برنامه ریزی توسعه ای پویای شبکه توزیع هوشمند تاب آور در برابر حملات سایبری به مشترکین نهایی

پیمان امیرپور گیگلو[۱] محمدرضا جنتی اسکوئی[۲] سجاد نجفی روادانق[۳]

۱- دانش آموخته کارشناسی ارشد- دانشکده مهندسی برق- دانشگاه شهید مدنی آذربایجان- تبریز- ایران
peymanam7211@gmail.com

۲- دکتری مهندسی برق- شرکت توزیع نیروی برق تبریز- تبریز- ایران
m.r.jannati@gmail.com

۳- استاد- دانشکده مهندسی برق- دانشگاه شهید مدنی آذربایجان- تبریز- ایران
s.najafi@azaruniv.ac.ir

چکیده: امنیت عرضه توان محرک اصلی در پیدایش و نیز توسعه شبکه توزیع هوشمند می‌باشد. برنامه‌ریزی توسعه شبکه توزیع هوشمند، برای مشخص کردن مکان، ظرفیت و زمان نصب تجهیزات جدید یا تقویت/جایگزینی دارایی‌های موجود با هدف بهینه‌سازی تامین به موقع و مقرون به صرفه تقاضای رو به رشد بار، با در نظر گرفتن الزامات و محدودیت‌های فنی و بهره‌برداری، صورت می‌گیرد. در این بین، سیستم مخابراتی نقش اساسی در توسعه شبکه های توزیع هوشمند دارد، ولی امنیت سایبری-فیزیکی سامانه‌های ارتباطی مخصوصا سطح مشترکین به شدت نسبت به حملات سایبری، آسیب‌پذیر هستند که امنیت عرضه انرژی را به مخاطره می‌اندازد. بنابراین، این مقاله روشی برای برنامه‌ریزی توسعه شبکه توزیع هوشمند تاب‌آور با رویکرد تاب‌آورسازی مقرون به صرفه سطح مشترکین به حملات سایبری، به صورت مدلسازی سه سطحی پویا ارائه داده است. به منظور ارزیابی اثربخشی روش پیشنهادی، شبیه‌سازی رایانه‌ای بر روی یک شبکه توزیع انجام و نتایج به بحث گذاشته شده است.

واژه‌های کلیدی: **شبکه توزیع، برنامه ریزی توسعه، برنامه نویسی پویا، تاب آوری، حملات سایبری**

نوع مقاله: پژوهشی

DOI: 10.61186/jiaeee.20.4.550

تاریخ ارسال مقاله: ۱۴۰۰/۰۸/۰۴

تاریخ پذیرش مشروط مقاله: ۱۴۰۱/۰۶/۲۵

تاریخ پذیرش مقاله: ۱۴۰۲/۰۱/۱۹

نام نویسنده‌ی مسئول: دکتر سجاد نجفی روادانق

نشانی نویسنده‌ی مسئول: تبریز- دانشگاه شهید مدنی آذربایجان- گروه مهندسی برق- آزمایشگاه تحقیقاتی شبکه های هوشمند تاب آور

فهرست علائم:

	بالانویس		شاخص
هزینه نصب	IC	شاخص و مجموعه زمان	i, j, t, T
هزینه توسعه	EC	شاخص و مجموعه بار	l, L
هزینه بهره برداری و نگهداری	OMC	شاخص و مجموعه اندازه گیرهای هوشمند	s, S
ظرفیت پست فوق توزیع s نصب شده در سال y و باس b	S_R	شاخص، مجموعه و شمار باس ها	k, b, B, N_b
توان اکتیو نامی منبع تولید پراکنده d نصب شده در سال y و باس b	$P_{R_{d,g,b,Y}}$	شاخص و شمار خطوط	br, N_{br}
	متغیرها	فیدر فشار متوسط	F
جریان فیدر f در ساعت h از سال y	$I_{(f,y,h)}$	منابع پراکنده شامل کنترل پذیر، بادی و خورشیدی	dg
توان برنامه ریزی شده باس b در ساعت h در سال y	$P_{Load_{(b,y,h)}} + jQ_{Load_{(b,y,h)}}$	کلید بریکر	CBS
تعداد حلقه های اصلی	NL_{mL}	کلید سکشنالایزر	$SecS$
توان افزایش یافته در باس b در ساعت hام در سال yام	$\bar{P}_{Load_{(b,y,h)}} + j\bar{Q}_{Load_{(b,y,h)}}$		**پارامترها**
توان حذف شده از باس b در ساعت hام در سال yام	$\Delta P^{Clip}_{Load_{(b,y,h)}} + j\Delta Q^{Clip}_{Load_{(b,y,h)}}$	حداکثر بارگیری	$MaxL$
قیمت اولیه برق قبل از مشارکت در برنامه مدیریت سمت بار	$LC_{l,0}$	حداکثر توسعه سالانه پست فوق توزیع s نصب شده در سال y و باس b	$MaxAE$
مجموع مصرف برق قبل از مشارکت در برنامه مدیریت سمت بار	$P_{l,0}$	حداکثر ظرفیت پست فوق توزیع s نصب شده در سال y و باس b	$MaxE$
قیمت برق بعد از مشارکت در پاسخگوئی بار	$LC_{l,n}$	ضریب توان	PF
مجموع مصرف برق بعد از مشارکت در برنامه مدیریت سمت بار	$P_{l,n}$	حداکثر تعداد منابع تولید پراکنده قابل نصب در شبکه در هر سال	$MaxN$
قیمت برق بعد از حمله سایبری	LC_{at}	امپدانس فیدر f	$R_f + jX_f$
اطلاعات تزریقی به اندازه گیرهای هوشمند	$at_{Sm,sm}$		
متغیر بایتری، اگر اندازگیر هوشمند s مورد حمله برابر ۱ در غیر این صورت صفر	$\psi_{Sm,sm}$	تلفات اکتیو و راکتیو در ساعت h از سال y	$P_{Loss_{(y,h)}} + jQ_{Loss_{(y,h)}}$
مصرف برق در باس b بعد از حمله سایبری	$\hat{P}_b$	دامنه ولتاژ در باس b در ساعت h از سال y	$V_{(b,y,h)}$
مصرف برق در باس b قبل از حمله سایبری	P_b	ولتاژ نامی	V_{Rated}
بودجه مهاجم	$ABud_a$	کمینه/بیشینه ولتاژ بحرانی	$V_{Crit}^{\min} / V_{Crit}^{\max}$
محدودیت منابع مالی مهاجم ($)	Bud	کمینه/بیشینه ولتاژ امن	$V_{Safe}^{\min} / V_{Safe}^{\max}$
سطح امنیت اندازه گیرهای هوشمند	$SecL$	الاستیسیته خودی	$E(i,i)$
نرخ سطح امنیت	β	الاستیسیته متقابل بیت ساعات i و j	$E(i,j)$
محدودیت حمله (کیلووات)	λ	حداقل و حداکثر قیمت انرژی	LC_{min}, LC_{max}

۱- مقدمه

هدف از برنامه ریزی توسعه‌ای مرسوم شبکه توزیع [۱] (DEP)، مشخص کردن زمان، مکان و ظرفیت نصب تجهیزات جدید یا جایگزینی/تقویت امکانات موجود، به منظور پاسخگویی بهینه، مقرون به صرفه و به موقع به نیاز رو به رشد مشترکین، با در نظر گرفتن تمام محدودیت ها و الزامات فنی، عملیاتی و قابلیت اطمینان است. در بین روش‌های برنامه‌ریزی، طرح پویا به تصمیم‌گذاری برای چندین سال در آن واحد که منجر به هزینه‌های کمتری، می شود، ختم می‌گردد [۱]. در سالهای اخیر، تحقیقات و تحولات به سمت طراحی، برنامه‌ریزی و بهره‌برداری از شبکه‌های توزیع هوشمند[۲] (SDN) هدایت شده است که در شرایط عادی بهره‌برداری در برابر تهدیدهای شناخته شده و قابل پیش‌بینی ایمن و همچنین در برابر حوادثی با احتمال وقوع پایین و شدت اثربخشی بالا[۳] (HILP) مقاوم باشند [۲]. وابستگی شدید SDNها به سیستم ارتباطی و آسیب‌پذیری امنیتی کانال‌های ارتباطی باعث می‌شود SDNها در برابر حملات سایبری[۴] (CAs) آسیب‌پذیر شوند [۳]. بنابراین، SDN به ارتباطات دو طرفه ایمن و توانمندسازی بازیگران مختلف شبکه نیاز دارد [۶-۴]. آسیب‌پذیری امنیتی در کانال‌های ارتباطی و به طور کلی در سیستم‌های فیزیکی سایبری به مهاجمان سایبری این اجازه را می‌دهد [۷و ۲۶] تا حملات پیچیده‌ای را انجام دهند که منجر به آسیب‌های فیزیکی و فنی فاجعه بار شود. CAها در گذشته، مانند حملات StuxNet [۸] و اخیراً مانند حمله به تجهیزات نظامی و وسایل الکتریکی [۹] این واقعیت را نشان می‌دهد که سیستم‌های فیزیکی سایبری در برابر حملات سایبری آسیب‌پذیر باقی مانده‌اند. برای دفاع بهینه در برابر CAها، امنیت سیستم‌های فیزیکی سایبری باید بهبود یابد و یکی از روش‌های بهبود امنیت سیستم فیزیکی سایبری، طبقه‌بندی انواع مختلف CAها و طراحی اقدامات مقابله‌ای بهینه برای هر نوع حمله است [۱۰]. یکی از انواع حمله‌ها، حمله تزریق داده های کاذب[۵] (FDI) می‌باشد که مهاجم، سیگنال‌های ورودی یا خروجی را با هدف افزودن داده‌های کاذب به اندازه‌گیرها دستکاری می‌کند [۱۱]. برای اولین بار، حمله FDI در سال ۲۰۱۱ توسط لیو و همکاران پیشنهاد شده است [۱۲]. حمله FDI، داده‌های اندازه‌گیرهای سیستم قدرت هدف حمله قرار می‌گیرد و مهاجم داده‌ها را برای ساخت بردار جدید بر اساس تخمین حالت دستکاری می‌کند [۱۳]. بنابراین، تولید و دیسپاچینگ تحت تأثیر عملکرد نادرست سیستم قرار می‌گیرد، زیرا حملات FDI کاملاً پنهان و تشخیص آن دشوار است. گسترش اثرات مخرب CAها بر SDN بیانگر آن است که طراحی، برنامه ریزی و بهره‌برداری از SDNها با توسعه‌ی تکنیک‌های موجود و طرح های رایج با چالش‌های جدی روبرو است. از این‌رو، برای داشتن یک SDN با سطح قابل قبولی از امنیت تامین بار، مسائل امنیت سایبری باید در برنامه ریزی توسعه‌ای شبکه توزیع هوشمند تاب آور در برابر حملات سایبری در نظر گرفته شود.

۱-۲- مرور مراجع

در [۱۴] مقاوم سازی شبکه توزیع به عنوان روشی برای ارتقا تاب آوری با تقویت دوام ساختار شبکه توزیع به صورت مسئله تصادفی دو سطحه مدلسازی شده است. در [۱۵] روش مبتنی بر ریسک برای طراحی شبکه توزیع شعاعی تاب آور در برابر طوفان ارائه شده است. در [۱۶] ارتقا تاب آوری شبکه توزیع با بهره گیری از مقاوم سازی، نصب ژنراتورهای پشتیبان و جایابی ادوات کلیدزنی، به صورت مسئله تصادفی دو سطحه مدلسازی شده است. در [۱۷] بازآرایی همزمان شبکه توزیع با بهره برداری از منابع انرژی پراکنده، به عنوان مبنای روش پیشنهادی برای مدیریت قطع بار هدف ارتقا تاب آوری شبکه توزیع، ارائه شده است. مدیریت سمت بار در شبکه توزیع به دلایل مختلفی همچون، برنامه ریزی، بهره‌برداری، امنیت سیستم، تجمیع انرژی‌های نو، مدیریت ریسک و ... انجام می‌شود[۱۸]. در [۱۹] مدلسازی چندهدفه از بهره برداری بهینه منابع تولید پراکنده، مدیریت سمت بار، تپ چنجرهای زیر بار و کنترل کننده استاتیکی ولتاژ ارائه شده است. برنامه‌ریزی بهینه منابع تولید پراکنده در شبکه توزیع با در نظر گرفتن مدیریت سمت بار، بازآرایی شبکه و قابلیت کنترل ولتاژ در مرجع [۲۰] مطالعه شده است. مدیریت سمت بار زمان واقعی و بازار برق با هدف مدیریت انرژی در ریزشبکه ترکیبی در مرجع [۲۱] ارائه شده است. با این حال، مقالات کمی در باب تاثیرات مدیریت سمت بار در ارتقا تاب آوری وجود دارد. در [۲۲] رویکرد دو سطحه مبتنی بر ریسک به منظور ایجاد هماهنگی بین پیکربندی پویایی ریزشبکه‌های چندگانه با بهره برداری روزانه منابع انرژی پراکنده با هدف ایجاد ایمنی در برابر خروج تجهیزات ارائه شده است. مدلسازی آماری برنامه‌ریزی توسعه ای همزمان تولید و شبکه توزیع برای سیستم‌های ایزوله با در نظر گرفتن مدیریت سمت بار و منابع ذخیره‌ساز در مرجع [۲۳] ارائه شده است. شایان ذکر است که مقالات متعددی در حوزه تاب آوری شبکه‌های توزیع هوشمند وجود دارد که غالبا حوادث آب و هوایی شدید را مورد مطالعه قرار داده اند و هنوز شکاف مطالعاتی عیمقی در حوزه امنیت سایبری شبکه‌های هوشمند وجود دارد. در [۲۴]، مکانیسم تشخیص حمله و کنترل کننده مقاوم در برابر حمله پیشنهاد شده است و یک سیستم کنترل قوی برای کاهش اثرات حمله با استفاده از تئوری تجزیه و تحلیل حساسیت طراحی شده است.

کلیه مقالات بررسی شده نشان می‌دهد که مقالات موجود بر مدلسازی ایستای مسئله که بر روی یک سال متمرکز هست استوار می‌باشند و هیچگونه طرحی برای سال های میانی و آتی ارائه نمی‌دهند. در حالیکه محدودیت های بودجه شرکت توزیع اجازه انجام تمام سرمایه‌گذاری در یک سال را نمی‌دهد و سرمایه‌گذاری‌ها باید در سال‌های مختلف تا سال هدف با استفاده از مدل‌سازی پویای مسئله برنامه‌ریزی، تقسیم گردد. . علاوه بر این، یک استراتژی مناسب برای تامین توان قابل اطمینان، با توجه به اولویت اقتصادی - اجتماعی

مشترکین نهایی، به کاهش انرژی تأمین نشده در صورت وقوع قطعی نیاز دارد. که تقریباً در تمام مقالات چاپ شده در زمینه سیستم‌های فیزیکی سایبری، محققان بر حملات به خطوط انتقال و توزیع متمرکز شده اند و بخش مشترکین دارای شکاف قابل توجهی در مطالعات امنیت سایبری می‌باشد.

۱-۳- انگیزه نگارش مقاله

با توجه به نکات ذکر شده در بخش قبلی و همچنین گپ‌های موجود در مطالعات شبکه در راستای توسعه شبکه و حملات سایبری، در این مقاله روشی برای برنامه‌ریزی توسعه شبکه هوشمند تاب آور و همچنین تاثیر حملات سایبری بر شبکه توزیع موجود در بخش مشترکین مورد بررسی قرار گرفته و روش دفاعی بهینه جهت کاهش اثرات حمله مورد ارزیابی عددی قرار گرفته است.

با توجه به محدودیت‌های بودجه شرکت توزیع، روش ارئه شده در این مقاله برای توسعه شبکه به صورت تدریجی و تا سال هدف و با در نظر گرفتن نقش منابع تولید پراکنده و عدم قطعیت‌های موجود (بار، تولید منابع تولید پراکنده و قیمت انرژی) می‌باشد. همچنین حمله سایبری ترزیق داده‌های کاذب به بخش مشترکین با درنظرگرفتن امنیت مترهای هوشمند و بودجه حمله کننده مدل شده است به طوری که سایبر اتکر با دستکاری سیگنال قیمت، قیمت انرژی را تغییر می‌دهد که این موضوع باعث به وجود آمدن مشکلات فنی می‌شود. همچنین در این مقاله برای کاهش اثرات مخرب جمله سایبری، بازآرایی شبکه توزیع به عنوان روش دفاعی پیشنهاد شده است.

۲- مدل بهینه‌سازی سه سطحه

روش پیشنهادی بر پایه بهینه‌سازی سه مرحله ای [۲۷] شامل برنامه ریزی توسعه شبکه توزیع هوشمند، حمله FDI و استراتژی دفاعی در شکل (۱) ارائه شده است. در سطح بالایی از روش پیشنهادی، شرکت توزیع[۶] (DisCo) برنامه‌ریزی بهینه تجهیزات مختلف شبکه توزیع و همچنین بهره‌برداری از آنها را در شرایط عادی، همگی از دیدگاه هزینه و البته با در نظر گرفتن قیود و الزامات فنی تجهیزات و شبکه مشخص می‌کند. در سطح میانی، مهاجم با توجه به بودجه محدود، شماری از اندازه‌گیرها را با عنوان هدف حمله و به منظور افزایش هزینه بهره‌برداری مشخص می کند. مدل حمله پیشنهادی بر روی سیگنال قیمت تأثیر می‌گذارد و در نتیجه مصرف برق را افزایش می‌دهد، که منجر به افزایش هزینه های عملیاتی و مشکلات فنی شبکه شده و در نهایت منجر به اضطراب و ناراحتی در مشترکین نهایی می‌گردد. سرانجام، در سطح پایین، DisCo و در قالب استراتژی دفاعی پیشنهادی متوجه می‌شود که مصرف برق، تلفات شبکه و هزینه بهره‌برداری افزایش یافته است و شروع به انجام اقدامات اصلاحی نظیر بازآرایی شبکه می کند تا اثر اغتشاش را کاهش دهد.

۲-۱- روش پیشنهادی برای سطح اول بر پایه برنامه ریزی توسعه‌ای شبکه در شرایط عادی

رویه تعریف شده بر دو اصل استوار است: کفایت و امنیت. تامین بار قابل اطمینان برای تقاضای روز افزون برق نیازمند نصب تجهیزات جدید و جایگزینی و یا تقویت امکانات قبلی شبکه توزیع می‌باشد. در طرف دیگر، DN هزینه بسیار بالایی دارد و بازگشت سرمایه‌گذاری در دراز مدت صورت می‌گیرد. بنابراین، DN باید مقرون به صرفه طراحی شود بنابراین، در سطح اول طرح پیشنهادی، DisCo برنامه‌ریزی و بهره‌برداری بهینه از تجهیزات مختلف DN را از دیدگاه هزینه انجام می‌دهد. واضح است که DN معمولاً به صورت حلقوی طراحی اما به صورت شعاعی بهره برداری می‌شود. بنابراین، هر فیدر شعاعی متشکل از باس بارها و خطوط تغذیه شده از یک پست HV می‌باشد. در روی بعضی از خطوط و نیز بین دو فیدر مجاور ممکن است کلید وجود داشته باشد. روش پیشنهادی برای برنامه‌ریزی توسعه‌ای شبکه توزیع هوشمند شامل همزمانی طراحی و توجه به پارامترهای مختلف اقتصادی و قیود با هدف دستیابی به بهترین طرح از شبکه توزیع در کمترین هزینه ممکن با در نظر گرفتن محدودیت‌های فنی، عملیاتی و قابلیت اطمینان می‌باشد. عملکردها و قیود شبکه شامل مواردی است که عموما در بهره‌برداری شبکه توزیع اعمال می‌شود که در نهایت به صورت زیر فرمول بندی شده است:

Objective function

$$Total\ Cost_{DisCo} = TCost_{HVS} + TCost_{F} + TCost_{SD} + TCost_{DG} + TCost_{loss} + ... \\ TCost_{PTransfer\ co} + TCost_{DNR} + TCost_{DR} + TCost_{ENS} + TDC \quad (۱)$$

$$Total\ Cost = TCost_{Planning} + TCost_{Operation} \quad (۲)$$

$$TCost_{Planning} = T\cos t_{IC_{HVS}} + T\cos t_{IC_{F}} + +T\cos t_{IC_{cbc}} + T\cos t_{IC_{secs}} + ... \\ T\cos t_{IC_{DG}} + T\cos t_{EP_{HVS}} + T\cos t_{EP_{F}} + T\cos t_{EP_{DG}} + \quad (۳)$$

$$TCost_{Operation} = TCost_{OMC_{HVS}} + TCost_{OMC_{DG}} + TCost_{loss} + TCost_{PTransfer\ co} + ... \\ TCost_{DNR} + TCost_{DR} + TCost_{ENS} + TDC \quad (۴)$$

از آنجا که روش پیشنهادی میزان سرمایه گذاری سالانه را تعیین می‌کند، بنابراین ارزش فعلی خالص (NPV) پول هزینه شده سالانه باید با استفاده از معادله زیر محاسبه شود:

$$NPV^{y} = (\frac{1 + Inflation\ Rate}{1 + Interest\ Rate})^{y} \quad (۵)$$

جزییات مربوط به موارد مختلفی که توابع هدف اجرایی را تحت تاثیر قرارد میدهد و نیز قیود مرتبط، در ادامه آمده است.

۲-۱-۱- مدل‌سازی عدم قطعیت‌های موجود

عدم قطعیت بار، قیمت و انرژی تجدیدپذیر باید به منظور تصمیم‌گیری درست، مدنظر قرار گیرد. بدین منظور، یک سال به مانند یک شبانه روز ۲۴ ساعته، که هر ساعت به بازه زمانی مشخص از کل سال برمی‌گردد، مدل شده است. برای هر ساعت، مقدار متوسط آن

پارامترها شامل بار، تولید منابع تجدیدپذیر (سرعت باد و تابش خورشید) و قیمت انرژی با استفاده از اطلاعات تاریخی سال‌های اخیر محاسبه می‌شود [۲۵].

۲-۱-۲- ارزش خالص فعلی هزینه پست‌های فوق توزیع

پست‌ها باید به گونه‌ای جایابی شوند که تمامی نقاط بار تغذیه گردند. پست(های) جدید در محل های کاندید از پیش تعیین شده می‌توانند نصب شوند و ظرفیت سالانه پست‌های موجود و نیز پست های جدید، با بهینه‌سازی مشخص خواهند شد. ارزش خالص فعلی هزینه پست در فرمول (۶) آمده است. مطابق با رابطه (۷)، هزینه نصب متناسب با هزینه زمین، هزینه احداث، هزینه تجهیزات از جمله ترانسفورماتور و هزینه مربوط به اتصال پست به شبکه انتقال می‌باشد. رابطه (۸) به هزینه توسعه پست برمی‌گردد که اختلاف بین هزینه نصب پست در ظرفیت های مختلف می‌باشد. روابط (۱۰)-(۱۲) نمایش دهنده قیود اعمالی در راستای نصب پست می‌باشد. در (۱۰)، برای بارگیری پست، حاشیه امنیت در نظر گرفته شده است. علاوه براین، محدودیت‌های فضای شهری، منابع مالی و توانمندی فنی، دلایل تعریف رابطه (۱۱)، حداکثر توسعه سالانه پست، و رابطه (۱۲)، حداکثر ظرفیت پست قابل نصب در باس بار مشخص، بوده‌اند.

$$TCost_{HVS} = \sum_{Y\in\chi^{year}} NPV^{Y} \times \sum \left(IC_{su,b,Y} + EC_{su,b,Y} + OMC_{su,b,Y}\right) \quad (۶)$$

$$IC_{Su,b,Y} = G_{Su} \times Cost_{G_b} + Cost_{Eq_{Su,b}} + Cost_{Cons_{Su,b}} + Cost_{CTT_{Su,b}} \quad (۷)$$

$$EC_{Su,b,Y} = IC_{Su,b,Y} - IC_{Su_{Su,b,Y-1}} \quad (۸)$$

$$OMC_{Su,b,Y} = S_{R_{Su,b,Y}} \times Cost_{OM_{HVS}} \quad (۹)$$

$$S_{L_{Su,b,Y}} \le MaxL \times S_{R_{Su,Y}} \quad (۱۰)$$

$$S_{R_{Su,b,Y}} \le S_{R_{Su,b,Y-1}} + MaxAN \quad (۱۱)$$

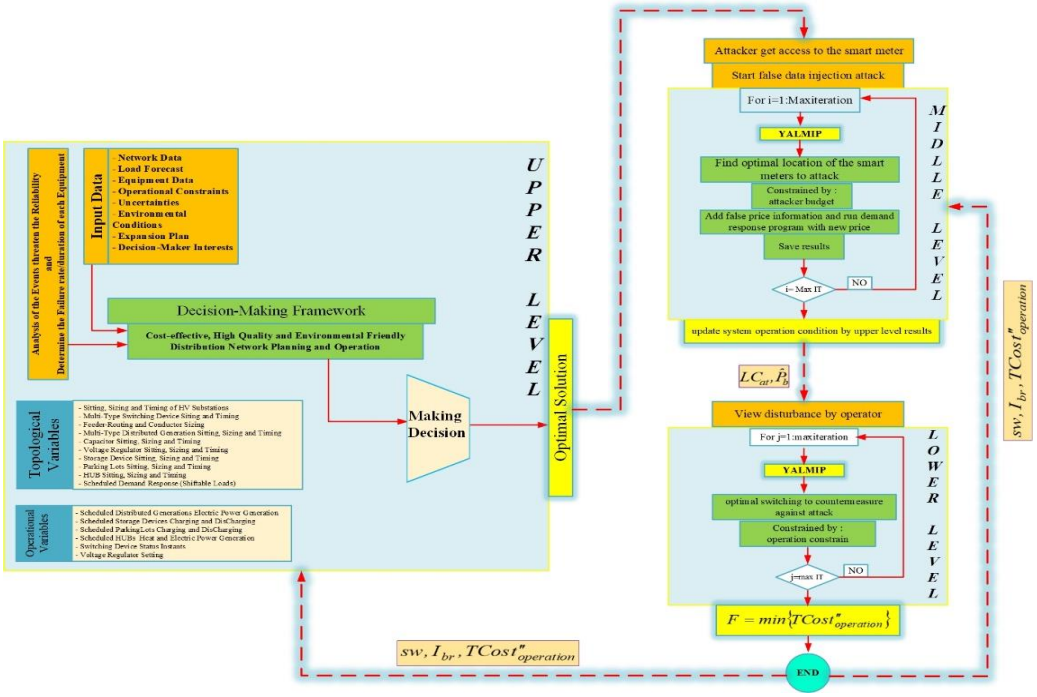
۲-۱-۴- ارزش خالص فعلی طراحی حلقوی شبکه توزیع همراه با تشکیل ریزشبکه

اساس طراحی حلقوی و بهره‌برداری شعاعی شبکه توزیع نیازمند نصب تجهیزات کلیدزنی از هر دو نوع در حالت عادی باز و در حالت عادی بسته است. کلیدهای استفاده شده یا از نوع بریکر هستند که به منظور جداسازی سریع تکه فیدر، و یا از نوع سکشنالایزر که قابلیت بازآرایی شبکه طی شرایط عادی/غیرعادی را مهیا می‌سازند. حداکثر تعداد کلید قابل نصب با استفاده از روابط (۱۸) و (۱۹) محدود شده است.

$$TCost_{SD} = \sum_{Y\in\chi^{year}} NPV^{Y} \times \sum_{f\in\chi^{F}} \left(IC_{CBS,f,Y} + IC_{SecS,f,Y}\right) \quad (۱۷)$$

$$IN_{CBS} \le MaxN_{CircuitBreaker} \quad (۱۸)$$

$$IN_{SecS} \le MaxN_{Sectionalizer} \quad (۱۹)$$



شکل (۱): فلوچارت مدل بهینه سازی سه سطحه ی پیشنهادی

$$S_{R_{Su,b}} \le MaxS_{Su,b} \quad (۱۲)$$

۲-۱-۳- ارزش خالص فعلی هزینه فیدر

روش پیشنهادی، مسیر فیدرها همراه با جنس هادی‌ها را مشخص می‌کند. هزینه نصب فیدر f-ام با هادی مشخص، مستقیما به طول آن (l_f) وابسته است.

$$TCost_{F} = \sum_{Y\in\chi^{year}} NPV^{Y} \times \sum_{Y\in\chi^{F}} \left(IC_{f,Y} + EC_{f,Y}\right) \quad (۱۳)$$

$$IC_{f,Y} = \xi \times l_f \times \text{Cost}_{F_{Overhead\ line,type}} \quad (۱۴)$$

$$EC_{f,Y} = IC_{f,Y} - IC_{f,Y-1} \quad (۱۵)$$

$$S_{L_{f,Y}} \le MaxL_F \times S_{R_{f,Y}} \quad (۱۶)$$

۲-۱-۵- ارزش خالص فعلی منابع تولیدپراکنده

روش پیشنهادی، زمان، مکان و ظرفیت بهینه نصب انواع منابع تولید پراکنده شامل کنترل پذیر، بادی و خورشیدی در شبکه توزیع و همچنین تولید ساعتی انها رو مشخص می‌کند. فرمول‌بندی ریاضی محاسبه هزینه و قیود اجرایی در ذیل آمده است. حداکثر ظرفیت تولید ($MaxP_{DG}$)، حداکثر تعداد ($MaxN_{DG}$) منابع تولید پراکنده قابل نصب، به ترتیب در روابط (۲۴) و (۲۵)، آورده شده است. به دلیل تاثیر قابل‌توجه توان راکتیو در خروج آنالیز پخش بار، فرض شده است که این منابع، توان راکتیو نیز تولید می‌کنند، رابطه (۲۸). افزایش یا کاهش ساعتی تولید منابع تولیدپراکنده بوسیله ($R_{\mathrm{U/D}_{DDG}}$) طبق رابطه (۲۹) محدود شده است. علاوه براین، به دلیل هزینه‌بر بودن و زمان‌بر بودن فرایند به مدار آوردن منابع تولید پراکنده قابل کنترل، این منابع در شرایط عادی، هرگز خاموش نخواهند شد و حداقل تولید آن‌ها طبق رابطه (۳۰) برابر با $MaxG_{DDG}$ خواهد بود. توان اکتیو و راکتیو تولیدی منبع d-ام در ساعت h-ام از سال y-ام منصوبه در باس b-ام، به ترتیب بوسیله $P_{gen_{dg,b,Y,t}}$ و $Q_{gen_{dg,b,Y,t}}$ نمایش داده شده‌اند.

$$T\ \mathrm{Cost}_{DG} = \sum_{Y \in \chi^{year}} NPV^{Y} \times \ldots \sum_{b \in \chi^{bus}} \left(IC_{dg,b,Y} + EC_{dg,b,Y} + N_{day} \times \sum_{t \in \chi^{time}} OMC_{dg,b,Y,t} \right) \quad (۲۰)$$

$$IC_{dg,b,Y} = G_{dg} \times Cost_{G_b} + Cost_{Eq_{dg,b}} + Cost_{Cons_{dg,b}} + Cost_{CIT_{dg,b}} \quad (۲۱)$$

$$EC_{dg,b,Y} = IC_{dg,b,Y} - IC_{dg,bY-1} \quad (۲۲)$$

$$OMC_{dg,b,Y,t} = P_{gen_{dg,b,Y,t}} \times Cost_{OM_{DG}} \quad (۲۳)$$

$$\sum_{b \in \chi^{bus}} P_{R_{dg,b}} \le MaxP_{DG} \quad (۲۴)$$

$$\sum_{b \in \chi^{bus}} \frac{P_{R_{dg,b}}}{Max\left(1, P_{R_{dg,b}}\right)} \le MaxN_{DG} \quad (۲۵)$$

$$P_{R_{dg,b,Y}} \le P_{R_{dg,b,Y-1}} + MaxAN_{dg,b} \quad (۲۶)$$

$$P_{R_{dg,b}} \le MaxE_{dg,b} \quad (۲۷)$$

$$PF_{DG} = cte \quad (۲۸)$$

$$\left| P_{gen_{dg,b,Y,t}} - P_{gen_{dg,b,Y,t-1}} \right| \le R_{U/D_{DDG}} \quad (۲۹)$$

$$P_{gen_{dg,b,Y,t}} \ge MaxG_{DDG} \quad (۳۰)$$

۲-۱-۶- ارزش خالص فعلی تلفات

سهم قابل توجهی از تلفات در سیستم قدرت مربوط به گستردگی شبکه توزیع می‌شود. به منظور محاسبه هزینه تلفات توان از رابطه زیر استفاده شده است:

$$P_{loss_{Y,t}} + \mathrm{jQ}_{loss_{Y,t}} = \sum_{f \in \chi^{F}} \sum_{Y \in \chi^{year}} \sum_{t \in \chi^{time}} I_{f,Y,t}^{2} \times \left(R_f + jX_f \right) \quad (۳۱)$$

$$T\ \mathrm{Cost}_{\mathrm{loss}} = \sum_{Y \in \chi^{year}} NPV^{Y} \times N_{day} \times \ldots \sum_{t \in \chi^{time}} \left(\mathrm{Cost}_{P_{loss_t}} \times P_{loss_{Y,t}} + \mathrm{Cost}_{Q_{loss_t}} \times Q_{loss_{Y,t}} \right) \quad (۳۲)$$

۲-۱-۷- ارزش خالص فعلی خرید انرژی از شبکه

به عنوان مرحله نهایی فرایند عرضه برق به مشترکین نهایی، شرکت توزیع، برق را از شبکه بالا دستی خریداری می‌کند. مقدار خرید توان و هزینه آن، از رابطه (۳۳) و (۳۴قابل محاسبه است:

$$P_{\mathrm{PTransfer}_{Y,s}} = \sum_{b \in \chi^{bus}} \sum_{Y \in \chi^{year}} \sum_{t \in \chi^{time}} \left(P_{\mathrm{load}_{b,Y,t}} - P_{\mathrm{GEN}_{dg,b,Y,t}} \right) + \ldots \sum_{Y \in \chi^{year}} \sum_{t \in \chi^{time}} P_{loss_{Y,t}} \quad (۳۳)$$

$$T\ \mathrm{Cost}_{\mathrm{PTransferCo}} = \sum_{Y \in \chi^{year}} NPV^{Y} \times N_{day} \times \ldots \sum_{t \in \chi^{time}} \mathrm{Cost}_{PTransferCo_t} \times P_{PTransferCo_{Y,t}} \quad (۳۴)$$

۲-۱-۸- ارزش خالص فعلی قابلیت اطمینان

محاسبات قابلیت اطمینان براساس خطاهای مرسوم و شناخته‌شده انجام می‌شود. روشن است که هزینه انرژی تامین نشده مشترکین برق، مهم‌ترین شاخص مرسوم در بهینه سازی قابلیت اطمینان در شبکه توزیع است که بهبود این شاخص به ارتقا دیگر شاخص‌های قابلیت اطمینان منجر خواهد شد. پارامترهای، مدت زمانی خرابی (r_f) و نرخ خرابی (λ_f) برای محاسبه انرژی از دست رفته نیاز است. علاوه براین، بهتر است که انرژی از دست رفته موزون، با در نظر گرفتن اولویت تامین توان ($P_{r_{(b)}}$) محاسبه شود. از این روی، باس های با اهمیت بالا در تامین توان، توجه بیشتری را جلب می‌کنند.

$$ENS_Y = \sum_{f \in \chi^{F}} r_f \times \gamma_f \times \left(\sum_{\substack{b \in \chi^{bus} \\ bus \in \{Faulted\ Area\}}} P_{r_b} \times ave\left(\overline{P}_{load_{b,Y}} \right) \right) \quad (۳۵)$$

$$TCost_{ENS} = \sum_{Y \in \chi^{year}} NPV^{Y} \times N_{day} \times ENS_Y \quad (۳۶)$$

۲-۱-۹- هزینه نارضایتی فنی

ولتاژ باس و جریان فیدر، پارامترهای بهره‌برداری مهمی هستند که باید در محدوده قابل قبول حفظ شوند. بنابراین، آنالیز پخش بار برای محاسبه حدود این پارامترها باید انجام شود. عدم رضایت از قید حدود ولتاژ و جریان در قالب ضریب جریمه تحت عنوان عدم رضایت فنی به صورت ریاضی وار در زیر آمده است:

$$TDC = dc \times Max\left\{ \left(1 - \mu^{V}\right), \left(1 - \mu^{I}\right) \right\} \quad (۳۷)$$

که، dc هزینه عدم رضایت است. به منظور محاسبه مقدار نهایی TDC فرایند زیر باید انجام گردد:

$$\mu_{b,Y,t}^{V}=\begin{cases}\dfrac{V_{b,Y,t}-V_{crit}^{min}}{V_{safe}^{min}-V_{crit}^{min}} & ,\ V_{crit}^{min}<V_{b,Y,t}<V_{safe}^{min}\\ 1 & ,\ V_{safe}^{min}<V_{b,Y,t}<V_{safe}^{max}\\ \dfrac{V_{b,Y,t}-V_{crit}^{max}}{V_{safe}^{max}-V_{crit}^{max}} & ,\ V_{safe}^{max}<V_{b,Y,t}<V_{crit}^{max}\\ 0 & ,\ else\end{cases} \quad (۳۸)$$

$$\mu^{V}=\frac{1}{N_{year}\times N_{time}\times N_{bus}}\times\sum_{b\in\chi^{bus}}\sum_{Y\in\chi^{year}}\sum_{t\in\chi^{time}}\mu_{b,Y,t}^{V} \quad (۳۹)$$

۲-۲-سطح دوم از روش پیشنهادی در قالب حمله تزریق داده کاذب

در SDN، قیمت انرژی توسط تأمین‌کنندگان انرژی با توجه به شرایط بازار تعیین شده و داده های به واحد کنترل کننده مصرف انرژی خانه هوشمند(ECC) فرستاده می‌شوند. واحدهای ECC با نظارت و کنترل مصرف برق و برنامه‌ریزی فعالیت دستگاه‌ها براساس قیمت برق، مصرف برق مشترک را برنامه‌ریزی می‌کنند. بنابراین، دستگاه‌های هوشمند می‌توانند توسط ECC برای روشن یا خاموش شدن براساس قیمت برق برنامه‌ریزی شوند مانند وسایل نقلیه الکتریکی، باتری‌ها (ذخیره‌ساز انرژی)، وسایل خانگی هوشمند و غیره. بنابراین، مصرف‌کنندگان برای تبادل اطلاعات بین تأمین‌کنندگان انرژی، به ویژه برای مشارکت در برنامه‌های مدیریت سمت بار[۷] (DRP)، به یک شبکه ارتباطی نیاز دارند. وابستگی زیاد بخش مصرف‌کننده به شبکه ارتباطی و امنیت سایبری پایین کانال‌های ارتباطی به دلایل اقتصادی و برخی محدودیت‌ها، این بخش را به عنوان کاندیدای بالقوه حمله سایبری تبدیل کرده است. بنابراین، مهاجم با تعیین مشترکین مشارکت‌کننده در DRP و نوع اندازه گیرهای هوشمند آنها پس از یک بررسی میدانی طولانی مدت، یک حمله کارآمد را آغاز می کند. این حملات با در نظر گرفتن نتایج تحقیقات، بودجه و امنیت سایبری اندازه‌گیرهای هوشمند انجام می شود. پس از تعیین محل حمله (با استفاده از الگوریتم بهینه سازی)، مهاجم با دستیابی به اندازه‌گیرهای هوشمند شروع به شنود می‌کند تا اطلاعاتی را برای یک حمله غیرقابل شناسایی و کارآمد بدست آورد. مهاجم با به دست آوردن اطلاعات و دستکاری سیگنال قیمت، قیمت انرژی را در اندازه‌گیر هوشمند در پیک بار کاهش می‌دهد. ECC به دستگاه‌های برنامه ریزی شده دستور می‌دهد تا بر اساس قیمت دستکاری شده از برق استفاده کنند، که منجر به افزایش مصرف انرژی در بخش مصرف کننده و توزیع مجدد بار در DN می‌شود. این نوع حمله می تواند سرانجام با رشد تنش و اضافه بار خط به شکست خط منجر شود. در این مقاله فرض شده است که برخی از اندازه‌گیره مشترکین مشارکت کننده در DRP برای افزودن داده‌های نادرست قیمت و بررسی تأثیر CA ها در برنامه پاسخگویی به تقاضای RTP مورد حمله قرار می‌گیرند. قیمت اضافه شده با حداقل و حداکثر میزان قیمت انرژی محدود می‌شود. همچنین، قدرت مهاجم با بودجه خاصی محدود می‌شود، بنابراین او می تواند تا زمانی که بودجه در دسترس باشد حمله کند.

$$LC_{at}=LC+at_{Sm,sm}\quad ,\quad \mathrm{LC}_{\min}\le LC_{at}\le LC_{\max} \quad (۴۰)$$

$$ABud_{at}<Bud \quad (۴۱)$$

همچنین، در نظر گرفته شده است که هر اندازه‌گیر هوشمند دارای یک ضریب سطح امنیتی (SecL) منحصر به فرد است. بنابراین، حمله با در نظر گرفتن بودجه مهاجم و SecL اندازه‌گیر شروع می‌شود. براساس این واقعیت، مهاجم مشتاق به دستکاری داده‌های اندازه‌گیرهایی است که حمله مقرون به صرفه درآید و حداکثر آسیب را به DN وارد کنند. اندازه گیر هوشمند SecL به شرح زیر است:

$$SecL=\left[SecL_1,SecL_2,...,SecL_n\right]\quad n\in Sm \quad (۴۲)$$

برای طراحی یک حمله موثر بر اندازه‌گیرهای هوشمند باید مسئله بهینه‌سازی زیر حل شود:

$$objective\ function \quad (۴۳)$$
$$Max\left\{TCost_{operation}\right\}$$

به شرطی که

$$-\lambda P_{bu}\le\hat{P}_{bu}-P_{bu}\le\lambda P_{bu} \quad (۴۴)$$

$$at_{Sm,sm}=0\ \Leftrightarrow\psi_{Sm,sm}=0\ \ \forall sm\in Sm \quad (۴۵)$$

$$100\sum_{Sm=1}^{N_{sm}}SecL\times\psi_{Sm,sm}\le ABud_{at} \quad (۴۶)$$

$$SecL\ge\beta\rightarrow\psi_{Sm,sm}=0 \quad (۴۷)$$

$$\psi_{Sm,sm}\in\{0,1\} \quad (۴۸)$$

تابع هدف سطح میانی افزایش هزینه بهره‌برداری با دستکاری در سیگنال قیمت کنتورهای هوشمند می‌باشد. معادلات (۴۴) تا (۴۸) محدودیت های حمله را مشخص می‌کنند. محدوده مجاز تغییر بار در (۴۴) نشان داده شده است. (۴۵) رابطه منطقی بین داده های تزریق-شده و بردار حمله را نشان می‌دهد. محدودیت (۴۶) حداکثر بودجه حمله را تضمین می‌کند. بر اساس (۴۷)، اندازه‌گیرها با امنیت سایبری بالا برای حمله در نظر گرفته نمی‌شوند. محدودیت (۴۸) ماهیت باینری حمله را تعریف می‌کند.

۲-۲-۱- برنامه مدیریت سمت بار بعد از حمله

در اینجا، یک مدل DR دنبال می‌شود که شامل تأمین‌کنندگان انرژی، ISO و مصرف‌کنندگان نهایی است و قیمت برق توسط ISO تعیین شده و به مشترکین و ارائه دهندگان انرژی اعلام می‌شود. در زیر، مدل ریاضی DR نشان داده شده است [۲۵]. مدل تک دوره‌ای DR به شرح زیر بدست می‌آید:

$$P_{l,n}(i)=P_{l,0}(i)\times\left\{1+E(i,i)\times\frac{LC_{l,n}(i)-LC_{l,0}(i)}{LC_{l,0}(i)}\right\}\quad\forall i,j\in t \quad (۴۹)$$

در رابطه الاستیسیته [۳۱]، اگر نسبت تغییرات بار به تغییرات قیمت ثابت باشد، مدل چند دوره DR به شرح زیر توصیف می‌شود:

$$P_{l,n}(i)=P_{l,0}(i)+\sum_{\substack{j=1\\ j\neq i}}^{24}E(i,j)\times\frac{P_{l,0}(i)}{LC_{l,0}(j)}\times\left[LC_{l,n}(j)-LC_{l,0}(j)\right] \quad (۵۰)$$

$\forall i,j\in t$

با توجه به معادلات (۴۹) و (۵۰)، مدل نهایی پایه زمانی DR به صورت (۵۱) تعیین می شود:

$$P_{l,n}(i)=P_{l,0}(i)\times\left\{\begin{array}{l}1+E(i,i)\times\dfrac{\left[LC_{l,n}(i)-LC_{l,0}(i)\right]}{LC_{l,0}(i)}+\\ \sum\limits_{\substack{j=1\\ j\neq i}}^{24}E(i,j)\times\dfrac{\left[LC_{l,n}(i)-LC_{l,0}(i)\right]}{LC_{l,0}(i)}\end{array}\right\}\quad\forall i\in t \quad (۵۱)$$

پس از حمله موفقیت‌آمیز و دستکاری سیگنال قیمت در پیک بار، قیمت برق کاهش و مصرف برق توسط مشترکین افزایش می‌یابد. بنابراین، این حمله در پیک بار اثرات گسترده‌ای بر DRP می‌گذارد و باعث ایجاد برخی تغییرات در فرمول بندی مدل نهایی DRP می‌شود:

$$P_{\mathrm{l,n}}(\mathrm{i})=P_{l,0,\mathrm{i}\neq t_a}(i)\times\left\{\begin{array}{l}1+E_{\mathrm{i}\neq t_a}(i,i)\times\dfrac{\left[LC_{l,n}(i)-LC_{l,0}(i)\right]}{LC_{l,0}(i)}+\\ \sum\limits_{\substack{j=1\\ j\neq i}}^{24}E_{\mathrm{i}\neq t_a}(i,j)\times\dfrac{\left[LC_{l,n}(j)-LC_{l,0}(j)\right]}{LC_{l,0}(j)}\end{array}\right\}+\ldots \quad (۵۲)$$

$$P'_{l,0,i=t_a}(i)\times\left\{\begin{array}{l}1+E_{i=t_a}(i,i)\times\dfrac{\left[LC_{l,n}(i)-LC_{l,0}(i)\right]}{LC_{l,0}(i)}+\\ \sum\limits_{\substack{j=1\\ j\neq i}}^{24}E_{i=t_a}(i,j)\times\dfrac{\left[LC_{l,n}(i)-LC_{l,0}(j)\right]}{LC_{l,0}(j)}\end{array}\right\}+\ldots$$

$$P''_{l,0,i=t_a}(i)\times\left\{\begin{array}{l}1+E_{i=t_a}(i,i)\times\dfrac{\left[LC_{a}-LC_{l,0}(i)\right]}{LC_{l,0}(i)}+\\ \sum\limits_{\substack{j=1\\ j\neq i}}^{24}E_{i=t_a}(i,j)\times\dfrac{\left[LC_{a}-LC_{l,0}(j)\right]}{LC_{l,0}(j)}\end{array}\right\}$$

در معادله (۵۲)، $P''_{l,0}$ و $P'_{l,0}$ به ترتیب مجموع بار حمله شده و بار حمله نشده است.

۲-۳-استراتژی دفاعی

استفاده از یک استراتژی دفاعی موثر برای تشخیص حمله توسط تخمین‌گر حالت و تکنیک‌های تشخیص برای محافظت از شبکه هوشمند در برابر CA (به ویژه حمله FDI) ضروری است. اگر مهاجمی بر پس مانده‌های اندازه‌گیری تأثیر نگذارد، حمله FDI شناسایی نمی‌شود زیرا تمام روشهای تشخیص داده‌های بد بر اساس باقیمانده اندازه‌گیری است. در این مقاله، فرض بر این است که حمله بر باقی مانده‌های اندازه‌گیری تأثیر نمی‌گذارد و بنابراین نمی‌توان حمله را تشخیص داد. به دلیل حمله FDI شناسایی نشده، دستکاری قیمت انرژی در برخی از اندازه گیرهای هوشمند و تغییر نقطه کارکرد بهینه شبکه، بسیاری از متغیرهای شبکه به عنوان بارگذاری خط، هزینه بهره برداری و ولتاژ باس ها تغییر می‌کنند. بنابراین، بهره‌بردار سیستم وجود یک اختلال در شبکه را مشاهده می‌کند که باعث افزایش هزینه بهره‌برداری شده است اما نمی‌تواند منابع اختلال را تشخیص دهد. DNR به عنوان یک استراتژی دفاعی از دیدگاه بهره‌بردار شبکه برای کاهش اثر اغتشاش پیشنهاد شده است. اصلاح ساختار DN با پیکربندی مجدد یکی از روشهای موثر برای توزیع مجدد بار، افزایش قابلیت اطمینان، کاهش هزینه بهره برداری و بهبود کیفیت توان است. DNR تغییر وضعیت تجهیزات کلیدزنی است که در صورت بروز نقص (یا آسیب تجهیزات) یا ایجاد اغتشاش در جهت تداوم تامین بار انجام می‌شود.

در این مقاله هزینه DNR از رابطه زیر بدست می آید:

$$T\ \mathrm{Cost}_{\mathrm{DNR}}=\sum_{Y\in\chi^{year}}NPV^{Y}\times\mathrm{Cost}_{DNR}\times\ldots$$

$$\left(\sum_{t\in\chi^{time}}\left(\begin{array}{l}\sum\limits_{f\in\chi^{F}}\left|z'_{cbs,f,t}-z_{cbs,f,t-1}\right|+\ldots\\ \sum\limits_{f\in\chi^{F}}\left|z'_{\mathrm{Sec}S,f,t}-z_{\mathrm{Sec}S,f,t-1}\right|\end{array}\right)\right);\ \ z\in\{0.1\} \quad (۵۳)$$

که Z نشان دهنده وضعیت کلید نصب شده روی فیدر f است.

پس از CA و دستکاری سیگنال قیمت در اندازه‌گیرهای هوشمند، بار در DN باز توزیع می‌شود. بنابراین، هزینه بهره‌برداری در مقایسه با وضعیت عادی متفاوت خواهد بود که از رابطه زیر قابل محاسبه است:

$$\mathrm{TCost}''_{\mathrm{Operation}}=$$

$$NPV\times\left(\begin{array}{l}\sum\limits_{b\in\chi^{bus}}\sum\limits_{\substack{t\in\chi^{time}\\ t\notin t_a}}\left(O\hat{M}C_{HVS_{su},b,t}+O\hat{M}C_{DG_{dg},b,t}\right)+\ldots\\ T\hat{C}ost_{loss}+T\hat{C}ost_{PtransferCo}+T\hat{C}ost_{DNR}+\ldots\\ T\hat{C}ost_{DR}+T\hat{C}ost_{ENS}+\mathrm{T\hat{D}C}+\ldots\\ \sum\limits_{b\in\chi^{bus}}\sum\limits_{t\in t_a}\left(O\tilde{M}C_{HVS_{su},b,t}+O\tilde{M}C_{DG_{dg},b,t}+\right)+\ldots\\ T\tilde{C}ost_{loss}+T\tilde{C}ost_{PtransferCo}+T\tilde{C}ost_{DNR}+\ldots\\ T\tilde{C}ost_{DR}+T\tilde{C}ost_{ENS}+\mathrm{T\tilde{D}C}\end{array}\right) \quad (۵۴)$$

استراتژی دفاعی پیشنهادی را می توان به شرح زیر فرمول بندی کرد:

objective function

$$\left\{\hat{P}_{br}\right\}=\arg\left\{\mathrm{TCost}''_{\mathrm{operation}}\right\} \quad (۵۵)$$

$$SW=\left[SW_1,SW_2,\ldots,SW_n\right] \quad (۵۶)$$

$$SW\in\{0,1\} \quad (۵۷)$$

$$NL_{mL}=NB_{br}-N_{bu}+1 \quad (۵۸)$$

$$\bar{P}_{\mathrm{Load}_{b_0,Y,t}}-P_{\mathrm{GEN}_{dg,b_0,Y,t}}=\ldots$$

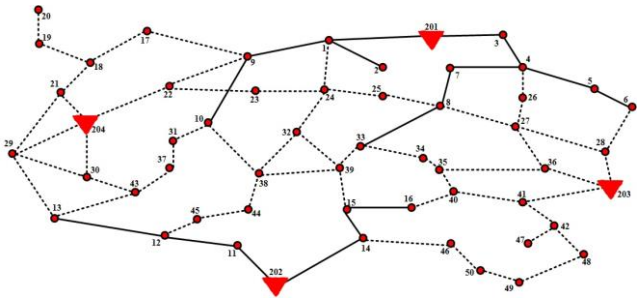
$$V_{b_0,Y,t}\times\sum_{b\in\chi^{bus}}V_{b_0,Y,t}\times V_{b,b_0}\times\mathrm{Cos}\left(\beta_{b,Y,t}-\beta_{b_0,Y,t}-\theta_{b,b_0}\right) \quad (۵۹)$$

$$\bar{Q}_{\mathrm{Load}_{b_0,Y,t}} - Q_{\mathrm{GEN}_{\mathrm{dg},b_0,Y,t}} = \ldots$$
$$V_{b_0,Y,t} \times \sum_{b\in\chi^{bus}} V_{b_0,Y,t} \times V_{b,b_0} \times \mathrm{Sin}\left(\beta_{b,Y,t} - \beta_{b_0,Y,t} - \theta_{b,b_0}\right) \quad (۶۰)$$

همین‌طور (۳۸) و (۳۹) نیز برای این سطح باید محاسبه گردد تا انحراف از قیود رخ ندهد. دفاع بهینه بهره‌بردار در برابر حمله برای کاهش هزینه بهره برداری با توجه به محدودیت‌های (۵۶) تا (۶۰) در سطح پایین‌تر فرمول‌بندی شده است. محدودیت‌های (۵۶) و (۵۷) وضعیت SW را نشان می‌دهند. محدودیت (۵۸) ساختار شعاعی DN را تضمین می‌کند. تجزیه و تحلیل جریان بار در محدودیت‌های (۵۹) و (۶۰) براساس توازن توان در هر گذرگاه شبکه می‌باشد.

۳- مطالعات شبیه‌سازی

برای اثبات امکان‌پذیری و صحت روش پیشنهادی، شبیه‌سازی بر روی شبکه توزیع ۵۴ باسه انجام شده است. همانطور که در شکل (۲) نشان داده شده است گره‌های ۲۰۱ و ۲۰۲ پست‌های فوق توزیع موجود و ۲۰۳ و ۲۰۴ کاندید نصب پست هستند. خطوط سیاه نمایانگر فیدرهای موجود و خطوط خط‌چین، مسیرهای کاندید هستند.



شکل(۲): شبکه ۵۴ باسه نمونه

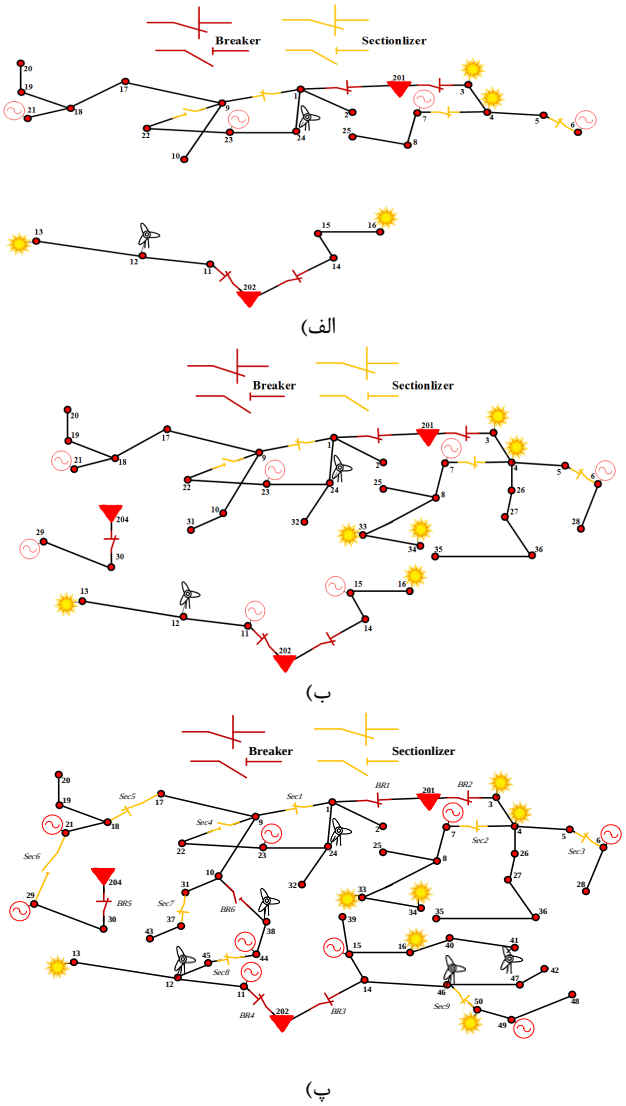
برای اجرای شبیه‌سازی سیستم، از نرم‌افزار شخصی مبتنی بر MATLAB، DisPOS (نرم‌افزار برنامه‌ریزی و بهره‌برداری از شبکه توزیع) استفاده شده است. این نرم‌افزار در مطالعات مختلف مورد آزمایش قرار گرفته است.

۳-۱- نتایج عددی

نتایج حاصل از شبیه سازی روش پیشنهادی به تفکیک ۳-سطح تعریف شده، در ذیل آمده است.

۳-۱-۱- نتایج مربوط به سطح اول روش پیشنهادی

شکل ۳ نشان‌دهنده ساختار سالانه شبکه توزیع بهینه است، که توانایی روش پیشنهادی را برای پیکربندی شبکه حلقوی که در آن مکان و نوع کلیدهای نصب شده مشخص است، را اثبات می‌کند. وضعیت باز/بست این کلیدها، نمایش داده شده در این شکل، مربوط به بهره برداری حالت عادی شبکه است که در صورت بروز خطا و جهت کمینه کردن مقدار انرژی از دست رفته؛ وضعیت این کلیدها تغییر خواهد کرد. در شکل ۳ الف، شبکه توزیع بهینه برای سال اول نشان داده شده است که با توجه به رشد بار در سال های بعد، این شبکه طبق آنچه که در ۳ ب و ج نمایش داده شده گسترش یافته است. پر واضح است که در افق سال های دور استفاده بیشتر از تجهیزات و منابع تولید پراکنده بیشتر خواهد شد.



شکل(۳): ساختار سالانه شبکه توزیع بهینه الف) سال اول ب) سال دوم پ) سال سوم تا پنجم

یکی دیگر از اهداف تعیین ظرفیت سالانه پست‌های فوق‌توزیع در شبکه است. جدول (۲) ظرفیت پست‌های نصب‌شده را در سال‌های مختلف دوره برنامه‌ریزی نشان می‌دهد. علاوه براین، در جدول (۳) بارگیری پست‌های فوق‌توزیع در سال‌های مختلف آمده است. نتایج موید آن است، که قیود موجود در نصب پست فوق توزیع از جمله حداکثر مقدار توسعه سالانه محدودیت بارگیری پست را رعایت کند.

جدول (۲): ظرفیت پست های فوق توزیع

شماره پست	مگا ولت آمپر				
	سال اول	سال دوم	سال سوم	سال چهارم	سال پنجم
۲۰۱	۳۰	۳۷/۵	۴۵	۵۲/۵	۶۰
۲۰۲	۱۵	۱۵	۱۵	۲۲/۵	۳۰
۲۰۳	۰	۰	۰	۰	۰
۲۰۴	۰	۷/۵	۷/۵	۷/۵	۷/۵

جدول (۳): بارگیری پست های فوق توزیع

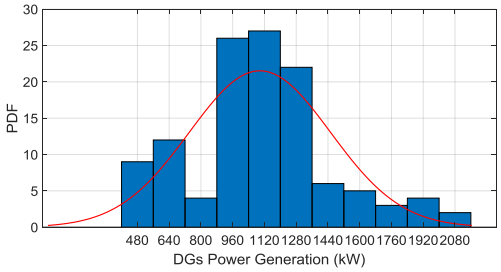
شماره پست	مگا ولت آمپر				
	سال اول	سال دوم	سال سوم	سال چهارم	سال پنجم
۲۰۱	۶۶/۴	۷۲/۷	۷۸/۹	۷۹/۴	۷۴/۲
۲۰۲	۴۵/۴	۴۷/۱	۷۸	۷۹/۱	۷۲
۲۰۳	۰	۰	۰	۰	۰
۲۰۴	۰	۸/۳	۱۷/۸	۲۹	۳۱/۱

هدف دیگری که در برنامه‌ریزی توسعه شبکه توزیع، مورد توجه جدی است، یافتن اندازه هادی مورد استفاده در فیدرها است. همانطور که در شکل (۳) مشخص است، انواع منابع تولید پراکنده در سال‌های مختلف در مکان‌های مختلفی نصب شده و در جدول (۴) ارائه می‌شود که در آن نوع، سال نصب، ظرفیت و باس آورده شده است.

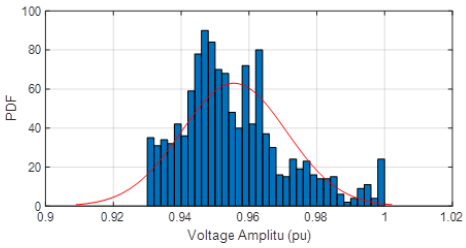
جدول(۴): مکان، ظرفیت، زمان نصب و باس منابع پراکنده

	(اندازه(کیلو وات)، مکان(شماره باس)، زمان(سال))
کنترل پذیر	(1, 6, 50); (1, 7, 400); (1, 21, 250); (1, 23, 250); (2, 11, 300); (2, 15, 250); (2, 29, 150); (3, 44, 150); (4, 49, 250);
بادی	(1, 12, 100); (1, 24, 100); (3, 41, 50); (3, 46, 50); (4, 38, 100); (5, 38, 100);
خورشیدی	(1, 3, 100); (1, 4, 50); (1, 13, 50); (1, 16, 50); (2, 13, 50); (2, 16, 50); (2, 33, 100); (2, 34, 100); (3, 50, 150); (4, 50, 50);

روشن است که شرکت توزیع به منظور بهره‌برداری اقتصادی از شبکه، باید مقدار تولید هر یک از منابع تولید پراکنده را مشخص نماید. از این روی، تابع توزیع تولید منابع تولید پراکنده طی دوره برنامه‌ریزی در شکل (۴) آمده است. شاخص مهم تأثیرگذار بر پارامترهای مختلف شبکه توزیع از جمله، تلفات، پایداری ولتاژ، جریان عبوری و... دامنه ولتاژ است. از این روی، محدودیتی برای دامنه ولتاژ در نظر گرفته می‌شود که راهکار نهایی باید رعایت کند. برای تأیید این که دامنه ولتاژ شبکه بهینه در محدوده قابل قبول حفظ شده است، تابع توزیع احتمال ولتاژ شبکه با در نظر گرفتن ولتاژ تمامی باس‌ها در طی دوره برنامه‌ریزی در شکل (۶) نشان داده شده است. محور افقی، نمایشگر دامنه ولتاژ می‌باشد. منحنی قرمز رنگ، برازش ستون‌های آبی با منحنی نرمال است. همانطور که از شکل پیداست، میانگین ولتاژ در محدوده قابل قبولی قرار دارد که خود موید کارایی روش پیشنهادی در طراحی شبکه با حفظ قیود فنی شبکه دارد.



شکل (۴): تولید منابع تولید پراکنده در دوره برنامه ریزی



شکل (۵): دامنه ولتاژ شبکه در طی دوره برنامه ریزی

در ادامه، جزییات مربوط به مقادیر اجزا مختلف تابع هدف‌های متفاوت در جدول (۵) آمده است.

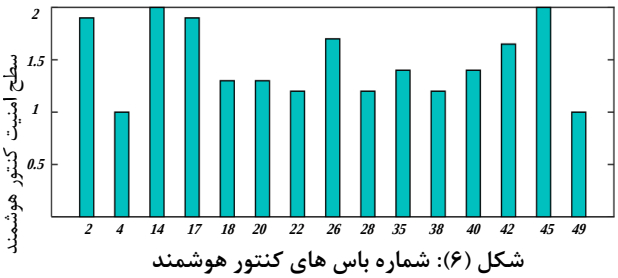
جدول (۵): مقادیر توابع هدف مختلف در بهترین جواب مصامحه

هزینه پست	۹۹۲۸۲۸۳/۸۳۴
هزینه فیدر	۱/۴۶۹۷۶e+۱۱
هزینه تجهیزات کلیدزنی	۲۱۳۸۴۷/۴۰۷۵
هزینه منابع تولید پراکنده	۴۶۷۳۳۸۳/۰۸۷
هزینه تلفات	۲۹۶۶۰۶۰۶/۲۴
هزینه انتقال توان	۳۰۵۱۰۵۴/۸۲۹
هزینه قابلیت اطمینان	۱۰۰۸۱۵۷۸۳۸۴

۳-۱-۲- نتایج مربوط به سطح دوم و سوم روش پیشنهادی

در این بخش اثر حمله‌ی سایبری از نوع تزریق داده‌های کاذب بر روی شبکه توزیع هوشمند مطالعه و همچنین تاثیر روش پیشنهادی دفاعی در مقابل حمله‌ی سایبری ارزیابی شده است. در این مقاله فرض بر این است که مشارکت کنندگان برنامه پاسخگویی بار هدف حمله هستند که مهاجم با توجه به بودجه ی محدود خود ($Bud=1000\$$) و سطح امنیتی اندازه گیرهای هوشمند، سیگنال قیمت برق را دستکاری کرده و قیمت برق مشترکین را در ساعت پیک بار ($t_a=21$) از $۴۵\ \$$ به $LC=۳۰\ \$$ کاهش می‌دهد. قیمت زمان واقعی برق برای ۲۴ ساعت یک روز و در جدول ۷ الاستیسیته خودی در مرجع [۱۱] ارایه شده است. شکل (۷) نشان دهنده مشترکین شرکت کننده در

برنامه پاسخگویی بار و سطح امنیت اندازه گیرهای هوشمند آنها می‌باشد. سطح امنیت اندازه گیرهای هوشمند بین ۱ و ۲ در نظر گرفته شده است که براساس تحقیقات آزمایشگاهی و میدانی بدست امده است و اندازه‌گیر هوشمند با سطح امنیت ۱ از نظر امنیت سایبری ضعیفترین و اندازه گیر هوشمند با سطح امنیت ۲ بهترین می‌باشد. در این مقاله فرض شده است که اندازه گیر هوشمند با سطح امنیت ۲ به دلیل احتمال بالای آشکار شدن حمله مورد حمله قرار نمی‌گیرد. بنابراین با افزایش سطح امنیت اندازه‌گیرهای هوشمند شانس مهاجم برای یک حمله موفق کاهش می‌یابد که اثربخش کردن این چنین حملات مستلزم هزینه بالایی است که اغلب خارج از توان مهاجم می‌باشد. به همین دلیل بخش مشترکین به یک کاندید بالقوه برای حمله تبدیل شده است که می‌تواند آثار مخرب و جبران‌ناپذیری به دنبال داشته باشد. اندازه‌گیرهای هوشمند حمله شده در سناریوهای مختلف در جدول ۸ آورده شده است که نمایش دهنده بهینه‌ترین مکان‌های حمله می‌باشد. این جدول نشان می‌دهد که برخی از اندازه‌گیرهای هوشمند با وجود سطح امنیتی بالا مورد حمله واقع شده است چون تاثیر مخرب زیادی داشته‌اند و شبکه را وارد یک استرس کرده است. در این جدول قابل مشاهده است که با یک بودجه ثابت با افزایش سطح امنیتی اندازه‌گیرهای هوشمند تعداد اندازه‌گیرهای مورد حمله واقع شده، کاهش یافته است که به نوبه خود نشان دهنده کاهش آثار مخرب حمله سایبری می‌باشد و همچنین بیانگر این نکته است که افزایش سطح امنیتی برای اندازه گیرهای هوشمند به رغم هزینه بالای آن الزامی می‌باشد.



شکل (۶): شماره باس های کنتور هوشمند

جدول (۶): مترهای هوشمند حمله شده

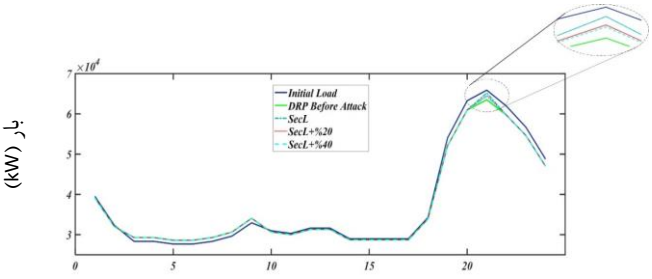
شماره سناریو	سطح امنیت	اندازه گیرهای هوشمند حمله شده
۱	SecL	۴۹-۴۲-۲۸-۲۶-۲۲-۲۰-۲
۲	SecL۲۰٪+	۴۹-۴۲-۳۵-۲۸-۲۲-۲۰
۳	SecL۴۰٪ +	۴۹-۳۵-۲۸-۲۲-۲۰-۴

جدول (۷) هزینه بهره‌برداری از شبکه توزیع هوشمند بهینه در سال پنجم طی سناریوهای مختلف برای بعد از حمله و بعد از اقدام دفاعی بهره بردار را نشان می‌دهد. با توجه به جدول، مشاهده می‌شود که هزینه بهره‌برداری بعد ازحمله ۳۱/۶۸درصد افزایش یافته است. افزایش هزینه بهره‌برداری در پیک بار با توجه به وجود منابع تولید پراکنده در شبکه می‌تواند شدیدا شبکه روا تحت تاثیر قرار دهد. بهره‌بردار بعد از مشاهده اغتشاش در شبکه با هدف مقابله با اغتشاش به وجود آمده شروع به بازآرایی شبکه می‌کند که درنتیجه، هزینه بهره‌برداری نسبت به حالت حمله ۱۴/۲۱درصد کاهش پیدا می‌کند. با افزایش سطح امنیت اندازه‌گیرهای هوشمند هزینه بهره‌برداری بعد از حمله کاهش قابل توجهی داشته بطوریکه با افزایش ۴۰ درصدی سطح امنیت اندازه‌گیرهای هوشمند ۱۹/۴۱ درصد از هزینه بهره‌برداری نسبت به سناریوی اول کاهش می‌یابد.

جدول (۷): هزینه بهره‌برداری از شبکه توزیع هوشمند در سال پنجم در سناریو های مختلف در ساعت حمله

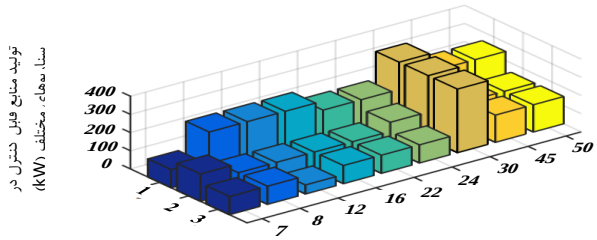
هزینه بهره برداری از شبکه در حالت عادی :$ ۴۱۹۳/۶۳۲			
شماره سناریو	سطح امنیت	هزینه بهره‌برداری بعد از حمله ($)	هزینه بهره‌برداری بعد از دفاع ($)
۱	SecL	۶۱۳۱/۷۶۷	۵۲۶۰/۳
۲	SecL ٪۲۰+	۵۶۴۶/۷۳	۴۹۶۳/۸۰۵
۳	SecL ٪۴۰ +	۴۹۴۱/۵۱۳	۴۳۱۲/۳۴۶

شکل (۷) منحنی بار شبکه را در حالت های مختلف نشان می‌دهد. با توجه به اینکه در پیک بار مهاجم با دستکاری سیگنال قیمت، قیمت برق را برای برخی از مشترکین کاهش داده است واحد کنترل مصرف مشترکین فرمان مصرف برق را برای وسایل هوشمند خانه مثل باتری‌ها و خودروهای الکتریکی و ... را صادر می‌کند و بدین ترتیب مصرف برق در پیک بار به رغم اجرای برنامه پاسخگویی و بر خلاف انتظارات افزایش می‌یابد. پیک بار در حالت عادی و بعد از اجرای برنامه پاسخگویی بار در شبکه پیشنهادی ۸/۳۲ درصد کاهش می‌یابد که این عدد بعد از حمله به ۱/۸۷ درصد افزایش داشته است (مصرف افزایش ۶/۴۵ درصد را تجربه می‌کند). افزایش غیر منتظره مصرف برق از سوی مشترکینی که تحت حمله سایبری هستند باعث به وجود آمدن مشکلات مالی، فیزیکی و فنی برای شبکه توزیع هوشمند می‌شود که می‌توان به افزایش هزینه بهره‌برداری، کاهش قابلیت اطمینان، افزایش تلفات و حتی قطع سراسری برق اشاره کرد.



شکل (۷): منحنی بار در سناریوهای مختلف

طبق شکل ۸، تولید توان توسط منابع تولید قابل کنترل در سناریوی اول و بعد از حمله برای جبران افزایش بار، افزایش یافته است. همینطور حالت بهینه کلیدها بعد از بازآرایی شبکه در جدول (۸) نشان داده شده است.



شکل (۸): توان تولیدی منابع تولید پراکنده قابل کنترل قبل، حین و بعد از حمله در سناریوهای مختلف

جدول (۸): حالت بهینه کلیدها در سناریوهای مختلف بعد از بازآرایی

	BR1	BR2	BR3	BR4	BR5	BR6	Sec1	Sec2	Sec3	Sec4	Sec5	Sec6	Sec7	Sec8	Sec9
SecL	۱	۱	۱	۱	۱	۰	۱	۱	۱	۰	۰	۱	۱	۱	۱
SecL+%10	۱	۱	۱	۱	۱	۱	۱	۱	۱	۰	۱	۰	۱	۰	۱
SecL+%20	۱	۱	۱	۱	۱	۰	۱	۱	۱	۰	۱	۰	۱	۱	۱

۴- نتیجه‌گیری

یک چالش بزرگ پیش روی شبکه توزیع هوشمند، آسیب‌پذیری شدید امنیت فیزیکی-سایبری سیستم ارتباطی در برابر حملات سایبری می‌باشد. گسترش اثرات مخرب حملات سایبری بر شبکه توزیع هوشمند نشان می‌دهد که طراحی، برنامه‌ریزی و عملکرد شبکه‌های توزیع هوشمند با استفاده از تکنیک‌های موجود و طرح‌های رایج با چالش‌های جدی روبرو است. برنامه‌ریزی توسعه مقرون به صرفه شبکه‌های توزیع هوشمند در حضور حملات سایبری و با استفاده دقیق از تجهیزات کلیدزنی، منابع انرژی پراکنده مختلف برای اطمینان از تداوم نیرورسانی ضروری است. همانطور که در بخش تحلیل نتایج شبیه‌سازی بیان شد هزینه بهره‌برداری از شبکه بعد از حمله ۳۱/۶۸ درصد افزایش یافته است که بعد از اجرای روش دفاعی پیشنهادی هزینه بهره‌برداری کاهش ۱۴/۲۱ درصدی نسبت به حالت حمله دارد که این امر نشان از کارایی روش پیشنهادی دارد. همچنین با افزایش سطح امنیت مترهای هوشمند هزینه بهره‌برداری کاهش چشمگیری داشته به‌طوریکه با افزایش ۴۰ درصدی سطح امنیت هزینه بهره‌برداری نسبت به سناریوی اول کاهش ۱۹/۴۱ درصدی را شاهد هستیم که اهمیت امنیت بالای مترهای هوشمند را نشان می‌دهد که این واقعیت مهم در منحنی الگوی مصرف نیز آشکار می‌باشد.

بنابراین راه حل به دست آمده از روش پیشنهادی، نقشه راه اقدامات شرکت توزیع تا سال هدف را ارائه می‌دهد، این اقدامات شامل نصب تجهیزات جدید یا جایگزینی یا تقویت تاسیسات قبلی از نظر فنی و امنیتی و همچنین عملکرد دارایی های مختلف در شرایط عادی عملکرد و زمانی که حمله سایبری رخ می دهد، است.

مراجع

[1] Vahidinasab, Vahid, Mahdi Tabarzadi, Hamidreza Arasteh, Mohammad Iman Alizadeh, Mohammad Mohammad Beigi, Hamid Reza Sheikhzadeh, Kamyar Mehran, and Mohammad Sadegh Sepasian. "Overview of Electric Energy Distribution Networks Expansion Planning." IEEE Access 8 (2020): 34750-34769.

[2] Sajad Najafi-Ravadanegh, Mohammad-Reza Jannati-Oskuee, Masoumeh Karimi and Hasan Hedayati, "Electric Power Infrastructure Resilience (in Farsi)", Azarbaijan Shahid Madani University, 2020, ISSN: ۰-۰۵-۰۹۷۸-۶۲۲-۶۷۳۷

[3] K. Kenneth, O. Vitalice and L. Kibet, Cyber security challenges for IoT-based smart grid networks, international journal of critical infrastructure protection, 25, pp.36–49, 2019.

[4] Paterakis, N.G.; Erdinç, O.; Catalão, J.P.S. An overview of Demand Response: Key-elements and international experience. Renew. Sustain. Energy Rev. 2017, 69, 871–891.

[5] Espe, E.; Potdar, V.; Chang, E.; Espe, E.; Potdar, V.; Chang, E. Prosumer Communities and Relationships in Smart Grids: A Literature Review, Evolution and Future Directions. Energies 2018, 11, 2528.

[6] Siano, P.; Sarno, D. Assessing the benefits of residential demand response in a real-time distribution energy market. Appl. Energy 2016, 161, 533–551.

[7] Y. Chen, S. Kar, J. M. F. Moura, Optimal Attack Strategies Subject to Detection Constraints Against Cyber-Physical Systems, IEEE Transactions on Control of Network Systems, 5(3), pp. 1157 – 1168, 2018

[8] Sh. Khan, S. E. Madnick, Cyber safety: A System-theoretic Approach to Identify Cyber-vulnerabilities & Mitigation Requirements in Industrial Control Systems, IEEE Transactions on Dependable and Secure Computing, 2021.

[9] L. Guo, J. Ye, L. Du, Cyber–Physical Security of Energy-Efficient Powertrain System in Hybrid Electric Vehicles Against Sophisticated Cyberattacks, IEEE Transactions on Transportation Electrification, 7(2), pp. 636 – 648, 2021

[10] Teixeira, D. Pérez, H. Sandberg, K. Johansson Attack models and scenarios for networked control systems HiCoNS '12: Proceedings of the 1st international conference on High Confidence Networked Systems, pp. 55–64, 2012

[11] P. Amirpour Giglou, S. Najafi Ravadanegh, Defending against false data injection attack on demand response program: A bi-level strategy, Sustainable Energy, Grids and Networks, 27, 2021

[12] Liu, Y., Ning, P., and Reiter, M. K. (2011). False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Secur. 14 (1), 1–33. doi:10.1145/1952982.1952995

[13] Zh. Qu, Y. Dong, N. Qu False Data Injection Attack Detection in Power Systems Based on Cyber-Physical Attack Genes, Frontiers in Energy Research 9, 2021

[14] Tan Y, Das AK, Arabshahi P, et al. Distribution systems hardening against natural disasters. IEEE Trans Power Syst 2018;33(6):6849–60.

[15] Popović, Željko N., Neven V. Kovački, and Dragan S. Popović. "Resilient distribution network planning under the severe windstorms using a risk-based

approach." Reliability Engineering & System Safety 204 (2020): 107114.

[16] Ma S, Li S, Wang Z, Qiu F. Resilience-oriented design of distribution systems. IEEE Trans Power Syst 2019; 34:2880–91. https://doi.org/10.1109/TPWRS.2019.2894103.

[17] Shi, Qingxin, Fangxing Li, Mohammed Olama, Jin Dong, Yaosuo Xue, Michael Starke, Chris Winstead, and Teja Kuruganti. "Network reconfiguration and distributed energy resource scheduling for improved distribution system resilience." International Journal of Electrical Power & Energy Systems 124: 106355.

[18] P. Babahajiani, Q. Shafiee, H. Bevrani, Intelligent demand response contribution in frequency control of multi-area power systems, IEEE Trans. Smart Grid 9 (2) (2018) 1282–1291.

[19] Xie S, Hu Z, Zhou D, Li Y, Kong S, Lin W, et al. Multi-objective active distribution networks expansion planning by scenario-based stochastic programming considering uncertain and random weight of network. Appl Energy 2018;219:207–25.

[20] Zhang S, Cheng H, Wang D, Zhang L, Li F, Yao L. Distributed generation planning in active distribution network considering demand side management and network reconfiguration. Appl Energy 2018;228:1921–36.

[21] Zadsar, M., S. Sina Sebtahmadi, M. Kazemi, S. M. M. Larimi, and M. R. Haghifam. "Two stage risk based decision making for operation of smart grid by optimal dynamic multi-microgrid." International Journal of Electrical Power & Energy Systems 118 (2020): 105791.

[22] Zadsar, M., S. Sina Sebtahmadi, M. Kazemi, S. M. M. Larimi, and M. R. Haghifam. "Two stage risk based decision making for operation of smart grid by optimal dynamic multi-microgrid." International Journal of Electrical Power & Energy Systems 118 (2020): 105791

[23] Asensio M, Meneses de Quevedo P, Munoz-Delgado G, Contreras J. Joint distribution network and renewable energy expansion planning considering demand response and energy storage – Part I: Stochastic Programming Model. IEEE Trans Smart Grid 2018;9(2):655–66.

[24] Yodo, Nita, and Tanzina Arfin. "A resilience assessment of an interdependent multi-energy system with microgrids." Sustainable and Resilient Infrastructure (2020): 1-14.

[25] Taghizadegan, Navid, Sajad Najafi Ravadanegh, Masoumeh Karimi, and Mohammad Reza Jannati Oskuee. "A Solution Compatible with Cost-Reliability for Multi-Stage Feeder Routing Problem with Considering Uncertainties." IETE Journal of Research 65, no. 4 (2019): 435-445.

[۲۶] مقیمی محمود، اکبری پور حسین، امین ناصری محمد رضا، "طراحی سیستم خبره به منظور تشخیص حمله‌های فیشینگ در بانکداری الکترونیکی"، مجله انجمن مهندسین برق و الکترونیک ایران، جلد ۱۲ شماره ۲، ۹۵-۱۰۴ ، ۱۳۹۵

[۲۷] علیزاده، محمد ایمان، غفارپور، رضا، رنجبر، علی محمد، "بهینه‌سازی سه سطحی مقاوم مشارکت واحدها با هدف تاب‌آوری در سیستم قدرت با نفوذ بالای منابع اتکاناپذیر" ، مجله انجمن مهندسین برق و الکترونیک ایران، جلد ۱۷ شماره ۲، ۱۱۳-۱۲۱، ۱۳۹۹.

[1] Distribution Network Expansion Planning

[2] Smart Distribution networks

[3] High Impact Low Probablity

[4] Cyber Attack

[5] False Data Injection

[6] Distribution Company

[7] Demand Response Program