1-(A_1^{\gamma_k})\frac{A_3}{A_4\gamma_k}]^{B_0} \\ r = P(D_k > \delta) \le [1-(A_1^{\gamma_k})\frac{1}{N_f N_c}\frac{A_3}{A_4\gamma_k}]^{B_0} \end{cases} \quad (۵۴)$$

همان‌طورکه در فرمول (۵۴) مشاهده می‌کنید، نرخ پیام‌های نامعتبر فقط در ضریب$\frac{1}{N_f N_c}$متفاوت است که این ضریب در به‌دست‌آوردن نقطه اکسترمم تأثیری ندارد، پس مقدا ر γ_k^*برای هر دو جمینگ واکنشی هماهنگ و غیرهماهنگ یکسان است.

۵-روش TACT

همان‌طورکه در بخش‌های قبلی نشان داده شد، بدترین نرخ پیام نامعتبر برای حالت جمینگ واکنشی بود؛ همچنین نشان داده شد که بار بهینه برای مخابرات هماهنگ و غیرهماهنگ یکسان است؛ ولی این سؤال پیش می‌آید که با این مقدار بار بهینه به‌دست آمده، می‌توان نرخ پیام نامعتبر را برای تمامی گره‌ها کمینه کرد؟ باید پاسخ داد نه، همان‌طورکه در فرمول‌های (۳۲)، (۳۸)، (۴۹) و (۵۰) نشان داده شد، نرخ پیام نامعتبر برای هر گره وابسته به مجموعه نرخ ترافیک سایر گره‌ها است که این نرخ‌ها وابسته به طول پیام‌های زمان بحرانی ارسالی توسط هر گره است؛ پس اگر بخواهیم نرخ پیام نامعتبر یکسانی برای تمامی گره‌ها در نظر بگیریم، به این معنی است که طول پیام‌های زمان بحرانی تمامی گره‌ها در تمامی زمان‌ها یکسان است؛ که این امر خلاف واقعیت است؛ چون امکان ندارد گره‌های مختلف در تمامی زمان‌ها دارای عملکرد یکسانی باشند که پیام‌های زمان بحرانی آنها یکسان باشد. برهمین اساس در [12] یک شیوهٔ ارسال تطبیقی ترافیک ابهام به‌نام TACT[1] ارائه شده است. این روش دارای دو نکته اساسی است که عبارتند از:

۱. در TACT باید از هماهنگ‌سازی گره‌ها اجتناب شود. به‌یقین هماهنگی گره‌ها می‌تواند به عملکرد تأخیر، کمک بیشتری کند؛ اما چالش امنیتی اضافی در تحویل پیام هماهنگ‌سازی تحت جمینگ را معرفی می‌کند. بنابراین TACT باید داری طبیعت توزیع شده باشد و کمینه پیچیدگی را به هماهنگی گره وارد کند.
۲. از آنجایی‌که تأخیر پیام بدترین حالت در بار ترافیکی مثبت کمینه می‌شود، TACT باید همواره برای افزایش بار ترافیکی تلاش کند. اگر عملکرد بعداز افزایش تنزل یافت می‌تواند بار را کاهش دهد.

هنگامی که TACT پیاده‌سازی می‌شود، سه نوع ترافیک عمده در شبکه وجود دارد:

۱. ترافیک عادی: برای کنترل و مانیتئورینگ استفاده می‌شود و نمی‌تواند تغییر کند و با تنظیمات دستگاه‌های قدرت تنظیم شده است.
۲. ترافیک کاوش: برای اندازه‌گیری عملکرد است و زمان ارسال پیام برابر باT_l است.
۳. ترافیک ابهام: برای متوازن‌کردن بار ترافیکی کلی شبکه است.

عملکرد در TACT به این صورت است که با استفاده از ترافیک کاوش میزان تحمل افزایش بار ترافیکی ابهام را در هر ارسال مورد بررسی قرار می‌دهد؛ اگر طبق بررسی انجام‌شده بار ترافیکی اضافه‌شده (ترافیک ابهام) مضر نباشد؛ پس در ارسال بعدی پیام ابهام بیشتری ارسال می‌کند و اگر مضر باشد، در ارسال بعدی میزان پیام را ابهام کاهش داده و تا اینکه این نوسان در اطراف نقطه بهینه صورت گیرد.

هنگامی‌که TACT در گره k پیاده‌سازی می‌شود، شروع به افزایش بار ترافیکی در گره k می‌کند که باعث

[1] transmitting adaptive camouflage traffic

افزایش λ_k می شود؛ ولی تأثیری در تأخیر گره k ندارد؛ چون مبتنی بر فرمول‌های (۳۲)، (۳۸)، (۴۹) و (۵۰) نرخ پیام نامعتبر وابسته به γ_kاست که طبق فرمول (۲۷) این پارامتر مستقل از λ_k است؛ پس افزایش ترافیک ابهام در گره k تأثیری در تأخیر گره k ندارد بلکه باعث بهبود تأخیر در سایر گره‌ها می‌شود. بر همین اساس گره k برای بهبود عملکرد نیازمند همین عملکرد از سایر گره‌ها است. بنابراین TACT به چنین رفتار هم‌گنی در همه گره‌ها استناد می‌کند. هرچند که نمی‌تواند هنگامی‌که گره‌ها نرخ ترافیک ناهمگون آشکار[۳] داشته باشند، عملکرد مناسبی تضمین کند. برای مثال فرض کنیم دو گره با نرخ ترافیک عادی ۱ و ۱۰۰۰ داریم که TACT برای آنها اعمال شده و بار بهینه تحت جمر غیرواکنشی برای آنها $\gamma_1^* = \gamma_2^* = 1000$ است، پس داریم که:

$$\gamma_2 = \sum_{j=1, j\neq 2}^{max} \lambda_j = 1$$

و

$$\gamma_1 = \sum_{j=1, j\neq 1}^{max} \lambda_j = 1000$$

هنگامی‌که TACT شروع شود گره دو از مقدار بهینه دور باشد به‌میزان زیادی بار ترافیکی بیشتری افزایش می‌دهد، ولی در مقابل گره یک به‌سرعت به مقدار بهینه می‌رسد و هرگز ترافیک بیشتری انتقال نمی‌دهد؛ پس درعمل گره دو به گره یک کمک کرده است؛ ولی گره ۱ به ۲ کمکی نکرده است. برهمین اساس باید علاوه‌بر ترافیک عادی یک بار ترافیک ابهام عادی با کمینه بار یکسان به‌صورت اجباری به تمامی گره‌ها اضافه تا عملکرد TACT تضمین شود. فرض کنیم به‌صورت خاص کمینه بار ترافیکی ابهام گره k برابر است با:

$$L_{\min -k} = \max_{1\leq i\leq m} (\alpha_i - \alpha_k)$$

که α_i نشان‌دهنده بار ترافیک عادی گره i است. بنابراین بار ترافیکی کل که باید توسط هر گره به‌صورت یکنواخت ارسال شود، برابراست با:

$$L_{\min -k} = \max_{1\leq i\leq m} \alpha_i$$

۶- فرآیندهای احتمالاتی مرتبط

همان‌طورکه در [12] بیان شد، در حالت کلی جمینگ یک فرآیند تجدیدپذیر مارکوف است. بر همین اساس در این بخش به بررسی فرآیند تجدیدپذیر مارکوف می‌پردازیم.

۶-۱- فرآیند تجدید پذیر مارکوف

درواقع فرآیند تجدیدپذیر مارکوف تعمیمی از فرآیند تجدیدپذیر (RP) است که دنباله زمان صرف‌شدهٔ یک فرآیند i.i.d نیست و توزیع فرآیند مبتنی بر زنجیره مارکوف است. اگر فرض کنیم S نشان‌دهندهٔ فضای حالت و X_n حالت‌های مختلف در زنجیره مارکوف باشد، از طرفی T_n زمان پرش از یک حالت به حالت دیگر است و τ اختلاف زمان بین پرش‌ها است آنگاه (X_n,T_n) نشان‌دهندهٔ یک متغییر تصادفی است که توصیف فرآیند مبتنی بر زنجیره مارکوف به‌صورت زیر است:

$$\begin{cases} P[\tau_{n+1} \leq \tau, X_{n+1} = j | (X_0, T_0), (X_1, T_1), ..., (X_n, T_n)] \\ = P[\tau_{n+1} \leq \tau, X_{n+1} = j | X_n = i] \end{cases} \quad (۵۵)$$

به‌عبارت دیگر در فرآیند تجدیدپذیر مارکوف رفتن به حالت $X_{n+1} = j$ و زمان ورود τ_{n+1} فقط وابسته به وضعیت جاری $X_n = i$ و مستقل از وضعیت‌های گذشته است [17]،[18]،[19].

۶-۲- فرآیند تجدیدپذیر

فرآیند تجدیدپذیر، توسعه‌ای از فرآیند پواسون است. اگر فرض کنیم دنباله $x_1, x_2, ...$ یک دنباله i.i.d از زمان بین دو ورود به‌صورت غیرمنفی باشد، به‌گونه‌ای که [19]،[20]:

$$x_1, x_2, ... \quad \sim iid \quad F(x)$$

از طرفی می‌توان مجموعه:

$$S_n = \sum_{i=1}^{n} x_i$$

و:

$$N(t) = \max\{n : S_n \leq t\}$$

که به مجموعه:

$$\{N(t)\}$$

نیز فرآیند تجدیدپذیر گویند. این فرآیند دارای ویژگی‌های زیر است:

اگر

$$\begin{cases} \mu = E[x_n] \\ m(t) = E[N(t)] \end{cases} \quad (۵۶)$$

$$\begin{cases} 1.P[N(t)=n] = P[S_n \le t] - P[S_{n+1} \le t] \\ \qquad = F_n(t) - F_{n+1} \\ 2.m(t) = E[N(t)] = \sum_{n=1}^{\infty} n(F_n(t) - F_{n+1}(t)) \\ \qquad = \sum_{n=1}^{\infty} F_n(t) \end{cases} \quad (۵۷)$$

حال می‌توان چهار ویژگی این فرآیند را به‌صورت زیر نشان داد:

$$\begin{cases} \lim_{n\to\infty} \frac{S_n}{n} = \mu \\ \lim_{t\to\infty} N(t) = \infty \\ \lim_{t\to\infty} \frac{N(t)}{t} = \frac{1}{\mu} \\ \lim_{t\to\infty} \frac{m(t)}{t} = \frac{1}{\mu} \end{cases} \quad (۵۸)$$

به‌منظور درک بهتر فرآیند تجدیدپذیر مفهوم این فرآیند را به‌صورت زیر می‌توان توضیح داد:

اگر یک فرآیند نقطه‌ای در نظر بگیریم به‌گونه‌ای که مجموعه‌ای از نقاط تصادفی t_i روی محور زمان قرار داشته باشند، پس می‌توان یک فرآیند تصادفی $x(t)$ تعریف کرد که نشان‌دهندهٔ تعداد نقاط t_i در فاصله $(0,t)$ باشد. برای مثال می‌توان به فرآیند پواسن اشاره کرد. اگر به هر فرآیند تصادفی t_i یک دنباله از متغییر تصادفی z_n نسبت دهیم به گونه‌ای که:

$$\begin{cases} Z_1 = t_1 \\ Z_2 = t_2 - t_1 \\ \ldots, \\ Z_n = t_n - t_{n-1} \end{cases} \quad (۵۹)$$

که در آن نزدیک‌ترین نقطه به مبدأ است؛ آنگاه فرآیند تجدیدپذیر شامل متغییرهای تصادفی z_i است، به‌طوری‌که [21]:

$$t_n = \sum Z_i$$

۶-۳- فرآیند پواسن

فرآیند پواسن: فرآیندی است که جریان تکرار رخدادها مستقل از هم است؛ به‌گونه‌ای که فرآیند در لحظه $t=0$ با مقدار اولیه $x(0)=0$ شروع و هر رخداد پیشامد مورد نظر دارای نمو ثابتی است. چون تکرار از هم مستقل است، پس با فرض:

$$t_1 \le t_2 \le t_3 \le \ldots$$

آن‌گاه داریم که:

$$x(t_1) \perp\!\!\!\perp (x(t_2) - x(t_1)) \perp\!\!\!\perp \ldots$$

اهمیت این فرآیند بدان دلیل است که بسیاری از رخدادهای طبیعی و صنعتی را توسط این فرآیند می‌توان مدل کرد. فرض کنید که $N(t_1,t_2)$ تعداد رویدادها دربازه t_1 تا t_2 است، آن‌گاه احتمال اینکه این تعداد برابر با n باشد برابر است با:

$$P\{N(t_1,t_2=n)\} = \frac{[\lambda(t_1,t_2=n)]^n}{n!} e^{-\lambda(t_1,t_2=n)} \quad (۶۰)$$

که نرخ داده λ در حالت کلی برابر است با نسبت تعداد رخدادهای مورد انتظار با طول دوره زمان رخداد است.

درواقع رویدادی با فرآیند پواسن در یک بازه زمانی به طول t که قرار است nرخداد را در این بازه رخ دهد که این رخدادها با توزیع یکنواخت و به‌صورت مستقل درکل بازه پراکنده شده‌اند [22].

۶-۴- زنجیره مارکوف

ابتدا لازم است با فرآیند مارکوف آشنا شویم. فرآیندی که در هر لحظه کلیه سابقه فرآیند را در خود خلاصه می‌کند و مقدار آن در هر لحظه فقط وابسته به لحظه قبل است. به‌عبارت دیگر:

$$f_{x_{n+1}}(X_{n+1}|\overline{X}=\overline{x}) = f_{x_{n+1}}(X_{n+}|X_n = x_n) \quad (۶۱)$$

به‌عبارت دیگر فرآیند مارکوف سعی دارد رفتار یک سامانه را به‌صورت تعدادی ازحالات مدل کند که در هر لحظه بر اساس نحوه تغییر ورودی سامانه و حالتی که در آن قرار دارد سامانه به یک حالت دیگر منتقل می‌شود؛ پس عناصر مهم در فرآیند مارکوف عبارت از زمان و حالت است.

زنجیره مارکوف یک فرآیند تصادفی است که ویژگی مارکوف را بر روی تعداد قابل شمارش حالت توصیف می‌کند. به‌عبارت دیگر زنجیره مارکوف یک فرآیند گسسته‌زمان با ویژگی مارکوف است، که توزیع شرطی برای سامانه در مرحله بعد فقط به‌حالت فعلی سامانه بستگی دارد و به‌حالت قبلی بستگی ندارد. زنجیره مارکوف را به‌صورت زیر بیان می‌شود [23]،[19]:

$$\begin{cases} P(S_n = s_n | S_{n-1} = s_{n-1}, ..., S_0 = s_0) \\ = \\ P(S_n = s_n | S_{n-1} = s_{n-1}) \end{cases} \quad (۶۲)$$

۷- نتیجه‌گیری

همان‌طور که در بخش‌های قبل بیان شد، مسئله جمینگ برای منع سرویس یکی از مهم‌ترین آسیب‌پذیری در شبکه‌های هوشمند انرژی است چون با این حمله می‌توان پیام‌های زمان بحرانی را جمنگ کرد و باعث اختلال در شبکه شد. از بین انوع مخابرات‌های بیان‌شده برای ارائه خدمات در شبکه‌های محلی مخابرات FHSS انتخاب شد و نشان داده شد که مبتنی بر مسئله ورشکستگی قمارباز بدترین حالت برای نرخ پیام‌های نامعتبر مدل غیر هماهنگ واکنشی است که برای برطرف‌کردن این آسیب‌پذیری در حالت کلی میزان بار ترافیکی بهینه محاسبه شد و نشان داده شد، این مقدار بار برای تمامی گره‌ها به‌صورت یکسان قابل اطلاق نیست؛ بر همین اساس مبتنی بر تکنیک TACT کمینه بار ترافیکی ابهام برای هر گره محاسبه شد. از آنجا که جمینگ در حالت کلی یک فرآیند تجدیدپذیر مارکوف استپس برای فهم بهتر این فرآیند به همراه سایر فرآیندهای احتمالی مرتبط شرح داده شد؛ اما نکته مهمی که در این مقاله به آن پرداخته نشد، این است که جمر چگونه می‌تواند پیام‌های زمان بحرانی را از سایر پیام‌های عادی تشخیص دهد. این مسئله به‌عنوان فرض اولیه جمینگ در این مقاله در نظر گرفته شده است. حال برای کارهای آینده می‌توان نحوه تشخیص پیام‌های زمان بحرانی را مبتنی بر یک تئوری ریاضیاتی تشریح کرد و روشی برای جلوگیری از تشخیص پیام‌های زمان بحرانی توسط جمر ارائه شود.

۸- مراجع

[1] F. Cleveland, "Uses of wireless communications to enhance power system reliability," in ***Power Engineering Society General Meeting, . 2007 IEEE***, pp.1–1 , June . 2007

[2] S. Mohagheghi, J. Stoupis, and Z. Wang, "Communication protocols and networks for power systems-current status and future trends," in ***Power Systems Conference and Exposition, . 2009 PSCE . 09' IEEE/PES***, pp.9–1 , March . 2009

[3] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, "On the performance of ieee 11 . 802 under jamming," in ***INFOCOM . 2008 The 27th Conference on Computer Communications. IEEE***, April . 2008

[4] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in ***Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing***, MobiHoc '05, (New York, NY, USA), pp.57–46 , ACM, . 2005

[5] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential dsss: Jamming-resistant wireless broadcast communication," in ***INFOCOM, 2010 Proceedings IEEE***, pp.9–1 , March . 2010

[6] C. Pöpper, M. Strasser, and S. Čapkun, "Jamming-resistant broadcast communication without shared keys," in ***Proceedings of the 18th Conference on USENIX Security Symposium***, SSYM'09, (Berkeley, CA, USA), pp.248–231 , USENIX Association, . 2009

[7] F. Cleveland, "Enhancing the reliability and security of the informationinfrastructureusedtomanagethepowers ystem," in ***Power Engineering Society General Meeting, . 2007 IEEE***, pp.8–1 , June . 2007

[8] M. Strasser, C. Pöpper, S. Capkun, and M. Cagalj, "Jammingresistant key establishment using uncoordinated frequency hopping," in ***2008 IEEE Symposium on Security and Privacy (sp 2008)***, pp.78–64 , May . 2008

[9] M. Strasser, C. Pöpper, and S. Čapkun, "Efficient uncoordinated fhss anti-jamming communication," in ***Proceedings of theTenthACM International Symposium on Mobile Ad Hoc Networking and Computing***, MobiHoc '09, (New York, NY, USA), pp.218–207 , ACM, . 2009

[10] I. Standard, "Iec 61850 communication networks and systems in substations," . 2003

[12] Z. Lu, W. Wang, and C. Wang, "Camouflage traffic: Minimizing message delay for smart grid applications under jamming," ***IEEE Transactions on Dependable and Secure Computing***, vol.12 , pp.44–31 , Jan . 2015

[13] Z. Lu, W. Wang, and C. Wang, "Modeling, evaluation and detection of jamming attacks in time-critical wireless applications," ***IEEE Transactions on Mobile Computing***, vol.13 , pp.1759–1746 , Aug . 2014

[14] D.Williams. ***ProbabilitywithMartingales***. Cambridgemathematical textbooks, Cambridge University Press, . 1991

[15] C. University, "Gambler's ruin problem," . 2008

[16] Z. Lu, W. Wang, and C. Wang, "From jammer to gambler: Modeling and detection of jamming attacks against timecritical traffic," in ***INFOCOM, 2011 Proceedings IEEE***, pp.1879–1871 , April . 2011

[17] C. C. J. D. Biggins, "Markov renewal processes, counters and repeated sequences in markov chains," ***Advances in Applied Probability***, vol.19 , no.3 , pp.545–521 , . 1987

[18] S. Yu. ***Hidden Semi-Markov Models: Theory, Algorithms and Applications***. Elsevier Science, . 2015

[19] J. Janssen and R. Manca. ***Semi-Markov Risk Models for Finance, Insurance and Reliability***. Springer US, . 2007

[20] K. Mitov and E. Omey. ***Renewal Processes***. SpringerBriefs in Statistics, Springer International Publishing, . 2014

[21] A. Papoulis and S. Pillai. ***Probability, Random Variables, and Stochastic Processes***. McGraw-Hill series in electrical engineering: Communications and signal processing, Tata McGraw-Hill, . 2002

[22] J. Kingman. ***Poisson Processes***. Oxford Studies in Probability, Clarendon Press, . 1992

[23] C. Grinstead and J. Snell. ***Introduction to Probability***. American Mathematical Society, . 2012

[11] H. Georg, N. Dorsch, M. Putzke, and C. Wietfeld, "Performance evaluation of time-critical communication networks for smart grids based on iec 61850," in ***Computer Communications Workshops (INFOCOM WKSHPS), 2013 IEEE Conference on***, pp.48–43 , April . 2013

محمدرضا گوهره‌یی درجه کارشناسی خود را در رشته برق گرایش الکترونیک از دانشکده فنی مهندسی دانشگاه رازی در سال ۱۳۹۰ و درجه کارشناسی ارشد خود را در رشته مهندسی مخابرات گرایش رمز از دانشگاه صنعتی مالک اشتر در سال ۱۳۹۳ اخذ کرد. تحلیل پروتکل‌های امنیتی، ارتباطی و امنیت در شبکه‌های مخابرات سیار از جمله زمینه‌های پژوهشی ایشان است.