بهار ۱۴۰۱
سال یازدهم

کهربا

فصلنامه تخصصی مهندسی برق و کامپیوتر



ISSN :2322-3723

شماره سی و پنجم

kahrobaonline.ir
Journal of Electrical and Computer Engineering

Li-Fi فناوری مبتنی بر LED

ربات گارسون ،فرم جدیدی از ارائه خدمات توسط ربات به انسان

بررسی مدل های امنیت اینترنت اشیاء در شبکه حمل و نقل هوشمند

تحلیل و طراحی و مدلسازی دوبعدی ترانزیستور تونلی شاتکی با دی الکتریک TiO۲

بررسی روش های تشخیص هرزنامه ها در شبکه های اجتماعی با استفاده از داده کاوی

کنترل سرعت موتور DC تحریک مستقل با کنترلکننده¬های On-Off و PID

شماره مجوز وزارت فرهنگ و ارشاد اسلامی ۷۷۸۲۱

سال یازدهم
شماره سی‌و پنجم
بهار ۱۴۰۱



صاحب‌امتیاز

سایت نواندیشان

مدیرمسئول

مهدی عارف خیابانی

سردبیر

امین شیخ نجدی

هیئت تحریریه

دکتر امیرحسین رحمانی – دکترای برق قدرت- استاددانشگاه‌های جندی شاپور دزفول و آزاد اسلامی واحد درفول

دکتر ملیحه نیک سیرت- دکترای علوم کامپیوتر- استادیار دانشگاه صنعتی بیرجند

دکتر محمد دوستی زاده- دکترای برق، قدرت- استاد دانشگاه آزاد اسلامی خرم آباد

مهندس آزاد رحیمی – کارشناس ارشد برق قدرت- عضو هیئت علمی دانشگاه فنی و حرفه ای سنندج

دکتر علویه میرفتح الهی- دکترای علوم اعصاب گرایش هوش مصنوعی- دانشگاه علم و صنعت ایران

مهندس امین شیخ نجدی-کارشناسی ارشد برق الکترونیک- استادیار مدعو گروه الکترونیک دانشگاه‌های شهدا اهواز، جندی شاپور دزفول، عصاریان دزفول و آزاد اسلامی واحد دزفول

دکتر موسی مجرد- دکترای کامپیوتر-نرم افزار – هیئت علمی دانشگاه فیروزآباد، رئیس دانشگاه آزاد اسلامی فراشبند

مهندس محمدحسین دوست محمدی- کارشناسی ارشد برق الکترونیک – هیئت علمی (مربی) دانشگاه صنعتی همدان

مهندس آزاد رحیمی- کارشناسی ارشد برق قدرت- هیئت علمی (مربی) و مدیرگروه دانشگاه فنی و حرفه‌ای سنندج

مهندس علی کمالی- کارشناس ارشد برق قدرت – کارشناس ارشد پژوهشکده خودرو محیط زیست دانشگاه تهران

مهندس مهسا سرائی – کارشناس ارشد برق مخابرات- دانشگاه فردوسی مشهد (مربی)

درباره کهربا ۳

یادداشت مدیرمسئول ۴

آشنایی با مشاهیر

پروفسور رضا ایروانی – استاد دانشگاه تورنتو ۵

مقالات

ربات گارسون، فرم جدیدی از ارائه خدمات توسط ربات به انسان ۷
پریسا حسنی – کمیته علمی و R&D شرکت مهندسی برق و الکترونیک قشم ولتاژ

بررسی روش‌های تشخیص هرزنامه‌ها در شبکه‌های اجتماعی با استفاده از داده کاوری ۱۶
صالح بیت شیخ احمد- دانشجوی کارشناسی ارشد کامپیوتر
مهناز رفیعی – استادیار گروه کامپیوتر – دانشگاه آزاد اسلامی واحد رامهرمز

بررسی مدل‌های امنیت اینترنت اشیاء در شبکه حمل و نقل هوشمند ۲۲
بابک توکلیان – مدیر فن آوری اطلاعات و ارتباطات شهرداری کازرون

کنترل سرعت موتور DC تحریک مستقل با کنترل‌کننده‌های On-Off و PID ۳۱
علیرضا محمودی‌فرد- استاد دانشگاه صنعتی قم
سینا تقی‌پور نقشی – دانشجوی کارشناسی پیوسته مهندسی برق

Li-Fi فناوری مبتنی بر LED ۴۰
مریم فریور – کارشناسی ارشد مهندسی برق – الکترونیک
مهران کریمیان ریزی – کارشناسی ارشد مهندسی پزشکی

تحلیل و طراحی و مدلسازی دوبعدی ترانزیستور تونلی شاتکی با دی‌الکتریک TiO_2 ۴۳
پریسا سروی – دانشجوی کارشناسی ارشد مهندسی برق الکترونیک
حامد امین‌زاده – استادیار دانشکده مهندسی برق و الکترونیک دانشگاه پیام نرور تهران شمال
جواد جوادی مقدم - استادیار دانشکده مهندسی برق و الکترونیک دانشگاه پیام نرور تهران شمال

ارتباط با کهربا ۵۱

درباره کهربا

مجله الکترونیکی کهربا، با همت و تلاش جمعی از دانشجویان و مهندسین برق، بخصوص اعضای انجمن علمی و پژوهشی نواندیشان، در سال هزار و سیصد و نود شروع به کارکرد. کهربا از سال ۹۱ با کسب شماره بین‌المللی استاندارد مجلات (ISSN:۲۳۲۲-۳۷۲۳) و ثبت در سازمان اسناد و کتابخانه ملی ایران، به‌عنوان فصلنامه‌ای رسمی و تخصصی در حوزه صنعت برق شناخته‌شده است. این نشریه تخصصی در سال ۹۵ موفق به اخذ پروانه انتشار از وزارت فرهنگ و ارشاد اسلامی، با مجوز شماره ۷۷۸۲۱ و ثبت در سامانه جامع رسانه‌های کشور(e-rasaneh) و بانک اطلاعات نشریات کشور(magiran) گردید. در سال ۹۷ طی تفاهم‌نامه‌ای با بانک مقالات کشور (سیویلیکا) مورد حمایت این پایگاه قرارگرفته و مقالات ارائه‌شده به نشریه پس از انتشار در سیویلیکا نمایه شده و در نظام رتبه‌بندی دانشگاه‌ها و پژوهشگاه‌ها مورد تحلیل و بررسی قرار می‌گیرند.

یادداشت مدیرمسئول

در یازدهمین بهار از فعالیت نشریه کهربا و پس از انتشار سی‌و چهار شماره از مجله مفتخریم با انتشار سی‌وپنجمین شماره از این نشریه در خدمت علاقه‌مندان این مجله تخصصی باشیم. تلاش ما از روز نخست، جمع‌آوری، تهیه و ارائه مطالبی ساده و کاربردی، درعین‌حال تخصصی، به قشر فرهیخته دانش‌پژوه و کسانی که مشتاق به دانستن علوم مهندسی برق و الکترونیک یا کامپیوتر هستند، بوده است. امید است با هدایت و راهنمایی شما هر شماره بهتر و پخته‌تر از شماره پیشین گردد. امید است که باهمت و همیاری دوستان بتوانیم قدمی هرچند کوچک، جهت جلب رضایت و بالا بردن سطح دانش شما برداریم؛ و روزبه‌روز شاهد پیشرفت و موفقیت‌های شما عزیزان باشیم.

آشنایی با مشاهیر



پروفسور رضا ایروانی– استاد دانشگاه تورنتو

دکتر رضا ایروانی استاد گروه مهندسی برق و کامپیوتر دانشگاه تورنتو است. وی یک کرسی در دپارتمان مهندسی برق و کامپیوتر برای دو دوره ۵ ساله متوالی از سال ۲۰۰۴ تا ۲۰۱۴ در این دانشگاه نیز دارد. دکتر ایروانی پس از اخذ مدرک کارشناسی خود در سال ۱۹۷۶ در رشته مهندسی برق دانشگاه صنعتی امیرکبیر, به عنوان مهندس مشاور از سال ۱۹۷۶ تا ۱۹۷۹ مشغول به کار شد.

پس از گذراندن دوره کارشناسی برای ادامه تحصیلات خود به کانادا رفت و دوره کارشناسی ارشد و دکترای خود را به ترتیب در سال های ۱۹۸۱ و ۱۹۸۵ در دانشگاه منیتوبا گذراند. از سال ۱۹۸۵ تا ۱۹۸۷ دستیار استاد در دانشگاه ویندزور (Windsor) بوده است.

مطالعات پژوهشی

مدل سازی و کنترل مبدل های قدرت برای:

ادغام و یکپارچه سازی انرژی خورشیدی و قدرت باد در سیستم های قدرت

ادغام واحدهای تولید و ذخیره سازی توزیع شده در ریز شبکه ها و نیروگاه های مجازی

سیستم های HVDC

کنترل منطقه ای و حفاظت تطبیقی سیستم های بزرگ HVDC-AC با تمرکز بر شبکه " "HVDCو بخش بندی مبتنی بر مفاهیم HVDC

عضویت در انجمن ها

عضو انجمن مهندسان برق ((IEEE

عضویت در کنفرانس بین المللی سیستم های برقی بزرگ CIGRE))

مهندسین حرفه ای ایالت انتاریو، کانادا

مقالات پروفسور رضا ایروانی

م.مطر((Matar، ر.ایروانی ((R. Iravani، اجرای موازی ماشین آلات AC برای شبیه سازی واقعی مبتنی بر FPGA از حالت‌های الکترومغناطیسی برای ارائه ترانس IEEE در تحویل قدرت.

www.kahrobaonline.ir

ب.بهرامی(Bahrani)، اچ.کریمی((H. Karimi، ر.ایروانی(R. Iravani)، "تحلیل پایداری و اعتبار تجربی از یک استراتژی کنترل برای خود مختار بهره برداری از واحد تولید پراکنده".

ا.مهریزی ثانی(Mehrizi-Saniو ر.ایروانی((R. Iravani، عملکرد پتانسیل بر اساس کنترل ریز شبکه ها در حالت های جزیره ها و شبکه های متصل

م.ز.کام(Z. Kamhو ر.ایروانی((R. Iravani، یک مدل یکپارچه سه فازه الکترونیکی توزیع شده در منابع انرژی برای تجزیه و تحلیل جریان قدرت.

م.سعیدی فرد(M. Saeedifardو ر.ایروانی(.(R. Iravani عملکرد پویای یک ماژول چند لایه ای سیستم های Back-to-Back HVDC

www.kahrobaonline.ir

ربات گارسون ،فرم جدیدی از ارائه خدمات توسط ربات به انسان

پریسا حسنی
کمیته علمی و R&D شرکت مهندسی برق و الکترونیک قشم ولتاژ ،تهران، ایران،
Trainingset@qeshmvoltage.com

چکیده- با پیشرفت تکنولوژی و توانایی ساخت میکروکامپیوتر ها ، امکان ساخت ربات فراهم شد. هر ساله پیشرفت های چشمگیری در عرصه رباتیک را ناظر هستیم . یکی از اهداف رباتیک آسانتر کردن زندگی برای انسان است. به همین منظور ساخت ربات هایی که فعالیت خدماتی انجام دهند یکی از اهداف است. ربات های گارسون دسته ای از این ربات ها هستند. تلاش زیادی تا کنون برای رسیدن به این مهم انجام گرفته اما تا رسیدن به ربات های سریع و دقیق راه طولانی وجود دارد.

کلیدواژگان-ربات ، رباتیک ،ربات گارسون ، تکنولوژی ، ربات انسان نما ، خدمات ، صنایع

مقدمه

ربات چیست؟ می توان بطور خلاصه و جامع، ربات را این طور تعریف کرد: یک جسم مصنوعی که به انسان شباهت دارد. وقتی ما در مورد شباهت، فکر می کنیم، ابتدا قیافه ظاهری را در نظر میگیریم. ربات، درست مانند انسان به نظر می رسد. زیرا می توان سطح خارجی آن را با مواد نرمی ساخت که شبیه پوست انسان باشد. ربات امکان دارد که دارای مو، چشم، صدا و تمام اشکال و اجزاء و اعضاء انسان باشد، بطوری که از نظر ظاهر، هیچ فرقی با انسان نداشته باشد.

بجز ویژگیهای ظاهری، بایستی توانائیهای رباتها را مد نظر قرار دهیم و ببینیم چه کارهایی می توانند انجام دهند. اگر ما فکر کنیم که رباتها قادر به انجام وظایف و کارهای بخصوصی هستند و این وظایف را سریع تر و بهتر از انسان انجام می دهند، در این صورت هر ماشینی را باید یک ربات بحساب بیاوریم.

یک چرخ خیاطی سریع تر از انسان دوزندگی می کند، یک دستگاه مته بادی، سریع تر از انسان در سطوح سخت نفوذ کرده و آنها را سوراخ می کند. یک دستگاه تلویزیون، امواج رادیوئی را میگیرد آنها را شکل می دهد در صورتی که ما نمی توانیم این کارها را انجام دهیم و غیره... بدین گونه ما باید عنوان ربات را برای ماشینی به کار ببریم که با دستگاه ها و ماشین های معمولی فرق می کند و ویژگی های بیشتری دارد. یک ربات عبارت است از یک ماشین کامپیوتریزه که قادر به انجام کارهائی است که بغیر از انسان، مغز هیچ موجود زنده ای نمی تواند آن را انجام دهد و هیچ ماشین یا وسیله غیر کامپیوتریزه نیز نمی تواند آن را انجام دهد. به عبارت دیگر، خلاصه ترین شکل تعریف یک ربات این است:

کامپیوتر + ماشین = ربات

بدیهی است، تا قبل از دهه ۱۹۴۰ که کامپیوتر اختراع شد و همچنین تا قبل از دهه ۱۹۷۰ که «میکروچیپ و کامپیوتر تکمیل تر گردید، طراحی و ساختن یک ربات کامل امکان پذیر نبود.

پس از قرون وسطی، دانشمندان بتدریج به این فکر افتادند که با استفاده از علوم و صنایعی که فراگرفته بودند، اشیاء مصنوعی بسازند و از قدرت آنها استفاده کنند.

وقتی ساختن ساعت مکانیکی تکامل یافت و یک مکانیسم کوچک شامل فنرها و چرخ های دندانه دار و امثال آنها، موجب به کار افتادن آن شد گردش ساعت) متوجه شدند که با این مکانیسم می تواند دستگاه های دیگری را هم به کار بیندازند.

دهه ۱۷۰۰ سالهای طلای و اوج ساختن دستگاه های مکانیکی بود. فنرهای کوکی و هوای فشرده برای انجام کارهای مختلف مورد استفاده قرار می گرفت. اسباب بازی هائی به شکل سرباز ساخته می شدند که می توانستند راه بروند. اردک هائی که صدا در می آورند و شنا می کردند و آب و دانه می خوردند. پسربچه هائی که

قلم را به مرکب می زدند و با آن می نوشتند. (البته یک کلمه را بطوری تکراری). این وسایل به اصطلاح خودکار در معرض نمایش گذاشته می شدند، و خیلی نیز مورد توجه عموم قرار می گرفتند. (و گاهی اوقات هم سود زیادی عاید صاحبان آنها می شد).

البته ساختن این وسایل که بیشتر جنبه اسباب بازی داشتند، کار زیاد مهمی نبود، ولی این فکر را تقویت کرد که می توان دستگاههای دیگری ساخت که کارهای مفیدتری انجام دهند.

علم بسرعت پیشرفت می کرد، در سال ۱۷۹۸ یک کالبدشناس ایتالیائی به نام «لوئیگی گالوانی» پی برد که ماهیچه های مرده در اثر شوک الکتریکی منقبض می شوند و تکان می خورند. آیا امکان داشت که الکتریسته منشا زندگی باشد؟

و در فیلمهائی هم که ساخته می شد، الکتریسته موجب زندگی بخشیدن به اشیاء مصنوعی تلقی می گردید.

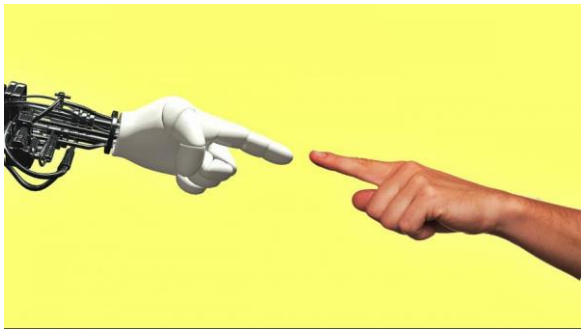
تا سال ۱۹۲۰ کسی لغت ربات را به کار نبرده بود. در این سال (که تصادفاً سال تولد من هم هست.) یک نمایشنامه نویسی چک به نام «کارل کا پک» نمایشنامه «آریو – آر» را نوشت، این نمایشنامه در مورد یک مرد انگلیسی به نام «روسوم» بود، که تعداد زیادی انسان مصنوعی ساخته بود که در سراسر جهان، تمام کارها را انجام می دادند، و بشریت با آسودگی و فراغت کامل زندگی می کرد.

کاپک، این آدمهای مصنوعی را «ربات» نامید، که یک لغت چک و به معنی «بیگاری» یا «برده» است. و اکنون کلمه «ربات» در همه زبانها (تا آن جا که من می دانم) مصطلح شده و همه، آدمهای مصنوعی را به این اسم می نامند.

کشف قطب نما، ناوبری را توسعه داد و موجب از بین رفتن تمدن در مکزیک و پرو گردید. اتومبیل بی نهایت مفید است، ولی هر سال دهها هزار نفر را به کام مرگ می افکند. پیشرفتهای پزشکی، جان میلیونها نفر را نجات داده و موجب ازدیاد و تراکم جمعیت و در نتیجه طغیان و شورش و بلوا گردیده است.

در این مقاله تلاش کردیم به مهمترین کاربرد ربات ها اشاره داشته باشیم.

استفاده از ربات ها برای آسان کردن کارها و از بین بردن تهدید های انسانی و خطاهای انسانی است.



با توجه به گسترش علم در حوزه های مختلف ، کاربرد ربات ها نیز گسترده تر شده و در مکان های مختلفی از آن ها استفاده میشود . به همین دلیل تعداد ربات ها به سرعت در حال افزایش است و هر سال افزایش چشمگیری دارد.

❖ صنعت

وقتی قابلیت های ربات ها بیشتر به چشم می‌آید که رباتها با انسان ها را مقایسه کنیم.

بسیاری از ربات ها از انسان ها سریع تر و دقیق تر هستند و بدون اشتباه کارها را انجام می دهند.

مزیت دیگر ربات ها نسبت به انسان ها می توان به موارد زیر اشاره کرد:

- حقوق نمی گیرد
- مرخصی نمی رود
- در روز های تعطیل کار میکند
- ۲۴ ساعت کار میکنند و نیاز به غذا و نه نیاز به استراحت ندارند.

(این موضوع زمانی جالب می‌شود که طبق تحقیقات انجام شده یک کارگر جوشکار ۱۰-۳۰ درصد زمان به جوشکاری می پردازد ولی در ربات ها ۵۰-۷۰ درصد زمان را به جوشکاری اختصاص می‌دهند. که این نشان دهنده راندمان ۳ برابری ربات های جوشکار نسبت به انسان ها است.)

- یک کار را هزاران بار انجام می دهد و خسته نمیشود

- بیمه نمی خواهد
- در صورت مصدومیت و آسیب دیدن هیچ گونه شکایت از شما به مرجع قضایی نمی کند
- دیگر نگران از دست دادن نیروی کاری و رفتن به شرکت رقیب نیستید.

❖ اکتشاف و شناسایی

از آنجا که اکتشافات و شناسی ها خصوصا مکان های جدید خطرات بسیاری دارد. برای همین در چنین اکتشافاتی از ربات ها کمک میگیرند.

حدود ۶ سال از فاجعه نیروگاه اتمی فوکوشیما در ژاپن می گذرد.

انقدر تشعشعات هسته ای بالا است که انسان نمی تواند در آنجا کاری کند. برای همین برای پاکسازی از ربات ها کمک میگیرند.



ربات پاکسازی کننده نیروگاه اتمی فوکوشیما

این یکی از انواع ربات شناسایی میباشد، رباتها دیگر مثل ربات مریخ نورد و ربات های که در عمق اقیانوس ها در حال اکتشاف هستند از این نوع دسته ربات ها به حساب می آیند.



❖ جراحی رباتیک

با طراحی و ساخت ربات های جراح و استفاده از ان ها تغییرات زیادی نسبت به روند قبلی در این حوزه به وجود امده است.

در عمل های جراحی رباتیک پزشک متخصص جراح از طریق رایانه کنترل عمل جراحی را بر دست دارد و این در حالی است که بازوهای رباتیک جراح به طور مستقل مسئولیت انجام عمل جراحی را روی فرد بیمار به عهده خواهد داشت.

به این ترتیب از طریق جراحی رباتیک جراح قادر خواهد بود از راه دور بیمار را که در گوشه دیگری از دنیاست تحت عمل جراحی قرار دهد.

اولین عمل جراحی رباتیک در سال ۷ سپتامبر ۲۰۰۱ توسط تیم جراحی در نیویورک بر روی زن ۶۸ ساله‌ای در بیمارستان CIVIL در شرق فرانسه انجام شد.

که در این عمل جراحی، کیسهٔ صفرای این بیمار برداشته شد.

باتوجه به موفقیت های اخیر در زمینه جراحی رباتیک ، ربات های متنوع و گوناگونی ساخته شده است که میتواند به واسطه انها عمل های جراحی پیچیده را انجام داد.

❖ پلیس

شاید این حرف ربات پلیس را ۵۰ سال پیش میگفتید به حالت تمسخر قرارتان می‌دادند و ان را غیرممکن می‌دانستند.

حتی تصور ربات پلیس در ۵۰ سال پیش غیرممکن بنظر میرسید اما امروزه با پیشرفت علم رباتیک دیگر این یک رویا نیست.

پلیس دبی قصد دارد تا سال ۲۰۳۰ ، ۲۵ درصد نیرو های پلیس خود را با ربات های پلیس جایگزین کند.در راستای همین هدف ، چند ماه پیش از رباتهای پلیس خود رونمایی کرد.



نمونه ای ربات پلیس دبی

این ربات یک نمونه اولیه میباشد که وظیفه ی فعلی آن گزارش تخلفات میباشد.مردم هم میتوانند با صفحه لمسی که روی ربات پلیس نصب شده است می توانند گزارش تخلفات را بنویسند و هم جرایم ترافیکی خود را پرداخت کنند.

پلیس دبی قصد دارد که ربات های پلیس را به یک افسر کامل نزدیک کند.باید منتظر بازخوردهای این ربات باشیم و باید دید این ربات چقدر از خواسته های سازندگانش را می تواند بر طرف کند.

❖ نظامی

ربات های نظامی برای شناسایی و جاسوسی از دشمن و خنثی کردن بمب و مین مورد استفاده قرار میگیرند.

چندین سال پیش اگر در مورد سلاح های کنترل از راه دور و سربازان رباتیک صحبت می شد همه یاد فیلم های هالیوودی و تبلیغاتی ارتش های غربی بخصوص آمریکا می‌افتادند

ولی حالا کشورهای مختلف از جمله ایران به چنین امکاناتی دست پیدا کرده اند.



ربات نظامی شناسایی بمب و مین

سامانه حامی یک سیستم کنترل از راه دور که به تجهیزات مسافت سنج لیزری و دوربین دید در شب و حرارتی مجهز میباشد.

این سامانه در مکان های که در آن تهدید های جانی وجود دارد استفاده می شود.

این سامانه میتواند در مکان هایی که شرایط آب و هوای سخت دارند و امکان تهدید های تروریستی وجود دارد به کار گرفته شود.

❖ سینما و تلویزیون

بیش از صد سال از استفاده ربات ها در فیلم های سینما می گذرد.اولین فیلم در سال ۱۹۰۹ بنام خدمتکار الکتریکی بود که در ان از ربات استفاده شد.



اگر ربات ها نبودن بسیاری از فیلم ها ساخته نمی شد. برخی از فیلم های معروف که در آن از ربات ها استفاده شده می توان به فیلم جنگ ستارگان ، ترمیناتور و انیمیشن وال ای اشاره کرد.

❖ ربات اسباب بازی

با پیشرفت تکنولوژی ربات ها به دنیای کودکان هم وارد شده اند . ربات های اسباب بازی محبوبیت زیادی بین کودکان پیدا کرده اند و یک رقیب جدی برای اسباب بازی های قدیمی هستند.

یکی از این ربات های اسباب بازی FURBY BOOM است. این ربات با نرم افزار مخصوص خود قابلیت وصل شدن به گوشی همراه را دارد که از طریق ان دستور های مختلف را اجرا میکند.



از نمونه های دیگر ربات های اسباب بازی میتوان به ربات پروت مدل JUMPING NIGHT BUZZ که توانایی عکس و فیلم برداری و پریدن تا ۷۵ سانت را دارد.



❖ ربات خدمتکار

همانطور که با پیشرفت تکنولوژی و ساخت ماشین های لباسشویی کار سخت و خسته کننده شستن لباس ها را برای همیشه از ذهن مردم خارج کرد. دیگر کمتر کسی را میتوان دید که با دست لباس بشوید حتی در بسیاری از روستا های کشور ماشین لباسشویی وجود دارد .

بنظر میرسد که ربات های خدمتکار پایان همیشگی برای کار های خسته کننده خانه باشند.

در حال حاضر ربات هایی وجود دارند که توانایی انجام کار های سخت و خسته کننده منزل را دارند.

مثل رباتی که جارو برقی می‌کشد یا چمن میزند و ... ولی قیمت بالای آنها هنوز مشکل جدی برای همگانی شدن آنهاست.



❖ ربات انباردار

فروشگاه آمازون در حال حاظر از ربات های انباردار برای جابه جایی وسایل سنگین از جایی به جایی دیگر در انبار های خود استفاده می‌کند.

فروشگاه خرید آنلاین آمازون قصد دارد در آینده ای نزدیک برای شناسایی کالا ها در قفسه ها و جابه جا کردن آنها نبز از ربات استفاده کند.

و برای تسهیل این کار با برگزاری مسابقات جهانی می خواهد هر چه سریع تر به این خواسته دست پیدا کند.

حتی فروشگاه آنلاین دیجی کالا هم با برگزاری مسابقاتی برای جابه جا کردن کالاها با پهپاد ها را دارد.

می‌خواهد در حوزه فرستادن کالاها به صورت رباتیک اولین فروشگاهی در ایران باشد که چنین کاری را انجام میدهد.

❖ ربات کشاورز:

رباتها در طول این چندین سال اخیر وارد صنعت کشاورزی شدند و دارند جای انسانها را خصوصا در کار های دشوار می‌گیرند.

رباتها میتوانند بسیار سریع تر و کار آمدتر از انسان ها می توانند کار های کشاورزی را انجام دهند.

کار هایی که ربات ها انجام میدن کاشت و برداشت ، آبیاری ، هرس ، وجین ، اسپره های حشر کش و نظارت بر رشد گیاهان و... از جمله کار های ربات ها در قسمت های کشاورزی می‌باشند.

روبات های خدماتی :

روباتهایی هستند که در فرم و عملکرد بسیار متفاوت عمل می کنند و کارهای منحصر به فرد، خطرناک، وقت گیر و یا تکراری و آزاد کردن وقت کارگران انسانی برای انجام کارهای شناختی بیشتر را انجام میدهند.

بیشتر روبات ها خدمات نیمه مستقل و یا کاملا خودمختار با نوعی تحرک هستند. روبات های خدماتی اکثرا به صورتی در نظر گرفته شده است تا با افراد ارتباط برقرار کنند، معمولا در خرده فروشی، مهمان نوازی، مراقبت های بهداشتی، انبار قرار می گیرند. دیگران در تنظیمات سخت تر مانند برنامه های کاربردی فضایی و دفاع، برنامه های کاربردی کشاورزی و تخریب قرار می گیرند تا کارهای خطرناک و پر اهمیت را به صورت خودکار انجام دهند.

علاوه بر پیشرفت های مداوم در سیستم های بینایی و فن آوری، کنترل حرکت و موتور، هوش مصنوعی و یادگیری ماشین، و همچنین محاسبات ابری، قابلیت ها و کاربردهای روبات های حرفه ای خدمات با سرعت بیشتری نسبت به گذشته افزایش می یابد.

مزایای روبات های سرویس حرفه ای:

روبات های حرفه ای خدمات خودکار بسیاری از وظایف مختلف را در مجموعه ای از برنامه های مختلف، اما مزایای آنها به طور معمول یکسان است. صرف نظر از صنعت و یا برنامه، شرکت ها به طور خودکار به فرایندهای خود می پردازند: ایمنی، کارایی و بهره وری.

❖ **ایمنی**

ایمنی هنگامی که شرکت ها تصمیم به راه اندازی روبات سرویس حرفه ای می گیرند، توجه اولیه ای است. روباتها به جای جایگزینی کارگران انسانی، می توانند از وظایف خطرناک برخوردار باشند در حالی که انسان ها بر روی وظایف شناختی بیشتر تمرکز می کنند که آنها را از موقعیت های خطرناک دور می کند. به عنوان مثال، روبات های حرفه ای خدماتی که در بخش دفاع استفاده می شود، هدف از محافظت سربازان از آسیب در هنگام مبارزه است. به طور مشابه، ربات های تخریب برای جلوگیری از خطرات ساختاری یا هسته ای در طی فرآیند تخریب استفاده می شود. روبات های حرفه ای خدمات می توانند با خیال راحت جایی که کارگران انسانی نمی توانند ورود پیدا کنند حضور یابند.

❖ **بهره وری**

علاوه بر ایمنی، بهبود بهره وری یکی دیگر از اهداف اصلی برای کسب و کارهایی است که از روباتهای حرفه ای استفاده می کنند. کارایی به طور معمول از طریق سطوح بی عیب و نقص از زمان بیداری ربات و کاهش هزینه های عملیاتی به دست می آید. روبات های بازرسی و روبات های تمیزکاری صنعتی با خرابی بسیار کم کار می کنند و به آنها امکان پوشش جامعتری از زیرساخت های بزرگ را می دهند. روبات های لجستیک می توانند حجم زیادی از محصولات را در حالی که هزینه های کار را کاهش می دهند، حمل کنند.

مانند همه ی اتوماسیون های روباتیک، روبات های حرفه ای خدمات اغلب درب را برای جمع آوری داده های بیشتر و تجزیه و تحلیل برای بهینه سازی در حال انجام در تمام عملیات باز می کنند. روبات های کشاورزی می توانند اطلاعات دیداری مهم را برای نظارت بر سلامت محصولات و دام ها انتقال دهند. روباتهای سرویس دهنده خدمات می توانند حتی در مواجهه با چهره به چهره رفتار مشتری را ردیابی کنند تا درک عمیق تر از انگیزه ها و خواسته های مصرف کننده داشته باشند. داده های عملیاتی مهم مانند این بسیار پیچیده تر و یا غیرممکن است که از طریق فرایندهای دستی جمع آوری شوند.

در نهایت، روباتهای سرویس حرفه ای همه در یک یا چند نوع دیگر به بهره وری کمک می کنند. بعضی از افراد ممکن است در ایمنی برتر باشند، در حالی که دیگران ممکن است در جمع آوری

داده ها یا کارایی پیشرفت کنند، اما نتیجه نهایی تقریبا همیشه یک افزایش قابل توجه در بهره وری است. دستاوردهای بهره وری از این ربات ها به همه انواع تجارت کمک می کند سرمایه گذاری در ربات های خدمات حرفه ای را توجیه می کند.

استفاده از ربات به جای کارگر:

گرچه بحث بر سر استفاده از ربات‌ها بجای کارگران امر تازه‌ای نیست، اما شاید بسیاری از ما ندانیم که ربات‌های کارگر در برخی از کشورهای جهان کار خود را آغاز کرده و جایگزین کارگران شده‌اند.

گزارش جدید بنیاد غیرانتفاعی اطلاعات، فناوری و نوآوری (ITIF)که یک اندیشکده سیاستگذاری عمومی است نشان می‌دهد که استفاده از ربات‌ها در صنایع گوناگون در کشورهای توسعه یافته رو به افزایش است.

مطالعات این اندیشکده در سال ۲۰۱۷ حاکی از آن است که کره جنوبی، سنگاپور و آلمان بیشترین تعداد ربات‌های کارگر را به خدمت گرفته‌اند. در کره جنوبی ۷۱۰ ربات به ازای هر صدهزار کارگر تولیدی وجود دارد و این رقم در سنگاپور ۶۵۸ و در آلمان ۳۲۲ است.

ربات‌های کارگر اغلب بیش از صدهزار دلار قیمت دارند، ولی استفاد از آن‌ها در کشورهای ثروتمند و در برخی صنایع به صرفه است. اما در کشورهای فقیر که دستمزد کارگران در پائین‌ترین سطح ممکن است، این ربات‌ها جایی ندارند.



نقش ربات در رستوران:

این روزها رقابت در عرصه رستوران داری علاوه بر طعم و چینش غذا به چگونگی استفاده از فناوری برای سرویس دهی به مشتریان هم سرایت کرده است. فراسوی مسابقه ای که شرکت های بزرگی چون آمازون و دومینو در زمینه «پیکِ بالگردی» و استفاده از پهپادها برای رساندن بسته های غذا به نقاط مختلف راه انداخته اند، برخی رستوران داران بزرگ به این فکر می کنند که چطور با فناوری های گوناگون بازی کنند.

وقتی حرف از فناوری در رستوران به میان می آید همه ما یاد چند برنامه ای می افتیم که به کمک شان می توانیم غذاهای مختلفی را سفارش بدهیم. بر اساس گزارشی که موسسه صنایع غذایی تکنومیک با عنوان «۱۰۰ رستوران برتر زنجیره ای در جهان» منتشر کرده است، ۶۸ درصد افرادی که در آسیا به رستوران می روند، از تلفن های همراه شان برای سفارش غذا استفاده می کنند.

این گزارش همچنین نشان می دهد که بیش از یک سوم رستوران های آمریکایی برای خودشان برنامه ای دارند که فایل راه اندازی روی تلفن های همراه است. شاید استفاده از فناوری به منظور مشتری مداری در کشور ما به راه اندازی وب گاه های سفارش غذا محدود مانده باشد اما با نگاهی به اخبار سرگرم

کننده علم و فناوری می توان فهمید که کشورهایی مثل ژاپن، چین و ایالات متحده به خلاقیت هایی در این زمینه دست زده اند که علاوه بر ارائه خدمات به مشتری، در جذب مشتریان بیشتر و افزایش درآمد نیز به آنها کمک کرده است.
از برنامه های رنگارنگی که رستوران داران را در صرفه جویی در وقت، افزایش تعداد مشتریان و جلوگیری از اشتباهات احتمالی یک قدم جلو برده اند که بگذریم، با برخی رستوران ها در سطح جهان مواجه می شویم که با جایگزین کردن گارسون ها با ربات ها یا تبلت های مجهز به برنامه های سفارش غذا یا حتی پیشنهادهای سرآشپز به مشتریان بر اساس خصوصیات ظاهری و حس و حال و سابقه آنها، مفهوم سرو غذا را تغییر داده اند.

اسم من آدم ماشینی است!

رستوران های چینی بیش از هر رستوران فناوری محور دیگری از سال ۲۰۰۶ به جایگزین کردن گارسون های شان با ربات ها روی آورده اند. اگرچه بسیاری از این ربات ها از پس کارهای متنوع رستورانی بر نمی آیند ولی همچنان هزینه کمتری نسبت به نیروی کار انسانی به رستوران داران تحمیل می کنند . طبیعی است که ربات هزار و ۲۰۰ دلاری به نیروی کاری که فقط برای چند ماه چنین مبلغی را از کارفرمای خود مطالبه می کند، برتری پیدا کند. اما دلیل اصلی پیروزی ربات های مهمان دار سرگرم کننده بودن آنهاست، نه قابلیت های شان. برای همین است که چینی ها به این ربات ها به چشم اسباب بازی نگاه می کنند و به آنها می گویند «جیکه رین» یعنی «آدم های ماشینی.«

قابلیت های واقعی ربات ها را وقتی بهتر در می یابید که بدانید برخی رستوران های چینی بزرگ، بیش از ۳۰ ربات را به استخدام خود در آورده اند و با کمک آنها روزانه به ۲۰۰ مشتری سرویس می دهند. سرآشپزان مچینی حتی اجازه ورود ربات ها به داخل آشپزخانه ها را نیز صادر کرده اند و از برخی مدل های خاص و توانمند آنها برای آماده کردن برخی مواد اولیه طبخ غذا کمک می گیرند.

با وجود این، ربات های رنگارنگ چینی کارهای ساده را به پیچیده ترها ترجیح می دهند، به همین دلیل، هیچ رستوران دار عاقلی اجازه نمی دهد ربات هایش ظرف های سنگین را حمل کنند. ضمن این که همه ربات ها نیازمند عبور از مسیرهای مغناطیسی هستند و از این روی، همه با هم نمی توانند در یک زمان به نقاط مختلف رستوران سرک بکشند؛ این است که به سرگرم کردن مشتری ها اکتفا می کنند.

بیشتر این ربات ها وقتی سوپ را حمل می کنند نمی توانند از ریختن مایع به داخل سینی جلوگیری کنند و به تشخیص چهره مشتری های رستوران قادر نیستند. برای همین لازم نیست چندان نگران آینده نیروی کار در این زمینه باشیم.

ربات گارسون:

هدف از ساخت ربات در مراکز خرید، معادن ، فرودگاه ها و مکان های دیگر جایگزین کردن آنها به جای انسان نیست. بلکه برای کاهش حجم کار انسان هاست.

طراحی و ساخت ربات گارسون

ربات گارسون یکی از ربات های خدمتکار می باشد که از آن برای سرویس دهی در رستوران، کافه و فست فود ها استفاده می شود. این ربات برای خوش آمد گویی و گرفتن سفارش، با استفاده از منوی لمسی تعاملی، به میز مشتری مراجعه می کند و سفارش مشتری را ثبت می کند.

پس از آماده شدن، هوشیار غذای مشتری را به صورت خودکار به میز مربوطه تحویل می دهد. برای ساخت این ربات از فناوری های نوین هوش مصنوعی همچون پردازش تصویر (بینایی ماشین)، مسیر یابی، کنترل و ناوبری خودکار استفاده شده است .استفاده از چنین ربات هایی برای سرویس دهی در رستورانها، طی چند سال اخیر در کشورهای صنعتی و پیشرفته مانند: ژاپن، چین، آلمان و آمریکا رواج پیدا کرده اما بدلیل هزینه های بالای تهیه و پشتیبانی و همچنین تفاوت های زبانی و فرهنگی، استفاده از نمونه های خارجی آن در ایران رواج پیدا نکرده است

موارد استفاده از ربات گارسون:

این ربات که در بخش خدمات مورد استفاده قرار می گیرد می تواند در فرودگاه ها، ایستگاه های اتوبوس، هتل ها، مراکز فروش، نمایشگاه ها، بازار ها، رستوران ها، کافه ها، موسسات آموزشی،

بیمارستان ها و سازمان هایی مانند نمایشگاه ها، کنسرت ها، مراسم ها، جشن ها قرار گیرد.

کاربردهای ربات گارسون:

- توزیع بروشور (توزیع بروشور در فرودگاه ها، مراکز خرید)
- خدمات خدمتکار (خدمات از آشپزخانه در کافه ها، رستوران ها)
- معرفی محصولات (در مراکز خرید، بازارها، مواد غذایی برای ترویج محصول)
- میزبان پذیرایی
- مراقبت های بهداشتی در بیمارستان ها (خدمات آب و غذا به بیمار، زمان بندی مصرف داروی بیماران)
- استفاده از کامپیوتر و اینترنت فعال
- برای برقراری ارتباط با افراد از طریق صفحه نمایش هوشمند در مقابل آنها
- برای انجام کار آشپزخانه ساده (دم کردن چای ، مخلوط کردن سوپ، خرد کردن سبزیجات)
- قادر به پاسخ دادن به حوزه آموزش و پرورش
- پذیرشگر
- قادر به توضیح اشکال هندسی ساده و عملیات ریاضی برای کودکان در دوره ابتدایی است
- حمل کالاهای تا ۱۰ کیلوگرم
- عمومی (یادآوری قرار ملاقات، آبیاری گل، پیاده روی سگ)

مشکل اصلی ربات های گارسون یا پیشخدمت سرعت کند آنهاست زیرا برخی مشتریان ترجیح می دهند تا غذایشان سریع تر روی میزشان قرار گیرد و علاقه ای به ربات های کند ندارند. مشکل دیگر ربات های گارسون غیر منعطف بودن آنهاست زیرا این ربات ها از قبل برنامه ریزی شده اند و در نتیجه گاهی می توانند برای رستوران ها مشکل ساز نیز بشوند.

نتیجه گیری

باتوجه به اینکه گسترش علم در حوزه های مختلف گسترش یافته است. به همین دلیل کاربرد ربات ها بسیار گسترده شده است و در مکان های مختلفی از آنها استفاده می شود. تعداد ربات ها در جهان هر سال افزایش چشم گیری پیدا میکند و تعداد آنها به سرعت در حال افزایش هست. هدف از ساخت ربات در مکان های مختلف جایگزین کردن

آنها به جای انسان نیست. بلکه برای کاهش حجم کار انسان هاست. هنوز سوالات بسیاری در مورد آینده رباتیک بی‌پاسخ مانده است. آیا ممکن است ربات‌هایی که حاصل نبوغ انسانند روزی جای او را در تمام عرصه‌ها بگیرند و به سلطه بشر بر این کره خاکی پایان بخشند؟

منابع:

۱. فصل هجدهم کتاب ایلیاد هومر
۲. کتاب دنیای ربات‌ها، نوشته ایزاک آسیموف
۳. www.rokna.ir
٤. https://fararu.com/fa/news/382610
۵. http://asanrobot.com
۶. http://robotmakers.ir/blog/
۷. https://aradmobile.com
۸. http://jamejamonline.ir
۹. www.robotics.org

بررسی روش‌های تشخیص هرزنامه‌ها در شبکه‌های اجتماعی با استفاده از داده‌کاوی

صالح بیت شیخ احمد[۱] و مهناز رفیعی[۲]
[۱]دانشجوی کارشناسی ارشد، گروه کامپیوتر، موسسه آموزش عالی غیرانتفاعی اروندان خرمشهر، salehste@gmail.com
[۲]استادیار، گروه کامپیوتر، واحد رامهرمز، دانشگاه آزاد اسلامی، رامهرمز، ایران، m.rafie@srbiau.ac.ir

چکیده - شبکه‌های اجتماعی به مجموعه‌ای از افراد گفته می‌شود که به صورت گروهی با یکدیگر ارتباط داشته و مواردی مانند اطلاعات، نیازمندی‌ها، فعالیت‌ها و افکار خود را به اشتراک می‌گذارند. ولی به وجودآمدن پیام‌های ناخواسته موجب آزار کاربران و پایین آمدن کارایی شده است. امروزه این پیام‌های ناخواسته که به عنوان هرزنامه شناخته می‌شوند به مشکل عمده ای تبدیل شده‌اند. هرزنامه‌ها منجر به اتلاف منابع شبکه، کامپیوترها و زمان می‌گردند. لذا جهت شناسایی و جلوگیری از هرزنامه‌ها تلاش‌های زیادی صورت گرفته است، ولی با پیشرفت این تلاش‌ها هرزنامه‌ها باز هم گسترش و پیشرفت می‌کنند. بنابراین هرزنامه به یک مشکل جدی تبدیل شده است. بدین منظور روش‌ها و الگوریتم‌های بسیاری جهت جلوگیری و فیلتر هرزنامه پیشنهاد شده است که هدف اصلی افزایش دقت روش تشخیص هرزنامه در پیام‌ها است. این مقاله، فعالیت ضد هرزنامه و کاربردهای آن در شبکه‌های اجتماعی را با استفاده از الگوریتم های داده کاوی مورد بررسی قرار داده است.

کلید واژه- هرزنامه، ماشین بردار پشتیبان، ویژگی کاربران، ارتباطات

۱. مقدمه

شبکه‌های اجتماعی به مجموعه‌ای از افراد گفته می‌شود که به‌صورت گروهی با یکدیگر ارتباط داشته و مواردی مانند اطلاعات، نیازمندی ها، فعالیت ها و افکار خود را به اشتراک می‌گذارند. امروزه، شبکه‌های اجتماعی برخط، ابزار بسیار محبوبی برای همکاری و ارتباط به‌شمار می‌روند که میلیون ها نفر از کاربران اینترنت را به خود جلب کرده‌اند. شبکه‌های اجتماعی برخط مانند فیسبوک، لینکداین و توییتر از پرطرفدارترین این برنامه‌ها به‌حساب می‌آیند. این شبکه‌ها، به‌ویژه آن‌هایی که کاربرد های معمولی و غیرتجاری دار ند، مکان هایی در دنیای مجازی هستند که مردم خود را به‌طور خلاصه معرفی کرده و امکان برقراری ارتباط بین خود و هم‌فکرانشان را در زمینه‌های مورد علاقه فراهم می‌کنند [۱]. اما زندگی در چنین فضایی آدابی دارد که باید به آن‌ها توجه ویژه‌ای نمود تا از مشکلات جدی جلوگیری شود. در سال های اخیر، نظرات جعلی و هرزنامه مشکلی است که به‌شدت در حال گسترش و افزایش است. هرزنامه‌ها، پیام‌های ناخواسته‌ای هستند که به‌طور گسترده به تعداد زیادی از کاربران با هدف کلاهبرداری، نشر اکاذیب، ایجاد شایعات، رعب و وحشت و همچنین تبلیغات ارسال می‌گردد. امروزه در حدود ۵۰ درصد نامه‌های کاری الکترونیکی، هرزنامه ه ستند [۲]. هرزنامه سبب م شکلاتی مانند ا شغال منابع، اتلاف پهنای‌باند و طولانی‌شدن زمان ارتباط می‌شود [۳]. افرادی که اقدام به ارسال پیام‌های هرزنامه می‌نمایند، هرزنامهر نامیده می شوند. توییتر به‌عنوان یکی از بزرگ‌ترین شبکه‌های اجتماعی محسوب می شود که روزانه پیغام‌های متنی زیادی در آن تولید و ارسال می‌شود. به این پیغام‌ها توییت گفته می‌شود. توییت‌ها معمولاً دارای ساختار متفاوتی با پیغام‌های سایر شبکه‌های اجتماعی ه ستند به‌طوری‌که ت شخیص هرزنامه در آنها پیچیده‌تر است. طبق مطالعاتی که انجام شده، حدود ۱۵ درصد کاربران توییتر بات‌ها هستند و معمولاً از هر ۲۰ توییت، یکی از آن‌ها هرزنامه است. لذا شبکه اجتماعی مزبور در این مقاله بیشتر مورد توجه واقع شده است. شایان ذکر است که تشخیص هرزنامه‌ها با استفاده از تکنیک‌های داده کاوی یکی از دغدغه‌های اصلی

کاربران و مدیران شـــبکه‌های اجتماعی اســـت، لذا تاثیر الگوریتم هایی همچون خوشـــه بندی، ماشـــین بردار پشـــتیبان، درخت تصمیم، بیزین و K-NN نیز مورد بررسی قرار گرفته است.

ساختار کلی مقاله به این ترتیب ا ست که در بخش دوم مبانی و پیشینه تحقیق بیان می شود و به برر سی کارهای انجام شده در این زمینه، معایب و مزایای آن می پردازد. بعد از برر سی کارهای انجام شـــده، بخش ســـوم به معرفی جزئیات روش پیشـــنهادی می‌پردازد. در نهایت در بخش چهارم، نتایج نهایی بیان می شود و راهکـارهـایی برای ادامـه تحقیق و بهبود آن در آینـده معرفی می‌گردد.

۲. روش‌های تشخیص هرزنامه‌ها

تحقیقات انجام گرفته نشان می‌دهد که توییت‌های جعلی با همان سرعت توییت‌های نرمال منتشر می‌شوند. ربات‌ها نقش زیادی در سرعت بخشیدن به گسترش هرزنامه‌ها دارند و کاربران انسانی هم به افزایش حجم آن‌ها کمک می‌کنند. برای تشخیص هرزنامه‌ها کارهای متعددی انجام شده است که در ادامه به معرفی چند مورد می‌پردازیم.

کار انجام شده توسط وانگ را می‌توان پیشگامی در تشخیص هرزنامه‌ها در توییتر بر اساس شناسایی ارتباط بین کاربران دانست. در این روش با استفاده از مدل گراف مستقیم وجود ارتباطات دنبال کننده-دوستی بین کاربران شناسایی می‌شود و با استفاده از ویژگی‌های متنی استخراج شده، هرزنامه‌ها شناسایی می‌شوند. به صورت کلی می‌توان کارهای انجام گرفته برای تشخیص هرزنامه‌ها در توییتر را به چند دسته‌ی کلی تقسیم‌بندی کرد: تحلیل ساختار گراف شبکه‌های اجتماعی مانند روش‌های [۶-۴]، تحلیل ساختار متن و استخراج الگوها مانند [۷]، تحلیل متا دیتای مربوط به پروفایل کاربران و بررسی URLهای استفاده شده مانند [۱۰-۸] و تحلیل رفتارهای تعاملی کاربران [۱۳-۱۱].

۲-۱ ویژگی‌های آماری مبتنی بر تشخیص زمان واقعی اسپم توییتر

در تحقیق [۱۴]، بر روی داده‌های توییتر با پنج هدف: ارائه فیلترینگ بلادرنگ، افزایش مقیاس‌پذیری، تصمیم‌گیری دقیق، قابلیت آموزش مجدد مدل با داده‌های جدید و طبقه‌بندی مستقل از متن پژوهشی انجام شده است. در این پژوهش از یک مجموعه داده‌ی ۵۰۰۰۰۰تایی استفاده شده است که ۴۰۰۰۰۰ عدد از آن‌ها برای داده‌های آموزشی و ۱۰۰۰۰۰ عدد از آن‌ها برای آزمایش مورداستفاده قرار گرفت. داده‌های آموزشی با ترکیب یک‌به‌یک (نیمی نرمال و نیمی هرزنامه) یک‌به‌چهار و یک‌به‌ده موردبررسی قرار گرفتند. دقت حاصل ۹۱ درصد است. مزیت این پژوهش این است که سیستمی بلادرنگ است که می‌تواند با تأخیر کوتاهی عمل فیلترینگ را انجام دهد. مقیاس‌پذیری بالایی دارد و می‌تواند برای داده‌های حجیم به‌درستی عمل کند. عیب این پژوهش عدم دسترسی تمامی مجموعه داده‌ها است و الگوریتم‌های دیگر را موردبررسی قرار نداده است. ازآنجایی‌که در مجموعه داده‌های موجود، تعداد کاربران اسپم نسبت به کاربران نرمال بسیار کم هستند برای ایجاد مدل و ارزیابی آن نمی‌توان از تمامی رکوردهای موجود در مجموعه داده‌ها استفاده نمود، زیرا مدل تنها ویژگی کاربران نرمال را در نظر گرفته و کاربران اسپم را نادیده می‌گیرد. برای رفع این مشکلات باید نسبت نمونه‌های مختلف از کلاس‌های مختلف متناسب در نظر گرفته شود.

۲-۲- استفاده از یک روش داده کاوی جهت تشخیص هرزنامه در فیسبوک

در [۱۵] با تکنیک درخت تصمیم J48، با استفاده از متن پیام‌های فیسبوک، تعداد کلمات کلیدی، میانگین تعداد کلمات، طول متن و تعداد لینک‌ها هرزنامه‌ها شناسایی می‌شوند. نرخ دقت و فراخوانی به دست آمده در مقاله به ترتیب ۶۱ و ۶۳ درصد است.

۲-۳ تشخیص اسپم‌های توییتر با استفاده از یادگیری عمیق

وو و همکاران در [۱۶] از تکنیک‌های یادگیری عمیق با استفاده از تبدیل کلمه به بردار برای تشخیص و شناسایی اسپم‌ها استفاده کرده‌اند. آن‌ها بر این عقیده هستند که تنها استفاده از ویژگی‌های آماری متون نمی‌تواند دقت کافی را برای یادگیری دسته‌بندها فراهم کند. آن‌ها از تعدادی ویژگی‌های خودساخته مربوط به کاربران و ارتباط آن‌ها در توییتر استفاده کرده‌اند. این ویژگی‌ها به نحوی کدگذاری شده‌اند که بتوان آن‌ها را به‌عنوان ورودی دسته‌بند در نظر گرفت. در ادامه از شبکه عصبی عمیق برای یادگیری و تشخیص هرزنامه‌ها استفاده شده است. ویژگی‌های مربوط به کاربران به صورت خودساخته و تجربی هستند و از ساختار درونی شبکه به درستی استفاده نشده است. در روش مزبور، ویژگی‌های ارتباط بین کاربران به شکلی پیدا می‌گردد که بتوان کاربران را از

لحاظ نزدیکی به هم رتبه‌بندی نمود و حتی بتوان گفت اگر کاربری با دو نفر رابطه دوستی دارد به کدام نزدیک‌تر است.

۲-۴ پرداختن به مشکل عدم تعادل کلاس در تشخیص اسپم‌های توییتر با استفاده از یادگیری دسته جمعی

لی‌یو و همکاران در [۱۷]، یک ساختار متفاوت برای تشخیص پست‌های هرزنامه در توییتر معرفی کردند. تاکید اصلی آن‌ها بر روی ساختار داده‌ها متمرکز بود. در این تحقیق بیان شده است که ترکیب نامتوازن داده‌های اسپم و غیر اسپم باعث بروز خطا توسط دسته‌بندهای یادگیری ماشین می‌شود. به‌طوری که در واقعیت معمولاً چیزی حدود ۵ الی ۱۰ درصد پست‌ها اسپم هستند، ولی در مجموعه داده‌های استفاده شده گاهاً داده‌های اسپم و غیر اسپم به‌نسبت ۵۰ به ۵۰ تقسیم بندی می‌شوند که این می‌تواند دقت کار را کاهش دهد. آن‌ها یک فرآیند سه مرحله‌ای برای تشخیص اسپم‌ها در توییتر معرفی کرده‌اند. در ابتدا با استفاده از سه روش مختلف نمونه‌برداری از داده‌ها انجام می‌گیرد و تعدادی نمونه متشکل از هرزنامه و غیر هرزنامه برای دسته‌بند مشخص می‌شوند. یک روش بدون جایگذاری، روش دیگر با جایگذاری و روش سوم با استفاده از تکنیک نمونه‌سازی فازی انجام شده است. در مرحله دوم برای هر کدام از سه روش مطرح شده با استفاده از دسته‌بندهای یادگیری ماشین مرحله دسته‌بندی انجام گرفته و پست‌های هرزنامه و غیر هرزنامه شناسایی می‌شوند. در این مقاله از دسته‌بندهای ماشین بردار پشتیبان، درخت‌تصمیم و بیزین ساده استفاده شده است. در نهایت در مرحله سوم بر اساس قانون رای اکثریت، تصمیم نهایی در مورد هرزنامه یا غیر هرزنامه بودن گرفته می‌شود. این روش از لحاظ دسته‌بند ساختار قدرتمندی دارد اما ویژگی‌های استفاده شده برای دسته‌بندها فقط اطلاعات آماری خود متن است که باعث می‌شود دقت کار پایین بیاید.

۲-۵ تشخیص اسپم توییتر با استفاده از خوشه‌بندی

میلر و همکاران در سال ۲۰۱۵ از خوشه‌بندی برای تشخیص هرزنامه‌ها در توییتر استفاده کرده‌اند. در این تحقیق تشخیص هرزنامه به عنوان یک مسئله کلاس‌بندی در نظر گرفته نمی‌شود بلکه به عنوان یک مسئله تشخیص ناهنجاری[۱] در نظر گرفته شده است. در این تحقیق در کنار استفاده از ۱۲ ویژگی مربوط به متن و ساختار ارتباطی کاربران از ۹۵ کاراکتر خاص از بین کاراکترهای کد اسکی تعداد عنوان 95 one-gram استفاده شده است. بنابراین در کنار ۱۲ ویژگی اولیه، ۹۵ ویژگی دیگر اضافه شده است و خوشه‌بندی با این ۱۰۷ ویژگی انجام گرفته است. فرآیند خوشه‌بندی به‌صورت جداگانه با استفاده از دو روش StreamKM++ و DenStream انجام گرفته است که توسط هر دو روش، نمونه‌ها به دو خوشه‌ی هرزنامه و غیر هرزنامه تقسیم‌بندی می‌شوند. معیار فراخوانی[۲] برای این دو روش حدود ۹۹ درصد است. یعنی در واقع ۹۹ درصد پست‌هایی که هرزنامه هستند را شناسایی می‌کند. اما مقدار False positive آن به نسبت زیاد است. یعنی تعداد زیادی از پست‌هایی که هرزنامه نیستند را نیز هرزنامه تشخیص می‌دهد و این باعث بروز مشکل خواهد شد. همچنین مجموعه داده‌ی مورد استفاده بسیار ساده بوده و توازن مناسبی بین تعداد هرزنامه و غیر هرزنامه وجود ندارد [۱۸].

۲-۶ استنتاج ماشین‌های بردار پشتیبان با استفاده از الگوریتم بهینه‌سازی وال جهت تشخیص پروفایل‌های اسپم در شبکه‌های اجتماعی برخط در متن‌های زبانی مختلف

الزوبی و همکاران در [۱۹]، یک فرآیند خودکار برای شناسایی کاربران اسپم معرفی کرده‌اند. با توجه به اینکه نسبت کاربران اسپم در توییتر بیشتر از نسبت توییت‌های اسپم به کل توییت‌ها است، بنابراین شناسایی کاربران اسپم می‌تواند در تشخیص هرزنامه‌ها و حتی جلوگیری از ارسال هرزنامه‌ها نقش موثری داشته باشد. در این روش از ترکیب دسته‌بند ماشین بردار پشتیبان و الگوریتم فرامکاشفه‌ای بهینه‌سازی وال استفاده شده است. در این ساختار ابتدا داده‌ها پیش‌پردازش شده و تعدادی ویژگی بر اساس ساختار متن و ارتباط کاربران شناسایی می‌شوند. داده‌های ورودی به دسته‌بند ماشین بردار پشتیبان داده می‌شود و فرایند یادگیری آغاز می‌گردد. در هر مرحله توسط الگوریتم بهینه‌سازی وال مشخص می‌گردد که آیا مقدار بهینه‌سراسری بدست آمده یا خیر. در نهایت بعد از اتمام مراحل، فرآیند یادگیری به اتمام رسیده و بر اساس داده‌های آزمایش نتیجه ارزیابی محاسبه می‌شود. در این روش از ویژگی‌های ساده استفاده شده است و همچنین پیچیدگی زیاد این روش باعث می‌شود که دقت و کارایی نمونه‌های آموزش بسیار بالا

[۱] anomaly

[۲] Recall

و نتایج آزمایش به نسبت کمتر باشد، به عبارتی وقوع بیش‌برازش[۳] در این روش بسیار محتمل است.

۲-۷ تشخیص هرزنامه به صورت نیمه نظارتی در توییتر

سدهای و همکاران در [۲۰]، از یک روش نیمه نظارتی برای تشخیص هرزنامه‌ها در توییتر استفاده کرده‌اند. در این روش یک چهارچوب بلادرنگ به نام S^3D برای تشخیص توییت‌های اسپم معرفی شده است. این چهارچوب شامل دو بخش کلی است. بخش اول به نام تشخیص هرزنامه و بخش دوم به نام بروزرسانی مدل نام‌گذاری شده است. بخش شناسایی هرزنامه خود شامل ۴ زیر بخش مختلف است: ۱- شناسایی لیست‌های سیاه و افراد گزارش شده توسط سایر کاربران. ۲- شناسایی توییت‌هایی که به صورت انبوه و تکراری ارسال می‌گردند. ۳- شناسایی کاربران معتبر، این افراد عموماً تایید شده هستند و پست‌های ارسال شده از طرف آن‌ها به صورت غیر هرزنامه دسته‌بندی می‌شوند. ۴- استفاده از یک دسته‌بند ترکیبی شامل سه دسته‌بند: بیزین ساده، لجستیک رگرسیون و جنگل تصادفی[۴]، فرآیند یادگیری و دسته‌بندی به صورت ترکیبی توسط این سه دسته‌بند انجام می‌گیرد. اما در بخش دوم بر اساس برچسب‌گذاری‌های انجام شده در بخش اول، مقادیر مربوط به پارامترها بروزرسانی می‌شوند تا فرآیند دسته‌بندی با دقت بیشتری انجام گیرد. امکان تبانی در این روش زیاد است به صورتی که اگر گروهی یک فرد را به عنوان هرزنامه گزارش کنند، چهارچوب استفاده شده، فرد را به عنوان هرزنامه شناسایی می‌کند.

۲-۸ رویکرد انتخاب ویژگی جهت شناسایی هرزنامه در شبکه اجتماعی فیس بوک

این مقاله در مورد تشخیص نظرات اسپم در شبکه اجتماعی فیس بوک است. با مرور پست‌ها، نظرات و بررسی ویژگی‌های آنها، یک سیستم فیلترشکن اسپم برخط در این مقاله طراحی شده است. سیستم فیلتر پیشنهادی قادر است از روش‌های مختلف اکتشافی و الگوریتم‌های بهینه سازی مانند بهینه‌سازی ذرات، بهینه سازی کلونی مورچه‌ها و تکامل تفاضلی برای کشف و فیلتر نمودن مطالب مخرب و جلوگیری از انتشار نظرات اسپم‌ها ، محیطی مطمئن را برای کاربران فراهم کند. این شبکه اجتماعی محبوب علاوه بر این از روش‌های یادگیری ماشینی، تکنیک‌های خوشه‌بندی و درخت تصمیم‌گیری استفاده نموده تا عملکردی دقیق و سرعتی مناسب برای سیستم فیلتر پیشنهادی ارائه دهد [۲۱].

۲-۹ سیستم تشخیص هرزنامه مبتنی بر داده کاوی برای شبکه‌های اجتماعی

در [۲۲]، یک سیستم تشخیص هرزنامه مقیاس‌پذیر بر اساس داده‌کاوی برای امنیت شبکه‌های اجتماعی پیشنهاد شده است. از الگوریتم خوشه‌بندی GAD برای خوشه‌بندی در مقیاس بزرگ و ادغام آن با الگوریتم یادگیری فعال استفاده شده است. از این الگوریتم یادگیری جهت مقابله با چالش‌های تشخیص زمان واقعی و مقیاس‌پذیری استفاده می‌شود.

۲-۱۰ دسته‌بند کارآمد جهت تشخیص هرزنامه در شبکه-های اجتماعی

در [۲۳] بر روی شناسایی عملکرد اسپم با استفاده از تجزیه و تحلیل ویژگی و استفاده از طبقه بندی کارآمد متمرکز شده است. هدف اصلی در این مقاله، یافتن رابطه بین ویژگی‌ها و الگوهای طبقه‌بندی جهت تشخیص پیام اسپم از سایت‌های ناخواسته است. این سیستم از الگوریتم‌های طبقه‌بندی کارآمد پس از تجزیه و تحلیل ارتباط ویژگی‌ها جهت شناسایی هرزنامه استفاده می‌کند. در این راستا، یک چارچوب طبقه‌بندی کارآمد برای پیش‌بینی و نظارت بر اسپم ارایه شده است. نتیجه این پژوهش برای کاربران شرکت کننده در شبکه‌های اجتماعی برای اهدافی همچون تجارت، بازاریابی و برقراری ارتباط بین مخاطبین می‌باشد. لذا عملکرد الگوریتم‌های طبقه‌بندی همچون بیزین، ID3، جنگل تصادفی، K-NN و ماشین بردار پشتیبان مقایسه شده است. کار آتی در این راستا ارایه مدلی جهت ادغام یک سیستم هوشمند در این چارچوب طبقه بندی جهت نظارت و تشخیص مستمر بر روی هرزنامه قابل انجام می باشد.

۲-۱۱ روشی ترکیبی برای شناسایی اسپم در شبکه‌های اجتماعی با استفاده از تجزیه و تحلیل گراف و رفتار کاربر

در [۲۴]، روشی مبتنی بر تحلیل گراف جهت تشخیص اسپم از طریق تجزیه و تحلیل رفتارهای آنها و ارتباط آنها با کاربران ارائه شده است. در ضمن، راه‌حلی جهت تسهیل روند تشخیص ارائه

[۳] Overfitting

[۴] Random Forest (RF)

شده است. هدف از این مقاله، استفاده از روش تحلیل گراف ترکیبی و تحلیل رفتاری، افزایش دقت تشخیص و میزان تشخیص با کمک الگوریتم‌های طبقه‌بندی مناسب و ویژگی‌های مؤثرتر است. بنابراین، دو سناریو جهت دستیابی به سطح دقت بالاتر و مثبت کاذب پایین‌تر استفاده شد. سناریوی اول مبتنی بر استفاده از کل داده‌ها برای ساخت و ارزیابی مدل است. نتایج نشان می دهد که علی‌رغم دقت بالای این رویکرد، به دلیل سطح بالای مثبت کاذب، این رویکرد مناسب نیست. در سناریوی دوم، نسبت کاربران عادی به اسپم‌ها ۲ به ۱ در نظر گرفته شد که منجر به نتایج رضایتبخش شد. پس از بررسی ماتریس سردرگمی و مثبت کاذب در الگوریتم‌های مختلف، الگوریتم لجستیک به عنوان یک الگوریتم مناسب انتخاب شده است که اهداف این مطالعه را برآورده می‌کند.

۳- راهکار پیشنهادی

تشخیص هرزنامه‌ها با استفاده از تکنیک‌های داده کاوی و یادگیری ماشین یکی از دغدغه‌های اصلی کاربران و مدیران شبکه‌های اجتماعی است. تابه‌حال کارهای زیادی در مورد تشخیص هرزنامه-ها در شبکه‌های اجتماعی انجام شده است اما برای تشخیص هرزنامه‌ها در توییتر کمتر کار شده است. ساختار اصلی اکثر روش-ها یکسان است. لذا با توجه به راهکارهای انجام شده پیشین و در راستای ارایه روشی موثر قصد داریم مکانیزمی جدید به‌منظور شناسایی توییت‌های اسپم درتوییتر معرفی نماییم [۲۵]. در این راستا نیاز است در ابتدا پیش‌پردازش‌هایی روی متون انجام گرفته و بعد از پالایش متن، تعدادی ویژگی استخراج شده و با استفاده از تکنیک‌های یادگیری ماشین مشخص می شود که کدام پیغام هرزنامه و کدام غیر هرزنامه است. شایان ذکر است که در روش‌های پیشین غالبا تنها از ویژگی‌های داخل متن برای این کار استفاده می‌شد. مثلا استفاده از کلمات خاص، یا فرمت‌های خاص پیغام، یا ارسال همزمان پیغام به تعداد زیادی از کاربران. اما این ویژگی‌ها به تنهایی موثر نخواهند بود. ما علاوه بر این ویژگی‌ها می‌خواهیم از ساختار شبکه‌های اجتماعی، اطلاعات کاربران، وجود رابطه بین گیرنده و فرستنده پیغام و... استفاده کنیم. به‌عنوان مثال ارسال پیغام از یک کاربر به کاربری ناشناس ممکن است هرزنامه تشخیص داده شود، اما در عین حال همین پیغام برای یک کاربر دوست یا هم‌گروه ممکن است هرزنامه نباشد. بنابراین ما سعی می‌کنیم از این ارتباطات و ساختار شبکه اجتماعی برای تشخیص هرزنامه یا عدم وجود آن استفاده کنیم به شکلی که بتوانیم انواع ارتباط بین افراد را پیدا کنیم. به عنوان مثال مشخص شود کاربری که با دو کاربر دیگر ارتباط دوستی دارد به کدام‌یک نزدیک‌تر است. یا اگر کاربری یک کاربر دیگر را در شبکه بلاک کرده است به‌عنوان یک ویژگی مورد استفاده قرار گیرد. همچنین بر اساس سابقه قبلی کاربران رتبه‌بندی می‌شوند و از قبل مشخص می‌شود که هر کاربر چقدر احتمال ارسال پیغام هرزنامه را دارد. که این ویژگی هم می‌تواند کمک‌کننده باشد. در پایان به کمک الگوریتم ماشین بردار پشتیبان (SVM) پیغام‌ها را با استفاده از این ویژگی‌های بیان شده به دو دسته هرزنامه و غیر هرزنامه طبقه بندی می‌شوند. لازم به ذکر است که SVM دسته‌بند قدرتمندی است که با داده‌های زیاد و وجود نویز هم به‌خوبی می‌تواند کار کند و برای مسائل پردازش متن، دسته‌بند مناسبی است.

۴- نتیجه‌گیری

استقبال گسترده از شبکه‌های اجتماعی و امکانات عظیم آنها و فرصت‌های رو به رشد، کاربران و مخاطبان بسیاری را به خود جلب نموده است. اما در کنار پیام‌ها، مباحث جذاب و جالب، محتوای نامناسب و بعضا مجرمانه مانند هرزنامه نیز در این شبکه‌ها منتشر می‌شود. هرزنامه‌های مخرب قصد ارسال مطالب نادرست یا نامربوط برای توزیع اطلاعات نادرست در شبکه‌های اجتماعی برخط را دارند. در این راستا، الگوریتم‌های بسیاری جهت جلوگیری از هرزنامه پیشنهاد شده است که هدف اصلی افزایش دقت روش تشخیص هرزنامه در پیام‌ها می باشد. لذا در این مقاله، فعالیت ضد هرزنامه و کاربردهای آن در شبکه‌های اجتماعی با استفاده از الگوریتم های داده کاوی مورد توجه قرار گرفته است. به عنوان کارهایی که در آینده در این راستا قابل انجام است استفاده از الگوریتم های داده کاوی به صورت تلفیقی را می توان نام برد.

مراجع

[1] N. Jindal و L. Bing., “Opinion spam and analysis”, In Proceedings of the 2008 International Conference on Web Search and Data Mining, 2008.

[2] M Alsaleh, A. Alarifi, F. Al-Quayed, A. S. Al-Salman, Combating Comment Spam with Machine Learning Approaches, in: 14th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 295–300, 2015.

[3] A. Heydari, M. a. Tavakoli, N. Salim and Z. Heydari, “Detection of review spam: A survey," Expert

Systems with Applications, Vol. 42, No. 7, pp. 3634-3642, 2015.

[4] C. Yang, R. Harkreader, J. Zhang, S. Shin, G. Gu, Analyzing Spammers' Social Networks for Fun and Profit: A Case Study of Cyber Criminal Ecosystem on Twitter, in: Proceedings of the 21st International Conference on World Wide Web, WWW '12, ACM, New York, NY, USA, pp. 71–80, 2012.

[5] H. Yu, M. Kaminsky, P. B. Gibbons, A. D. Flaxman, SybilGuard: Defending Against Sybil Attacks via Social Networks, IEEE/ACM Transactions on Networking, Vol. 16, No. 3, pp. 576–589, 2008.

[6] G. Danezis, P. Mittal, SybilInfer: Detecting Sybil Nodes using Social Networks, in: Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, California, USA, 2009.

[7] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, B. Y. Zhao, Detecting and characterizing social spam campaigns, in: Proceedings of the 10th ACM SIGCOMM Internet Measurement Conference (IMC), Melbourne, Australia, pp. 35–47, 2010.

[8] K. Thomas, C. Grier, J. Ma, V. Paxson, D. Song, Design and Evaluation of a Real-Time URL Spam Filtering Service, in: 32nd IEEE Symposium on Security and Privacy (S&P), Berkeley, California, USA, pp. 447–462, 2011.

[9] S. Lee, J. Kim, WarningBird: Detecting Suspicious URLs in Twitter Stream, in: 19th Annual Network and Distributed System Security Symposium (NDSS), San Diego, California, USA, pp. 183–195, 2012.

[10] F. Benevenuto, G. Magno, T. Rodrigues, V. Almeida, Detecting Spammers on Twitter, in: In Collaboration, Electronic messaging, Anti-Abuse and Spam Conference (CEAS), Vol. 6, 2010.

[11] O. Varol, E. Ferrara, C. A. Davis, F. Menczer, A. Flammini, Online Human-Bot Interactions: Detection, Estimation, and Characterization, in: International AAAI Conference on Web and Social Media, AAAI Press, pp. 280–289, 2017.

[12] K. Lee, B. D. Eoff, J. Caverlee, Seven Months with the Devils: A Long-Term Study of Content Polluters on Twitter, in: Proceedings of the Fifth International Conference on Weblogs and Social Media, pp. 185–192, 2011.

[13] P. N. Howard, B. Kollanyi, Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum, Social Science Research Network (SSRN), 2016.

[14] C. Chen, Y. Wang, J. Zhang, Y. Xiang, W. Zhou, G. Min, Statistical features-based real-time detection of drifted twitter spam, IEEE Transactions on Information Forensics and Security, Vol. 12, No. 4, pp. 914–925, 2017.

[15] M. Soiraya, S. Thanalerdmongkol and C. Chantrapornchai, "Using a Data Mining Approach: Spam Detection on Facebook," International Journal of Computer Applications, Vol. 58, No. 13, pp. 26-31, 2012.

[16] T. Wu, S. Liu, J. Zhang, Y. Xiang, Twitter spam detection based on deep learning, in: Proceedings of the Australasian Computer Science Week Multiconference, ACM, 2017.

[17] Sh. Liu, Y. Wang, J. Zhang, Ch. Chen, Y. Xiang, Addressing the Class Imbalance Problem in Twitter Spam Detection Using Ensemble Learning, Computers & Security, pp. 321-330, 2017.

[18] Z. Miller, B. Dickinson, W. Deitrick, Twitter spammer detection using data stream clustering, Journal of Information Sciences, Vol. 260, pp. 64–73, 2015.

[19] A. M. Al-Zoubi, H. Faris, J. Alqatawna, M. A. Hassonah, Evolving Support Vector Machines using Whale Optimization Algorithm for spam profiles detection on online social networks in different lingual contexts, Knowledge-Based Systems, Vol. 65, No. 6, pp. 123-132, 2018.

[20] S. Sedhai, A. Sun, Semi-supervised spam detection in twitter stream, IEEE Transactions on Computational Social Systems, Vol. 5, No. 1, pp. 169–175, 2018.

[21] Mohammad Karim Sohrabi, Firoozeh Karimi, A Feature Selection Approach to Detect Spam in the Facebook Social Network, Arabian Journal for Science and Engineering, Vol. 43, No. 2, pp 949–958, 2018.

[22] Xin Jin, Cindy Xide Lin, Jiebo Luo, Jiawei Han, Social Spam Guard: A Data Mining Based Spam Detection System for Social Media Networks, 37th International Conference on Very Large Data Bases, Vol. 4, No. 12, pp. 1458-1461, 2011.

[23] E.Nalarubiga,, M.Sindhuja, Efficient Classifier for Detecting Spam in Social Networks, International Journal of Innovative Science, Engineering & Technology (IJISET), Vol. 2, No. 10, 2015.

[24] Mona Najafi Sarpiri, Taghi Javdani Gandomani, Mahsa Teymourzadeh, Akram Motamedi, A Hybrid Method for Spammer Detection in Social Networks by Analyzing Graph and User Behavior, Journal of Computers, Vol. 13, No. 7, pp. 823-828, 2018.

[۲۵] Erbs, Nicolai, Keyphrase Extraction using Textual and Visual Features, 52nd Annual Meeting of the Association for Computational Linguistics, 2014.

بررسی مدل های امنیت اینترنت اشیاء در شبکه حمل و نقل هوشمند

بابک توکلیان[۱]، b.tavakolian@gmail.com
[۱]مدیر فن آوری اطلاعات و ارتباطات شهرداری کازرون

چکیده : *امروزه اینترنت اشیاء و کاربرد های آن با استفاده از هوشمند سازی تجهیزات مختلف بیش از پیش مورد توجه قرار گرفته است. در این پژوهش به بررسی یکی از اساسی ترین دغدغه های کاربران و شرکت های تولید کننده تجهیزات IoT یعنی امنیت پرداختیم. به طور کلی بخش عمده ای از این کاربردها ، کاربردهای حساس و پر اهمیت هستند. استفاده از این فناوری، همچنین فناوری های حساس باعث شده تا اهمیت امنیت و پیاده سازی آن در این شبکه ها بیشتر از سایر شبکه ها مورد توجه و بررسی قرار گیرد. این در حالی است که مسائلی همچون توپولوژی و مقیاس پذیری جغرافیایی شبکه به این مشکلات دامن زده و بحث برقراری امنیت را امری دشوار و پیچیده نموده است. در مجموع وجود این مسائل برای شبکه های اینترنت اشیاء باعث ایجاد تفاوت ها و پیچیدگی های خاص در حوزه امنیت و برقراری امنیت ارتباطات این شبکه ها شده است. بر همین اساس و با توجه به اهمیت بالای بحث امنیت در شبکه های اینترنت اشیاء ، تا کنون مقالات گسترده ای برای بهبود این مقوله حیاتی معرفی شده اند. در این مقاله به بررسی امنیت در سیستم حمل و نقل هوشمند پرداخته ایم.*

واژه‌های کلیدی : *امنیت اینترنت اشیا،حمل و نقل هوشمند،امنیت،هوشمند سازی، اینترنت اشیاء*

۱. مقدمه

اینترنت اشیاء (Internet of things (IoT)) شبکه ای است که هر شیء را به اینترنت متصل می کند و از ادغام و ترکیب چندین فناوری از جمله شناسایی خودکار امواج رادیویی، حسگر، سیستم موقعیت یاب جهانی و اسکنرهای لیزری تشکیل شده است که باعث برقراری تبادل اطلاعات و ارتباطات می شود و هدف اصلی آن شناسایی هوشمند، ردیابی محل، نظارت و مدیریت است. [۲،۱]. تکنولوژی های تحت وب با سرعت بالایی در حال پیشرفت است و دستیابی به ایده های شهر هوشمند را تحقق پذیر کرده است. مفهوم جدید اینترنت اشیاء امکانات غیرقابل تصوری را برای توسعه مفهوم شهر هوشمند بوجود آورده است . با این وجود سرعت تکنولوژی هایی که امنیت کاربران و اطلاعات آنها را تضمین کند ، به مراتب از تکنولوژی اینترنت اشیاء عقب تر است و مطالعات کمتری در این حوزه مهم صورت گرفته است. امروزه تکنولوژی اینترنت اشیاء بیشترین اهمیت و کاربرد خود را در حوزه ترافیک و حمل و نقل شهری نشان داده است. تعداد بسیار زیادی سفرهای درون شهری برای انجام فعالیت های روزمره در سطح شهر با مسافت های مختلف صورت می گیرد که همین موارد باعث ایجاد ترافیک و آلودگی هوا می شود . اینترنت اشیاء این امکان را دارد که با استفاده از سنسور های فعال خود موجب کاهش این مشکلات گردد . اما مسئله ای که مدیران در کشور های درحال توسعه همچون ایران برای بکار گیری این فناوری نوین بعنوان مانع با آن رو به رو شده اند ایجاد اعتماد کاربران برای پذیرش فناوری اینترنت اشیاء جهت استفاده در امور زندگی شهروندان می باشد . این درحالی است که میزان فعالیت های کاربران در نقاط شهری کشور های توسعه یافته به فناوری اینترنت اشیاء را می توان از شمار دستگاه های متصل به اینترنت که در سال های اخیر اعلام شده است سنجید. پیش بینی می شود در سال ۲۰۲۵ این تعداد بالغ بر ۴۵ میلیارد دستگاه در جهان برسد. این روند رو به رشد نشان دهنده گسترش روز افزون و تاثیرات عمیق کاربرد فناوری اینترنت اشیاء در زندگی روز انسان ها است [۳]. از این رو صنعت نیز علاقه زیادی به IoT نشان داده و به آن توجه زیادی نموده

است [۱۴]. این علاقه موجبات توسعه هزاران حسگر برای اپلیکیشن های مختلف مثل حس کردن مکان، پیش بینی آب و هوا، اپلیکیشن های بیومدیکال و موارد دیگر را فراهم آورده است. اما یکی از مهم ترین کاربرد های این فناوری در دنیای امروزه که نقش مهمی را نیز ایفا می کند بحث حمل و نقل هوشمند است. از چالش برانگیز ترین مباحث در حوزه اینترنت اشیاء بحث امنیت در اینترنت اشیاء می باشد، امنیت در ابعاد و تکنولوژی های مختلف یکی از موارد اساسی و مهم می باشد. این مهم در تکنولوژی های نو ظهور با توجه به تازه بودن و فراگیر بودن مورد اهمیت ویژه ای قرار می گیرد. اما برای کارشناسان شرکت های بزرگ تجاری، مدیران شهری و کاربران اینترنت اشیاء بیش از آن که مفهوم اینترنت اشیاء مهم باشد، مفهوم چالش های معماری و تهدیدات امنیتی در فن آوری اهمیت دارد [۴]. لذا برای پذیرش فن آوری اینترنت اشیاء به صورت شبکه، ابتدا بایستی به موضوع امنیت و محرمانگی آن توجه شود . به عبارت دیگر مسئله اصلی و چالش پیش روی فناوری اینترنت اشیاء به ویژه در کشورهای در حال توسعه، فقدان امنیت در ارتباطات میان اشیاء متصل به اینترنت می باشد. این مشکل می تواند برای پذیرش فن آوری برای کاربران مانع بزرگی محسوب شود و هزینه های زیر ساختی که از سوی دولت های برای راه اندازی این شبکه در نظر گرفته می شود را بی حاصل گرداند. بسیاری از سفر های درون شهری برای انجام کارهای اداری یکی از مواردی است که باعث ایجاد ترافیک و آلودگی هوا می شود. اینترنت اشیاء این امکان را فراهم می کند که این آلودگی ها به حد زیادی کاهش یابد. لذا در این پژوهش مدلی برای امنیت اینترنت اشیاء در حمل و نقل هوشمند را مورد بررسی قرار می دهیم.

بخش اول این مقاله مرور و ادبیات می باشد با توجه به ماهیت بین رشته ای نیاز است برخی مفاهیم بررسی و دیدگاه مشترکی حاصل گردد. لذا این پژوهش فصل مشترکی از مباحث حوزه های حمل و نقل هوشمند، اینترنت اشیاء و امنیت را در بر می گیرد. در بخش دوم روش تحلیل عواملی که با عنوان روش تحقیق برای آزمون فرضیه های مدل پیشنهادی برای افزایش امنیت اینترنت اشیا در حوزه حمل و نقل شهر هوشمند به کار رفته معرفی شده است. در بخش سوم نتایج حاصل از تحلیلها مورد بررسی قرار می گیرد و در بخش نهایی به جمع بندی تحلیل نتایج می پردازیم.

۲. مرور و ادبیات تحقیق

امروزه تکنولوژی های مختلفی به سرعت در حال پیشرفت هستند که فن آوری اینترنت اشیاء و کاربرد آن در حمل و نقل هوشمند هم یکی از آنهاست و بخش قابل توجهی از فن آوری اینترنت اشیاء در این حوزه کار شده است. با این وجود سرعت تکنولوژی که امنیت کاربران و اطلاعات آن ها تظمین کند، به مراتب عقب تر از خود تکنولوژی است. در سالهای اخیر نگاه ویژه تری به این موضوع شده اما همچنان خلع های بسیاری در این حوزه دیده می شود. عوامل مختلفی در این حوزه تاثیر گذار است که در این پژوهش سعی می شود فاکتور های اثر گذار امنیت اینترنت اشیاء در حمل و نقل هوشمند شناسایی و مورد بررسی قرار گیرد. در سالهای اخیر با توجه به رشد تکنولوژی های 4G,5G,cloud computing و ... اینترنت اشیاء به تدریج به صورت فراگیر وارد زندگی ما شده است تا برای کنترل و نظارت هوشمند و قوی تر و زندگی آسان تر مورد استفاده قرار گیرد.

اوین اشاتون در سال 1999 برای نخستین بار نظریه اینترنت اشیاء را مطرح نمود ، اینترنت اشیاء مقوله جدید و نا آشنایی نیست اولین نمونه استفاده از این تکنولوژی، تولید و رونمایی از توستر متصل به اینترنت توسط یک کمپانی طی یک کنفرانس در سال 1989بود[۶و۳]

اینترنتِ اشیاء بعنوان مفهومی جدید در دنیای فن آوری وارتباطات، فن آوریِ مدرنی است که در آن برای هر موجودی (انسان، حیوان و یا اشیاء) قابلیت ارسال داده از طریق شبکه ها ارتباطی، اعم از اینترنت یا اینترانت، فراهم می گردد. بستر اینترنت اشیاء بر امواج رادیویی بی سیم قرارداده شده که به دستگاه های مختلف این امکان را می دهند تا از طریق اینترنت با یکدیگر به برقراری ارتباط بپردازند.

در حال حاضر دامنه کاربردهای IoT تنها به تصورات ما محدود می شود بر اساس بررسی مقالات انجام شده، کاربرد ها به حوزه های اصلی زیرساخت هوشمند، بهداشت، لجستیک/ زنجیره تامین، کاربردهای اجتماعی و سایر کاربردها تقسیم می شود که در ادامه با توجه به مبحث مقاله به تعاریف مختصری در حوزه لجستیک و حمل و نقل هوشمند خواهیم پرداخت.

لجستیک و زنجیره تامین: از گذشته تا بحال از RFID و شبکه های حسگر استفاده گسترده می شده است. از حسگرها درخطوط مونتاژ اماکن تولیدی و نیز از RFID برای رهگیری محصولات در طول بخشی از زنجیره تامین آن توسط هر شرکت استفاده می شود. اگرچه استفاده از این تکنولوژی ها در زنجیره تامین امری جدید نیست، اما IoT امکان استفاده از این تکنولوژی ها را درکل مرزهای جغرافیایی و سازمانی ممکن می کند. بویژه IoT می تواند کارایی زنجیره تامین را از طریق اطلاعاتی که دارای جزئیات بیشتر و به روزتر است بیشتر از قبل بهبود ببخشد که این امر منجر به بهبود قابلیت رهیگری محصولات می شود. برای مثال مدتی است که از RFID برای رهگیری محصولات و بخشهای مختلف آنها در زنجیره تولید استفاده می شود با این حال هنگامی که محصول از فروشگاه خارج می شود دیگر تولید کننده توانایی خود برای رهگیری آن را از دست می دهد. به همین شکل، مصرف کنندگان نمی توانستند به چرخه زندگی محصولات خریداری شده دسترسی پیدا کنند. به واسطه ی اختصاص یک شناسه منحصر به فرد برای هر محصول و امکان دسترسی به داده های آن از طریق وب، IoT امکان رهگیری محصولات را در طول کل چرخه عمر آنها امکانپذیر می کند[۷].

صنعت حمل و نقل: اینترنت اشیاء در بحث حمل و نقل و مدیریت تردد به کمک حکومت می آید و مانیتور ترددها و ترافیک را تسهیل سازی می کند. وسایل نقلیه مستقل می توانند پویایی حمل و نقل و تدارکات تحت پوشش شهر را تغییر دهند. بعنوان نمونه هواپیمای بدون سرنشین تجهیزات پزشکی می تواند به نجات زندگی انسان در مناطق دسترسی سخت و صعب العبور کمک نماید و تاکسی های بدون راننده می تواند با استفاده از تشخیص مسیر های بدون ترافیک به مسافران خود کمک کنند[۸].

۱،۲. معماری و پروتکلهای اینترنت اشیاء

در این بخش یک معماری کلی مورد استفاده برای اینترنت اشیاء مورد بررسی قرار می گیرد و یک معماری مبتنی بر استاندارد هفت لایه ISO و پروتکل های مرتبط معرفی می شود تا در ادامه این فصل و بحث های امنیتی از این معماری به عنوان اساس کار مسایل امنیتی اینترنت اشیاء مورد استفاده قرار بگیرد.

اینترنت اشیاء در واقع شبکه ای از اشیاء قابل شناسایی، اتصال و تجمیع آنها با اینترنت و نمایش[۵] آن ها در دنیای دیجیتال یا مجازی می باشد. برای ایجاد یک شبکه اینترنت اشیاء، طیف وسیعی از تکنولوژی ها درگیر می باشند. به عنوان مثال شناسه های RFID برای شناسایی تجهیزات و مکان یابی آنها، پروتکلهای بهبود یافته برای پوششهای شخصی[۶] و گسترده، تکنولوژی های وب و غیره برای تکامل شبکه اینترنت اشیاء درگیر خواهند بود. این تکنولوژی ها در کنار یکدیگر منجر به ایجاد دنیای مجازی[۷] از اشیاء بر روی دنیای حقیقی فیزیکی خواهد شد که در آن اشیاء با استفاده از مخابرات ماشین به ماشین (M2M)[۸]قابلیت صحبت با هم خواهند داشت. با این وجود، این اشیاء با هدایت انسان قادر به جمع آوری داده برای انسان یا انجام برخی دستورات انسان در محیط پیرامون یا به عنوان یک سری واحدهای منفعل قادر به جمع آوری داده برای واحدهای هوشمندتر خواهند بود. شبکه های حسگر بی سیم[۹] (WSN) یکی از تکنولوژی های اتصال دنیای مجازی و فیزیکی است که در آن حسگرها به عنوان گره های شبکه قادر به برقراری ارتباط خودکار بین خودشان و سیستم‌های هوشمندتر هستند. شبکه های حسگر ابتدایی مجموعه ای از تجهیزات حسی است که داده های محیطی را حس، جمع آوری و با همکاری یکدیگر به یک گره اصلی برای پردازش ارسال می کند. این نسل از شبکه های حسگر فاقد استاندارد خاصی بوده و معمولا برای مانیتور کردن محیط های دور از دسترس از قبیل جنگل ها، بیابان ها یا میدان های جنگی مورد استفاده قرار می گیرند.

شبکه های حسگر فعلی یا پیشرفته در محیط های نزدیکتر به انسان و برای اهدافی از قبیل کنترل ترافیک، مانیتورینگ پل ها و تونل ها، کنترل و انتقالات صنعتی پیاده سازی شده اند. بطورکلی IoT می تواند به سه لایه کلی تقسیم شود. شکل۱ ، معماری لایه های اینترنت اشیاء را نشان می دهد[۸].

-سطح اول لایه ادراک: اساسی ترین لایه، لایه ادراک یا لایه تشخیص می باشدکه تمامی اطلاعات را از طریق تجهیزات فیزیکی

[۵] Representation

[۶] Personal area network

[۷] Virtual world

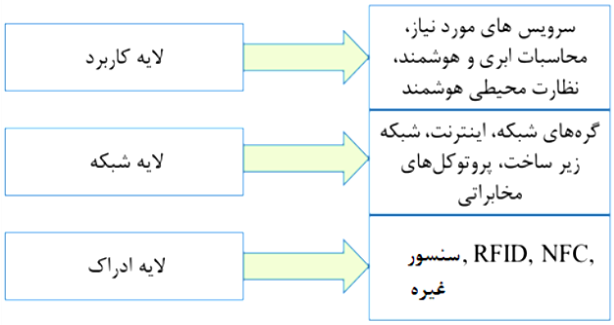
[۸] Machine to machine (M2M)

[۹] Wireless sensor networks (WSN)

جمع آوری کرده و دنیای فیزیکی را شناسایی می کند، این اطلاعات شامل خصوصیات اشیاء، شرایط محیطی و ... و تجهیزات فیزیکی شامل خواننده،RFID تمامی انواع سنسورها، GPS و دیگر تجهیزات می باشد. مولفه اساسی در این لایه، سنسورها برای دریافت و بیان دنیای واقعی در دنیای دیجیتال است.

-سطح دوم، لایه شبکه: مسئول ارسال اطلاعات از لایه ادراک، پردازش اولیه اطلاعات، دسته بندی و پردازش می باشد. در این لایه، ارسال اطلاعات مبتنی بر چندین شبکه پایه بوده که شامل اینترنت، شبکه مخابرات سیار، گره های ماهواره ای، شبکه بیسیم و شبکه زیرساخت بوده و پروتکل های مخابراتی نیز جهت تبادل اطلاعات بین تجهیزات ضروری است.

-لایه کاربرد: که مدیریت نقش و کاربرد اینترنت اشیاء را مشخص می کند و ممکن است از یک زیر لایه برای ایجاد یک بستر قابل اطمینان استفاده کند.



شکل ۱- -معماری لایه ای اینترنت اشیاء

۲,۲. پیشینه تحقیق

احمد اتملی [۱۰] و اندرئو مارتین [۱۱] در سال ۲۰۱۵ بر روی موضوع تحلیل امنیتی مبتنی بر تهدید در اینترنت اشیاء تحقیق و یک مدل تهدید درIoT ارائه نمودند که برای تعیین محل سرمایه گذاری به منظور امن شدن این سیستم ها با توجه به تلاشهای انجام شده در این زمینه استفاده می شود. آنها به این نتیجه رسیدند که اقدامات توصیه شده در ارائه تأمین امنیت و تضمین حفظ حریم خصوصی هنگام استفاده ازIoT به ماکمک خواهند کرد. چشم انداز اینترنت اشیاء و ارتباط آن با سایر پژوهش ها در زمینه امنیت و حریم خصوصی دراینترنت اشیاء بحث شده است. همچنین رویکردهای مختلفی که توسط بسیاری از محققین در امنیت و حریم خصوصی نشان داده شده ارائه گردیده است. رویکرد مبتنی برتحلیل تهدیدهای اتخاذ شده، مدل تهدید را بعنوان روشی برای تحلیل تأثیر تهدیدها درکاربردهای مختلف ارائه می نماید. از این مدل تهدید، ویژگی های حریم خصوصی و امنیت استنباط می شود. این ارزیابی ما را در مشخص نمودن تلاشها و توجهات بیشتر در فعالیتهای آینده که باید در توسعه مکانیزمهای امنیتی در اینترنت اشیاء سرمایه گذاری شود راهنمایی خواهد کرد[۹].

ژی کای ژانگ [۱۲] و همکارانش در سال ۲۰۱۱ بر روی موضوع تهدیدهای امنیتی و اقدامات متقابل در حال ظهور در اینترنت اشیاء تحقیق نموده اند. این مقاله ، سناریوهای ارتباطات اینترنت اشیاء را برشمرده و تهدیدها را در مقیاس بزرگ ، فضای غیر قابل اعتماد و در محیط محاسبات فراگیر بررسی نموده است. برای مقابله با این چالش های جدید، معماری امنیتی متعارف بازبینی خواهد شد. به خصوص، الگوهای احراز هویت مختلفی برای اطمینان از محرمانه بودن و صحت داده های مبادله شده ارزیابی می شود. علاوه برموضوع تهدیدهای امنیتی و اقدامات متقابل در حال ظهور در اینترنت اشیاء، بطور ویژه چالش های تبادل اطلاعات حساس و خصوصی بین اشیاء در حال جابجایی، اشیاء در منزل و اشیاء در سازمان ارزیابی شده اند. نامگذاری، مدیریت و احراز هویت اشیاء درIoT از مسائل کلیدی برای برقراری ارتباطات امن و بازیابی داده ها هستند. براساس سناریوهای مختلف ارتباطات در IoT ، چند الگوی احراز هویت بالقوه که قابل اجرا هستند عنوان شده است[۱۰].

کی جینگ [۱۳] و همکارانش در سال ۲۰۱۷ بر روی موضوع چشم اندازها و چالش های اینترنت اشیاء پژوهش نمودند که تمرکز آنها بر روی مشکلات امنیتی در میان دیگر چالش ها می باشد. همانطور که IoT براساس اینترنت ساخته شده است ، مشکلات امنیتی اینترنت نیز در IoT نشان داده خواهد شد. این مقاله مشکلات امنیتی هر سه لایه ادراک، انتقال و کاربرد را به صورت جداگانه تجزیه و تحلیل نموده و سعی شده مشکلات جدید و راه حل آنها را بیابد. این مقاله همچنین مسائل یکپارچگی در بین لایه های غیرهمگن و جزئیات مسائل امنیتی را تجزیه و تحلیل می کند و بطور کلی در مورد مسائل امنیتی IoT بحث و تلاش می کند برای آنها راه حل هایی بیابد. همچنین این مقاله به مقایسه

[۱۰] Ahmad Atamli
[۱۱] Andrew Martin
[۱۲] zhi kai zhang
[۱۳] Qi Jing

مسائل امنیتی بین IoT و شبکه های سنتی و بحث در مورد باز کردن مسائل امنیتی IoT می پردازد[۱۱].

امروزه، نگرانی های حریم خصوصی و امنیت به یک مانع و عامل کاهش پیشرفت بسیاری از فن آوری ها تبدیل شده است. بسیاری از فنآوری ها در ارائه مناسب مکانیزم های امنیتی و حریم خصوصی شکست خورده اند ، در نتیجه باعث آزردگی و آسیب شده اند. به منظور به دست آوردن اعتماد عمومی در اینترنت اشیاء ما نیاز داریم بپذیریم که حریم خصوصی و امنیت این سیستم ها پذیرفته نمی شود ، مگر با اعمال مکانیزم های مناسب به منظور تضمین امنیت اشیائی که از ابتدا در IoT وجود دارند. هدف اصلی این مقاله بررسی و شناسایی تهدیدات امنیتی استفاده از اینترنت اشیاء در حمل و نقل هوشمند است.

۳. چالش های امنیتی اینترنت اشیا

به منظور برآورده کردن مسئله امنیت، اینترنت اشیاء با چالش های بیشتری نسبت به شبکه های موجود مواجه است. با توجه به تعداد تجهیزات متصل شده به شبکه، ارتباط این تجهیزات و اشیاء با یکدیگر و توسعه اینترنت اشیاء در بستری از شبکه های موجود از قبیل اینترنت، شبکه موبایل و شبکه حسگرها و ... اینترنت اشیاء با چالشهای امنیتی بیشتری مواجه است. در نتیجه، برخی از تکنولوژی ها و روش های جدید، باید جهت برآورده کردن نیازمندی های بیشتر بر حسب قابلیت اطمینان، امنیت و حریم خصوصی، توسعه داده شود. امنیت اطلاعات و شبکه باید با خصوصیاتی از جمله شناسایی، قابلیت اعتماد، رمزنگاری و غیرقابل انکار بودن و... برآورده شود. در نتیجه، امنیت در حوزه IoT در مسئله قابل دسترسی بودن و مستقل بودن، دارای اهمیت بیشتری است.

چالش های این حوزه بسیارند، که هم اجتماعی اند و هم فنی و باید آنها را رفع کرد تا IoT مورد استفاده و پذیرش عمومی قرار گیرد. می توان این چالش ها را به سه دسته امنیت ارتباط ، حریم خصوصی و مسئولیت پذیری/مسائل حقوقی تقسیم بندی کرد[۱۲و۱۳و۱۴].

-امنیت ارتباط

دستگاههای IoT غالباً وایرلس هستند و ممکن است در مکانهای عمومی واقع شوند. ارتباط وایرلس از طریق رمزنگاری کردن امن تر می شود و در نتیجه رمزنگاری کردن داده برای اشیاء یک روش افزایش امنیت اطلاعات است. با این وجود، بسیاری از دستگاههای IoT فعلی به اندازه ای قوی نیستند که از روش رمزنگاری مناسب پشتیبانی کند. پس، برای ممکن کردن رمزنگاری در این شبکه، لازم است در دستگاههای IoT از الگوریتم های کاراتر و با مصرف انرژی کمتر استفاده کرد و همچنین به روشهای کارآمد تری از نظر توزیع کلید رو آورد. علاوه بر رمزنگاری، احراز هویت هم مسئله امنیتی مهمی بوده و برای دست یافتن به آن، وجود شناسه های یکتا برای دستگاه های IoT امری مهم می باشد. این شناسه ها حتی ممکن است برای تعیین کردن هویت شیء در نهادهای ملی، شناسایی فعالیت های قانونی و سایر عملکردها استفاده شوند . از اینرو، حصول اطمینان از اینکه اشیاء هوشمند دقیقاً همانهایی هستند که ادعا می کنند، برای موفقیت امنیت IoT حیاتی است. بطور کلی فرض می شود ساختار اینترنت اشیا در طول کل بازه زمانی، پایدار باقی می ماند و نشان داده شده است که مکانیزم امنیت در هر لایه منطقی نمی تواند سیستم امن کاملی را پیاده سازی کند، در نتیجه، این موضوع و استفاده از الگوریتم های بین لایه ای هنوز به عنوان یک چالش در اینترنت اشیاء مطرح است. این مساله در مرحله بعدی منجر به لزوم داشتن یک مکانیزم امن مدیریت اساسی کل شبکه می شود.

-حریم خصوصی

همچنانکه اشیاء بیشتری از طریق IoT قابل رهگیری می شوند، تهدیدها برای حریم خصوصی جدی تر شده اند علاوه بر ایمن سازی داده ها جهت عدم قرارگیری آنها در اختیار افراد غیرهدف، لازم است مساله مالکیت داده ها نیز حل شود تا کاربران بتوانند راحت تر در IoT مشارکت کنند. از این رو، مالیکت داده های گردآوری شده از اشیاء هوشمند باید به وضوح مشخص شود. لازم است مالک داده را مطمئن کرد که داده ها بدون رضایت وی استفاده نمی شوند بویژه به هنگام به اشتراک گذاری داده ها . سیاستهای حریم خصوصی می تواند رویکردی برای حصول اطمینان از محرمانگی داده ها باشند. اشیاء هوشمند و دستگاههای خوانشگر در IoT را می توان به تنظیمات سیاستهای حریم مجهز کرد. پس، زمانی که شی و خوانشگر وارد ارتباط می شوند، آنها می توانند قبل از تکمیل فرآیند ارتباط، اقدام به بررسی سیاست حریم خصوصی یکدیگر جهت سازگاری کنند.

۴. فناوری سنسور[۱۴]

استفاده از سنسور ها برای تبدیل حمل و نقل سنتی به هوشمند ضروری و از نیاز های اولیه است . در واقع سنسور عنصری است که عوامل خروجی را به شکل سیگنال و به عنوان ورودی دستگاه ها جهت پردازش و تصمیم گیری به مرکز پردازشی اینترنت اشیاء می‌فرستد، در شکل ۲ سنسور های موجود در یک خوردو هوشمند نشان داده شده است.

- در مواقع مشکل و خطا سنسور ها سریعا به واحد های ترافیکی و امدادی اطلاع می دهند
- نیاز به نیروی انسانی ماهر را کاهش می دهند.
- در نهایت محصول با کیفیت بهتری را می توانند ارائه دهند.

به طور کلی خروجی ها و تصمیم گیری های یک عامل هوشمند (چراغ ها، مسیر یابی، خودرو ها و...) در حمل و نقل هوشمند و تصمیم گیری عامل ها نقش موثری دارند[۱۴]. در صورت براورده شدن این نقش ها به درستی، ایمنی حمل و نقل تضمین می شود که در نهایت باعث رضایت مسافران ، رانندگان و کلیه استفاده کنند گان از سیستم حمل و نقل عمومی می شود. همانگونه که در تصویر شماره ۲ مشخص است برخی از سنسور ها برای نظارت و کنترل عملکرد، موقعیت ،کارایی و سیستم ایمنی نصب شده اند به طور متوسط برای یک خودرو هوشمند بین ۵۰ تا ۱۰۰ سنسور



شکل ۲ - سنسور های موجود در خورو های هوشمند

نصب گردیده است . برای یک خودرو هوشمند تر تعداد سنسور ها به ۲۰۰ سنسور نیز می‌رسد[۱۵].

۵. امنیت در شبکه های اینترنت اشیاء مورد استفاده در حمل و نقل

همانگونه که در قسمت هایی از مقاله پیش رو بیان گردید شبکه های اینترنت اشیاء بنا بر مزایایی که فراهم می سازند، امروزه به یکی از مهم ترین تکنولوژی ها در عرصه های مختلف عنوان شده که روز به روز بر کاربرد این فناوری افزوده می شود[۱۶و۱۷]. به طور کلی بخش عمده ای از این کاربرد ها ، کاربرد های حساس و پر اهمیت هستند و استفاده از این فن آوری باعث شده تا اهمیت امنیت و پیاده سازی امنیت در این شبکه ها بیشتر از سایر شبکه ها مورد توجه و بررسی قرار گیرد. این در حالی است که مسائلی همچون توپولوژی و مقیاس پذیری جغرافیایی شبکه به این مشکلات دامن زده و بحث برقراری امنیت را امری بسیار دشوار و پیچیده نموده است. در مجموع وجود این مسائل برای شبکه های اینترنتی اشیاء باعث ایجاد تفاوت ها و پیچیدگی های خاص در حوزه امنیت و برقراری امنیت ارتباطات این شبکه ها شده است .

وجود مسائل و مباحث عنوان شده ، به ضرورت ارائه مدل هایی متمایز به جهت برقراری و پیاده سازی امنیت در شبکه های اینترنت اشیاء (به عنوان نیاز و ضرورتی انکارناپذیر) اشاره دارد . بر همین اساس و با توجه به اهمیت بالای بحث امنیت در شبکه های اینترنت اشیاء ، تا کنون مقالات گسترده ای برای بهبود این مقوله حیاتی معرفی شده اند . در یک دسته بندی کلی این روش ها را می توان به دو دسته کلی به قرار زیر بخش بندی و ارزیابی نمود [۱۸و۱۹].

- روش های رمزنگاری

هدف این سیستم، رمزنگاری داده ها به جهت پیشگیری از دسترسی های غیرمجاز است . مهم ترین مسئله این روش عدم مقابله با حملات فعال است.

- روشهای مبتنی بر اعتماد[۱۵]

هدف ایجاد اعتماد بین گره های شبکه به جهت تشخیص انواع حملات مخرب است. مهم ترین مسئله این روش عدم وفق پذیری با پویایی و عدم قطعیت محاسبات اعتماد است .

تمامی روش های پیشنهادی برای اینترنت اشیاء بر اساس دو روش رمزنگاری و یا مدل های اعتماد طراحی شده اند. این درحالی است که بیشتر این تحقیقات مبتنی بر مدل های اعتماد طراحی و توسعه یافته اند. این مدل ها برای برقراری اعتماد در اینترنت اشیاء بسیار کارا بوده و همچنین با خصوصیات این فناوری بسیار

[۱۴] Sensor Technology

[۱۵] Trust Mechanism

سازگارتر هستند. روش های معرفی شده بر پایه این مدل قابلیت مقابله با هر دو نوع حملات عوامل خودخواه و عوامل بدخواه را فراهم ساخته و در شرایط مختلف شبکه ، پاسخگوی نیازهای مختلف امنیتی هستند [۱۹و۲۰]. این مدل ها بر پایه اعتماد اجتماعی طراحی شده و منطبق با این اصل عمل می کنند. در این روش گره های شبکه با انجام رفتار های درست با افزایش اعتماد و اعتبارشان تشویق شده و در صورت سوء رفتارها با کاهش اعتماد مجازات خواهند شد. از نتایج این افزایش و کاهش اعتماد به منظور تفکیک عوامل خوش رفتار از عوامل مخرب استفاده می شود . به طوری که اگر اعتماد عاملی به زیر مقدار مشخصی سقوط کند ، عامل مورد نظر مهاجم در نظر گرفته شده و به منظور مجازات در شبکه قرنطینه خواهد شد.

۶. مروری بر روش های پیشنهادی امنیت حمل و نقل هوشمند بر مبنای اینترنت اشیاء

بنابر آنچه در ارتباط با اهمیت امنیت و اعتماد در اینترنت اشیاء ارائه و عنوان شد، تا کنون مقالات و تحقیقات گسترده ای در راستای بهبود این مبحث کلیدی معرفی شده اند. در این بخش برخی از جدیدترین مدل های اعتماد و امنیت ارائه شده برای شبکه های اینترنت اشیا که در حمل و نقل هوشمند نیز بکار می رود را از لحاظ قابلیت و محدودیت ها بررسی خواهیم کرد.

- روش های رمز نگاری

این روش ها بر مقابله با حملات دسترسی یا به اصطلاح حملات غیر فعال متمرکز شده و تمرکز آن ها بر رمزنگاری و پیشگیری از دسترسی غیر مجاز به اطلاعات است. برای این منظور اغلب این روش ها از تکنیک های رمزنگاری استفاده می گردد.[۱۴].

- روش های احراز هویت

این روش ها بر احراز هویت گره ها متمرکز شده و هدف آن ها مقابله با حملات خارجی است. در واقع این روش ها با تدابیری که فراهم می سازند، قابلیت تشخیص گره های شبکه را فراهم می سازد و با همین روش قادر به مقابله با این سوء رفتار هستند[۱۵].

- روش های مبتنی بر تکنیک های فرا ابتکاری[۱۶]

این روش بر پایه الگوریتم های فرا اکتشافی مانند گرگ خاکستری و سایر الگوریتم های زیست محیطی گسترش یافته و بر پایه قابلیت های این روش ها طراحی گردیده اند. این روش ها اغلب به برقراری اعتماد توام با توسعه مسیر متمرکز شده و از این حیث موفق اند. اما این روش ها با افزایش سربار های کنترلی همراهند[۱۵].

- روش های متمرکز بر ازریابی چند معیاره

در روش های متمرکز بر ارزیابی چند معیاری، قابلیت اعتماد وابسته به چند عامل محاسبه شده و معمولا ترکیبی از QOS یا قابلیت اطمینان می باشد. برای مثال علاوه بر اعتماد به عملکرد گره ها،کیفیت اتصال و انرژی گره ها نیز در نظر گرفته شده که از آن ها با عنوان اعتماد به اتصال و اعتماد به انرژی یاد می شود[۱۹].

- روش های مبتنی بر خوشه بندی

این روش ها بر مبنای خوشه بندی گره ها طراحی شده و بر این اساس سعی بر برقراری امنیت دارند. برای این منظور گره ها به خوشه هایی مجزا تقسیم شده و برای هر گره یک سر خوشه انتخاب می شود . معمولا انتخاب سر خوشه ها بر اساس انرژی باقی مانده بیشتر یا تلفیقی از این دو عامل انجام می شود. پس از خوشه بندی، اعتماد اعضا خوشه توسط گره سر خوشه ارزیابی و ذخیره شده و در ادامه بر مبنای این اعتماد برای تشخیص گره مخرب تصمیم گیری می شود . مزیت این روش ها را می توان بهینه سازی انرژی و مدیریت موثر اعتماد عنوان کرد. اما از محدودیت های این دسته از روش ها می توان به پیچیدگی و تاخیر بالا اشاره نمود [۱۵و۱۶و۱۹] .

- روش های متمرکز بر حملات مسیریابی

تمرکز این دسته از روش ها بر مقابله با حملات مسیریابی از جمله حمله رتبه ، حمله سیاه چاله ، حمله گودال کرم ، حمله چاله خاکستری و غیره می باشد . اغلب این روش ها بر حوزه مسیر یابی و ارزیابی فرایند های مسیریابی (مانند ارزیابی تعداد و محتویات پیام های DIO و DAO) متمرکز شده و بر اساس نتایج این ارزیابی سعی بر تشخیص حملات دارند . برترین قابلیت این روش ها را می توان مقابله با حملات مسیریابی و بزرگ ترین مشکل آن ها را می توان ناکارآمدی در مقابله با سایر حملات عنوان نمود [۱۶و۲۰].

16 Meta Heuristic

نتیجه گیری

در این مقاله به معرفی تکنولوژی نو ظهور اینترنت اشیاء و در ادامه به بررسی امنیت در اینترنت اشیا و استفاده و کاربرد اینترنت اشیاء در حمل و نقل پرداخته شد. همانگونه که بیان شد به طور کلی بخش عمده ای از این کاربرد ها حساس و پر اهمیت هستند و استفاده از این فناوری باعث شده تا اهمیت امنیت و پیاده سازی امنیت در این شبکه ها بیشتر از سایر شبکه ها مورد توجه و بررسی قرار گیرد. این در حالی است که مسائلی همچون توپولوژی و مقیاس پذیری جغرافیایی شبکه به این مشکلات دامن زده و بحث برقراری امنیت را امری بسیار دشوار و پیچیده نموده است. در مجموع وجود این مسائل برای شبکه های اینترنت اشیاء باعث ایجاد تفاوت ها و پیچیدگی های خاص در حوزه امنیت و برقراری امنیت ارتباطات این شبکه ها شده است. وجود مسائل و مباحث عنوان شده ، به ضرورت ارائه مدل هایی متمایز به جهت برقراری و پیاده سازی امنیت در شبکه های اینترنت اشیاء (به عنوان نیاز و ضرورتی انکارناپذیر) اشاره دارد . بر همین اساس و با توجه به اهمیت بالای بحث امنیت در شبکه های اینترنت اشیاء، تا کنون مقالات گسترده ای برای بهبود این مقوله حیاتی معرفی شده اند که در این پژوهش مورد بررسی قرار گرفتند.

مراجع

[1] Ashton K (2009) That ‘internet of things’ thing. RFID J 22(7):97–114

[2] Kobayashi G, Quilici-Gonzalez JA, Broens MA, Quilici- Gonzalez ME (2011) Ubiquity of virtual disguisers and potential impact on ethical behavior. In: 2011 fourth international conference on Ubi-media computing. IEEE, Piscataway

[3] Kobayashi G, Quilici-Gonzalez ME, Broens MC, Quilici-Gonzalez JA (2016) The ethical impact of the Internet of Things in social relationships: technological mediation and mutual trust. IEEE Consumer Electron Mag 5(3):85–89

[4] Zheng S, Jiang T, Baras J (2011) Exploiting trust relations for nash equilibrium efficiency in ad hoc networks. In: IEEE international conference on communications (ICC), 2011. IEEE, Piscataway

[5] Ricci F, Rokach L, Shapira B (2015) Recommender systems: introduction and challenges. In: Recommender systems handbook. Springer, Berlin, pp 1–34

[6] Kalaï A, Zayani CA, Amous I, Abdelghani W, Sèdes F (2017) Social collaborative service recommendation approach based on user’s trust and domain-specific expertise. Future Gen Comput Syst 80:355–367

[7] Montori, Federico, et al. "Machine-to-machine wireless communication technologies for the Internet of Things: Taxonomy, comparison and open issues." Pervasive and Mobile Computing 50 (2018): 56-81.

[8] Dey, Amlan Jyoti, and Hiren Kumar Deva Sarma. "Routing techniques in internet of things: a review." Trends in Communication, Cloud, and Big Data (2020): 41-50.

[9] Marietta, J., and B. Chandra Mohan. "A review on routing in internet of things." Wireless Personal Communications 111.1 (2020): 209-233.

[10] Asghari, Parvaneh, Amir Masoud Rahmani, and Hamid Haj Seyyed Javadi. "Internet of Things applications: A systematic review." Computer Networks 148(2019): 241-261.

[11] Dhanvijay, Mrinai M., and Shailaja C. Patil. "Internet of Things: A survey of enabling technologies in healthcare and its applications." Computer Networks 153 (2019): 113-131.

[12] Harbi, Yasmine, et al. "A review of security in internet of things." Wireless Personal Communications 108.1 (2019): 325-344.

[13] Ogonji, Mark Mbock, George Okeyo, and Joseph Muliaro Wafula. "A survey on privacy and security of Internet of Things." Computer Science Review 38 (2020): 100312.

[14] Wang, Lanjing, et al. "ISA evaluation framework for security of internet of health things system using AHP-TOPSIS methods." IEEE Access 8 (2020): 152316-152332.

[15] Alshehri, Mohammad Dahman, and Farookh Khadeer Hussain. "A fuzzy security protocol for trust management in

the internet of things (Fuzzy-IoT)." Computing 101.7 (2019): 791-818.
[16] Fu, Yulong, et al. "An automata based intrusion detection method for internet of things." Mobile Information Systems 2017 (2017).
[17] Suryani, Vera, Selo Sulistyo, and Widyawan Widyawan. "Two-phase security protection for the Internet of Things object." Journal of Information Processing Systems 14.6 (2018): 1431-1437.
[18] Yan, Zheng, Peng Zhang, and Athanasios V. Vasilakos. "A survey on trust management for Internet of Things." Journal of network and computer applications 42 (2014): 120-134.
[19] Mohammadi, Venus, et al. "Trust-based recommendation systems in Internet of Things: a systematic literature review." Human-centric Computing and Information Sciences 9.1 (2019): 1-6
[20] Sharma, Avani, et al. "Towards trustworthy Internet of Things: A survey on Trust Management applications and schemes." Computer Communications (2020)

کنترل سرعت موتور DC تحریک مستقل با کنترل‌کننده‌های On-Off و PID

علیرضا محمودی‌فرد alireza10.m10@gmail.com[1]
سینا تقی‌پور نقشی sina.taghipour.stpn@gmail.com[2]
[1]مدرس مدعو دانشگاه صنعتی قم، قم، ایران
[2]دانشجوی کارشناسی پیوسته مهندسی برق دانشگاه صنعتی قم، قم، ایران

چکیده: در این مقاله، هدف کنترل سرعت الکتروموتور DC تحریک مستقل و طراحی کنترل‌کننده On-Off و PID (شامل P، PI و PID) مطلوب برای این موتور است؛ به این منظور، الکتروموتور با یک سیستم مرتبه اول با ترم تاخیر مدل‌سازی می‌شود و با چهار روش Z-N، IAE، ISE و ITAE کنترل‌کننده P، PI و PID طراحی می‌شود؛ پس از طراحی با استفاده از نرم‌افزار MATLAB، سیستم حلقه‌بسته شبیه‌سازی شده و سرعت خروجی الکتروموتور بر حسب دور بر دقیقه مشخص می‌گردد و نتایج حاصل از محاسبات با شبیه‌سازی صورت گرفته، مورد بررسی قرار می‌گیرد.

کلید واژه‌ها: *الکتروموتور DC تحریک مستقل، کنترل‌کننده PID، کنترل‌کننده On-Off، طراحی کنترل‌کننده، سرعت، شبیه‌سازی*

۱. مقدمه

برای بهبود عملکرد سیستم‌ها، طراحی کنترل‌کننده امری ضروری می‌باشد که در ابتدا باید روابط و معادلات حاکم بر سیستم را به‌دست آورد و سپس به طراحی کنترل‌کننده پرداخت؛ کنترل‌کننده را بسته به نیاز، با روش‌های مختلفی طراحی می‌کنند که در این بخش، کنترل‌کننده On-Off و PID[1] برای بهبود عملکرد موتور الکتریکی DC تحریک مستقل با روش‌های تصحیح خطا متفاوت طراحی می‌شوند که هدف از این کار، رسیدن به موارد مطلوبی است که موتور با سرعت متناسب و مطلوبی کار کند.

۲. روش کار

موتور DC تحریک جداگانه‌ای مفروض است؛ ورودی موتور، جریان آرمیچر i_a (بر حسب آمپر) و خروجی آن، سرعت شفت موتور ω بر حسب دور بر دقیقه[2] (RPM) می‌باشد؛ می‌توان این سیستم را به صورت زیر مدل کرد [۱]:

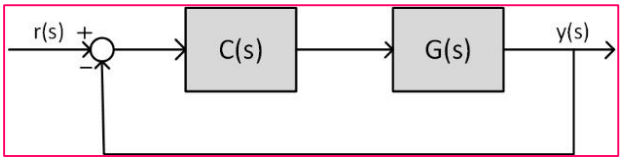
$$G(s) = \frac{\omega(s)}{i_a(s)} = \frac{k_e}{(Is + C_z)} \quad (1)$$

که در آن I ممان اینرسی، C_z ضریب اصطکاک ویسکوز و k_e یک ضریب ثابت می‌باشد. ساختار کنترلی شکل ۱ را در نظر بگیرید که

در آن C(s)، تبدیل لاپلاس کنترل‌کننده می‌باشد که باید طراحی گردد؛ پارامترهای مدل، مقادیری مثبت به‌طور دلخواه می‌باشد.

[1] Proportional_Integral_Derivative (PID)

[2] Round Per Minute or Revolutions Per Minute (RPM)



شکل ۳: بلوک دیاگرام سیستم حلقه‌بسته

۳. کنترل‌کننده On-Off و سنسور با تاخیر نیم-ثانیه

هدف، طراحی یک کنترل‌کننده هیسترزیس می‌باشد (منظور تعیین تمام پارامترهای کنترل‌کننده است) به‌طوری‌که سرعت موتور را در بازه $\omega = 1000 \pm 20[\text{RPM}]$ قرار دهد.

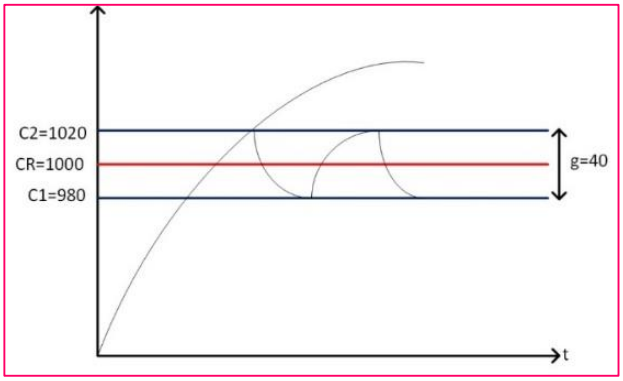
با وجود این کنترل‌کننده، رفتار حلقه‌بسته را ابتدا تحلیل کرده (به‌عنوان مثال از نظر فرکانس نوسانات خروجی و غیره) و با استفاده از شبیه‌سازی توسط نرم‌افزار MATLAB تحلیل مورد ارزیابی قرار می‌گیرد (برای ارزیابی از نمودارهای مستخرج از نرم‌افزار MATLAB استفاده شده است).

- کنترل‌کننده هیسترزیس

این نوع کنترل‌کننده، نوعی کنترل‌کننده On-Off می‌باشد که برای رفع مشکل کلیدزنی ارائه شده است؛ خروجی سیستم حلقه‌بسته، میان دو مقدار (gap) قابل تنظیم تغییر می‌کند و می‌توان با تغییر دامنه خروجی این کنترل‌کننده، دوره تناوب بین این دو نقطه را تغییر داد. زمانی که خطا از مقدار مشخصی کم‌تر شود، به این معنی است که سرعت خروجی از میزان رفرنس خود بیشتر شده و خروجی کنترل‌کننده صفر می‌شود؛ پس از گذشت زمانی که میزان خطا از حد مشخصی بیشتر شد و یا به عبارتی، سرعت خروجی موتور از سرعت رفرنس خود کم‌تر شد، خروجی کنترل‌کننده فعال شده و جریان الکتریکی با دامنه مشخصی به موتور اعمال می‌شود.

سرعت الکتروموتور DC ذکر شده، باید میان 980RPM تا 1020rpm باشد. با تنظیم پارامترهای کنترل‌کننده نسبت به مشخصات موتور می‌توان سرعت را کنترل نمود. حاصل ضرب DCgain موتور در دامنه خروجی کنترل‌کننده باید بزرگ تر از 1020RPM باشد تا سرعت بتواند بین دو مقدار 980RPM و 1020RPM تغییر کند.

سنسور دارای تاخیر نیم‌ثانیه‌ای است. این تاخیر موجب می‌شود تا سیگنال خطای تولید شده، وابستگی به خروجی زمان گذشته داشته باشد و زمانی که باید عمل قطع و وصل صورت گیرد، این اتفاق نمی‌افتد و تاخیر باعث افزایش gap می‌شود. با دانستن مقدار تاخیر می‌توان کنترل‌کننده را طوری طراحی کرد تا سیگنال خروجی در بازه مطلوب نوسان کند.

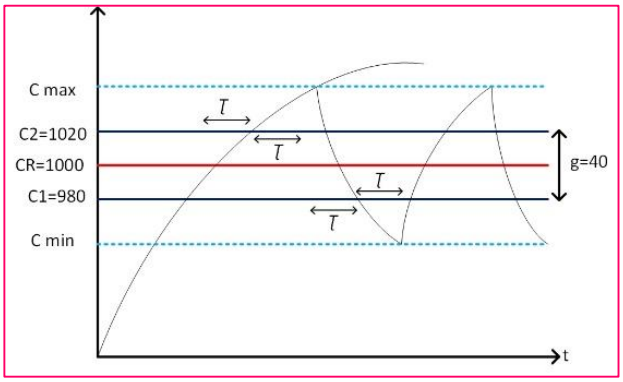


شکل ۴: سرعت خروجی سیستم حلقه‌بسته

زمانی که تاخیر وجود ندارد، ثابت زمانی موتور می‌تواند هر مقدار دلخواهی داشته باشد ولی با وجود چنین تاخیری، سیستم‌های با ثابت زمانی کوچک مناسب چنین کنترلی نمی‌باشند.

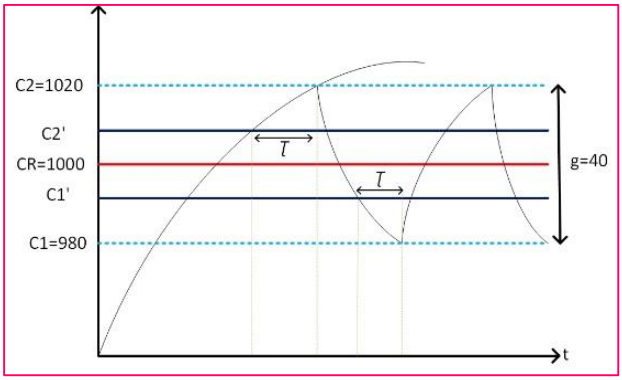
- آنالیز سیستم قطع و وصل برای پروسس درجه یک با تاخیر

اگر ورودی قطع و وصل شود، به‌خاطر وجود ترم تاخیر، خروجی فیدبک شده نمی‌تواند فورا تحت تاثیر قطع و وصل تحریک قرار گیرد، بلکه پس از مدت زمانی برابر تأخیر سیستم این امر صورت می‌گیرد؛ در این حالت، بازه تغییرات سرعت زاویه‌ای موتور بستگی به میزان تاخیر در سنسور دارد و با افزایش ترم تاخیر، دامنه نوسانات خروجی بیشتر می‌شود؛ افزایش دامنه نوسانات تا به حد اشباع رسیدن سرعت خروجی موتور ادامه دارد.



شکل ۵: تناسب افزایش دامنه نوسانات با افزایش ترم تاخیر

همان‌طور که در تصویر ۳ مشخص است، سیگنال خطا ساخته شده بستگی به زمان **τ** ثانیه قبل دارد. اگر میزان تاخیر به صفر میل کند، خروجی در بین C1 و C2 قرار می‌گیرد؛ برای حل این مشکل، باید حوزه کنترل (gap) را به میزانی کوچک در نظر گرفت که در نهایت با وجود ترم تاخیر، خروجی سیستم حلقه‌بسته در میان مقدار مطلوب نوسان کند.



شکل ۶: کوچک کردن حوزه کنترل یا gap

با استفاده از روابط سیستم مرتبه اول در حالت شارژ و دشارژ می‌توان C_2' و C_1' را محاسبه نمود. پارامتر $\frac{\tau}{T}$ که نسبت تاخیر به ثابت زمانی پلنت یا موتور DC تحریک مستقل است با θ نمایش داده می‌شود و پارامتر مهمی در پایداری سیستم خواهد بود. پارامترهای حوزه کنترل جدید به‌صورت زیر می‌باشد:

$$C_2' = ak + (c_2 - ak)e^{\theta} \quad (2)$$

$$C_1' = c_1 e^{\theta} \quad (3)$$

k مقدار DC gain پلنت است و a دامنه خروجی کنترل-کننده هیسترزیس، زمانی که کنترل‌کننده فعال می‌باشد. با انتخاب پارامترها به صورت فوق، سرعت سیستم در بازه 980- 1020RPM قرار می‌گیرد و پریود نوسانات به‌صورت کنترل هیسترزیس بدون تاخیر محاسبه می‌شود:

$$T_0 = T\ ln\frac{C_2}{C_1}.\frac{ak - C_1}{ak - C_2} \quad (4)$$

نکته مهم و قابل توجه آن است که ثابت زمانی موتور DC استفاده شده، هر مقداری را نمی‌تواند در اختیار داشته باشد. اگر ثابت زمانی پلنت کوچک باشد، خروجی نوسانات سریع‌تری را تجربه می‌کند ولی با وجود ترم تاخیر دیگر نمی‌توان سرعت خروجی را در بازه مطلوب نگه داشت [۲].

- طراحی کنترل‌کننده مطلوب

پارامتر ضریب ویسکوز مقداری کوچکی دارد، به‌طور دلخواه برابر با 0.1 فرض شده است ($C_z = 0.1$). سرعت نهایی خروجی به DCgain موتور و دامنه جریان ورودی (سیگنال کنترلی ساخته شده توسط کنترل‌کننده هیسترزیس) بستگی دارد؛ از این جهت، اگر ثابت آرمیچر یا ضریب ویسکوز تغییر کند، باید دامنه خروجی کنترل‌کننده نیز تغییر نماید تا مقدار نهایی سرعت موتور بدون کنترل، بیشتر از 1020RPM شود؛ مقدار ثابت آرمیچر نیز برابر با 10 فرض شده است ($k_e = 10$)؛ با قرار دادن مقادیر ذکر شده، تابع تبدیل موتور به‌صورت زیر به‌دست می‌آید:

$$G(s) = \frac{\omega(s)}{i_a(s)} = \frac{k_e}{(Is + C_z)} \quad (1)$$

$$\frac{\omega(s)}{I_a(s)} = \frac{k_e/C_z}{I/_{C_z}\, s + 1} \rightarrow \tau = I/_{C_z} \quad , \quad k = k_e/C_z$$

$$\frac{\omega(s)}{I_a(s)} = \frac{100}{(\tau s + 1)} \quad (5)$$

برای چنین کنترلی با وجود ترم تاخیر، نمی‌توان هر موتوری با ثابت زمانی‌های دلخواه را در بازه 980-1020RPM کنترل کرد؛ در واقع پلنت‌هایی با ثابت زمانی کوچک و ترم تاخیر بزرگ را نمی‌توان با چنین کنترل‌کننده‌ای کنترل نمود؛ مینیمم ثابت زمانی‌ای که مناسب است، به‌صورت زیر محاسبه می‌شود:

$$C_1' < 1000 \rightarrow e^{\theta} = \frac{1000}{980} \rightarrow \ln\frac{1000}{980} = \frac{0.5}{\tau} \rightarrow \tau > 24.75$$

هرچه مقدار ثابت زمانی بیشتر باشد، سیستم کندتر می‌شود و از زمان شروع به‌کار موتور، زمان بیشتری صرف می‌شود تا سرعت موتور به بازه مطلوب برسد؛ از طرفی با ثابت زمانی در نزدیکی 24.75s سیستم سریع‌تر شده و میزان نوسانات خروجی آن نیز بیشتر می‌شود؛ ثابت زمانی را به میزان 25s قرار داده و پارامترها به‌صورت زیر به‌دست می‌آید:

$$\frac{\omega(s)}{I_a(s)} = \frac{100}{(25s + 1)} \quad (6)$$

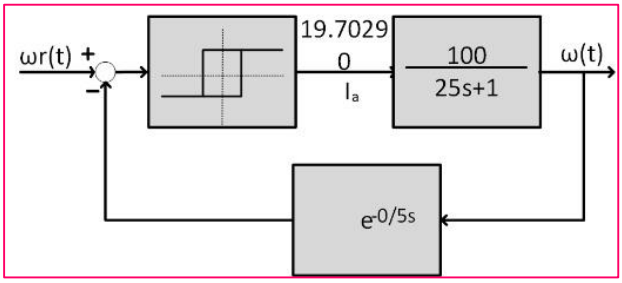
$$\tau = I/_{C_z} \rightarrow I = 2.5\ [\frac{kg}{m^2}]$$

$$C_1' = c_1 e^{\theta} \rightarrow C_1' = 980e^{\frac{0.5}{25}} \approx 999.8\ RPM$$

اختلاف میان رفرنس و حد پایین حوزه کنترل برابر با 0.2 می‌باشد، پس به میزان 0.2 از مقدار رفرنس، حد بالای کنترل-کننده است؛ داریم:

$$C_2' = 1000.2 = ak + (1020 - ak)e^{\frac{0.5}{25}}$$
$$\rightarrow 1000.2 - 1040 = -0.0202ak$$
$$\rightarrow ak = 1970.29$$
$$k = 100 \rightarrow a = 19.7029$$

a یا دامنه خروجی کنترل‌کننده به‌صورت فوق به‌دست آمد؛ با انتخاب‌هایی که صورت گرفته است، اگر ak کمتر یا بیشتر از این میزان شود، خروجی در بازه 980-1020RPM قرار نمی-گیرد و علت آن وجود ترم تاخیر در سنسور می‌باشد؛ اگر ترم تاخیر وجود نداشت، میزان ak فقط روی سرعت سیستم موثر بود و روی حوزه کنترل یا gap اثری نداشت.



شکل ۷: بلوک دیاگرام به‌دست آمده با کنترل‌کننده هیسترزیس

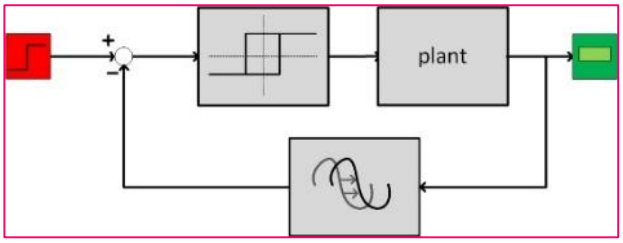
میزان نوسانات خروجی نیز به‌صورت زیر و با روابط ذکر شده در قسمت ۴-۱-۱ به‌دست می‌آید:

$$T_0 = T\ ln\frac{C_2}{C_1}.\frac{ak - C_1}{ak - C_2}$$
$$= 25\ln\frac{1020}{980}.\frac{1970.29 - 980}{1970.29 - 1020}$$
$$\approx 2.03\ s$$
$$f_0 = \frac{1}{T_0} \approx 0.4926\ Hz$$

اگر ثابت زمانی موتور بیشتر از مقدار 25s بود، فرکانس خروجی کمتر شده و به‌عبارت دیگر میزان قطع و وصل کردن کنترل‌کننده نیز کاهش می‌یابد و اگر کنترل‌کننده المان مکانیکی داشته باشد (مانند رله)، از این جهت مناسب است.

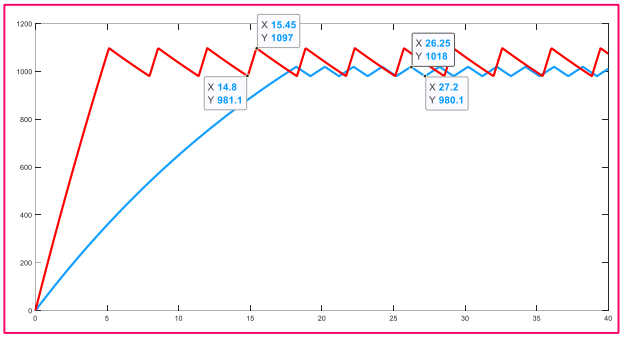
- شبیه‌سازی در MATLAB و مقایسه با روش تحلیلی

با استفاده از محیط سیمولینک نرم‌افزار MATLAB، سیستم حلقه‌بسته را رسم نموده و با تغییر پارامترها می‌توان اثر هر پارامتر را در خروجی مشاهده کرد. برای ایجاد تاخیر در قسمت فیدبک از بلوک Transport Delay استفاده می‌شود و بلوک Relay، کنترل‌کننده On-Off می‌باشد؛ به‌جای plant در تصویر ۶، از Transfer Function استفاده می‌شود و پارامترهای موتور DC تحریک مستقل در آن قرار می‌گیرد.



شکل ۸: سیستم حلقه‌بسته رسم شده در سیمولینک نرم‌افزار MATLAB

برای بررسی اثر ak یا حاصل ضرب مقدار DCgain موتور و ماکسیمم جریان ورودی به موتور (خروجی کنترل‌کننده در زمان on بودن)، دو حالت که در یک سیستم مقدار ak سه برابر مقدار ak در سیستم دیگر می‌باشد، رسم شده و از این طریق می‌توان خروجی دو سیستم را مورد بررسی قرار داد.



شکل ۹: خروجی دو سیستم حلقه‌بسته با ak متفاوت

همان‌طور که در شکل ۷ مشاهده می‌شود، با افزایش DC gain موتور یا افزایش دامنه جریان ورودی به موتور، زمان نشست کاهش، دوره تناوب خروجی افزایش، فرکانس خروجی کاهش و دامنه خروجی افزایش می‌یابد.

$$C_1' = c_1 e^{\theta}\ (3)$$

میزان حد پایین حوزه کنترل به ak بستگی ندارد ولی حد بالای حوزه کنترل با افزایش ak، افزایش می‌یابد.

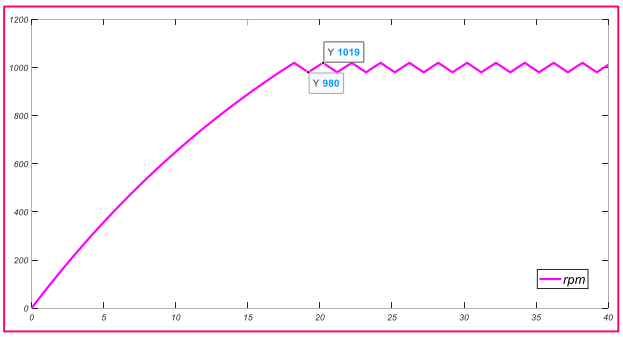
$$C_2' = ak + (c_2 - ak)e^{\theta}(2) \rightarrow C_2' = cte\ , ak \uparrow$$
$$\rightarrow\ c_2 \uparrow$$

اگر مقدار ثابت زمانی سیستم بزرگ‌تر شود، فرکانس خروجی کمتر می‌شود و برای ماندن خروجی در بازه 980-1020RPM میزان gap کنترل‌کننده به‌دست می‌آید.

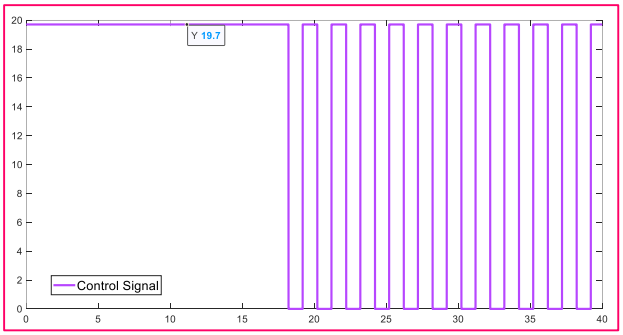
در تصویر (۹)، در شروع به‌کار سیستم، میزان خطا مثبت بوده و تا زمانی که خطا برابر با 0.2- شود، کنترل‌کننده On-Off روشن می‌ماند.

$$T_0 = 21.2 - 19.2 = 2\ s$$

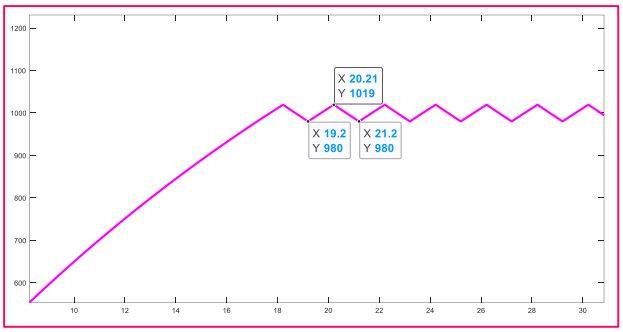
مقدار دوره تناوب 0.03 با مقدار محاسبه شده متفاوت بوده و دلیلش تقریب در محاسبات است؛ سیگنال خروجی کنترل-کننده به‌همراه خروجی سیستم حلقه‌بسته در یک تصویر رسم شده و علت کوچک بودن دامنه سیگنال کنترلی، مقدار DC gain موتور می‌باشد.



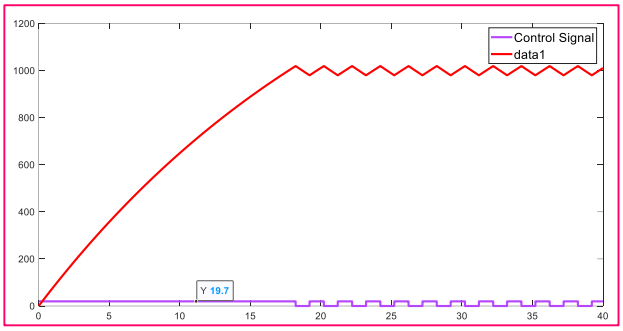
شکل ۱۰: سرعت خروجی سیستم حلقه‌بسته مطلوب



شکل ۱۱: سیگنال خروجی کنترل‌کننده On-Off



شکل ۱۲: دوره تناوب و مقدار gap خروجی



شکل ۱۳: سیگنال کنترلی به‌همراه خروجی سیستم حلقه‌بسته با k=100

۴. طراحی کنترل‌کننده PID

فرض می‌شود سنسور دارای تاخیر نیم‌ثانیه است و سپس به طراحی کنترل‌کننده P، PI و PID به چهار روش Z-N، IAE، ISE و ITAE پرداخته می‌شود [۳].

- تنظیم کنترل‌کننده

کنترل‌کننده باید به‌گونه‌ای طراحی شود تا خروجی از فرمان سیستم تبعیت کند (Tracking) و تنظیم خروجی علی‌رغم اختلالات با ورودی ثابت (Regulation) انجام شود [۳].

تابع معیار

برای اینکه بتوان سرعت (زمان) و تغییرات خطا (e) را بتوان با معیار خاصی سنجید و مقایسه کرد، تابعی به نام تابع معیار تعریف شده است.

$$\mathcal{J}(u) = \mathcal{J}(e,t) \quad (7)$$

تابع معیار بستگی به سیگنال کنترلی (u) دارد که سیگنال کنترلی نیز به تغییرات خطا (e) و سرعت یا زمان (t) دارد؛ پارامترهای کنترل‌کننده باید طوری تنظیم شوند که میزان به حداقل برسد.

$$\frac{\partial \mathcal{J}}{\partial K} = 0 \ , \qquad \frac{\partial \mathcal{J}}{\partial T_i} = 0 \ , \qquad \frac{\partial \mathcal{J}}{\partial T_d} = 0$$

معیارهای مختلفی تعریف شده است که چهار معیار مهم آن به‌صورت زیر تعریف می‌شود:

- **معیار انتگرال مجذور خطا یا ISE[۳]**

$$\mathcal{J} = \int_0^{\infty} e^2 . dt \quad (8)$$

[۳] Integral of square error

این معیار به خطاهای بزرگ حساسیت بیشتری نشان داده و بر خطاهای کوچک، اثر زیادی ندارد.

- **معیار انتگرال قدرمطلق خطا یا IAE[۴]**

$$\mathcal{J} = \int_0^\infty |e(t)|.dt \quad (9)$$

در این معیار، خطاهای مثبت و منفی از ارزش یکسانی برخوردار هستند.

- **معیار انتگرال قدرمطلق خطا در زمان یا ITAE[۵]**

$$\mathcal{J} = \int_0^\infty t|e(t)|.dt \quad (10)$$

این معیار به خطاهایی که مدت زیادی در سیستم باقی مانده‌اند، اهمیت بیشتری می‌دهد، ولی به خطاهای اولیه تاکید کم‌تری دارد (چون t کم است).

- **معیار Z-N[۶]**

در این معیار، خطا در هر پریود به نسبت یک چهارم ($\frac{1}{4}$) کم می‌شود. زیگلر و نیکولز عدد $\frac{1}{4}$ را از تجربیاتی که داشته‌اند، به‌دست آوردند. از این معیار در سیستم‌های سریع استفاده می‌شود. این محاسبات برای پروسس درجه یک توأم با تاخیر و برای کنترل‌کننده‌های مختلف در قسمت بعدی آمده است [۷].

جداول تنظیم کنترل‌کننده‌ها

در ابتدا فرض می‌شود که پلنت (G(s))، سیستم مرتبه اول تاخیردار است.

$$G(s) = \frac{k}{Ts+1}e^{-\tau s} \quad (11)$$

k مقدار بهره DC، مقدار T ثابت زمانی و **τ** نیز میزان تاخیر پلنت می‌باشد.

- **کنترل‌کننده P**

مقادیر a و b از جدول (۱) تعیین می‌شود.

$$C(s) = K = \frac{1}{k}a(\theta)^{-b} \quad (12)$$

جدول ۱: جدول تنظیم پارامترهای کنترل‌کننده P

	a	b
Z-N	1	1
IAE	0.9	0.98
ISE	1.4	0.92
ITAE	0.5	1.08

- **کنترل‌کننده PI**

مقادیر a، b، c و d از جدول (۲) تعیین می‌شود.

$$C(s) = K\left(1 + \frac{1}{T_i s}\right) \quad (13)$$

جدول ۲: جدول تنظیم پارامترهای کنترل‌کننده PI

	a	b	C	d
Z-N	0.9	1	3.32	1
IAE	0.98	0.98	1.65	0.71
ISE	1.3	0.96	2.03	0.74
ITAE	0.86	0.98	1.48	0.68

- **کنترل‌کننده PID**

مقادیر a، b، c، d، e و f از جدول (۳) تعیین می‌شود.

$$C(s) = K\left(1 + \frac{1}{T_i s} + T_d s\right) \quad (14)$$

جدول ۳: جدول تنظیم پارامترهای کنترل‌کننده PID

	a	b	c	d	e	f
Z-N	1.2	1	2	1	0.5	1
IAE	1.43	0.92	1.14	0.75	0.48	1.14
ISE	1.5	0.95	0.92	0.77	0.56	1
ITAE	1.46	0.95	1.18	0.74	0.48	1

حال در ادامه برای موتور DC تحریک مستقل ذکر شده، به ترتیب کنترل‌کننده‌های P، PI و PID را به چهار روش Z-N، IAE، ISE و ITAE کنترل‌کننده‌ها بدست آورده و تفاوت این چهار روش در هر نوع کنترل‌کننده بررسی می‌شود. تاخیر را در پلنت در نظر گرفته و پلنت به صورت سیستم مرتبه اول تاخیردار می‌شود.

$$G(s) = \frac{100}{25s+1}e^{-0.5s} \quad (15)$$

طراحی کنترل‌کننده P برای موتور DC تحریک مستقل

در این قسمت، هدف طراحی کنترل‌کننده P به چهار روش $Z-N$، IAE، ISE و ITAE می‌باشد. پارامتر $\theta = \frac{\tau}{T}$، پارامتر مهمی در پایداری سیستم‌ها می‌باشد و برای سیستم فوق، برابر با 0.02 است.

جدول ۴: طراحی کنترل‌کننده P

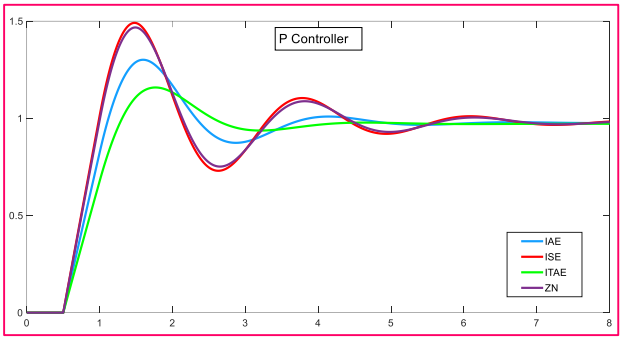
	ZN	IAE	ISE	ITAE
K	0.5	0.5119	0.3419	0.4146

[۴] Integral of absolute error

[۵] Integral time absolute error

[۶] Ziegler-Nichols

با قرار دادن مقادیر فوق در سیستم کنترلی، خروجی سیستم به‌صورت شکل ۱۲ می‌باشد.



شکل ۱۲: خروجی سیستم حلقه‌بسته با کنترل‌کننده P برای T=25

شکل ۱۲، پاسخ به ورودی پله واحد می‌باشد و می‌توان در سرعت رفرنس ضرب نمود و خروجی نیز در آن مقدار به تناسب ضرب می‌شود؛ اگر خروجی مد نظر، 1000 دور بر دقیقه باشد، کافی است تا پله ورودی در مقدار 1000 ضرب شود.

هرچه ثابت زمانی کوچک‌تر باشد، سیستم سریع‌تر است و زودتر به مقدار مطلوب می‌رسد.

نوع یا Typeسیستم حلقه‌باز برابر با صفر می‌باشد و در پاسخ به ورودی پله با استفاده از کنترل‌کننده P، میزانی خطای حالت ماندگار دارد. در این قسمت، خطای حالت ماندگار با روش ISE کمتر از بقیه روش‌های بررسی شده است و علت آن بزرگ بودن ضریب تناسبی این روش نسبت به بقیه روش‌ها می‌باشد. به‌علت وجود خطای حالت ماندگار، کنترل‌کننده نوع P، مناسب پلنت (موتور DC تحریک مستقل) نمی‌باشد.

همان‌طور که در نمودار فوق مشخص است، روش ISE سریع است ولی نوسانات زیادی دارد و علت آن زیاد بودن بهره کنترل‌کننده می‌باشد؛ منطقی است که روش ISE به خطاهای کوچک توجه زیادی نمی‌کند و این امر موجب نوسانات حول نقطه رفرنس می‌باشد.

در معیار ZN، بهره مقداری کوچک‌تر از روش ISE می‌باشد و نوسانات نیز تا حدی کم‌تر شده و خطا در هر پریود، $\frac{1}{4}$ می‌شود؛ در معیار IAE، خطاهای مثبت و منفی به‌صورت یکسان لحاظ می‌گردند؛ از این نظر، نوسانات سریع‌تر از روش ZN میرا می‌شود؛ در معیار ITAE، مقدار ثابت تناسبی، کمتر از بقیه است. به‌علت اثر زمان در این روش، خطا سریعا صفر می‌شود.

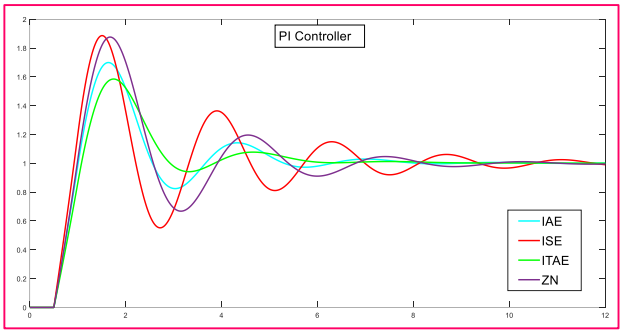
طراحی کنترل‌کننده PI برای موتور DC تحریک مستقل

در این قسمت، هدف طراحی کنترل‌کننده PI به چهار روش Z-N، IAE، ISE و ITAE می‌باشد [۶].

جدول ۵: طراحی کنترل‌کننده PI

	ZN	IAE	ISE	ITAE
K	0.45	0.4531	0.5558	0.3976
T_i	1.66	2.5654	2.8067	2.5876

با قرار دادن مقادیر فوق در سیستم کنترلی به ازای ورودی پله واحد، خروجی سیستم به‌صورت شکل ۱۳ می‌باشد.



شکل ۱۴: خروجی سیستم حلقه‌بسته با کنترل‌کننده PI برای T=25

طراحی با چنین کنترل‌کننده‌ای، مناسب‌تر از روش قبل می‌باشد و به علت افزودن یک قطب به سیستم (انتگرال‌گیر)، خطای حالت ماندگار به ورودی پله برابر با صفر می‌شود؛ از این جهت، می‌توان در مواردی که حالت گذرا مطرح نیست و فقط حالت ماندگار مطلوب می‌باشد، از این نوع کنترل‌کننده برای پلنت موردنظر استفاده شود. وجود یک قطب (انتگرال‌گیر)، موجب کند شدن سیستم نسبت به زمانی که انتگرال‌گیر وجود ندارد، می‌شود.

هرچه ثابت زمانی کوچک‌تر باشد، سیستم سریع‌تر است و زودتر به مقدار مطلوب می‌رسد. پارامتر ثابت زمانی، از مشخصات پلنت است و قابل تغییر نمی‌باشد؛ ثابت زمانی الکتروموتور DC تحریک مستقل، رابطه مستقیم با ممان اینرسی و رابطه عکس با ضریب ویسکوز دارد.

روش ISE سریع است ولی نوسانات زیادی دارد و علت آن زیاد بودن بهره کنترل‌کننده می‌باشد؛ منطقی است که روش ISE به خطاهای کوچک توجه زیادی نمی‌کند و این امر موجب نوسانات حول نقطه رفرنس می‌باشد؛ میزان T_i در روش ISE، بزرگ‌تر از بقیه روش‌ها بوده و سیستم را کند می‌کند.

در معیار ZN، بهره مقداری کوچک‌تر از روش ISE می‌باشد و نوسانات نیز تا حدی کمتر شده و خطا در هر پریود، $\frac{1}{4}$ می‌شود؛ از طرف دیگر، مقدار T_i در روش ZN کم‌تر از بقیه روش‌ها است و موجب افزایش سرعت سیستم می‌شود.

در معیار IAE، خطاهای مثبت و منفی به صورت یکسان لحاظ می‌گردند، از این نظر، نوسانات سریع‌تر از روش ZN میرا می‌شود.

در معیار ITAE، مقدار ثابت تناسبی، کم‌تر از بقیه است. به علت اثر زمان در این روش، خطا سریع‌تر از بقیه روش‌ها صفر می‌شود.

طراحی کنترل‌کننده PID برای موتور DC تحریک مستقل

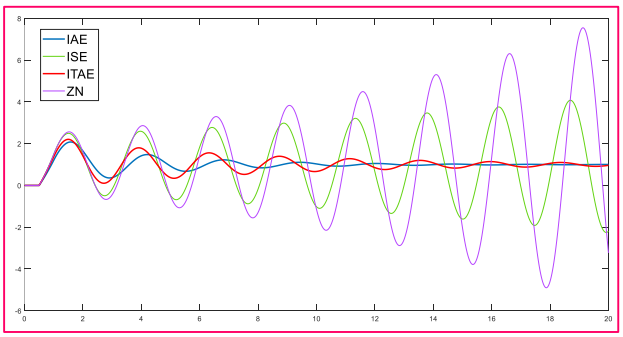
در این قسمت، هدف طراحی کنترل‌کننده PID به چهار روش Z-N، IAE، ISE و ITAE می‌باشد [۸].

جدول ۶: طراحی کنترل‌کننده PID

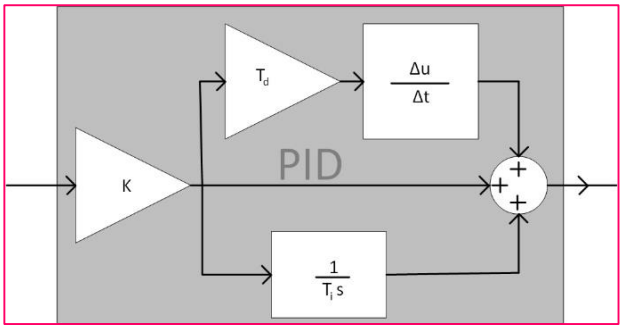
	ZN	IAE	ISE	ITAE
K	0.6	0.5229	0.6167	0.6003
T_i	1	1.5157	1.1311	1.6314
T_d	0.25	0.1388	0.28	0.24

ثابت زمانی این موتور نسبت به ثابت زمانی سیستم‌های الکتریکی، بالا است (T=25s). اگر با بلوک PID Controller در نرم‌افزار MATLAB قسمت سیمولینک پیش رفت، به علت وجود نویزگیر که در ساختار خود دارای یک قطب دور می‌باشد و اثری کمی در سیستم حلقه‌بسته می‌گذارد و احتمال پایداری سیستم را پایین می‌آورد.

اگر بلوک PID Controller نرم‌افزار MATLAB استفاده شود، با دو روش ISE و ZN خروجی ناپایدار می‌شود.

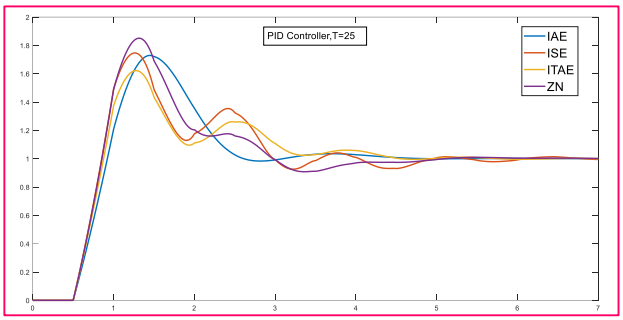


شکل ۱۵: خروجی سیستم با کنترل‌کننده PID (با استفاده از بلوک PID)



شکل ۱۶: ساخت بلوک PID با استفاده از بلوک‌های دیگر

سیستم مورد بررسی (کنترل سرعت موتور DC تحریک مستقل)، بدون اثر نویز و اغتشاش در نظر گرفته شده است و با استفاده از بلوک فوق، می‌توان اثر ناپایداری را برطرف نمود.



شکل ۱۷: خروجی سیستم با کنترل‌کننده PID (با بلوک PID اصلاح شده) برای T=25

خطای حالت ماندگار به ورودی پله، به‌علت وجود انتگرال‌گیر برابر با صفر است. افزودن مشتق‌گیر (صفر در مبداء) موجب افزایش حاشیه پایداری شده و سیستم را سریع‌تر از سیستم با کنترل‌کننده P و PI می‌کند؛ به بیان دیگر، مشتق‌گیر سیستمی است که به مقدار خطا توجهی ندارد و فقط به شیب خطا توجه می‌کند و باعث دمپ شدن نوسانات می‌شود.

روش ISE سریع‌تر است ولی نوسانات زیادی دارد و علت آن زیاد بودن بهره کنترل‌کننده می‌باشد؛ منطقی است که روش ISE به خطاهای کوچک توجه زیادی نمی‌کند و این امر موجب نوسانات حول نقطه رفرنس می‌باشد. میزان T_d در روش ISE، بزرگ‌تر از بقیه روش‌ها می‌باشد و باعث افزایش سرعت سیستم، بهبود حالت گذرا و دمپ نوسانات می‌شود.

در معیار ZN، بهره مقداری کوچک‌تر از روش ISE می‌باشد و نوسانات نیز تا حدی کم‌تر شده و خطا در هر تناوب، $\frac{1}{4}$ می‌شود؛ مقدار T_i در روش ZN کم‌تر از بقیه روش‌ها است و موجب افزایش سرعت سیستم می‌شود.

در معیار IAE، خطاهای مثبت و منفی به صورت یکسان لحاظ می‌گردند، از این نظر، نوسانات سریع‌تر از روش ZN میرا می‌شود.

در معیار ITAE، مقدار ثابت تناسبی، کم‌تر از بقیه است. به علت اثر زمان در این روش، خطا سریعا صفر می‌شود.

کنترل‌کننده مطلوب، نمی‌تواند کنترل‌کننده P باشد؛ زیرا این نوع کنترل‌کننده دارای خطای ماندگار است و سرعت خروجی آن به میزان رفرنس نمی‌رسد.

اگر طراحی از نظر زمان نشست مورد بررسی باشد، سیستم PI مناسب نیست و کند شدن سیستم به علت وجود پارامتر انتگرال‌گیر می‌باشد. این اثر در کنترل‌کننده PID به علت وجود پارامتر مشتق‌گیر برطرف می‌شود و سرعت سیستم افزایش می-یابد.

میزان فراجهش یا overshoot از جهتی مناسب است، زیرا که ورودی پلنت، جریان است و جریان رابطه مستقیمی با گشتاور دارد. در لحظه راه‌اندازی، شفت موتور در حالت ساکن است و نیاز به گشتاور بالا برای راه‌اندازی دارد؛ در نتیجه، overshoot باعث راحت‌تر به راه افتادن موتور می‌شود. گشتاور سریع در زمان راه‌اندازی می‌تواند به قسمت‌های متحرک موتور آسیب وارد کند. البته باید در نظر داشت که افزایش جریان از یه حدی به بعد، موجب آسیب رسیدن به آرمیچر موتور، از بین رفتن عایق برا اثر گرما و موارد دیگری در الکتروموتور DC شود.

۵. مراجع

[1] Principles of Electric Machines and Power Electronics. Seprate excitation DC Motor.

[۲] کتاب کنترل صنعتی نوشته احمد طهماسبی

[۳] کتاب سیستم‌های کنترل خطی نوشته اوگاتا

[4] Astrom,K.J., and Hagglund, T. PID Controllers: Theory, Design and Tuning, Instrument Society of America, Research Triangle Park, NC, 1995.

[5] J. Nagrath, M.Gopal, “Control System Engineering”, New Age International Publications, 3rd Edition, 2002.

[6] M. L. Ruz, F. Morilla AND F. Vazquez, “Teaching Control with first order time delay model and pi controllers”, IFAC, 2009.

[7] J. Ziegler and N. Nichols, “Optimum settings for automatic controllers”, Transactions of the ASME, vol. 64,pp. 759-768, 1942.

[8] K.J.Astrom, I.Hagglund, “Revisiting the Ziegler-Nichols step response methid for PID control”, Journal of Process Control 14 (2004)634-650.

Li-Fi فناوری مبتنی بر LED

مریم فریور[۱]

مهران کریمیان ریزی[۲]

[۱] کارشناسی ارشد، مهندسی برق-الکترونیک، سازمان آموزش فنی و حرفه‌ای، farivar.maryam@yahoo.com

[۲] کارشناسی ارشد، مهندسی پزشکی، دانشگاه تبریز، ایران، mehrankarimian97@ms.tabrizu.ac.ir

چکیده: تقاضا بطور چشمگیری برای استفاده از اینترنت در حال رشد است. تکنولوژی آنقدر پیشرفت کرده است که ما برای همه کارها ای اینترنت استفاده می‌کنیم . در این میان امنیت، پهنای باند مناسب، سرعت کافی و در دسترس بودن و هزینه مناسب در استفاده از اینترنت برای ما اهمیت به سزایی دارد. . این باور وجود دارد که ***Li-Fi*** نسل بعدی اینترنت باشد، جایی که از نور به عنوان وسیله‌ای برای انتقال داده استفاده می‌شود.

کلید واژه‌ها: *Li-Fi* ، *LED*، اینترنت پرسرعا

۱ . مقدمه

با رونق تلفن‌های هوشمند، اینترنت اشیاء(IOT)، اتوماسیون‌های صنعتی، سیستم‌های خانه هوشمند و... تقاضا برای اینترنت نیز به طور چشمگیری در حال رشد است. تکنولوژی آنقدر پی شرفت کرده ا ست که ما برای همه چیز از اتومبیل گرفته تا یخچال و فریزر، به اتصال به اینترنت نیاز داریم. اما این مسئله سوالات دیگری ایجاد می‌کند مانند اینکه: آیا پهنای باند کافی برای همه این دستگاه‌ها وجود دارد؟ آیا این داده‌ها ایمن خواهند بود؟ آیا سیستم موجود برای همه این داده‌ها به اندازه کافی سریع خواهد بود؟ آیا ارتباط زیادی در ترافیک شبکه وجود خواهد داشت؟

تمام این سوالات توسط این تکنولوژی که Li-Fi نام دارد حل خواهد شد. اصطلاح Li-Fi مخفف "Light Fidelity" است. این باور وجود دارد که این وسیله نسل بعدی اینترنت باشد، جایی که از نور به عنوان وسیله‌ای برای انتقال داده استفاده می‌شود. این همان نوری است که شما در خانه‌ها و دفاتر خود ا ستفاده می‌کنید و با کمی تغییرات می تواند داده‌ها را به تمام دستگاه‌های شما که به اینترنت نیاز دارند منتقل کند.

۲. دلایل نیاز به تغییر تکنولوژی

ما از ابتدا از اینترنت RF برای انتقال داده‌ها از یک انتها به سر دیگر به صورت بی‌سیم استفاده کرده‌ایم. محیط RF از امواج رادیویی استفاده می‌کند، داده‌هایی که منتقل می‌شوند در این امواج مدوله شده و سپس در سمت گیرنده تغییر شکل می‌دهند. ما با انتقال چند کیلو بایت داده در هر ثانیه شروع کردیم و پیشرفتی که تاکنون داشته‌ایم نشان می دهد امروزه میانگین

سرعت جهانی اینترنت در حدود ۷,۲ مگابایت در ثانیه است، که برای اکثر ما کافی است. اما، تکنولوژی با استفاده از یک محیط RF برای انتقال داده‌ها از اشکالات بسیاری رنج می‌برد:

- تقاضای زیادی برای اینترنت وجود دارد که با روشی که در حال حاضر وجود دارد نمی‌تواند تأمین شود، که منجر به اثری به نام Spectrum crunch (اختلال در طیف) می‌شود.
- از آنجا که سرعت شبکه بالایی مورد نیاز است، تقاضا برای پهنای باند بالا وجود دارد.
- استفاده از بستر RF برای بیمارستان‌ها، نیروگاه‌ها، هواپیماها و... بی‌خطر نیست. و همچنین این مکان‌ها برای دوره جدید به اتصال به اینترنت نیاز دارند.
- فرکانس رادیویی ایمن نیست، زیرا داده‌های شما می‌توانند از طریق دیوارها خارج شوند و نمی‌توانند در یک منطقه خاص قرار بگیرند.

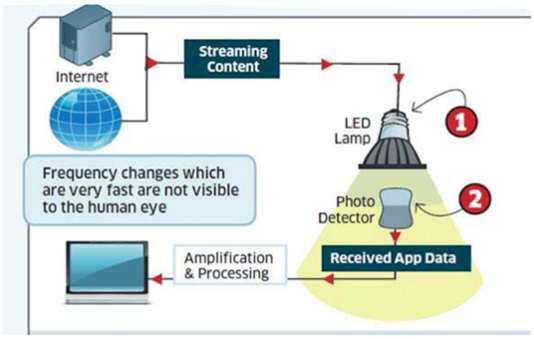
همه این اشکالات نیاز به یک فناوری جدید دارد، این فناوری جدید Li-Fi نامیده می‌شود.

آیا می‌دانید امروزه بیشترین استفاده از اینترنت بی‌سیم(Wi-Fi)به طور تصادفی توسط دکتر جان اوسالیوان اختراع شده است. او در واقع سعی داشت انفجار حفره‌های سیاه کوچک را آزمایش کند، اما منجر به اختراع Wi-Fi در سال ۱۹۹۱ شد که اکنون به ۶۰٪ از ترافیک اینترنت جهانی کمک می‌کند.

۳. نحوه کار Li-Fi

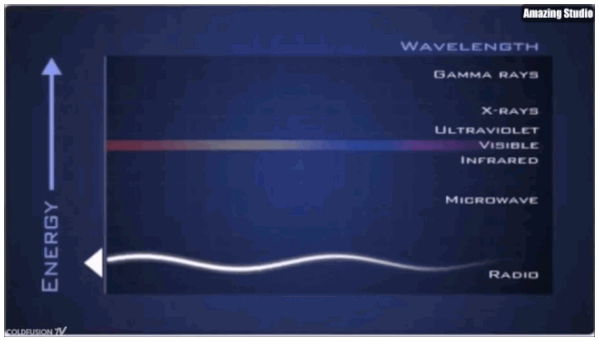
همان‌طور که قبلاً گفته شد Li-Fi برخلاف امواج رادیویی از نور برای انتقال داده استفاده می‌کند. این ایده اولین بار توسط پروفسور هارالد هاس در یکی از سخنرانی‌های TED خود در سال ۲۰۱۱ مطرح شد. تعریف Li-Fi را می‌توان به این صورت ارائه داد: Li-Fiیک شبکه دو طرفه با سرعت بالا و ارتباطات سیار داده با استفاده از نور است.Li-Fi تشکیل شده از چندین لامپ است که یک شبکه بی‌سیم را تشکیل می‌دهد، تجربه‌ای مشابه Wi-Fi را با استفاده از طیف نور ارائه می‌دهد.

پس هر کجا که یک لامپ داشته باشید به اینترنت متصل خواهید شد اما در اینجا، اصطلاح لامپ به چراغ‌های رشته‌ای معمولی در خانه ما اشاره نمی‌کند، این‌ها چراغ‌های LED اصلاح شده خاصی هستند که می‌توانند داده‌ها را انتقال دهند. همانطور که می‌دانیم LED یک دستگاه نیمه‌هادی است و مانند تمام نیمه‌هادی‌ها دارای ویژگی سوئیچینگ است. از این ویژگی سوئیچینگ برای انتقال داده استفاده می‌شود. در تصویر زیر نحوه انتقال داده با استفاده از نور توضیح داده شده است.

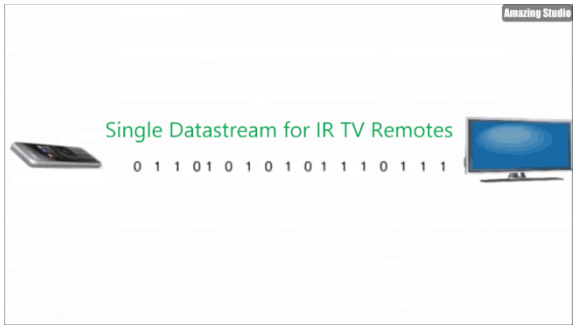


شکل ۱

هر لامپ LED باید از طریق یک درایور LED تغذیه شود، این درایور LED اطلاعات را از سرور اینترنت دریافت می‌کند و داده‌ها در درایور رمزگذاری می‌شوند. بر اساس این داده‌های رمزگذاری شده، لامپ LED با سرعتی بسیار زیاد چشمک می‌زند که چشم انسان متوجه آن نمی‌شود. اما آشکارساز تصویری در طرف دیگر قادر به خواندن همه سوسو زدن‌ها خواهد بود و این داده‌ها پس از تقویت و پردازش رمزگشایی می‌شوند. انتقال اطلاعات در اینجا بسیار سریعتر از RF خواهد بود. همانطور که همه ما می‌دانیم نور سریعتر از هوا حرکت می‌کند، یعنی نور ده هزار برابر سریعتر از امواج رادیویی است زیرا فرکانس امواج رادیویی فقط ۳۰۰ گیگاهرتز است اما نور می تواند تا ۷۹۰ ترا هرتز افزایش یابد.



شکل۲



شکل ۳

محققان دانشگاه آکسفورد محدودیت‌های Li-Fi را برای کار با سرعت چشمگیر ۲۲۴Gbps آزمایش و تحت فشار قرار داده‌اند. برای اینکه ایده‌ای از سرعت این دستگاه به شما بدهیم بدانید که این سرعت برای بارگیری ۱۰ فیلم با وضوح بالا در یک ثانیه کافی است.

شاید تکنولوژی انتقال داده از طریق نور جدید به نظر برسد اما مدت‌هاست که از آن استفاده می‌کنیم.

انتقال داده از طریق دیودهای تصویری برای مدتی طولانی از طریق ریموت‌های IR ما اتفاق می‌افتد. هر بار که دکمه ای از ریموت کنترل تلویزیون خود را فشار می‌دهیم، IR LED در پالس‌های ریموت کنترل بسیار سریع توسط تلویزیون دریافت می‌شود و سپس برای اطلاعات رمزگشایی می‌شود. اما، این روش قدیمی بسیار کند است و نمی توان از آن برای انتقال داده‌ها استفاده کرد. بنابراین Li-Fi این روش با استفاده از بیش از یک LED و عبور بیش از یک جریان داده در یک زمان مشخص ساخته می‌شود. از این طریق می توان اطلاعات بیشتری را منتقل کرد و از این رو ارتباط سریعتر داده امکان پذیر است.

میزان مصرف جهانی اینترنت به طور صعودی در حال افزایش است و میزان داده‌های مصرف شده در سال ۲۰۱۶ بیشتر از کل داده‌های مصرفی از زمانی است که اینترنت به وجود آمده است. همچنین تخمین زده می‌شود که تا پایان سال ۲۰۱۸ بیست میلیارد دستگاه متصل به اینترنت وجود داشته باشد، در حالی که جمعیت جهان فقط ۷,۶ میلیارد نفر است.

۴. نتیجه‌گیری

مفهوم Li-Fi صرفا یک مفهوم نظری نیست، در واقع وقتی پروفسور هارالد هاس (بنیانگذار Li-Fi)، مفهوم Li-Fi را در یک ویدیوی TED معرفی کرد، وی با پخش یک فیلم HD زنده به نمایش عملی این تکنولوژی برای مخاطب پرداخت و باعث شد که آن‌ها از این تکنولوژی متحیر شوند. از آن زمان، بسیاری از افراد با استعداد شروع به کمک و بهبود مفهوم Li-Fi کردند. امروزه کمپانی‌هایی مانند Pure Li-Fi وجود دارند که آماده ارائه خدمات Li-Fi برای خانه یا دفتر کار شما از طریق دانگل Li-Fiخود هستند که می‌تواند به USB لپ تاپ شما متصل شده و داده‌ها را از هر چراغ فعال شده با Li-Fi بخواند. بنابراین ما از چراغ مطالعه خود نه تنها برای روشن کردن میز کار بلکه برای ارائه اتصال به اینترنت فاصله زیادی نداریم.

۵. مراجع

۱- فناوری Li-Fi: معرفی، کاربردها، چالش‌ها و ارزیابی امنیتی، سامان کشوری و مصطفی عباسی، نشریع علمی پدافند غیرعامل، سال یازدهم، شماره ۲، تابستان ۱۳۹۹

۲- فناوری Li-Fi و نقش آن در اینترنت اشیا IOT، الناز رسولی نیک و مرضیه حسنی، هشتمین کنفرانس بین المللی راهکارهای نوین در مهندسی، علوم اطلاعات و فناوری در قرن پیش رو، ۱۴۰۰

تحلیل و طراحی و مدلسازی دوبعدی ترانزیستور تونلی شاتکی با دی‌الکتریک TiO_2

پریسا سروی[۱] parisa.sarvi71@gmail.com
حامد امین زاده[۲] hamedmr1@yahoo.com
جواد جوادی مقدم[۳] javadi5599@yahoo.com
[۱]دانشجوی کارشناسی ارشد/ دانشکده مهندسی برق و الکترونیک، دانشگاه پیام نور مرکز تهران شمال، تهران، ایران
[۲]دانشیار/ دانشکده مهندسی برق و الکترونیک، دانشگاه پیام نور مرکز تهران شمال، تهران، ایران
[۳]استادیار/ دانشکده مهندسی برق و الکترونیک، دانشگاه پیام نور مرکز تهران شمال، تهران، ایران

چکیده: در این مقاله طراحی و تحلیل و مدل سازی ترانزیستور تونلی شاتکی با استفاده از TiO_2 برای دی الکتریک گیت انجام شده است. وجود یک تونلینگ شاتکی در رابط کانال سورس و جریان درین به دلیل تونل سازی پیشرفته از یک باند شارژ به باند دیگر در ناحیه رابط تقاطع ها باعث بهبود قابل توجه ترانزیستور میشود. با این کار هدایت و در نتیجه میزان تونل زنی افزایش میابد. در نهایت باعث افزایش کارایی ترانزیستور میشود. مدل مورد استفاده در طراحی ترانزیستور بر مبنای پتانسیل سطح در امتداد کانال با استفاده از معادله پواسون دو بعدی با شرایط مرزی مناسب طراحی کوتاهترین فاصله بین سورس / کانال و جریان سورس درین استوار میباشد. با توجه به افزایش میزان تونل زنی، که این امر موجب کاهش جریان میشود، ترانزیستور پیشنهادی مدلی برای مکمل های فلزی اکسیدهای نیمه هادی و (CMOS) است. که شبیه ساز این مدل را با سیلواکو انجام دادیم.

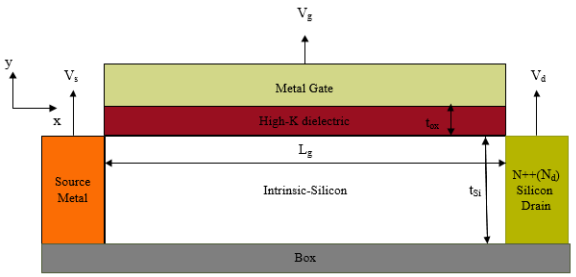
کلید واژه‌ها: *ترانزیستور، تونل، جریان، دی الکتریک، سیلواکو.*

۱. مقدمه

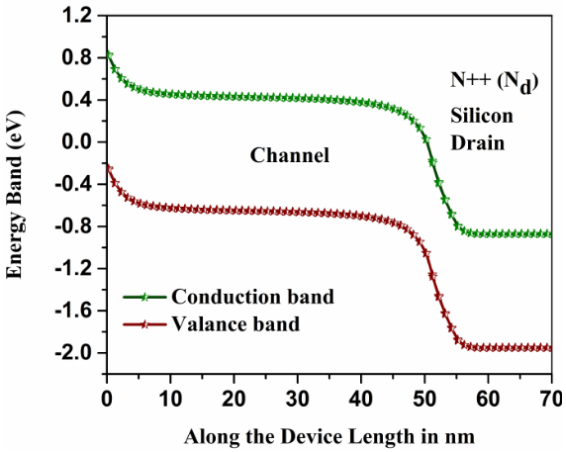
کاهش اندازه گیری CMOS (مکمل ترانزیستورهای ماده اکسید) با محدوده زیر ۱۰۰ نانومتر، MOSFET های معمولی مشکلات متعددی مانند جریان های نشتی حالت خاموش، شیب زیراستانه بالا و چندین اثر کانال کوتاه (SCE) را نشان میدهد. این مشکلات نشان دهنده قدرت پیشرفته ای در مقیاس بندی ولتاژ سورس تغذیه میباشد. بنابراین، برای حل این مشکلات غیر معمول MOSFET ها، SB FET ها به طور گسترده برنامه ریزی شده است [۴-۱]. در SB FET مزایای اساسی مانند محافظت از اثرات کانال کوتاه، طول تا ابعاد زیر 10 نانومتر و کاهش مقاومت سورس درین را نشان میدهند [۵،۶]. با این حال، SB FET ها از دو حالت استفاده میکنند، که شامل کاهش جریان در حالت ON و افزایش جریان در حالت OFF میباشد [۹-۷]. بنابراین،برای بهبود جریان در حالت ON و همچنین کاهش جریان در حالت OFF در SB FET، تحقیقات زیادی انجام شده است [۱۰]. طبق تحقیقات [۱۳-۱۱] که در ان برای کاهش جریان در حالت OFF، از یک باند نازک Si_3N_4 بین کانال سورس و کانال درین استفاده میشود. علاوه بر این، با گسترش بین رابط کانال درین میتوانیم به طراحی نامتقارن کانال های سورس/درین بپردازیم. اما هیچ یک از این تحقیقات فوق برای طراحی SB FET بهینه نیستند. این روش ها عمدتا مشکل ساخت را افزایش میدهند و برای ساخت ترانزیستور در مقیاس نانومتر دشوار هستند. FET های تونل زنی شاتکی در

SBT FET موجب افزایش جریان و افزایش نسبت سوییچینگ I_{ON}/I_{OFF} میشود. از این رو، یک مدل تحلیلی مبتنی بر پتانسیل سطحی ماده جدید برای تونل زنی شاتکی دو گیتی SBT FET ارائه شده است. با تغییر ماده سورس در منطقه تونل سازی، موجب میدان الکتریکی بالاتری در منطقه اتصال شاتکی شده و جریان درین را افزایش می دهد. در اینجا، یک مدل ریاضی جدید برای ماده دو گیتی SB FET مطرح شده است. از طرفی، سیلیکون به عنوان ماده سورس و درین انتخاب شده است. معادلات ریاضی دوبعدی برای پتانسیل سطحی دو گیتی SB FET سیلیکونی با طول کانال دقیق با استفاده از معادله پواسون بررسی میشود. علاوه بر این، مدل ریاضی به وسیله نتایج شبیه سازی سیلواکو تایید میشود [۱۴].

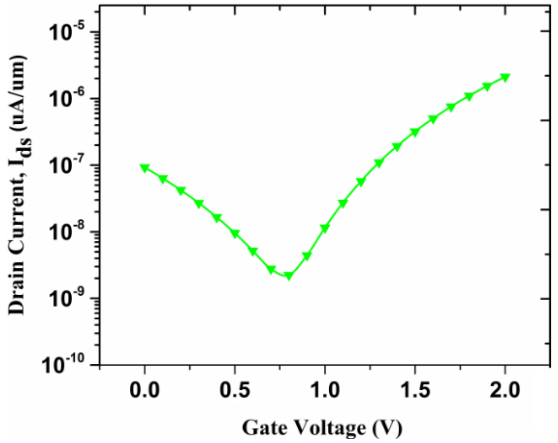
نمای شماتیک دو بعدی تونلی زنی شاتکی SBT FET با استفاده از ماده TIO_2 به عنوان ماده دی الکتریک در شکل ۱ با مشخصات مطرح شده مدل سازی و شبیه سازی میشود: NiSi به عنوان سورس با مقدار SBH=0.65ev میباشد، دوپینگ کانال $10^{16}cm^3$ میباشد، دوپینگ درین سیلیکون $N_d=10^{19}cm^3$ میباشد، ضخامت اکسید $t_{ox}=2nm$ میباشد، ضخامت سیلیکون $t_{si}=10nm$ میباشد، طول گیت $L_g=50nm$که $\phi_{m1}=4ev$ و $\phi_{m2}=5.1ev$ میباشد و طول سورس و درین 20nm میباشد. با کاهش جریان حالتOFF ، مقدار دوپینگ سمت درین کاهش میابد. و همچنین افزایش کانال در حالت Ion موجب کاهش مقاومت میشود. همچنین، موجب عدم تطابق در فرایند ساخت تونل کوتاه کانالFET میشود. در ناحیه درین، با مقدار سیلیکون +N دوپینگ میابد، منطقه تونل زنی را کاهش میدهد. در این جا V_{gs} بایاس گیت سورس و V_{ds} بایاس درین سورس میباشد. در شبیه سازی مقدار الکترون های باند انرژی و حفره های باند انرژی SBT FET برای منطقه حالت ON با توابع ماده گیت در شکل۲ نشان داده شده است. ارتفاع گیت و عرض تونل زنی باعث افزایش حاملها در ناحیه تماس تماس کانال سورس موجب افزایش جریان حالت ON میشود. همچنین، از NiSi برای تشکیل سورس استفاده میشود که دارای مقادیرSBH=0.61-0.67ev میباشد. شکل ۳ کاهش اساسی مدل باند به باند حامل های تونل زنی SB FET را توسط تحقیقات R.Javaheri و V.Nagavarapu و همکاران بیان میکند [۱۵]. ویژگی های الکتریکی از داده های استخراج شده از مدل مرجع با ابعاد دقیق اندازه گیری شده [۱۵] و ساختار SBT FETبا دی الکتریک TiO_2 در شکل ۳ مشاهده میشود. مدل باند به باند محلی، تونل زنی الکترون ها و حفره ها دقیق هستند و با داده های ساختاری برای تعیین کالیبراسیون برابر هستند. که مقادیر $m_e=0.27m0$ و $m_h=0.555m0$ میباشد. شکل ۳ برای جریان درین SBT FET پیشرفته را در حالت شبیه سازی و داده های تحقیقاتی نشان میدهد [۱۵]. واضح است که خروجی های شبیه سازی شده و خروجی های تحقیقاتی برای مدل SBT FET [۱۵]تقریبا مشابه هستند، بنابراین این شبیه سازی معتبر میباشد. مشاهده میشود که SBT FETبا ساختار دی الکتریک TiO_2 کارایی قابل توجهی (در هر دو حالت ON و OFF) نسبت به معادل SBT FETمعمولی خود به دلیل مزایای حاصل از مفاهیم مهندسی ماده سورس را نشان میدهد. بنابراین مکانیزم تونل زنی با افزایش جریان تونل، برای کاربرد های VLSI کم مصرف با ایمنی کانال کوتاه پیشرفته مناسب تر است.



شکل ۱: نمای شماتیک دو بعدی گیت دو فلزی شاتکی تونل زنی FET (SBT) با استفاده از دو گیت فلزی TiO_2 به عنوان دی الکتریک گیت



شکل ۲: نمودار باند انرژی SBT FET در حالت روشن با دی الکتریک TiO_2



شکل ۳: مقدار I_{ds}-V_{gs} شبیه سازی TiO_2

مدلسازی تحلیلی توزیع پتانسیل

تابع کار SBT FET با استفاده از دو نوع گیت ϕ_{M1}و ϕ_{M2} برای ترانزیستور فوق مدل سازی شده است، که $\phi_{M1}<\phi_{M2}$، و اثرات کانال کوتاه و بهره وری الکترون را بازیابی میکند [۱۶،۱۷]. ابعاد ترانزیستور در شکل ۱ نشان داده شده است. SBT FET دوبعدی با استفاده از شبیه ساز Silvaco نشان داده شده است [۱۱]. دوپینگ یکنواخت در ناحیه اکسید گیت و سیلیکون به عنوان کانال در باياس پایین شبیه سازی شده است. از اینرو معادلات پواسون به شکل زیر تعریف میشوند:

$$\frac{\partial^2\varphi(x,y)}{\partial x^2}+\frac{\partial^2\varphi(x,y)}{\partial y^2}=\frac{qN^a}{\varepsilon_{Si}} \qquad (۱)$$

که N_a دوپینگ پذیرنده در منطقه سیلیکون و q بار الکترون است. جهت y-جهت پتانسیل سطحی است که تابع سهموی میباشد [۱۳].

(۲)

$$U_{11}(x)y+\varphi_{S1}(x)+U_{12}(x)y^2=\varphi_1(x,y)\ for\ 0\le y\le t_{Si},0\le x\le L_1$$

(۳)

$$U_{21}(x)y+\varphi_{S2}(x)+U_{22}(x)y^2=\varphi_2(x,y)\ for\ 0\le y\le t_{Si},0\le x\le L_1+L_2$$

ثابتهای U_{21} (x)، U_{12} (x)، U_{21} (x) و U_{22} (x) U_{11} (x) توابعی از X هستند که با اعمال شرایط مرزی محاسبه میشوند.

(i) پتانسیل در مرز کانال سورس سیلیکونی:

$$\varphi_1(0,0)=\varphi_{S1}(0)=V_{bi,S/D} \qquad (۴)$$

پتانسیل سطحی در مرز کانال سورس درین سیلیکونی:

$$\varphi_1(L_1+L_2,0)=\varphi_2(L_1+L_2)=V_{bi,S/D}+V_{DS} \qquad (۵)$$

$\Delta\phi_{bS}$ ماده نیمه هادی است که سورس را کاهش می دهد [۹] V_{bi}، پتانسیل داخلی در نزدیکی S / D است.

$$\Delta\varnothing_{bS}=K\left[\frac{lq}{4\pi\varepsilon_S}\right]^{\frac{1}{2}}E_{Source}^{\frac{1}{2}}$$

$$V_{bi,S/D}=X+\frac{E_g}{2}+\varnothing_F-\varnothing_{S/D}$$

E_{Source} میدان الکتریکی نزدیک سورس جانبی است که ϕ_F = V_T ln (Na / ni) پتانسیل فرمی در لایه سیلیکون با مقادیر κ = 1 و ℓ = 1.5 است.

در محل اتصال ماده گیت TiO_2 میدان الکتریکی ثابت است. که در این حالت شرایط مرزی زیر را به دست میاوریم [۱۸].

$$\frac{d\varphi_1(x,y)}{dy}|_{y=0}=\frac{\varepsilon_{OX}}{\varepsilon_{Si}}\frac{V_{FB1}+\varphi_1(x,y)|_{y=0}-V_{GS}}{t_{ox,f}} \qquad (۶)$$

$$=\frac{d\varphi_2(x,y)}{dy}|_{y=0}=\frac{\varepsilon_{OX}}{\varepsilon_{Si}}\frac{V_{FB2}+\varphi_2(x,y)|_{y=0}-V_{GS}}{t_{ox,f}} \qquad (۷)$$

ε_{ox}و ε_{si} مقادیر مجاز سیلیکون هستند، V_{FB1} ولتاژ باند سطح کانال ماده ۱، V_{FB2} ولتاژ باند کانال مسطح ماده۲، t_{ox} اکسید گیت و V_{gs} ولتاژ گیت سورس است.

(d) میدان الکتریکی نزدیک محل اتصال کانال پشتی و اکسید تحتانی است:

$$\frac{d\varphi_1(x,y)}{dy}|_{y=t_{Si}}=\frac{\varepsilon_{OX}}{\varepsilon_{Si}}\frac{V_{SUB}-V_{FB,b}-\varphi_B(x)}{t_{box,b}} \qquad (۸)$$

$$\frac{d\varphi_2(x,y)}{dy}|_{y=t_{Si}} = \frac{\varepsilon_{OX}}{\varepsilon_{Si}} \frac{-V_{FB,b} - \varphi_B(x) + V_{SUB}}{t_{box,b}} \quad (۹)$$

V_{FB}، ولتاژ باند سطح کانال است، $\varphi_B(x)$ پتانسیل در سراسر کانال پشتی و اکسید تحتانی، V_{SUB} ولتاژ بستر است، t_{si} ضخامت لایه سیلیکون و t_{box} ضخامت اکسید تحتانی است.

(e) پتانسیل سطحی در کانال ثابت است. ما ممکن است شرایط مرزی زیر را در دو ماده متفاوت به دست اوریم.

$$\varphi_1(L_1,0) = \varphi_2(L_1,0) \quad (۱۰)$$

(f) میدان الکتریکی در محل اتصال دو ماده متمایز ثابت است.

$$\frac{d\varphi_1(x,y)}{dx}|_{x=L_1} = \frac{d\varphi_2(x,y)}{dx}|_{x=L_1} \quad (۱۱)$$

با حل معادلات ریاضی از (۶ تا ۹) میتوانیم مقادیر U11(x) ، U12 (x)، U21(x) و U22(x) را بدست می‌اوریم. سپس با گذاشتن این مقادیر در عبارات برای φ1(x , y) ، و y = 0، میتوانیم عبارات زیر را به دست اوریم:

$$\frac{d^2\varphi_{S1}}{dx^2} - \alpha\varphi_{S1}(x) = \beta_1 \; and \; \frac{d^2\varphi_{S2}}{dx^2} - \alpha\varphi_{S2}(x) = \beta_2 \quad (۱۲)$$

$$\alpha = \frac{C_{ox,f}C_{Si} + C_{ox,f}C_b + C_bC_{Si}}{t^2_{Si}C_{Si}(2C_{Si} + C_b)} \quad (۱۳)$$

(۱۴)

$$\beta_1 = \frac{qN_a}{\varepsilon_{Si}} - 2(V_{GS} - V_{FB1,f})\left(\frac{C_{ox,f}(C_{Si}+C_b)}{t^2_{Si}C_{Si}(2C_{Si}+C_b)}\right) - 2(V_{SUB} - V_{FB,b})\frac{C_b}{t^2_{Si}C_{Si}(2C_{Si}+C_b)}$$

(۱۵)

$$\beta_2 = \frac{qN_a}{\varepsilon_{Si}} - 2(V_{GS} - V_{FB2,f})\left(\frac{C_{ox,f}(C_{Si}+C_b)}{t^2_{Si}C_{Si}(2C_{Si}+C_b)}\right) - 2(V_{SUB} - V_{FB,b})\frac{C_b}{t^2_{Si}C_{Si}(2C_{Si}+C_b)}$$

جایی که CSi ظرفیت خازن لایه سیلیکون، Cox اکسید گیت و Cb اکسید تحتانی هستند.

$C_{si}=t_{si}$, $C_{oxf}=t_{ox}$. $C_b=t_{box,b}$

راه حل معادله (۱۲) باید در شرایط مرزی صدق کند.

$$\varnothing_{01}(0) = V_{bi,\frac{S}{D}} - \Delta\varphi_{bS} \; and \; \vartheta_{02}(L_1+L_2) = V_{bi,\frac{S}{D}} + V_{DS}$$

معادله دیفرانسیل ناهمگن با ضریب ثابت راه حل بعدی را توضیح میدهد.

(۱۶)

$$\varnothing_{S1}(x) = H_1\exp(\gamma x) + H_2\exp(-\gamma x) - \mu_1$$

(۱۷)

$$\vartheta_{S2}(x) = H_3\exp(\gamma(x-L_1)) + H_4\exp(-\gamma(x-L_1)) - \mu_2$$

با استفاده از شرایط مرزی (۴)، (۵)، (۱۰) و (۱۱) مقادیر H_1، H_2، H_3 و H_4 به دست میاید:

$$H_1 = \frac{(V_{bi} + V_{DS} - \mu_2) + \alpha_{11} - (V_{bi} - \mu_2 - \Delta\varphi_{bS})e^{-\gamma(L_1+L_2)}}{e^{\gamma(L_1+L_2)}\left(1 - e^{-2\gamma(L_1+L_2)}\right)} \quad (۱۸)$$

$$H_2 = \frac{(V_{bi} + V_{DS} - \mu_2) - (V_{bi} - \mu_1 - \Delta\varphi_{bS})e^{-\gamma(L_1+L_2)} + \alpha_{11}}{e^{\gamma(L_1+L_2)}\left(1 - e^{-2\gamma(L_1+L_2)}\right)} \quad (۱۹)$$

$$H_3 = Ae^{\gamma(L_1)} + \frac{(\mu_1 - \mu_2)}{2} \quad (۲۰)$$

$$H_4 = Ae^{-\gamma(L_1)} + \frac{(\mu_1 - \mu_2)}{2} \; ; a_{11} = (\mu_1 - \mu_2)\cosh(\gamma L_2) \quad (۲۱)$$

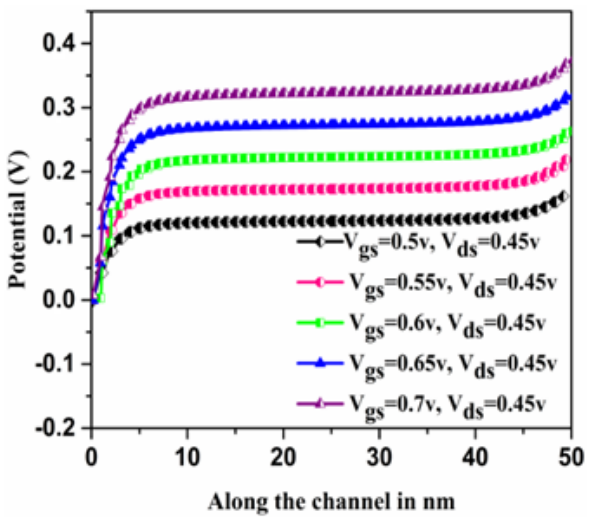
مشخصات میدان الکتریکی در طول کانال را میتوان با اختلاف پتانسیل سطح حل کرد. میدان الکتریکی جانبی را میتوان به صورت زیر نوشت:

$$E_1(x) = \frac{d\varphi_1(x,y)}{dx} = H_{1\gamma\exp(\gamma x)} - H_{2\gamma\exp(-\gamma x)} \quad ; \quad 0 \le x \le L_1$$

$$E_2(x) = \frac{d\varphi_2(x,y)}{dx} = H_{3\gamma\exp(\gamma(x-L_1))} - H_{4\gamma\exp(-\gamma(x-L_1))} \quad ; \; 0 \le x \le L_2$$

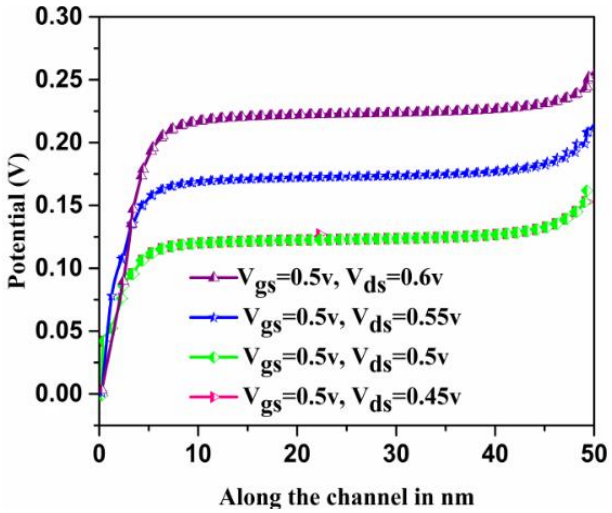
اعتبارسنجی مدل تحلیلی با نتایج شبیه سازی

توزیع پتانسیل ساختار SBT FET پیشنهادی در محور X با مقادیر V_{gs}=0.5V-0.7V در بایاس درین V_{ds}=0.45 در شکل ۴ نشان داده شده است. در اینجا، برای بایاس درین ثابت، پتانسیل سطح با افزایش بایاس گیت به دلیل کنترل بیشتر گیت بر روی سطح کانال سیلیکون افزایش میابد. نتایج مدل با داده های شبیه سازی شده با دقت زیاد تایید میشود. علاوه بر این، پتانسیل در ناحیه ماده سورس به ناحیه کانال با انتخاب تونل زنی شاتکی و تابع کار گیت تونل زنی حامل ها مطلوب میباشد.



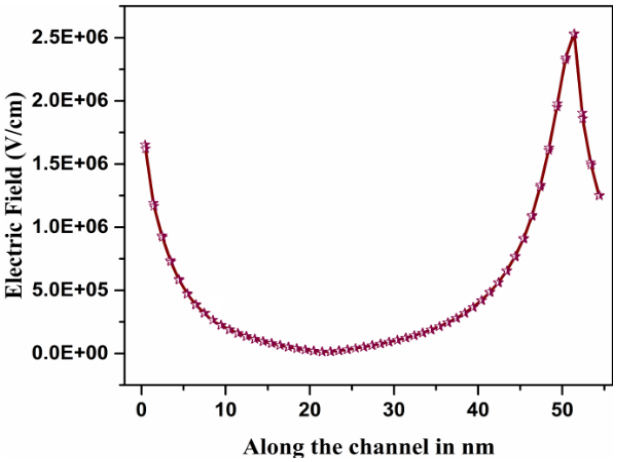
شکل ۴: توزیع گیت در امتداد کانال در V_{ds} = 0.45V

شکل ۵ تغییرات پتانسیل را در طول کانال برای بایاس درین مختلف V_{ds} ترانزیستور پیشنهادی نشان میدهد. با V_{gs} ثابت با مقادیر 0.5V، و V_{ds}های متغییر در ساختار SBT FET پیشنهادی ما را نشان میدهد.



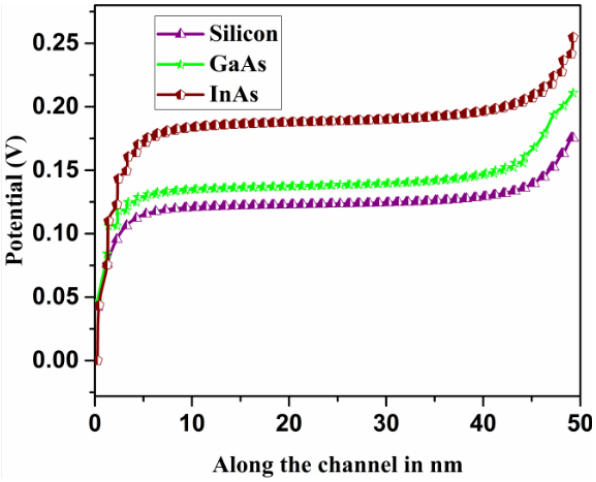
شکل ۵: پتانسیل در امتداد طول کانال درگیت V_{gs}=0.5V

شکل ۶ مقادیر میدان الکتریکی Vgs=Vds=0.5V را برای ساختار SBT FET نشان میدهد. این نمودار نتایج شبیه سازی میدان الکتریکی در طول کانال برای ترانزیستور پیشنهادی است. در SBT FET با افزایش میدان الکتریکی عمودی، امکان تونل زنی افزایش میابد. طراحی ترانزیستور پیشنهادی بسیار سازگارتر میباشد.



شکل ۶: الکتریک فیلد همراه با فاصله جانبی

در ترانزیستور پیشنهادی، لایه نازک سیلیکون بررسی میشود. شکاف باند انرژی بیشتر است، به همین دلیلSBT FET جریان تونل زنی را نشان میدهد. بنابراین، برای افزایش ON جریان SBT FET، استفاده از مواد مختلف موجب افزایش تحرک الکترون میشود. هدف مهم فروپاشی شکاف باند انرژی و افزایش جریان درین است. مواد مورد استفاده InAs وGaAs میباشد. نتایج شبیه سازی با مواد مختلف در شکل ۷ نشان داده شده است. مهمترین هدف استفاده از مواد مختلف موجب افزایش تونل زنی نسبت به لایه نازک سیلیکون میباشد. علاوه بر این، شکاف باند انرژی کاهش و جریان درین و همچنین پتانسیل سطح سیلیکونSBT FET افزایش می یابد [۱۹،۲۰]. با کاهش باند انرژی حامل ها افزایش میابد که موجب افزایش جریان تونل زنی میشود. InAs کمترین باند برای پتانسیل سطحی ترانزیستور پیشنهادی است. به این دلایل بین مواد مختلف InAs مطلوب تر میباشد [۲۱].



شکل ۷: پتانسیل سطح کانال در مواد مختلف

نتیجه گیری

یک مدل ریاضی دو بعدی تونل زنی شاتکی SBT FET دو گیتی با دی الکتریک TiO_2 بررسی میشود. در این تحقیق، پتانسیل سطح کانال با استفاده از معادلات پواسون حل میشود. ما عملکرد SBT FET را با پارامترهای مختلف از نظر کاهش اثرات با عملکرد SB FET از نظر عملکرد افزایش تونل زنی در مقایسه با ترانزیستور معمولی مورد بررسی قرار دادیم. مدل پیشنهادی با توجه به نتایج شبیه سازی و ریاضی تایید میشود.

مراجع

[1] Baie, X. and J. Colinge, *Two-dimensional confinement effects in gate-all-around (GAA) MOSFETs.* Solid-State Electronics, 1998. **42**(4): p. 499-504.

[2] Masahara, M., et al., *Fabrication and characterization of vertical-type, self-aligned asymmetric double-gate metal-oxide-semiconductor field-effect-transistors.* Applied Physics Letters, 2005. **86**(12): p. 123512.

[3] Chaudhry, A. and M.J. Kumar, *Controlling short-channel effects in deep-submicron SOI MOSFETs for improved reliability: a review.* IEEE Transactions on Device and Materials Reliability, 2004. **4**(1): p. 99-109.

[4] Kumar, P. and B. Bhowmick, *Comparative analysis of hetero gate dielectric hetero structure tunnel FET and Schottky Barrier FET with n+ pocket doping for suppression of ambipolar conduction and improved RF/linearity.* Journal of Nanoelectronics and Optoelectronics, 2019. **14**(2): p. 261-271.

[5] Larson, J.M. and J.P. Snyder, *Overview and status of metal S/D Schottky-barrier MOSFET technology.* IEEE Transactions on Electron Devices, 2006. **53**(5): p.۱۰۵۸-۱۰۴۸ .

[6] Kumar, P. and B. Bhowmick, *Scaling of dopant segregation Schottky barrier using metal strip buried oxide MOSFET and its comparison with conventional device.* Silicon, 2018. **10**(3): p. 811-820.

[7] Sun, L., et al., *A planar asymmetric Schottky barrier source/drain structure for nano-scale MOSFETs.* Semiconductor science and technology, 2006. **21**(5): p. 608.

[8] Zhang, Y., et al., *Design of 10-nm-scale recessed asymmetric Schottky barrier MOSFETs.* IEEE Electron Device Letters, 2002. **23**(7): p. 419-4.۲۱

[9] Kumar, P. and B. Bhowmick, *2-D analytical modeling for electrostatic potential and threshold voltage of a dual work function gate Schottky barrier MOSFET.* Journal of Computational Electronics, 2017. **16**(3): p. 658-665.

[10] Rahmani, M., et al., *Analytical modeling of trilayer graphene nanoribbon Schottky-barrier FET for high-speed switching applications.* Nanoscale research letters, 2013. **8**(1): p. 1-13.

[11] Raeini, A.G.N. and Z. Kordrostami, *Modified Schottky Barrier CNTFET with lightly doped drain.* Micro & Nano Letters, 2018. **13**(4): p. 442-447.

[12] Kim, H.W., et al., *Schottky barrier tunnel field-effect transistor using spacer technique.* JSTS: Journal of Semiconductor Technology and Science, 2014. **14**(5): p. 572-578.

[13] Zhu, S., et al., *Schottky-barrier S/D MOSFETs with high-k gate dielectrics and metal-gate electrode.* IEEE Electron Device Letters, 2004. **25**(5): p. 268-270.

[14] Manual, A.U.s., *Silvaco int.* Santa Clara, CA, 2008. **5**.

[15] Jhaveri, R., V. Nagavarapu, and J.C. Woo, *Asymmetric Schottky tunneling source SOI MOSFET design for mixed-mode applications.* IEEE transactions on electron devices, 2008. **56**(1): p. 93-99.

[16] Kumar, M.J. and A.A. Orouji, *Two-dimensional analytical threshold voltage model of nanoscale fully depleted SOI MOSFET with electrically induced S/D extensions.* IEEE Transactions on Electron Devices, 2005. **52**(7): p. 1568-1575.

[17] Kumar, P. and B. Bhowmick, *2D analytical model for surface potential based electric field and impact of wok function in DMG SB MOSFET.* Superlattices and Microstructures, 2017. **109**: p. 805-814.

[18] Kumar, P. and B. Bhowmick, *A physics-based threshold voltage model for hetero-dielectric dual material gate Schottky barrier MOSFET.* International Journal of Numerical Modelling: Electronic Networks, Devices and Fields, 2018. **31**(5): p. e2320.

[19] Kumar, P. and B. Bhowmick, *Suppression of ambipolar conduction and investigation of RF performance characteristics of gate-drain underlap SiGe Schottky barrier field effect transistor.* Micro & Nano Letters, 2018. **13** :(۵)p. 626-630.

[20] Nishisaka, M., S. Matsumoto, and T. Asano, *Schottky source/drain SOI MOSFET with shallow doped extension.* Japanese Journal of Applied Physics, 2003. **42**(4S): p. 2009.

[21] Kumar, P., et al., *analysis and Simulation of Schottky tunneling using Schottky barrier FET with 2-D analytical modeling.* Silicon, 2021: p. 1-7.

گواهی پذیرش مقاله

پژوهشگر محترم آقا/خانم

مقاله شما تحت عنوان

با پذیرش سردبیر مجله و نظر هیئت محترم داوران جهت انتشار در فصلنامه تخصصی کهربا به شماره مجوز ۷۷۸۲۱ و شماره استاندارد بین المللی ISSN: ۲۳۲۲-۳۷۲۳ با کد مقاله ..... مورد موافقت و تائید علمی قرار گرفت . مقالات این فصلنامه پس از انتشار در پایگاه های معتبر علمی (به شرح لوگوهای مندرج در گواهی نامه) نمایه و درج می گردد.

بدینوسیله از تلاش و فعالیت علمی شما تقدیر نموده و موفقیت روزافزونتان را در عرصه های علمی و پژوهشی از خداوند منان خواهانیم.

دبیرخانه علمی فصلنامه
واحد ارزیابی

وزارت فرهنگ و ارشاد اسلامی

این گواهینامه بدون مهر و نشان فصلنامه فاقد اعتبار است

ارتباط با کهربا

متخصصان و مهندسین گران‌قدر می‌توانند از طریق آدرس سایت مجله www.kahrobaonline.ir سایر اطلاعات مجله ازجمله نحوه ارسال مقالات جهت انتشار در نشریه و نیز فرم اشتراک مجله را دریافت کنند. همچنین به اطلاع می‌رسانیم طی توافق صورت گرفته بین پایگاه علمی سیویلیکا و مجله کهربا ازاین‌پس به مقاله برتر هر شماره یک کارت اشتراک رایگان دانلود از این پایگاه هدیه داده می‌شود.

اپلیکیشن این مجله را می‌توانید از مارکت نرم‌افزارهای موبایل (گوگل پلی) به آدرس زیر دریافت کنید.

https://play.google.com/store/apps/details?id=com.kahroba.wwwnoandishaan

ایمیل مجله kahroba@noandishaan.com پل ارتباطی ما با مهندسین و متخصصین می‌باشد، لطفاً ما را از پیشنهادها و انتقادات ارزشمند خود بهره‌مند سازید. جهت حمایت‌های مالی و معنوی از نشریه و یا معرفی محصولات خود نیز می‌توانید از طریق همین ایمیل با ما در ارتباط باشید.