دوازدهمین کنفرانس مهندسی برق ایران
۲۴-۲۲ اردیبهشت ۱۳۸۳

تشخیص خطای امپدانس بالا در خطوط توزیع قدرت با استفاده از الگوریتم شناسایی خودی از بیگانه درسیستمهای ایمنی

محمد حسن محمدیان حبیب رجبی مشهدی جواد ساده
گروه برق - دانشکده مهندسی دانشگاه فردوسی مشهد
mh_mohamadian@hotmail.com h_mashhadi@um.ac.ir javsadeh@yahoo.com

چکیده: حفاظت از سیستمهای توزیع قدرت دربرابر رخدادهای غیر طبیعی شبکه از جمله اتصال کوتاه، صاعقه، اضافه ولتاژ و جریان وغیره از جمله مسائلی است که از گذشته تا امروز همواره مورد نظر محققان و کارشناسان صنایع برق بوده است. از مهمترین خطاهایی که در شبکه توزیع قدرت می تواند رخ دهد، اتصال کوتاه شدن خط با یک امپدانس بالا می باشد. در اینحالت رله های جریانی که براساس دامنه شکل موج جریان عمل می کنند قادر به تشخیص نبوده و بنابر این عمل نمی کنند. در این مقاله بر اساس شناسایی خودی از بیگانه که در سیستمهای ایمنی بدن بکار می رود، برای تشخیص وقوع یک خطای امپدانس بالا در خطوط توزیع قدرت استفاده می شود. برای تشریح چگونگی انجام این کار ابتدا مبانی ریاضی و الگوریتم کار توضیح داده شده، سپس روش پیاده سازی این الگوریتم برای شبکه توزیع قدرت ارائه می گردد. در انتها نیز نتایج شبیه سازی برای حالتهای مختلف آورده شده است.

واژه های کلیدی: خطای امپدانس بالا[1]، خودی و بیگانه[2]، آشکارساز[3]، امپدانس بالا.

۱- مقدمه

خطاهای امپدانس بالا خطاهایی هستند که تغییرات کوچکی در اندازه جریان خط ایجاد نموده و بنابر این قابل تشخیص توسط فیوزهاو رله های جریانی معمولی نمی باشند. خطاهای امپدانس بالا معمولا با قطع یکی از خطوط و افتادن آن بر روی زمین اتفاق می افتند. در اینحالت اینکه خط قطع شده بر روی چه زمینی بیافتد رفتار جریان عبوری در خط عوض خواهد شد. بعنوان مثال افتادن خط برروی زمین خشک یا مرطوب و با جنسهای متفاوت از قبیل چوب، سنگ، آهن وغیره منجر به تغییر شکل موج جریان خواهد شد. از آنجاییکه وقوع خطا در خطوط توزیع یک پدیده تصادفی می باشد، بنابراین رفتار خط یک رفتار تصادفی بوده و بایستی باآن بصورت یک رخداد تصادفی برخورد نمود. باتوجه به اینکه امپدانس اتصال کوتاه بزرگ می باشد بنابر این دامنه جریان عبوری از این مسیر کوچک بوده پس از دید شبکه با آن بصورت یک بار برخورد می شود. نکته مهم دراین نوع خطاها تغییر رفتار لحظه ای شکل موج نسبت به بارهای عادی می باشد. با توجه به توسعه روز افزون سیستمهای کامپیوتری می

1- High Impedance Fault
2- Self and Non-self
3- Detector

توان ازالگوریتمهای خاصی برای شناسایی این خطاها سود جست[2-1]. تفاوت الگوریتمها درسرعت و توانایی تشخیص می باشد.

در این مقاله یک الگوریتم شناسایی جدید بر پایه مکانیزم تشخیص خودی از بیگانه که در سیستم ایمنی بدن بکار می رود را طراحی می کنیم. در بخش بعدی، الگوریتم شناسایی خودی از بیگانه که در سیستم ایمنی بدن بکار می رود تشریح شده و بیان خواهد شد که بدن چگونه از ورود غیر مجاز یک شی خارجی آگاه می شود. سپس از این الگوریتم بهره گرفته ودر شناسایی سیگنالهای خودی "شکل موج جریان خط برای بارهای عادی شبکه"از سیگنالهای بیگانه "جریان اتصال کوتاه با امپدانس بالا" کمک خواهیم گرفت.

۲- تشخیص خودی از بیگانه در سیستم ایمنی بدن

۲-۱- شبکه ایمنی بدن[3]

واکنش سیستم ایمنی بدن در برابر عوامل خارجی دارای ویژگیهای جالبی است که آنرا به عنوان یک سیستم هوشمند معرفی می کند. از مهمترین این ویژگیها می توان به حافظه دار بودن سیستم ایمنی، داشتن پاسخ اختصاصی بر علیه آنتی ژنهای مختلف، قابلیت یادگیری و تشخیص سلولهای خودی از بیگانه اشاره کرد. بررسی عملکرد سیستم ایمنی و مدلسازی ریاضی آن، میدان تحقیقاتی وسیعی را برای محققین رشته های مختلف گشوده است[4]. همگام با شناخت بیشتر سیستم ایمنی، زمینه برای الهام از روشهای به خدمت گرفته شده در این سیستم طبیعی و کاربرد این روشها در حل مسایل مصنوعی فراهم گشته است[7-5]. شبکه ایمنی از سه نوع سلول تشکیل شده است.

ماکروفاژ[1]: این سلولها، سلولهای بیگانه خوار در ایمنی ذاتی بوده و ارائه کننده سلولهای آنتی ژن می باشند.

سلولهایT[2]: این سلولها دارای دو کلاس اصلی بوده ویک زیرمجموعه از لمفوسیتها[3] می باشند. کلاس اول این سلولها، ویروسها و عوامل مزاحم را از بین می برند. کلاس دوم شامل سلولهایی است که با دیگر سلولها از قبیل سلولهایB[4] و ماکروفاژها همکاری می کنند.

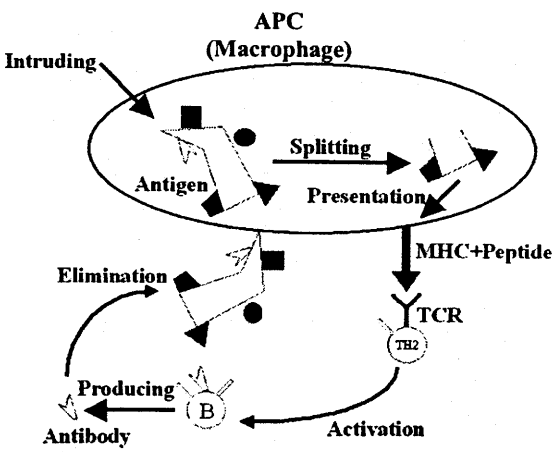
سلولهایB: این سلولها یکی از دو کلاس اصلی لمفوسیتها می باشند. گیرنده آنتی ژن بر روی لمفوسیت B که گاهی اوقات گیرنده سلول B نامیده می شود، یک سطح سلولی مولکول ایمونوگلوبین می باشد.

روش کار سیستم ایمنی بدن به این صورت می باشد که ابتدا یک آنتی ژن در ماکروفاژ تولید شده و سپس ماکروفاژ، آنتی ژن را به اجزای کوچکتری به نام پپتید[5] تقسیم کرده و به سطح سلولی ارائه می نماید. پس از آن سلولهایT به تشخیص پپتید پرداخته و با کمک سلولهایB سعی می نمایند آنتی بادیها را با آنتی ژن مربوطه تطابق دهند. چنانچه آنتی بادیی از قبل وجود داشته باشد، پس از تشخیص شروع به تولید نموده و باعث از بین رفتن سلولهای بیگانه می شوند. در غیر اینصورت شروع به ساخت آنتی بادی خاص این آنتی ژن نموده و پس از تولید علاوه بر از بین بردن سلول بیگانه، در حافظه شبکه باقی می ماند. شکلهای (۱)و (۲) شبکه ایمنی بدن و روش کار آنرا نشان می دهد.

۲-۲- مبانی ریاضی

همانگونه که در بخش ۲-۱ آمد، سلولهای ایمنی بصورت تصادفی ساخته شده ودر حافظه نگهداری می شوند.

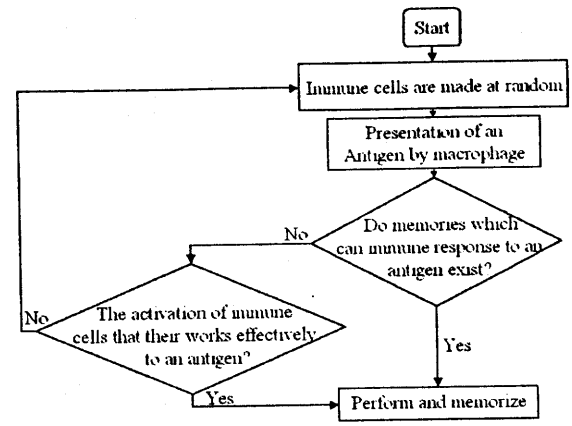
پس اگردر زمانی خاص درحافظه شبکه ایمنی، آنتی بادی لازم موجود باشد بدن شروع به ساخت می نماید.



شکل۱: شبکه ایمنی

1- Macrophage
2- T cells
3- Lymphocytes
4- B cells
5- Peptide

در غیر این صورت بدن شروع به تولید آنتی بادیهای جدید نموده تا به آنتی بادی مورد نظر برسد. در این بخش ما از این مسئله کمک گرفته و به تشریح آن می پردازیم.



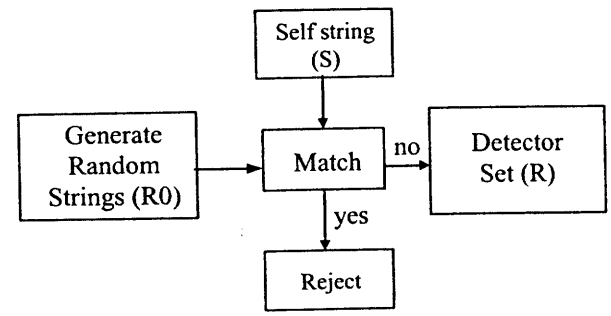
شکل۲: نحوه عملکرد سیستم ایمنی

در اکثر سیستمهای صنعتی اطلاعات بصورت دیجیتالی بوده و معمولا بشکل رشته ای از اعداد باینری می باشند. بنابراین برای رفتارهای طبیعی، پاسخ سیستم را بعنوان رشته های خودی و رفتارهای غیر طبیعی را بعنوان بیگانه در نظر می گیریم. برای تشخیص خودی از بیگانه نیاز به آشکارسازمی باشد. انجام کار در دو مرحله صورت می گیرد.

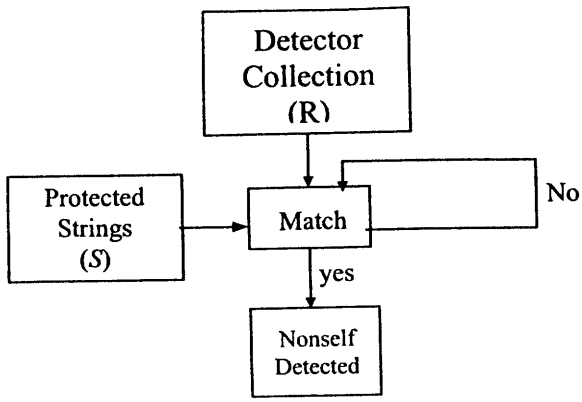
مرحله اول: تولید یک مجموعه از آشکار سازها. هر آشکار ساز یک رشته می باشد که با هیچکدام از رشته های آشکار شده مطابقت ندارد.

مرحله دوم: رشته های آشکار شده با آشکار سازها مقایسه می شود. چنانچه رشته ورودی با یکی از رشته های آشکار ساز مطابقت داشته باشد بعنوان بیگانه تلقی می شود. در غیراینصورت رشته خودی خواهد بود.

شکلهای(۳)و(٤)این مراحل را نشان می دهند.



شکل۳: تولید رشته های آشکارساز



شکل۳: تشخیص خودی از بیگانه

با توجه به مطالب گفته شده مسئله این است که بتوانیم میزان تطابق دو رشته را مشخص نماییم. به عبارت دیگر مناسب است که احتمال p_m را که میزان تطابق دو رشته در حداقل r بیت کنار هم می باشد را بدانیم. بنابر این اگر

m: تعداد نمادها

l: طول رشته ها

r: تعداد بیتهای محاور هم که تطابق دارند

باشندآنگاه احتمال p_m از رابطه(۱) بدست می آید[8].

$$p_m \approx m^{-r}\left[(l-r)(m-1)/(m+1)\right] \qquad (۱)$$

این تخمین زمانی خوب خواهد بودکه $m^{-r} \prec\prec 1$ شود. حال چنانچه:

N_{R0}: تعداد رشته های آشکارساز اولیه

N_R: تعداد رشته های آشکارساز پس از حذف

N_S: تعداد رشته های خودی

p_m: احتمال تطابق دو رشته تصادفی

$f=(1-p_m)^{Ns}$ احتمال عدم تطابق یک رشته تصادفی باهمه N_S ها

احتمال اینکه N_R آشکارساز، در آشکار سازی یک : p_f عبور غیر مجاز شکست بخورند

تعریف شوندواگر p_m کوچک و N_S بزرگ باشد،آنگاه $f \approx e^{-P_m \cdot N_S}$ شده وبنابراین داریم:

$$N_R = N_{R0} \cdot f \qquad (۲)$$

$$P_f = (1-P_m)^{N_R} \qquad (۳)$$

اگر P_m کوچک و N_R نیز بزرگ فرض شود آنگاه $P_f \approx e^{-P_m \cdot N_R}$ شده و بنابر این

$$N_R = N_{R0} \cdot f = -\ln p_f / p_m \qquad (٤)$$

پس می توان نوشت:

$$N_{R0} = \frac{-\ln p_f}{P_m (1-P_m)^{N_S}} \qquad (٥)$$

معادله(۵) تعداد رشته های اولیه مورد نیاز برای آشکارسازی یک تغییر تصادفی در رشته ها را ارائه می کند.

با توجه به معادلات (۱)تا(۵)، مشخص می شود که هنوز تعداد مجهولات از تعداد معادلات بیشتر می باشد. بنابراین روش فراهم کردن شرایط اولیه به اینصورت است که ابتدا پارامترهای r, l, m رامشخص نموده، سپس از رابطه(۱)احتمال P_m را محاسبه می کنیم. باانتخاب P_f ،مقدار N_{R0} برای شروع الگوریتم از رابطه(۵) فراهم می گردد.

۳- الگوریتم پیشنهادی و روش پیاده سازی آن

با توجه به مطالب گفته شده در بخش ۲، الگوریتم پیشنهادی زیر را می توان ارائه کرد.

گام اول: با شبیه سازی یک سیستم توزیع نمونه ازجریان خط نمونه برداری می کنیم. با توجه به اینکه فرکانس برق ۵۰ هرتز می باشد، حداقل از هر سیکل ۱۰۰ نمونه بر می داریم.

گام دوم: اگر ازA/D دوازده بیتی استفاده نماییم، نمونه های برداشته شده را بترتیب کنار هم مرتب نموده تا یک رشته ۱۲۰۰ بیتی فراهم گردد.

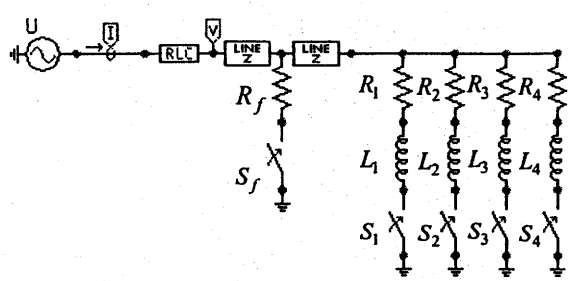
گام سوم: رشته بوجود آمده را با رشته های آشکار ساز مقایسه می کنیم. چنانچه رشته نمونه برداری شده با یکی از این رشته ها مطابقت داشته باشد، پس خطایی در سیستم اتفاق افتاده است(ر.ک.به شکل۳). با برداشتن نمونه های دیگر از خط ودر پریودهای دیگر می توان اطمینان حاصل کرد که آیا خطاواقعا در سیستم رخداده است یاخیر. نکته مهم در این الگوریتم، تعریف رشته خودی می باشد. زیرا علیرغم اینکه شکل موج جریان خط در حالت عادی سینوسی می باشد اما با تغییر بار، شکل موج جریان تا حدودی دچار اعوجاج شده که این اعوجاجها بمنزله بیگانه نباید تلقی گردد.

برای لحاظ کردن این موضوع دانستن حدود بارهای ورودی به شبکه با تقریبی حدود ده درصد مورد نیاز می باشد(حداقل و حداکثر)، تا بتوان رشته های خودی را تعریف کرد. در زمانهایی که سیستم منتظر نمونه برداری می باشد می توان رشته های آشکارساز را با توجه به شکل(۳) تولید و در حافظه نگه داشت.

از توانمندیهای این الگوریتم، حافظه دار بودن آن می باشد. یعنی می توان از خطاهای رخداده در قبل برای آشکار سازی خطاهای احتمالی بهره گرفت.

٤- شبیه سازی

برای شبیه سازی الگوریتم ارائه شده در بخش سوم، مدار توزیع را بصورت شکل(۵) در نظر می گیریم. در این مطالعه تنها بارهای خطی در نظر گرفته شده است ولی میتوان بارهای غیر خطی را نیز در شبیه سازیها، با توجه به حافظه دار بودن روش پیشنهادی در نظر گرفت. بدین منظور بایستی الگوهای متناظر با خطاهای گذرا و بارهای غیر خطی را نیز در الگوریتم لحاظنمود.



شکل۵: مدار توزیع قدرت

با توجه به شکل(۵)، در ابتدای خط یک ژنراتور تکفاز، در انتهای خط چهار بار مختلف که می توانند در فواصل زمانی مختلف وارد ویا از مدار خارج شوند و محل اتصال کوتاه با امپدانس R_f در نظر گرفته شده است. برای بدست آوردن سیگنالهای خودی ابتدا سوئیچ S_f را قطع فرض می کنیم. سپس با قطع و وصل کردن سوئیچهای S_1 تا S_4 شکل موج جریان را برای حالتهای مختلف بدست می آوریم. این شکل موجها، بعنوان سیگنالهای خودی تلقی می شوند. حالتهای مختلفی که برای سوئیچهای S_1 تا S_4 در نظر گرفته شده اند در جدول۱ آمده است. لازم بذکر است که شبیه سازی شبکه توزیع با نرم افزارEMTP تحت ویندوز انجام شده است.

جدول۱: حالتهای مختلف برای شبیه سازی شبکه توزیع(خودیها)

Time of simulation = 2 Sec
Tc : Time of close To : Time of open
L1, L2 : Length of Line (40 km)
Rf = 100 Phase = 0

No	S1		S2		S3		S4	
	Tc	To	Tc	To	Tc	To	Tc	To
1	3	5	3	5	3	5	-1	3
2	3	5	3	5	0.5	3	-1	3
3	3	5	1	3	0.5	3	-1	3
4	1.5	3	1	3	0.5	3	-1	3
5	-1	3	-1	3	-1	3	-1	3
6	-1	3	-1	3	-1	3	-1	0.5
7	-1	3	-1	1	-1	3	-1	0.5
8	-1	3	-1	1	-1	1.5	-1	0.5
9	-1	0.5	-1	1.5	-1	3	-1	1.5
10	-1	1	-1	1	-1	3	-1	1
11	-1	3	-1	1	-1	1	-1	1
12	-1	1	-1	1	-1	1	-1	3

پس از شبیه سازی سیگنالهای خودی، برای شبیه سازی سیگنالهای غیر خودی سوئیچ S_f را بسته تا خطا در خط اتفاق بیافتد. در این حالت با تغییر R_f، محل اتصال کوتاه وفاز ژنراتور ورودی می توان عمل شبیه سازی را انجام داده تا سیگنالهای بیگانه بدست آیند. حالتهای مختلف اتصال کوتاه در جدول۲ آورده شده است. نتایج شبیه سازی در شکلهای (٦) و (٧) و (٨) آمده است. شکل(٦) حالتی را نشان می دهد که عمل اتصال کوتاه در فواصل مختلف خط با طول ٤٠ کیلومتر اتفاق افتاده است. منحنی خط چین "سیگنال خودی" و بقیه "سیگنالهای بیگانه" می باشند. با توجه به شکل، تا قبل از اتصال کوتاه همه منحنیها بر هم منطبقند. اما پس از اتصال کوتاه در ثانیه یکم رفتار شکل موج جریان عوض می شود. در جدول۳ کدهای مربوط به این سیگنالها برای سه نمونه اول آمده است. شکل(۷)، شبیه سازی برای امپدانسهای متفاوت اتصال کوتاه و شکل(۸) شبیه سازی برای فاز ٤٥درجه را نشان می دهند. نتایج شبیه سازی نشان می دهد که رفتارهای اولیه جریان خط بهنگام وقوع خطا تغییر کرده و قابل شناسایی توسط الگوریتم ارائه شده در این مقاله می باشد.

جدول۲: حالتهای مختلف برای شبیه سازی شبکه توزیع(بیگانگان)

Time of simulation = 2 Sec
Sf : Tc = 1 , To = 3

حالت اول				
S1 : Tc = 3 To = 5				
S2 : Tc = 3 To = 5				
S3 : Tc = 3 To = 5				
S4 : Tc = -1 To = 3				
No	L1	L2	Rf	Phase
1	20	20	10	0
2	20	20	100	0
3	20	20	1000	0
4	20	20	100	30
5	20	20	100	60
6	20	20	100	90
7	20	20	100	120
8	20	20	100	150
9	5	35	100	0
10	10	30	100	0
11	15	25	100	0
12	25	15	100	0
13	30	10	100	0
14	35	5	100	0

حالت دوم	حالت سوم
S1 : Tc = 3 To = 5	S1 : Tc = 3 To = 5
S2 : Tc = 3 To = 5	S2 : Tc = 1 To = 3
S3 : Tc = 0.5 To = 3	S3 : Tc = 0.5 To = 3
S4 : Tc = -1 To = 3	S4 : Tc = -1 To = 3

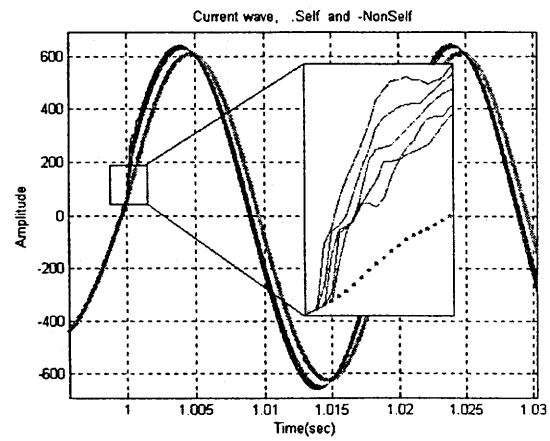
حالت چهارم	حالت پنجم
S1 : Tc = 1.5 To = 3	S1 : Tc = -1 To = 3
S2 : Tc = 1 To = 3	S2 : Tc = -1 To = 1
S3 : Tc = 0.5 To = 3	S3 : Tc = -1 To = 1.5
S4 : Tc = -1 To = 3	S4 : Tc = -1 To = 0.5

جدول۳: نمونه های برداشته شده از خط برای محلهای اتصال کوتاه متفاوت

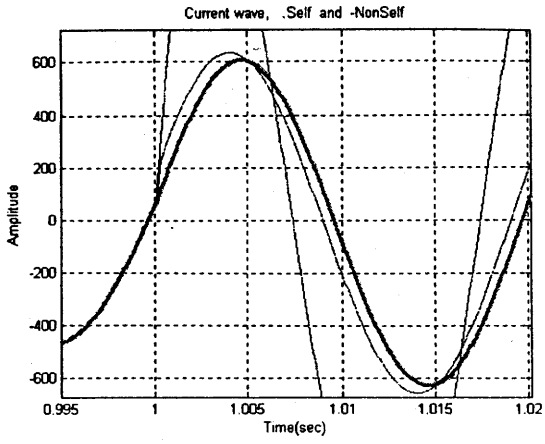
	نمونه سوم	نمونه دوم	نمونه اول
خودی	000001000110	000001001011	000001010011
بیگ۱	000010101110	000011000100	000011010101
بیگ۲	000010010010	000010011101	000010110110
بیگ۳	000010001010	000010010000	000010011000
بیگ٤	000001101011	000010001101	000010011100
بیگ٥	000010001110	000010010010	000010011000

۵- نتیجه گیری

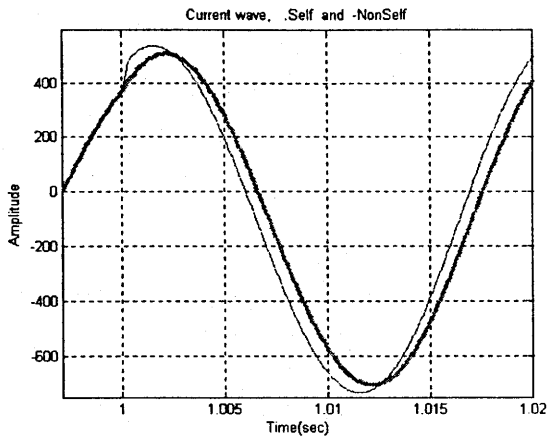
شبیه سازیهای انجام شده نشان می دهد که الگوریتم پیشنهادی قادر به تشخیص وقوع خطا در شبکه های توزیع می باشد. با توجه به هوشمند بودن این الگوریتم میتوان از خطاهای رخداده در گذشته نیز بهره گرفت. از آنجا که روش پیشنهادی دارای حافظه بوده و قادر به فراگیری الگوهای مختلف است، لذا میتوان الگوهای مختلفی از جمله بارهای غیر خطی و حالات گذرای دیگر سیستم که از نوع خطای امپدانس بالا نیست مانند کلیدزنی خازن و ... را نیز به عنوان سیگنالهای خودی در نظر گرفت. اما این الگوریتم هنوز در ابتدای راه بوده و برای رسیدن به نرم افزاری که بتواند بخوبی در شبکه های توزیع استفاده شود کار زیادی باید صورت بگیرد. که تحقیقات بیشتر به منظور تکمیل دست آوردهای روش ارائه شده در حال انجام است.



شکل٦: سیگنال خودی و بیگانه برای حالت اتصال کوتاه در فواصل مختلف



شکل۷: سیگنال خودی و بیگانه برای حالت اتصال کوتاه با امپدانسهای مختلف



شکل۸: سیگنال خودی و بیگانه برای حالت اتصال کوتاه با فاز٤٥ درجه

مراجع

[1] C. L. Banner and B. D. Russell. *"Practical high impedance fault detection on distribution feeders"*. IEEE Transaction on industry application, vol 33, No.3, May/June 1997.

[2] S. Forrest, A. S. Perelson, L. Allen, R. Cherukuri. *"Self-nonself discrimination in a computer"*. IEEE symposium on research, 1994.

[3] N. Toma, S. Endo, K. Yamada. *"Immune algorithm with immune network and MHC for adaptive problem solving"*. IEEE, 1999.

[4] D. Dasgupta and S. Forrest, *" Novelty detection in time series data using ideas from immunology "*.

[5] F. Esponda, S. Forrest, P. Helman. *" A formal framework for positive and negative detection schemes "*. IEEE, July 17, 2002.

[6] P. D'haeseleer, S. Forrest, P. Helman. *" An immunological approach to change detection: algorithms, analysis and implications"*. IEEE symposium on security and privacy, 1996.

[7] S. Hofmeyr, S. Forrest, A. Somayaji. *"Intrusion detection using sequences of systems"*. 1997.

[8] P. D'haeseleer, S. Forrest, P. Helman. *"A distributed approach to anomaly detection"*. August 30, 1997.