

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



پروژه دوره کارشناسی رشته مهندسی کامپیوتر گرایش نرم افزار

موضوع:

شبکه‌های ادهاک وسایل نقلیه VANET

استاد مربوطه:

تهیه کننده:

شماره دانشجویی:

رسول خدا فرمودند:

« مَنْ عَلَّمَنِي حَرْفًا فَقَدْ سَيَّرَنِي عَبْدًا »

از تمامی معلمین، اساتید، دوستان و خانواده‌ام در کل دوران تحصیل سپاسگزارم.

تقدیم بہ:

تمامی رہنویان راہ علم و معرفت

چکیده

شبکه‌های ادهاک وسایل نقلیه VANET

از نقطه نظر مسئولین نیروی انتظامی، خطاهای انسانی و تخطی از قوانین و علائم راهنمایی و رانندگی عمده‌ترین عوامل تصادف می‌باشند. علی‌رغم تلاش‌های گسترده‌ای که از سوی نیروی انتظامی جهت کنترل و نظارت بیشتر جاده‌ها و بزرگراه‌ها و بسترسازی‌های فرهنگی در این راستا صورت پذیرفته است، تاکنون به دلایل مختلف و از جمله مسائل حقوقی، خودروهای اتوماتیک بدون راننده عمومی نشده‌اند؛ اما می‌توان از تکنولوژی سیستم‌های حمل و نقل هوشمند به عنوان کمک‌یار راننده و نه به جای راننده استفاده نمود. عملیاتی مانند شناسایی جاده و خط جاده، موانع و عابرین و تخمین سرعت و فاصله مد نظر می‌باشد شبکه‌های بین خودرویی مبنای سیستم‌های نقلیه هوشمند هستند که به جلوگیری از تصادف و کنترل ترافیک و کاربردهای دیگر اختصاص یافته‌اند و باعث امکان بروز رفتار خودمختار هوشمند توسط خودروها در تصادفات می‌شوند. در این شبکه‌ها، هشدارهای علائم جاده و مشاهده ترافیک به صورت لحظه‌ای، شناسایی خط جاده، موانع و عابرین، حسگرهای احساس تصادف و ضبط وقایع، تخمین سرعت و فاصله خودروهای دیگر قدرت لازم را برای بهترین تصمیم‌گیری به راننده می‌دهد. همچنین ارتباطات چندرسانه‌ای و اینترنت نیز مد نظر قرار گرفته‌اند. پرداخت خودکار هزینه پارکینگ و عوارض جاده از دیگر کاربردهای این شبکه‌ها است. برای این کار تجهیزات خاص الکترونیکی در هر وسیله نقلیه جاسازی می‌شود. این شبکه‌ها بین خودروها و ادوات کنار جاده برقرار می‌شوند. آنها چندین فناوری شبکه‌بندی موردی از جمله Wi-Fi (IEEE 802.11 a/b/g)، WiMAX (IEEE 802.16) و بلوتوث را یکپارچه می‌کنند تا ارتباط آسان، ساده، دقیق و موثر بین خودروها در یک بستر بیسیم فراهم شود. این نوع شبکه از فناوری‌های ارتباطی موجود از جمله DSRC و ارتباطات ماهواره‌ای و سلولی نیز استفاده می‌نمایند.

واژه‌های کلیدی: تصادف، وسیله نقلیه، خودروهای اتوماتیک، سیستم‌های حمل و نقل هوشمند، شبکه‌های بین

خودرویی، VANET

فهرست مطالب

عنوان	صفحه
فصل اول - آشنایی با VANET	1
1-1- مقدمه	1
2-1- تاریخچه	2
3-1- عیب‌های فنی اطلاعات توزیع شده ترافیکی	4
4-1- نحوه عملکرد اجزای خودرو در شبکه	4
5-1- شبکه‌های هوشمند موردی بین خودرویی	5
1-5-1- انواع شبکه‌های خودرویی	5
1-1-5-1- شبکه‌های خودرویی سلولی	6
2-1-5-1- شبکه‌های خودرویی اختصاصی	7
3-1-5-1- شبکه‌های بین خودرویی موردی	8
6-1- پروتکل‌ها	13
AODV 1-6-1	13
SRB 2-6-1	15
1-2-6-1- گره‌های حلقه‌ی امن (SRN)	16
2-2-6-1- گره‌های خارجی (ON)	16
3-2-6-1- گره‌های داخلی (IN)	17
DRNS 3-6-1	17
GVGrid 4-6-1	17
DOLPHIN 5-6-1 برای سیستم ارتباطی بین وسایل نقلیه	19
WTRP 6-6-1	19
7-1- کاربردها و ملزومات VANET	22
1-7-1- کاربردهای ایمنی الکترونیکی	27
2-7-1- کاربردهای رفاهی	28

28.....	3-7-1 کاربردهای مدیریت ترافیک
29.....	4-7-1 کاربردهای نگهداری و تعمیر و خدمات جانبی برای آسایش راننده
30.....	8-1 مهمترین زیر سیستم های مرتبط با پیشگیری از تصادفات و برخی محصولات تجاری
30.....	1-8-1 سیستم های پیشگیری از تصادفات در چهارراه ها و تصادفات جلو به عقب
30.....	2-8-1 سیستم های هشدار انحراف از خط
32.....	3-8-1 سیستم های شناسایی موانع
33.....	9-1 اجزای شبکه های VANET
35.....	10-1 چالش های شبکه های VANET
36.....	1-10-1 چالش های فنی و مکان یابی در VANET
38.....	2-10-1 چالش های VANET از منظر اجتماعی و اقتصادی
39.....	فصل دوم- روش های جلوگیری از تصادف خودروی مبتنی بر VANET
39.....	1-2-1 مقدمه
43.....	2-2-1 بررسی چند مورد از جنبه های خاص VANET
43.....	3-2-1 کاربردهای VANET
44.....	1-3-2 امنیت
44.....	2-3-2 کارایی حمل و نقل
44.....	3-3-2 کاربردهای آماری و تفریحی
45.....	4-2-1 مروری بر تحقیقات انجام گرفته و برخی محصولات تجاری
45.....	1-4-2 سیستم پیشگیری از تصادفات
50.....	2-4-2 سیستم شناسایی انحراف از خط
51.....	5-2-1 چالش های موجود در شبکه های بین خودرویی
51.....	1-5-2 چالش های فنی و مکان یابی در VANET
52.....	2-5-2 چالش امنیت
52.....	3-5-2 چالش کانال ارتباطی
53.....	4-5-2 چالش ارسال چند گام
53.....	5-5-2 چالش گره پنهان

54.....	6-2- روش پیشنهادی
55.....	7-2- نتیجه
56.....	فصل سوم - امنیت در MANET
56.....	1-3- تحلیل امنیت
57.....	2-3- امنیت و حریم خصوصی
57.....	3-3- خصوصیات یک ارتباط قابل اعتماد
58.....	3-4- دو چالش عمده در شبکه‌های موردی بین خودرویی
59.....	3-5- شبکه‌های موردی و چالش‌های امنیتی
61.....	3-6- حمله تغییر درگاه
65.....	فصل چهارم - نتیجه‌گیری و منابع
65.....	1-4- نتیجه‌گیری
68.....	منابع

فهرست اشکال

- شکل 1- اجزای اصلی در سامانه ارتباطات هوشمند خودرویی 5
- شکل 2- شبکه‌های خودرویی سلولی 7
- شکل 3- شبکه‌های خودرویی اختصاصی 8
- شکل 4- شمایی کلی از شبکه‌های بین خودرویی موردی (VANET) 9
- شکل 5- کاهش تراکم ترافیکی 12
- شکل 6- فرآیند مسیریابی در AODV 14
- شکل 7- همپخششی کردن پیام RERR 14
- شکل 8- a و b گره‌های فرستنده، p گره گیرنده 16
- شکل 9- جدول اتصال 20
- شکل 10- وارد شدن گره G به داخل حلقه 21
- شکل 11- خروج گره C از داخل حلقه 21
- شکل 12- امنیت یکی از کاربردها و اهداف شبکه‌های VANET است 23
- شکل 13- برخی از کاربردهای VANET 25
- شکل 14- هشدار عبور از علامت توقف 28
- شکل 15- نمونه‌ای از کاربردهای رفاهی در (FleetNet) 28
- شکل 16- نمایی از خودروهای کمک‌یار راننده شرکت ولوو 30
- شکل 17- محاسبه زمان برخورد توسط MobileYE 30
- شکل 18- رانندگی در مه توسط تجهیزات شبکه‌های بین خودرویی 31
- شکل 19- نمای جاده با استفاده از تجهیزات شناسایی موانع 33

- شکل 21- نمایی شماتیک از حسگرهای شبکه VANET..... 35
- شکل 23- محدوده‌های تحت پوشش سنسورهای شبکه‌های VANET..... 35
- شکل 22- محدوده‌های تحت پوشش سنسورهای شبکه‌های VANET..... 35
- شکل 23- عوامل موثر بر تصادفات..... 41
- شکل 24- عوامل موثر در تصادفات با ذکر درجه اهمیت..... 42
- شکل 25- اختطار کاهش فاصله در سیستم MobilEye: 2 ثانیه، 1 ثانیه و 0.6 ثانیه تا برخورد با خودروی جلویی..... 45
- شکل 26- (الف) اجزای اصلی سیستم kown، (ب) مراحل اصلی سیستم kown..... 46
- شکل 27- (الف) نحوه‌ی حرکت خودرو با DSTC و بدون آن در شرایط لغزنده (ب)..... 48
- شکل 28- ساختار سیستم هشدار تصادف..... 49
- شکل 29- عملکرد سیستم هشدار تصادف در VANET..... 49
- شکل 30- نمایی از محصولات تجاری ADAS و MobileEye در شناسایی خط و انحراف از خط در روز و شب... 50
- شکل 31- نمونه‌هایی از عملکرد سیستم‌های تشخیص عابر پیاده..... 51
- شکل 32- خود گره‌ها در عمل مسیریابی شرکت می‌کنند..... 52
- شکل 33- طرح ساده‌ای از مشکل گره پنهان..... 54
- شکل 34- یک شبکه موردی فرضی..... 61
- شکل 35- سرآیند بسته‌ها در پروتکل TCP/IP..... 62
- شکل 37- یک شبکه موردی فرضی با نودها و لینک‌های فعال و سالم..... 63
- شکل 38- نود مهاجم M در حالت ایجاد ارتباط میان نود مبدا و مقصد..... 64

فصل اول – آشنایی با VANET¹

1-1- مقدمه

سیستم‌های ایمنی فعال به منظور پیشگیری فعالانه تصادفات ارائه شده‌اند و بر کاهش نرخ و شدت تصادفات تمرکز دارند. تاکنون نمونه‌هایی از این گونه سیستم‌ها در دنیا ارائه و هم اکنون در بسیاری از ماشین‌ها تعبیه شده‌اند. به عنوان مثال سیستم ترمز ضد قفل یا سیستم الکترونیکی پایداری توانسته‌اند به راننده‌ها کمک نمایند تا از تصادفات زیادی جلوگیری گردد. این امر از توفیق نسبی برخوردار بوده و توانسته است جلوی رشد فزاینده تعداد تصادفات را بگیرد همچنین با کاستن از شدت تصادف‌ها به نحو چشمگیری آمار تلفات و مرگ و میر کاهش یافته است. به‌رغم این تلاش‌ها، مطالعات آماری نشان می‌دهد با وجود اینکه سیستم‌های فعال و غیرفعال ایمنی توانسته‌اند جلوی سیر افزایشی تعداد تصادفات را بگیرند حدود ۱۵ سال است که تصادفات تقریباً بدون تغییر باقی‌مانده است این امر به خوبی این نکته را آشکار می‌نماید که سیستم‌های ایمنی کنونی قادر نیستند بیش از این نرخ تصادفات را کاهش دهند در نتیجه این نیاز وجود دارد که فکری جدید در مورد راهکارهای کاهش میزان تصادفات اندیشیده شود. به نظر می‌رسد اگر بتوان سطح اطلاعات راننده از محیط اطراف و همچنین محدوده اطلاعاتی او را گسترش داد، تحول شگرفی در ایمنی حمل و نقل به وجود می‌آید.

¹ Vehicular AdHoc Network

1-2- تاریخچه

نخستین تصادف رانندگی در ایران در سال 1305 میان اتومبیل مظفرالدین شاه و درشکه درویش خان نوازنده در خیابان سپه تهران اتفاق افتاد. در دنیا نخستین انسانی که در یک حادثه رانندگی جان خود را از دست داد، یک خانم انگلیسی بود. بریجیت درسکول 44 ساله اولین کسی در دنیا است که در یک سانحه رانندگی جان خود را از دست داده است. وی روز هفدهم آگوست سال 1896 در میدان کریستال یالاس لندن بر اثر تصادف فوت کرد.

اگر بخواهیم مختصری در مورد تاریخچه این شبکه توضیح دهیم باید بگوییم که اولین بار در سال 1769 نیکولاس جوزف کائانت اولین خودرو مکانیکی متحرک به نام "واگن بخار" را ساخت. اولین تصادف در سال 1771 بود که آقای کائانت خودروی بخار خود را به یک دیوار آجری کوبید! هنری فورد در 1913 اولین لاین برای اتومبیل ها را ساخت و در 1927 حدود 15 میلیون لاین ساخته شدند. در 1956 اولین وسایل ایمنی (کمربند ایمنی) برای خودروهای شرکت فورد و در 1978 ترمزهای ABS در مرسدس بنز ساخته شد.

در اولین سال های تولید اتومبیل و تولید این ساخته دست بشر تا به امروز شاهد پیشرفت های زیادی در این صنعت بوده ایم که یکی از بنیادی ترین صنایع قرن حاضر می باشد. در این مقوله الکترونیک خودروها تا حدی از قافله پیشرفت عقب افتاد؛ چون در ابتدا بیشتر توجه خودروسازان بر طراحی موتور، شاسی، فرم اتاق و ... متمرکز شده بود. همچنین استفاده وسیع از وسایل الکترونیکی تا به این حد که امروزه در خودروها کاربرد دارد، مورد توجه نبود. اما با توجه به مسایل بالا و افزایش قیمت قطعات مصرفی و دستمزد بالا، سعی بر کاهش هزینه و بالا بردن کیفیت خودرو، توجه خودروسازان را به لزوم ساده کردن سیم کشی موجود خودرو و ارتقاء این سیستم برای به کارگیری منابع مصرف کننده در خودرو معطوف کرد. در این بین توجه متخصصان به سیستمی که در صنایع مخابراتی مورد استفاده بود، معطوف شد که تلفیق این سیستم با سایر تکنولوژی های موجود امروزی، در خودروسازی مورد استفاده قرار گرفت. با ورود دانش فناوری ارتباط به دنیای اتومبیل سازی، شرکت های اتومبیل سازی بیشترین سعی خود را در ساختن تجهیزات ارتباطی داخل خودرو برای افزایش ایمنی، کاهش اتلاف منابع، مسیریابی صحیح برای کاهش اتلاف وقت و بهبود در تجربه رانندگی و جلوگیری از ترافیک و همینطور استفاده از امکانات تفریح و سرگرمی و راحتی بیشتر افراد نموده اند. پس از استفاده از کمترین ایمنی و سیستم های دفاعی نظیر کیسه هوا با وجود اینکه آمار تلفات و خسارات کمتر شد، اما این آمار با به طرز

قابل توجهی بسیار زیاد به نظر می‌رسد. سالانه 800 هزار تصادف در ایران رخ می‌دهد که از حیث آمار مرگبارترین حوادث جاده‌ای، ایران رتبه اول را در جهان دارد.

هدف اصلی سیستم‌های بین خودرویی ایجاد امنیت و راحتی برای رانندگان و مسافران می‌باشد. در این راستا تلاش‌های زیادی صورت گرفته تا از تصادفات جلوگیری شود و همچنین وضعیت ترافیک بهتر شود. در شبکه‌های موردی بین خودرویی هر خودرو مجهز به فناوری است که به رانندگان این امکان را می‌دهد تا با یکدیگر و با زیرساختار جاده ارتباط برقرار کند. زیرساختار جاده‌ای که به عنوان واحدهای کنار جاده معروف هستند. در برخی از نقاط حیاتی خیابان‌ها و جاده‌ها مانند هر چراغ راهنمایی که سر تقاطع می‌باشد یا هر علامت ایست قرار گرفته‌اند تا وضعیت عبور و مرور را بهبود بخشیده و رانندگی را ایمن‌تر سازند.

به عنوان نمونه در زمان وقوع یک تصادف، راننده‌ای اقدام به ترمز ناگهانی می‌نماید. در چنین وضعیتی هرگونه تعلل رانندگان واقع در خودروهای عقبی، می‌تواند باعث ایجاد تصادف‌های زنجیره‌ای گردد و زیان‌های مالی و بعضاً جانی زیادی را به دنبال داشته باشد. در این شرایط، شبکه‌های بین خودرویی این امکان را دارند تا بدون دخالت رانندگان، تا حد امکان جلوی این امر را بگیرند. مکانیزم کاری شبکه‌های بین خودرویی به این شکل است که به هنگام ترمز، سیستم ارتباطی شبکه‌های بین خودرویی اقدام به انتشار پیام اخطار برای ماشین‌های پشت سر می‌نماید. ماشین‌های دریافت‌کننده پیام، با مشاهده‌ی پیام اخطار، به صورت خودکار اقدام به کاهش سرعت خودرو می‌نمایند. البته در شبکه‌های بین خودرویی، به صورت دوره‌ای پیام‌های مختلفی به منظور ایجاد فضای لازم برای رانندگی ایمن، منتشر می‌گردد. وقوع تصادفات جاده‌ای سالانه میلیاردها دلار خسارت در سراسر جهان بر جای می‌گذارد.

جذابیت این شبکه‌ها در عدم نیاز به یک سازمان متمرکز پردازش داده‌های ترافیکی است و سیستم به راحتی قابل گسترش به تمام مناطق است. در هر قسمتی از جاده، یک شبکه بین خودرویی شکل می‌گیرد و جاده‌های مختلف توسط شبکه‌های کوچکتر به یکدیگر متصل می‌شوند. ارتباط خودرو با خودرو و با تجهیزات کنار جاده، موجب می‌شود تا نقش آنها از ابزارهای حمل و نقل به ادوات هوشمند تغییر پیدا کند. در این شبکه‌ها از قابلیت‌های مخابرات بین خودرویی در جهت ایجاد سامانه کنترل ترافیک استفاده می‌شود. در یک سامانه کنترل ترافیک سنتی، با استفاده از حسگرهایی عمل پایش ترافیک انجام می‌شود. بعد از این مرحله، اطلاعات جمع‌آوری شده برای تحلیل به مرکز اطلاعات ترافیک ارسال شده، نتیجه تحلیل به صورت بسته‌های پیام به کانال ارسال می‌شود. در نهایت، بسته‌های پیام توسط ایستگاه‌های رادیویی FM ارسال و در اختیار گیرنده قرار می‌گیرند. روش دیگر ارائه شده در ارسال پیام‌های ترافیکی، ارسال پیام‌های ترافیکی بر حسب تقاضا و توسط شبکه‌های سلولی بی‌سیم می‌باشد.

1-3- عیب‌های فنی اطلاعات توزیع شده ترافیکی

در حال ارائه سرویس مرکزی برای اطلاعات توزیع شده ترافیکی چندین عیب فنی دارد:

- تعداد زیادی حسگر بایستی مورد استفاده قرار گیرد، در نتیجه سرمایه‌گذاری زیادی برای زیر ساخت‌های مخابراتی لازم است. همچنین لازم است که حسگرها با یکدیگر و با سامانه کنترل مرکزی در ارتباط باشند که نیازمند اتصالات بی‌سیم و سیمی زیادی می‌باشد.
- اطلاعات جمع‌آوری شده باید به یک واحد مرکزی پردازش ارسال شود که این امر تأخیر را بالا می‌برد.
- با توجه به اینکه واحد مرکزی مساحت نسبتاً زیادی را پوشش می‌دهد، و پهنای باند محدود، برای ارسال پیام‌های ترافیکی فقط وقایع بااهمیت‌تر ارسال می‌شوند. در نتیجه امکان ارائه‌ی جزئیات به روز برای کاربران درون خودرو بسیار سخت خواهد بود.

بنابر دلایل فوق، ارائه سامانه اطلاعات ترافیکی خودسازمانده دارای اهمیت فراوانی خواهد بود. روشی دیگر برای پایش ترافیک و توزیع پیام‌های ترافیکی، استفاده از سامانه‌های خودسازمانده است. پیاده‌سازی چنین سامانه‌ای با فرض اینکه خودروها دارای یک نقشه دیجیتال، سامانه موقعیت‌یابی و قابلیت‌های ارتباط بی‌سیم با دیگر خودروها هستند، امکان‌پذیر خواهند بود. در این روش یک خودرو دیگر وسایل نقلیه را از موقعیت ترافیک محلی اطراف خود آگاه می‌سازد. در حالت کلی برای چنین پیکربندی، هیچ زیر ساخت مخابراتی نیاز نیست. البته برای بهینه‌سازی مسیر سراسری می‌توان اطلاعات سامانه‌ی خودسازمانده را به پایگاه‌های جاده‌ای و یا سامانه‌های متمرکز سنتی ارسال کرد تا برای کاربردهای دیگر مورد استفاده واقع شود. استفاده از سامانه‌های خودسازمانده برای رسیدن به سامانه‌ی حمل و نقل هوشمند یک ضرورت اصلی است.

1-4- نحوه عملکرد اجزای خودرو در شبکه

داخل خودروهای شبکه‌های موردی بین خودرویی، تجهیزات بسیاری نصب می‌شود تا امکان برقراری ارتباط با شبکه را داشته باشند. در بازه‌های زمانی خاص، پیام‌های مربوط به سرعت، ترافیک، علائم جاده‌ای، وضعیت ترمزها و جهت حرکت توسط واحد داخل خودرو¹ به سایر خودروها همه پخش می‌شود و پیام‌های مربوط به سایر خودروها به خودروی مورد نظر ارسال شده و مورد

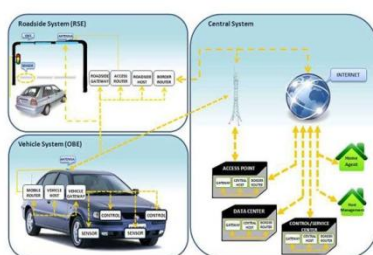
¹ OBU

پردازش قرار می‌گیرند. در صورت وجود ترافیک یا تصادف و یا هر موقعیت اضطراری در مسیر، خودروها توسط سیستم موقعیت‌یابی جهانی¹، مکان خود را به مرکز خاصی اعلام می‌کنند که با اطلاعات دریافتی، سعی در استخراج تصویر لحظه‌ای شبکه و خودروها دارد. همچنین در فواصل مشخصی اطلاعات مربوط به پیام‌ها، توسط تجهیزات کنار جاده‌ای به ایستگاه مرکزی² اطلاع داده می‌شود تا پیش‌بینی کلی در مورد رویدادهای تمام مناطق به دست آید. پیام‌های ترافیکی توسط ایستگاه پایه نیز به خودروها اطلاع داده می‌شود. ثبت اطلاعات خودرو مانند مکان، سرعت و زمان هنگام وقوع اتفاقات ضروری است که توسط واحد ضبط‌کننده وقایع³ انجام می‌گیرد و مانند جعبه سیاه هواپیما عمل می‌کند. اطلاعات توسط افرادی مانند مکانیک و یا پلیس استخراج می‌گردند تا در بررسی صحنه تصادف و یا شناسایی مقصر و سایر اطلاعات تصادف، مورد استفاده قرار گیرند. همچنین اطلاعات مربوط به پیام‌ها توسط مراکز تصدیق هویت ثبت می‌شود تا در صورت لزوم از آن‌ها استفاده شود.

1-5- شبکه‌های هوشمند موردی بین خودرویی

شبکه‌های بین خودرویی هوشمند در ایجاد سیستم حمل و نقل هوشمند بسیار مؤثر است که نمونه‌ای از کاربرد هوش مصنوعی در خودروها می‌باشند و باعث بروز رفتار خودمختار هوشمند توسط خودروها در مواقعی مانند تصادف، رانندگی در حین مستی، ناشی بودن راننده و ... می‌شوند. این تکنولوژی همچنین می‌تواند برای خودروهای توپدار و زرهی در هنگام مأموریت در صحنه نبرد و زمان صلح استفاده شود.

در شبکه‌های بین خودرویی هر خودرو مانند یک گره در شبکه عمل می‌کند، این گره‌ها می‌توانند با یکدیگر همکاری نمایند تا کارایی شبکه افزایش یابد. در واقع شبکه‌های بین خودرویی نوعی از شبکه اقتضایی می‌باشند که زیرساختار ثابت ندارند و وابسته به خودروهای شبکه هستند تا عملیات و توابع شبکه همچون مسیریابی بسته و مدیریت شبکه را انجام دهند.



شکل 1- اجزای اصلی در سامانه ارتباطات هوشمند خودرویی

¹ GPS

² RSU

³ TPD

1-5-1- انواع شبکه‌های خودرویی

ارتباط میان خودروها با دنیای خارج و ارتباط میان خودروها در هنگام حرکت، رؤیای قدیمی بشر بوده است و تاریخچه نخستین تلاش‌ها برای تحقق این رؤیا به بیش از چهل سال پیش برمی‌گردد. در آن زمان با نصب یک آنتن روی خودروهای خاصی مانند خودروهای پلیس یا اورژانس و تنظیم کردن آنتن‌ها روی یک فرکانس خاص در یک محدوده جغرافیایی، سعی می‌کردند یک ارتباط رادیویی و شبه تلفنی را ایجاد کنند. در سال 1999 کمیسیون ارتباطات فدرال ایالات متحده¹ با تصویب استانداردها و پهنای باند لازم برای ارتباط خودروها با تجهیزات ثابت کنار جاده، عملاً فاز جدیدی از شبکه‌های بین خودرویی را ایجاد کرد که این حرکت با تصویب استاندارد DSRC² در سال 2003 تکمیل شد. در این استاندارد پهنای باند 5/9 گیگاهرتز به ارتباطات بین خودرویی اختصاص یافته است و روی این فرکانس بین هفت تا ده کانال (5/850 گیگاهرتز تا 5/926 گیگاهرتز) تعریف می‌شود که یک کانال به صورت ویژه به افزایش ضریب امنیت خودروها و سایر کانال‌ها به کاربردهای خاص، اختصاص یافته است. پس از این رخدادها، انواع ارتباطات میان خودروها براساس فناوری‌ها و زیرساخت‌های متفاوت مطرح شده و هریک مسیری جداگانه برای توسعه و مجهز کردن خودروها به امکانات شبکه‌ای در پیش گرفتند. اگر بخواهیم شبکه‌های خودرویی را بر اساس رسانه انتقال اطلاعات تقسیم‌بندی کنیم، به سه دسته کلی می‌رسیم: شبکه‌های مبتنی بر امواج رادیویی³، مبتنی بر مکان‌یابی و مبتنی بر حسگرها و تراشه‌های داخلی. تقسیم‌بندی بعدی شبکه‌های بین خودرویی می‌تواند بر اساس زیرساخت شبکه باشد. در این تقسیم‌بندی سه نوع شبکه کلی سلولی، اختصاصی و موردی داریم که در ادامه دو نوع نخست به صورت اختصار و نوع سوم به صورت کامل بررسی می‌شود.

1-5-1-1- شبکه‌های خودرویی سلولی

در شبکه‌های سلولی از فناوری‌های G3، G4 و GSM استفاده می‌شود و به طور عمده اپراتورهای تلفن همراه و سرویس‌دهنده‌های باند پهن موبایل بازیگران اصلی این حوزه هستند. همان‌طور که در شکل 3 مشخص است در کنار جاده

¹ FCC

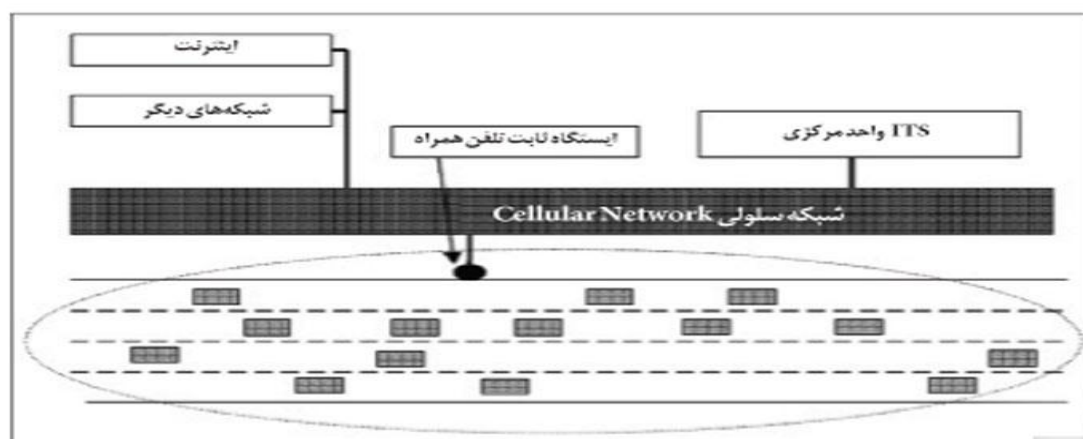
² Dedicated Short Range Communications

³ Wireless

یک سری ایستگاه مرکزی ثابت¹ وجود دارد که می‌توانند به اینترنت و شبکه‌های درون شهری متصل باشند. خودروها از طریق امکانات موبایل می‌توانند به این ایستگاه‌ها متصل شده و اطلاعات ترافیکی یا آب و هوا را دریافت کنند. همچنین می‌توانند به اینترنت متصل شده و از طریق سرویس‌های کلاود به شبکه محل کار یا خانه دسترسی پیدا کنند. مزیت این شبکه‌ها استفاده از زیرساخت‌های آماده موبایل و باند پهن ارائه شده توسط اپراتورهای موبایل است. پیش‌بینی می‌شود با ورود نسل جدید G4 و افزایش سرعت و پهنای باند، این نوع شبکه‌ها رواج و استقبال بیشتری را شاهد باشند. عیب بزرگ شبکه‌های سلولی عدم امکان استفاده برای کاربردهای ایمنی خودروها به خاطر تأخیرهای ذاتی این نوع شبکه‌ها است اما چنین شبکه‌هایی برای استفاده‌های معمول مانند استفاده از اینترنت و سرگرمی بسیار مناسب هستند.

«مزیت شبکه‌های خودرویی سلولی استفاده از زیرساخت‌های آماده موبایل و باند پهن ارائه‌شده توسط اپراتورهای موبایل

است.»



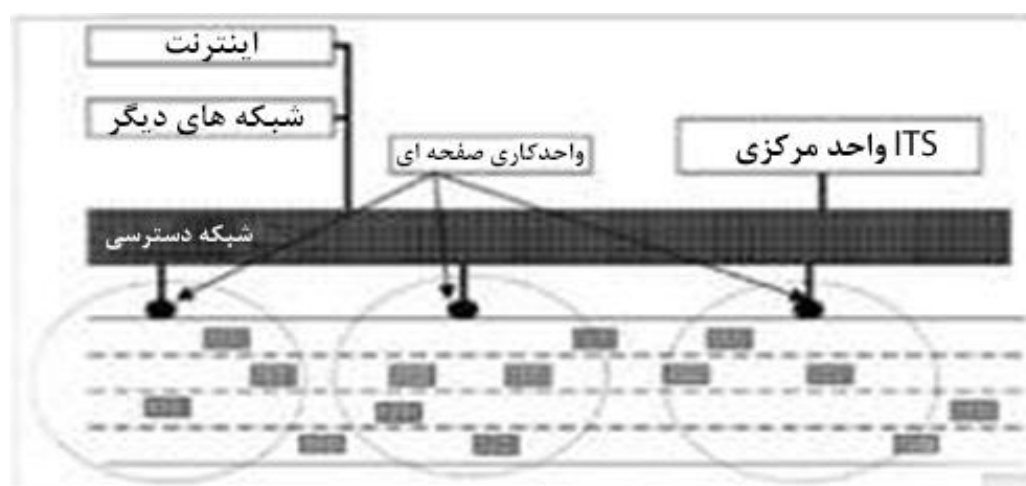
شکل 2- شبکه‌های خودرویی سلولی

1-5-2- شبکه‌های خودرویی اختصاصی

در شبکه‌های اختصاصی، یک شرکت ثالث می‌تواند با نصب تجهیزات ثابت کنار جاده‌ها یا در تقاطع‌ها و ایجاد یک سری ایستگاه‌های سرور و نصب رابط‌ها در خودروها، بین خودروها و دنیای خارج ارتباط برقرار کند (شکل 4). سیستم VICS در ژاپن نمونه‌ای از این نوع شبکه‌ها است که اطلاعات ترافیکی را از خودروهای مختلف جمع‌آوری کرده و به یک سیستم مرکزی هدایت

¹ Base Station

می‌کند. سیستم مرکزی به صورت هوشمند؛ پس از تجزیه و تحلیل اطلاعات دریافتی وضعیت ترافیکی جاده‌ها و خیابان‌های مختلف، اطلاعات مورد نیاز سایر راننده‌ها را استخراج کرده و دوباره به ایستگاه‌ها کاری کنار جاده‌ها ارسال می‌کند تا خودروها این اطلاعات را دریافت و برای مسیرهای بعدی خود تصمیم‌گیری کنند. این نوع شبکه‌ها معایب زیادی دارند. هزینه بالای نصب و راه‌اندازی تجهیزات و زیرساخت لازم در تمام جاده‌ها و مراکز اصلی تردد خودروها، تأخیر در ارسال و دریافت اطلاعات و تأخیر در دسترسی به اطلاعات استخراج شده از وضعیت ترافیکی جاده‌ها و الگوریتم‌های هوشمند مربوط به محاسبات، برخی از معایب شبکه‌های خودرویی اختصاصی هستند.



شکل 3- شبکه‌های خودرویی اختصاصی

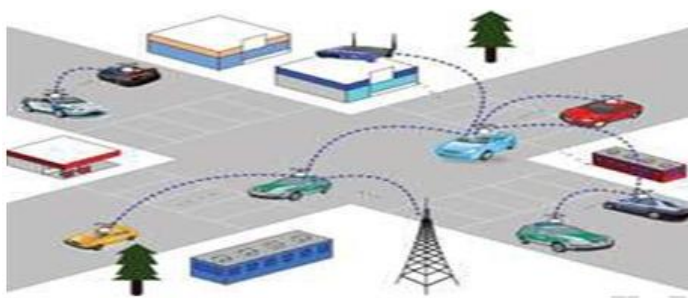
1-5-1-3- شبکه‌های بین خودرویی موردی

ایده اولیه شبکه‌های VANET برای نخستین بار در سال 1998 توسط یک گروه مهندسی به نام «دلفی دِلکو الکترونیک سیستم»¹ با همکاری شرکت آی‌بی‌ام² مطرح شد. شبکه VANET با استفاده از امواج رادیویی انواع ارتباط‌های خودرو به خودرو (V2V) و خودرو به زیرساخت (V2I) را ایجاد می‌کند. خودروها به صورت کاملاً خود مختار با یکدیگر ارتباط برقرار کرده و یک شبکه غیر ساختارمند بی‌سیم ایجاد می‌کنند.

¹ Delphi Delco Electronics Systems

² IBM

«تفاوت اصلی شبکه‌های VANET با شبکه‌های سلولی و اختصاصی این است که هیچ ایستگاه یا نود مرکزی، مدیریت و کنترل شبکه را بر عهده ندارد و شبکه از یک سری خودرو تشکیل شده است.»



شکل 4- شمایی کلی از شبکه‌های بین خودرویی موردی

شکل 5- شمایی کلی از شبکه‌های بین خودرویی موردی

تفاوت اصلی شبکه‌های VANET با شبکه‌های سلولی و اختصاصی این است که هیچ ایستگاه یا نود مرکزی، مدیریت و کنترل شبکه را بر عهده ندارد و شبکه از یک سری خودرو (در اینجا فرض کنید نود شبکه) تشکیل شده که متحرک بوده و جای ثابتی ندارند و هیچ یک نقش روتر یا اکسس پوینت را بازی نمی کنند. در حقیقت شبکه‌های VANET یک نوع خاص شبکه‌های MANETs¹ هستند که نودهای آن خودروها خواهند بود. هر خودرو می تواند در هر لحظه خودروهای اطرافش را شناسایی کرده و با اتصال به آنها یک شبکه تشکیل داده و ارتباطات لازم را برقرار کند. این خودرو کمی بعدتر با خودروهای جدید اطرافش یک شبکه دیگر ایجاد خواهد کرد. مبنای اصلی شبکه‌های VANET غیر ساختارمند بودن آنها و استفاده از استاندارد 802.11p و DSRC است. بنابراین این نوع شبکه‌ها به سرعت می توانند تغییر توپولوژی داده و با توجه به این که از نظر مصرف انرژی و منابع محاسباتی مشکلی ندارند، انعطاف پذیری زیادی ایجاد کنند. برای نمونه، یک خودرو می تواند همزمان به چندین شبکه VANET متصل باشد و اطلاعات لازم را دریافت کند. محدوده‌های جغرافیایی شبکه VANET می تواند دایره‌هایی به شعاع حداکثر چند کیلومتر باشد و هر خودرو می تواند برای مثال با خودروهای جلویی در فاصله دو یا سه کیلومتر ارتباط برقرار کند.

¹ Mobile Adhoc Networks

VANET سه کاربرد اصلی و مشخص دارد: ایمنی، راحتی و کاربرد تجاری. بنابراین یک ویژگی دیگر این نوع شبکه‌ها برد کوتاه آن است. در شبکه‌های VANET می‌توان به ایستگاه‌های مرکزی¹ یا اینترنت نیز متصل شد و با آنها تبادل اطلاعات کرد، اما مبنای اصلی شبکه، ارتباطات بین خودرویی است. VANET یکی از اجزای اصلی سیستم‌های حمل و نقل هوشمند است و در چند سال اخیر تحقیقات و پژوهش‌های زیادی روی آن انجام شده است و امیدهای فراوانی به آن وجود دارد. علت این اهمیت نیز ارتباط مستقیم این نوع شبکه‌ها با ایمنی خودروها و ترافیک است.

VANET یک نمونه شبکه سیار است که برای برقراری ارتباط بین وسایل نقلیه مجاور (IVC²) و همچنین وسایل نقلیه با تجهیزات ثابت مجاور (RVC³) که معمولاً تجهیزات کنار جاده‌ای هستند ایجاد شده است.

برای دستیابی به این هدف یک دستگاه خاص الکترونیکی در هر وسیله نقلیه جاسازی می‌شود که امکان برقراری ارتباط موردی⁴ بین مسافران را برقرار می‌کند.

چنین شبکه‌ای باید بدون محدودیت‌های ساختارهای ارتباطی شبکه‌ای کلاینت - سرور پیاده‌سازی شود. هر وسیله نقلیه‌ای که به یک دستگاه VANET مجهز شده باشد همانند یک گره در شبکه موردی⁵ است و قادر به دریافت و ارسال پیام‌های دیگران از طریق شبکه بی‌سیم خواهد بود.

هشدارهای ترافیکی، علائم جاده‌ای و مشاهده ترافیک به صورت لحظه‌ای که از طریق چنین شبکه‌ای می‌تواند منتقل شود، ابزارهای لازم را برای تصمیم‌گیری در مورد بهترین مسیر به راننده می‌دهد.

همچنین ارتباطات چند رسانه‌ای و اینترنت در رنج بی‌سیم هر وسیله نقلیه فراهم می‌شود. پرداخت خودکار هزینه پارکینگ و عوارض جاده‌ای از دیگر کاربردهای شبکه VANET است.

InVANET¹ یا VANET هوشمند در واقع بیانگر یک روش هوشمند در به کارگیری شبکه‌ی بین خودروهاست.

¹ BS

² Inter Vehicle Communication

³ Roadside to Vehicle Communication

⁴ Adhoc

⁵ Adhoc

InVANET چندین تکنولوژی شبکه‌بندی موردی از جمله WiMAX IEEE، WiFi IEEE 802.11 b/g

802.16، بلوتوث^۲، IRA و ZigBee را یکپارچه می‌کند تا ارتباط آسان، ساده، دقیق و مؤثر بین خودروها در یک بستر بی‌سیم

فراهم شود.

این نوع شبکه همچنین از دیگر تکنولوژی‌های ارتباطی موجود از جمله DSRC: که در واقع نوعی WiFi است برای

ارتباطات ماهواره‌ای و سلولی استفاده می‌کند.

VANET را می‌توان به عنوان جزئی از سیستم هوشمند حمل و نقل^۳ دید.

نفوذ مفهوم مکالمات بی‌سیم در خودروها در سال 1980، مورد توجه محققان بوده است و در چند سال اخیر، شاهد افزایش

فراوان توسعه و تحقیق در این حوزه بوده‌ایم. عوامل چندی منجر به این پیشرفت شده‌اند از جمله: به کارگیری وسیع فناوری IEEE

- که کاهش قیمت را به همراه داشته است - استقبال سازندگان خودرو از فناوری اطلاعات برای پاسخگویی به مسائل امنیتی و

محیطی و توجه به راحتی خودروهایشان، الزام دولت‌ها برای اختصاص گسترده بی‌سیم برای ارتباطات خودروها، گرچه شبکه‌های

سلولی ارتباطات مناسب صوتی را امکان‌پذیر می‌سازند و امکانات تفریحی را برای رانندگان و سرنشینان آن‌ها فراهم می‌آورند. با

این حال برای ارتباطات مستقیم خودرو با خودرو و خودرو با سیستم زیر ساختی مناسب نمی‌باشند، اما VANET برای ارتباطات

خودرو با خودرو با واحدهای کنار جاده‌ای^۴ پیشنهاد می‌شود و قادر به فرستادن و دریافت اعلام خطر یا اطلاعاتی از موقعیت‌های

جاری ترافیکی با حداقل تأخیر است. از اواخر سال 1990، با تولید گیرنده‌های ارزان قیمت GPS و دستگاه‌های فرستنده، گیرنده

شبکه‌های بی‌سیم محلی^۵، تحقیق در حوزه مکالمات بین خودرویی شتاب قابل توجهی گرفت.

اصولاً این فناوری در دو سطح ماکرو و میکرو توصیف می‌شود. امروزه عمده مطالعات در زمینه مدل‌های متحرک وسایل نقلیه

در محدوده سطح ماکرو است در حالی که توجه کمی به میکرو شده است. وقتی به جنبه ماکرو نگاه می‌کنیم نه تنها به توپولوژی

جاده‌ها نظر داریم، بلکه به مسیرهای حرکت خودروها، توان افزایش مسیرها یا حتی به عوامل مهم فرعی دیگر نیز توجه می‌کنیم که

¹ Intelligent VANET

² Bluetooth

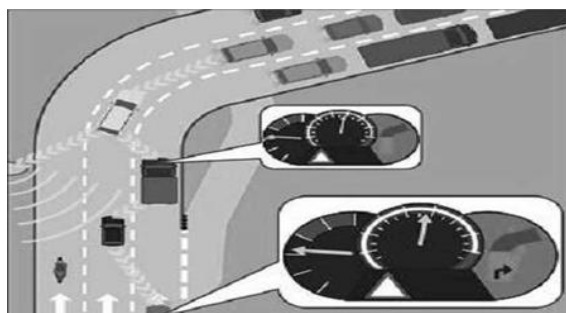
³ Intelligent Transport System

⁴ RSU_s

⁵ WLAN

همگی در الگوی حرکتی وسایل نقلیه در توپولوژی جاده‌ها تأثیر دارد. میکرو به عوامل انسانی و مسائلی نظیر حرکات داخل خودرو، عوامل تأثیرگذار خودروهای دیگر، تغییر مسیر، مدیریت چهارراه‌ها و مواردی از این قبیل توجه می‌کند.

هدف از فعالیت‌ها و تحقیقات انجام شده، ارتقاء امنیت جاده‌ای، افزایش کارایی حمل و نقل، همچنین کاهش اثرات حمل و نقل بر محیط است؛ هر سه این کاربردها کاملاً بر هم عمود نیستند. به عنوان مثال کاهش تعداد تصادفات به نوبه خود می‌تواند میزان تراکم ترافیکی را کاهش داده که این نیز می‌تواند منجر به کاهش اثرات محیطی شود.



شکل 5- کاهش تراکم ترافیکی

به سبب اهمیت فردی و اجتماعی این اهداف، پروژه‌های متعددی در کشورهای مختلف در دست اقدام بوده است یا اخیراً کامل شده و چندین کنسرسیوم نیز برای تحقق امکان بالقوه این فناوری ایجاد شده‌اند. این پروژه‌ها اساساً توسط دولت‌ها پی‌ریزی می‌شود. همچنین دولت‌ها در دامنه عمل محدود، مشارکت می‌کنند. این دامنه‌ها به طور معمول در باند 9، 8/5، 5 و در ژاپن حداقل 600 مگاهرتز¹ می‌باشد. در اصل واژه VANET جهت بازتاب طبیعی موقتی بودن این شبکه کاملاً قابل انعطاف انتخاب شده است.

¹ MHz

AODV -1-6-1

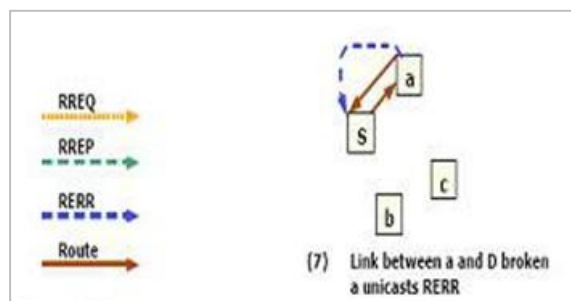
Destination (DE)	Cost (CO)	Next Hop (NH)
A	1	A
B	0	B
C	∞	-
D	1	D
E	∞	-

این روش می‌تواند همه‌پخشی^۳، یک‌به‌یک^۴ و یک‌به‌چند^۵ را بدون هیچ پروتکل دیگری حمایت کند. برای مسیریابی یک‌به‌یک، سه پیام کنترل استفاده می‌شود: RREP، RREQ و RERR. اگر یک گره بخواهد یک بسته را به گره دیگری ارسال کند (با توجه به شکل) ابتدا یک پیام RREQ را همه‌پخشی می‌کند. گره دریافت کننده RREQ یک مسیر برگشتی به فرستنده ایجاد می‌کند. اگر گره دریافت کننده پیام RREQ، مقصد نهایی بسته نباشد آن گره پیام RREQ به روز شده را rebroadcast می‌کند و به طور خاص، شماره هاب^۶ را افزایش می‌دهد. اگر گره به عنوان مقصد نهایی ارسال اطلاعات شناخته

S establishes Route

شد، آن گره یک $RREP^1$ ایجاد می‌کند. اگر یک گره متوجه شود که به دیگر گره‌ها دسترسی ندارد یک پیام RREP را همه‌پخشی می‌کند.

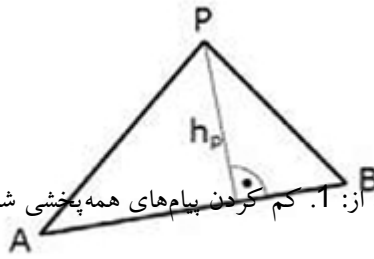
شکل 6- فرآیند مسیریابی در AODV



شکل 7- همه‌پخشی کردن پیام RERR

¹ Rout Reply

SRB¹ -2-6-1



اهداف اصلی SRB عبارتند از: 1. کم کردن پیام‌های همه‌پخشی شده، و 2. ایجاد مسیر پایدار. در SRB گره‌های دریافت کننده به سه گروه تقسیم می‌شوند: گره‌های داخلی IN، گره‌های خارجی ON، گره‌های حلقه‌ی امن SRN.

گره‌های داخلی (IN) نزدیکترین گره‌ها به گره فرستنده، گره‌های خارجی (ON) دورترین گره‌ها از گره فرستنده و گره‌های حلقه‌ی امن (SRN) گره‌هایی در فاصله مناسبی از گره فرستنده قرار دارند، می‌باشند.

با استفاده از توان دریافتی در هر گره می‌توان گره‌ها را در این کلاس‌بندی قرار داد. پارامتر IBT را مقدار آستانه گره‌های داخلی و پارامتر OBT را مقدار آستانه گره‌های خارجی تعریف می‌کنیم. از آن جا که $rxdiff$ میزان توان دریافتی در هر گره می‌باشد، داریم: اگر $IBT < rxdiff$ آنگاه گره متعلق به گروه IN است. اگر $OBT < rxdiff$ آنگاه گره متعلق به گروه ON است. اگر $IBT < rxdiff < OBT$ آنگاه گره متعلق به گروه SRN است.

دو پارامتر SRB-P و SRB-C به این صورت تعریف می‌شوند: SRB-P تعداد گره‌های فرستنده یک درخواست - گره‌هایی با پیشینه متفاوت - به یک گره دیگر را در نظر می‌گیریم. در SRB-C گره دریافت کننده درخواست و دو گره فرستنده درخواست را در سه راس مثلث در نظر گرفته، سپس ارتفاع مثلث از طرف گره گیرنده (h_p) را محاسبه می‌کنیم.

شکل 8- a و b گره‌های فرستنده، p گره گیرنده

1-2-6-1- گره‌های حلقه‌ی امن (SRN)

گره‌های مربوط به گروه SRN برای rebroadcast کردن درخواست ترجیح داده می‌شوند.

SRB-P: اگر یک گره درخواست یکسانی از دو گره با پیشینه متفاوت در زمان مکث¹ دریافت کرد، آن گره درخواست را

رها می‌کند، در غیر این صورت درخواست را rebroadcast می‌کند.

SRB-C: اگر ارتفاع h_p کمتر از مقدار آستانه (50 متر) باشد، گره بسته را رها می‌کند، در غیر این صورت آن را

rebroadcast می‌کند.

1-2-6-2- گره‌های خارجی (ON)

اگر هیچ‌یک از گره‌های مربوط به گروه SRN درخواست را rebroadcast نکند، rebroadcast کردن آن به عهده گره

خارجی است.

SRB-P: اگر یک گره درخواست یکسان از سه گره با پیشینه متفاوت در زمان مکث دریافت کرد، آن گره درخواست را

رها می‌کند. اگر آن گره دوباره درخواست را دریافت کرد آن گره به اندازه زمان مکث منتظر می‌ماند، اگر همان گره برای سومین

بار درخواست را دریافت کرد آن گره درخواست را رها می‌کند.

SRB-C: ما تنها گره‌هایی که ارتفاع h_p آنها کمتر از مقدار آستانه (50m) است را در نظر می‌گیریم، اگر یک گره

درخواست یکسان از سه گره با پیشینه متفاوت در زمان مکث دریافت کرد، آن گره درخواست را رها می‌کند. اگر آن گره دوباره

درخواست را دریافت کرد آن گره به اندازه زمان مکث منتظر می‌ماند، اگر همان گره برای سومین بار درخواست را دریافت کرد

آن گره درخواست را رها می‌کند.

¹ holdtime

3-2-6-1- گره‌های داخلی (IN)

SRB-P: اگر یک گره درخواست یکسان از دو گره با پیشینه متفاوت در زمان مکث دریافت کرد، آن گره درخواست را رها می‌کند، در غیر این صورت آن را rebroadcast می‌کند.

SRB-C: اگر ارتفاع h_p آنها کمتر از مقدار آستانه (100m) باشد گره بسته را رها می‌کند، در غیر این صورت آن را rebroadcast می‌کند.

3-6-1- DRNS¹

در یک بزرگراه گره‌های انتخابی در حال حرکت در جهت مخالف، نقطه اصلی شکست می‌باشد. یک راه‌حل ممکن برای حل این مسئله استفاده از DRNS است. پردازش بسیار ساده، یک گره‌ای که درخواست دریافت می‌کند ابتدا چک می‌کند که آیا پرچم DRNS یک است، اگر جواب مثبت است چک می‌کند آیا جهت حرکت یکسان است، اگر جهت یکسان است گره درخواست را rebroadcast می‌کند، در غیر این صورت درخواست را رها می‌کند.

4-6-1- GVGrid²

GVGrid یک مسیر را براساس نیاز، از یک منبع (یک گره ثابت یا ایستگاه جاده‌ای) به یک خودرو متحرک یا ساکن ایجاد می‌کند. هدف اصلی GVGrid ایجاد یک مسیر پایدار برای خودرو متحرک و یک مسیر با کیفیت بالا است. در GVGrid ناحیه جغرافیایی را به نواحی مربعی با اندازه یکسان بخش‌بندی می‌کنند که به این نواحی «توری»³ گفته می‌شود و آن توری که شامل گره u است را با $G(u)$ نمایش می‌دهیم. هر بخش جاده‌ای⁴ یک streetID دارد. یک مسیر در یک شبکه network route نامیده می‌شود و یک مسیر در گراف جاده‌ای «مسیر رانندگی»⁵ نامیده می‌شود، جهت انتخاب گره‌های همسایه برای گره u به صورت زیر عمل می‌کنیم:

¹ Direct Route Node Select

² A QOS Routing for VANETs

³ grid

⁴ road segment

⁵ driving route

- یک گره روی بخش جاده‌ای مربوط به گره u ($road(u)$) یا روی بخش جاده‌ای همسایه (مثلاً e) اولویت دارد، چون که $road(u)$ و e در یک $street$ هستند.
 - یک گره روی بخش جاده‌ای همسایه $road(u)$ مثلاً e انتخاب می‌شود، هرچند که $road(u)$ و e در یک $street$ نیستند.
- در شکل زیر گره u در $grid11$ ، a را در $grid02$ و گره g را از $grid00$ بنا به راهکار 2 انتخاب می‌کند. گره b از $grid01$ بنا به راهکار 1 انتخاب می‌شود. در $grid01$ ، گره‌های b و c نسبت به گره‌های c و e اولویت دارند زیرا جهت‌شان با گره u یکسان است.
- روش به روز رسانی جدول مسیریابی و انتقال اطلاعات به شرح ذیل می‌باشد. گره s به عنوان فرستنده و گره d را به عنوان گیرنده اطلاعات در نظر می‌گیریم، ابتدا گره s همسایه‌هایش را شناسایی کرده سپس با ارسال $RREQ$ به آنها، گره‌های همسایه $RREQ$ را دریافت می‌کنند، اگر آن گره مقصد نهایی ارسال اطلاعات نباشد همان گره مجدداً $RREQ$ را rebroadcast می‌کند شماره $gridID$ خود را در پیام $RREQ$ ذخیره می‌کند و به این ترتیب پیام $RREQ$ اطلاعاتی از قبیل $gridID$ گره‌هایی که از آنها عبور کرده تا به مقصد رسیده است را شامل می‌شود، و گیرنده نهایی با بررسی $RREQ$ ‌هایی که از مسیرهای مختلف به آن رسیده کوتاه‌ترین مسیر را تشخیص داده و پیام $RREP$ را از همان مسیر به سوی گیرنده ارسال می‌کند. هدف اصلی $GVGrid$ فراهم کردن کیفیت بالای مسیر می‌باشد.
- QOS معمولاً به این صورت تعریف می‌شود:

- مدت پایداری مسیر
- نرخ دریافت بسته

1-6-5 DOLPHIN برای سیستم ارتباطی بین وسایل نقلیه^۱

در این پروتکل هر گره قبل از ارسال اطلاعات ابتدا وضعیت سیگنال حامل را چک می‌کند. پروتکل‌های MAC مربوطه

عبارتند از Non-Persistent CSMA و p-Persistent CSMA.

- Non-Persistent CSMA: اگر سیگنال حامل مشغول باشد، آنگاه گره به مدت زمان تصادفی منتظر

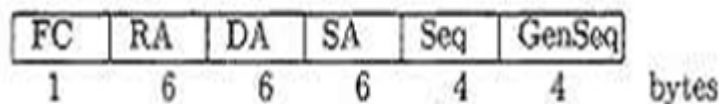
می‌ماند و مجدداً سیگنال حامل را چک می‌کند، چنانچه سیگنال حامل آزاد شد در این صورت گره شروع به ارسال اطلاعات می‌کند.

- P-Persistent CSMA: وقتی که یک گره آماده ارسال شد ابتدا سیگنال حامل را چک می‌کند، اگر

سیگنال حامل آزاد بود آن گره با احتمال p ارسال اطلاعات می‌کند و چنانچه سیگنال حامل، مشغول باشد به مدت زمان تصادفی منتظر می‌ماند، و مجدداً سیگنال حامل را چک می‌کند.

1-6-6 WTRP

WTRP پروتکلی است که برای شبکه‌های موردی استفاده می‌شود. WTRP یک پروتکل WirelessLAN است که به



وسیله‌ی «گذرگاه نشانه»^۲ با استاندارد IEEE 802.4 حمایت می‌شود.

یک ایستگاه فریم، نشانه^۳ را از سلف^۴ دریافت می‌کند و آن را به جانشین^۵ ارسال می‌کند. شکل فریم نشانه به صورت زیر

است:

¹ DOLPHIN for inter-vehicle communication system

² Tokenbus

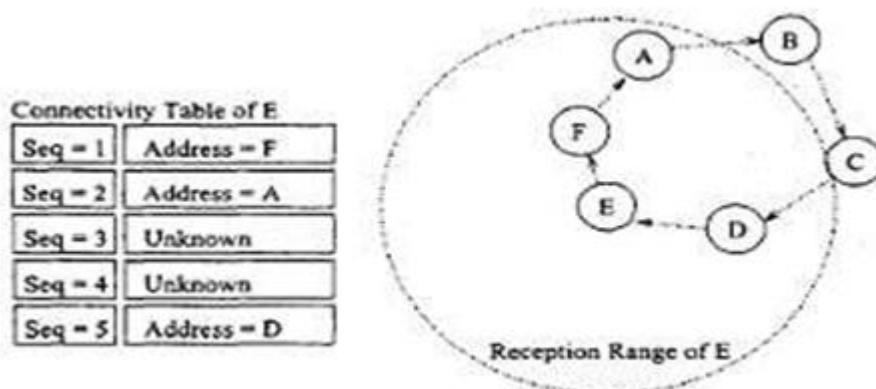
³ Token

⁴ predecessor

⁵ successor

FC: نوع بسته را معین می کند، SA: آدرس منبع را مشخص می کند، DA: آدرس مقصد را مشخص می کند، Seq: از صفر شروع شده و با عبور از هر ایستگاهی یک واحد به آن اضافه می شود، RA: به حلقه ای که نشانه متعلق به آن است اشاره می کند، GenSeq: از صفر شروع می شود و با یک دور کامل در حلقه توسط گره سازنده نشانه یک واحد به آن افزوده می شود. توجه شود که سازنده نشانه به عنوان مالک حلقه شناخته می شود.

در گره سازنده نشانه جدول اتصال ذخیره می شود و در این جدول اطلاعاتی راجع به گره های موجود در حلقه مربوطه و Seq هریک از آنها وجود دارد. با توجه به شکل گره E به عنوان سازنده نشانه آن را به گره F ارسال می کند و گره F هم با تغییر Seq به یک، آن را به گره A ارسال می کند و به همین ترتیب، حال اگر گره های B و C تحت شنود گره E قرار نداشته باشند، گره E با توجه به Seq می فهمد که دو گره تحت شنود نبوده ولی در حلقه قرار دارند.



شکل 9- جدول اتصال

هر ایستگاهی که سازنده نشانه است، تایمر Idle را تنظیم می کند. اگر نشانه در حلقه گم شد هیچ گونه پیام ACK در مدت زمان Idle به ایستگاه نرسیده و مدت زمان تایمر Idle به پایان می رسد و ایستگاه شروع به ارسال مجدد همان نشانه می کند. توجه شود که یک نشانه با GenSeq بالاتر دارای اولویت بالاتر است. مکانیزم بازیابی حلقه در این روش به این شکل است که وقتی گره ای متوجه شود که جانشین آن در دسترس نیست Set-Token PREDECESSOR را به گره اتصال بعدی ارسال می کند. مسئله دیگر اجازه ورود گره های دیگر به داخل حلقه در WTRP می باشد. با توجه به شکل 11 مدیریت کنترل ورود در ایستگاه B با ارسال یک SOLICIT-SUCCESSOR به بیرون، گره های دیگر را برای پیوستن به داخل حلقه دعوت می کند،

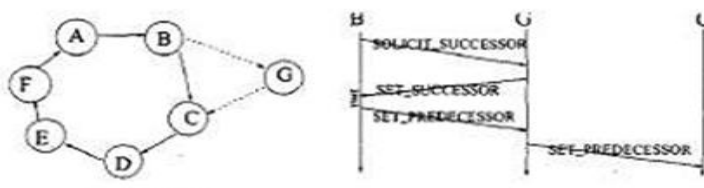
همچنین گره G پیام Set-SUCCESSOR Token را ارسال کرده و سپس گره B پیام Set-Token

PREDECESSOR را به گره G ارسال می کند و گره G پیام Set-PREDECESSOR را به گره C می فرستد. چنانچه در

شکل 12 نشان داده شده است، فرض کنید ایستگاه C می خواهد حلقه را ترک کند، بسته Set-SUCCESSOR همراه به

آدرس MAC مربوط به گره D را به گره B ارسال می کند. اگر D تحت شنود B قرار داشته باشد، گره B با ارسال Set-

PREDECESSOR با گره D اتصال برقرار می کند.



شکل 10- وارد شدن گره G به داخل حلقه



شکل 11- خروج گره C از داخل حلقه

استاندارد DSRC به هفت باند فرکانسی ده مگاهرتز تقسیم می شود. باند فرکانسی 178 برای کنترل باندهای فرکانسی دیگر

جهت اطمینان از ارتباطات امن روی شبکه به کار می رود. همچنین دو باند فرکانسی به ارسال و دریافت اطلاعات اختصاص داده

شده است. مؤسسه IEEE برای شبکه های VANET چهار استاندارد منتشر کرده است:

- (1) IEEE 1609: برای مدیریت منابع WAVE¹ مورد استفاده قرار می گیرد.
- (2) IEEE1609: استانداردهای امنیتی شبکه VANET را بیان می کند و شامل فرمت های پیغام ها، فرآیندها و تغییرات است.
- (3) IEEE1609: سرویس های مسیریابی و انتقال و نحوه استفاده از IPv6 را توضیح می دهد.
- (4) IEEE1609: مشخصات کانال ها روی استاندارد DSRC را مشخص می کند WAVE. از پروتکل تغییر یافته 802.11a به نام p802.11 برای لایه MAC استفاده می کند و از CSMA/CA به عنوان برنامه دسترسی رسانه انتقال سود می برد. در حقیقت، پروتکل p802.11 با استفاده از مدولاسیون FDM و در نظر گرفتن سرعت خودروها و جابه جایی سریع آنها، حداکثر محدوده پوشش دهی امواج رادیویی را مشخص کرده و یک دامنه چند کیلومتری را سیگنال دهی می کند.

1-7- کاربردها و ملزومات VANET

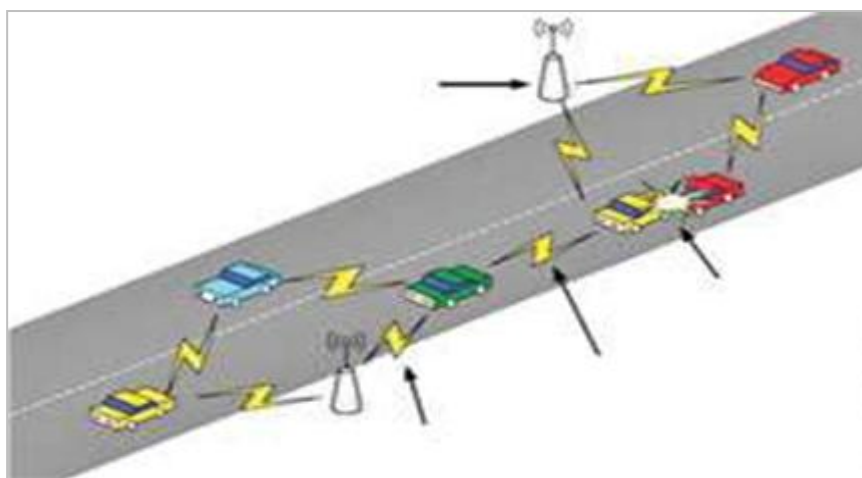
چرا شبکه های بین خودرویی VANET تا این اندازه اهمیت دارند؟ چه مزایا و معایبی نسبت به شبکه های سلولی و اختصاصی دارند که باعث شده تا به صورت جداگانه توسعه یابند و شرکت های خودروساز سرمایه گذاری های زیادی روی آن انجام دهند و کشورهایی مانند آمریکا از یک دهه پیش، استانداردها، پروتکل ها و مجوزهای لازم را تصویب و تعریف کند و از آنها در سیستم های هوشمند حمل و نقل کشورهای پیشرفته استفاده شود؟

«مهم ترین بخش شبکه VANET حسگرهایی هستند که باید در قسمت های مختلف خودرو به کار گرفته شوند و وضعیت خودرو و محیط خارجی را به راننده و کنترل کننده گزارش کنند یا به عکس، فرامین راننده یا اطلاعات دریافتی از خودروهای دیگر را اعمال کنند.»

قابلیت های ذاتی شبکه های موردی مانند برد کوتاه، سرعت زیاد در تشکیل شبکه و تغییر توپولوژی و انتقال یک سیگنال از مبدا به مقصد، بهترین کاربرد را برای ایمنی خودروها و مباحث ترافیکی ایجاد می کند. خودروها به سرعت و در کسری از ثانیه

¹ Wireless Access for Vehicular Environments

می‌توانند از یک حادثه در چند صد متری خود مطلع شده و تغییر مسیر دهند، ترافیک را تشخیص داده و از خودرو جلویی یا عقبی سوال و جواب کنند یا از وضعیت ترافیک خیابان یا کوچه‌های کناری و چهارراه پیش رو اطلاع یابند. شکل می‌تواند به خوبی این وضعیت را نشان دهد. وقتی یک اتفاق ناگهانی در خیابان یا جاده رخ می‌دهد، خودروهای جلویی یا عقبی به سرعت می‌توانند به یکدیگر خبر داده و همچنین با ارتباط‌گیری با ایستگاه‌های مرکزی به پلیس یا مدیریت ترافیک شهری خبر دهند. راننده‌ها با اطلاعاتی که از خودروهای اطراف به دست می‌آورند، می‌توانند تصمیم‌گیری‌های به مراتب مطمئن‌تر و بهتری داشته باشند و یک رانندگی ایمن و راحت‌تر و همراه با لذت را تجربه کنند. کاربردهای شبکه‌های VANET در شرایط بد آب‌وهوایی نمود بیشتری می‌یابد. در هوای ابری یا مه‌آلود خودروها با ارتباطات خود می‌توانند یکدیگر را راهنمایی کرده و مانع بروز حادثه شوند. در این شبکه‌ها از برنامه امنیتی ¹SVA برای هشدار دادن، کم کردن سرعت یا توقف خودرو، ²EEBL برای ترمز ناگهانی، ³RHCN برای هشدارهای مرکز کنترل ترافیک، ⁴PCN برای ارسال هشدارهای تصادف و ⁵CCW برای اعلام هشدار برخوردها استفاده می‌شود.



شکل 12- امنیت یکی از کاربردها و اهداف شبکه‌های VANET است

¹ Slow/Stop Vehicle Advisor

² Emergency Electronic Brake-Light

³ Road Hazard Control Notification

⁴ Post Crash Notification

⁵ Cooperative Collision Warning

در بخش ترافیکی نیز برنامه‌های CRN¹ برای هشدارهای ترافیکی، PAN (Parking Availability Notification) برای هشدارهای پارکینگ و TOLL برای پرداخت عوارض بدون توقف خودرو مورد استفاده قرار می‌گیرند. از نظر تجاری نیز شبکه‌های VANET کارکردهای جالبی می‌توانند داشته باشند. برنامه RVP/D² می‌تواند خودرو را براساس سلاقی و نیازهای راننده سفارشی‌سازی کند. موزیک دلخواه، اطلاعات عمومی شهری یا کانال‌های رادیویی، بازی و انواع سرگرمی‌های دیگر می‌توانند از طریق ایستگاه‌های مرکزی کنار جاده به راننده یا خودرو منتقل شوند. برنامه دیگری به نام SA³ می‌تواند انواع اطلاعات را مطابق نیاز راننده انتخاب کرده و در خودرو پخش کند. CMDD⁴ امکان دانلود انواع نقشه‌ها و اطلاعات جانبی دیگر برای مسیرها، مراکز فروشگاهی، فرودگاه، ایستگاه مترو، قطار دیگر مراکز موجود در طول مسیر را فراهم می‌کند RTVR⁵ نیز سرویس تجاری دیگری برای تماشای فیلم‌های ویدیویی است که می‌تواند روی بستر شبکه‌های بین خودرویی موردی به کار گرفته شود و مسائل تجاری آن مدنظر قرار گیرد. برنامه‌های دیگری نیز برای این شبکه‌ها ارائه یا تعریف شده است که در چند سال آینده شاهد استفاده از آنها در خودروها خواهیم بود.

پروژه‌ها و کنسرسیوم‌ها فهرست گسترده‌ای از کاربردها و ملزومات این فناوری را بررسی کرده‌اند. به طور کلی طبقه‌بندی این الزامات عبارتند از: امنیت، کارایی حمل‌ونقل، کاربردهای آماری و تفریحی.

این فناوری به عنوان زیرساختی است که می‌تواند از دو دید به آن نگاه کرد: قبل از حادثه و بعد از حادثه مثال‌هایی برای آنها عبارتند از:

- مساعی در هشدارهای تصادفات پیش رو؛ یعنی پرهیز از تصادفات دنباله‌دار
- چراغ ترافیکی راهنما برای تعیین سرعت مناسب، یعنی راهنمایی به راننده برای حرکت در یک وضعیت سبز
- عیب‌یابی از راه دور، یعنی ایجاد وضعیت دسترسی جهت عیب‌یابی از راه دور خودرو
- جمع‌آوری اطلاعات آماری، ایجاد پایگاه جامع اطلاعاتی، یافتن جاده‌ها و راه‌های حادثه خیز و...

¹ Congested Road Notification

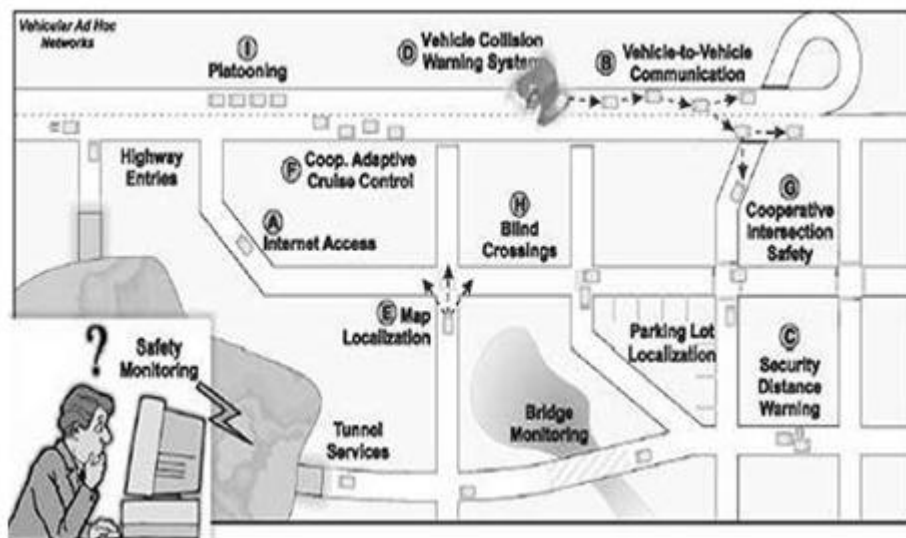
² Remote Vehicle Personalization/Diagnostics

³ Service Announcements

⁴ Content Map Database

⁵ Using Real Time Video Relay

- شبیه‌سازی صحنه تصادف و نحوه وقوع آن
- شبیه‌سازی سیستم ترافیکی
- شبیه‌سازی راندها راهبری
- رهگیری خودروهای مسروقه
- اطلاع‌آنی به شرکت بیمه‌گر، واحدهای امدادرسا، پلیس و نهادهای دیگر هنگام تصادف



شکل 13- برخی از کاربردهای VANET

میزان موفقیت کاربردها، از این نظر که آیا این ملزومات آنها می‌توانند فراهم شوند و تا چه اندازه‌ای می‌توانند پرسود باشند ارزیابی شده است. یکی از عوامل برجسته و ملزوم این فناوری میزان نفوذ مطلوب است تا عملکرد قابل قبول کاربردها را تحقق بخشد. به عنوان مثال نرخ خودروهایی که به فناوری VANET مجهز شده‌اند نسبت به خودروهای عادی بیشتر است.

ملزومات فنی مواردی از قبیل اندازه بسته‌ها، فرکانس‌های مطلوب یا دقت و تازگی اطلاعات، دامنه ارتباطات، محدودیت‌های تأخیر، سطوح امنیتی و زیرساخت‌های لازم را تعیین می‌نماید. از جنبه ارزش افزوده، کاربردها نسبت به میزان افزایش سطح امنیت یا افزایش کارایی حمل و نقل و یا میزان ارائه اطلاعات مطلوب سنجیده می‌شوند. ارزیابی کمی ارزش افزوده گمراه‌کننده است چرا که عوامل انسانی نیز در آن دخیل می‌شوند. به عنوان مثال؛ ثابت شده است که تشخیص دقیق ترافیک جاده‌ای کار بسیار مشکلی است، زیرا در این ارزیابی‌ها بایست حلقه بازخوردی مسئله یا چگونگی واکنش انسانی به این تشخیص‌ها را نیز در نظر گرفت.

برای کاربردهای امنیتی، کنسرسیوم ارتباطات امن خودرویی هشت کاربرد مهم بالقوه را تعیین کرده است:

- اختلالات تخطی از علائم ترافیکی
- اختلال سرعت در پیچ‌ها
- چراغ الکترونیکی ترمز اضطراری
- احساس پیش تصادف
- اختلالات تصادف پیشرو
- کمک کننده گردش به چپ
- اختلالات تغییر مسیر و راهنمایی علائم ایست متحرک

نکته این است که چهار کاربرد از این کاربردها مربوط به ارتباطات خودرو و چهار کاربرد دیگر مربوط به ارتباطات زیرساخت‌های جاده‌ای با خودرو است. ملزومات فنی اخذ شده نشانگر اهمیت بخش ارتباطات یک قدمی می‌باشد. منظور از ارتباطات یک قدمی این است که وقتی خودرویی بسته‌ای را ارسال می‌کند هر خودرویی که قادر به دریافت مستقیم آن بسته باشد همسایه یک قدمی آن منظور می‌شود. ارتباطات یک قدمی در دو حالت یکنواخت و تناوبی است. پیام‌های یکنواخت وقتی ارسال می‌شوند که یک موقعیت خطرناک، تشخیص داده شود.

پیام‌های متناوب خودروهای همسایه را به طور مؤثری آگاه می‌سازند؛ برای مثال موقعیت خودروی فرستنده پیام را نیز مشخص می‌نماید. VSC انتشار یک قدمی متناوب را پیشنهاد می‌کند؛ به عنوان مثال اختلالات تصادفات پیشرو تواتری از 10 پیام در هر ثانیه با حداکثر تأخیرها و حداقل برد 150 متر نیاز دارد. در ضمن مطالعات نشان می‌دهد در ترافیک‌های فشرده این پیام‌های متناوب می‌تواند بار زیادی بر کانال‌های رادیویی تحمیل کند. بنابراین قدرت انتقال سازگار و مکانیزم میزان کنترل به صورتی که در زیر بحث شده مورد نیاز است. کنسرسیوم ارتباطات خودرو به خودرو به عنوان نمونه به تجزیه و تحلیل بعضی کاربردهای مؤثر در حمل و نقل پرداخته است: مسیریابی و راهبری پیشرفته؛ راهنمایی حداکثر سرعت در چراغ سبز و راهنمایی ترکیب مسیر از آن جمله است، در حالی که زیرساخت‌های کنار جاده‌ای برای دو کاربرد اول (مسیریابی و راهبری پیشرفته) به عنوان پیش نیاز در نظر گرفته می‌شوند، راهنمایی ترکیب مسیرها مبنای ارتباطات خودرو با خودرو فرض می‌شود.

Car-to-car cc بر اهمیت سطوح معقولی از امنیت برای ایجاد اطمینان لازم برای گرفتن اطلاعات تأکید دارد. نظرات مختلف در مورد کاربردهای آماری و تفریحی از مجموعه نسبتاً متنوعی به قرار زیر تشکیل یافته است؛ اخذ عوارض، اعلان میزان بهره‌وری مدیریت مصرف سوخت، دستیابی چندگانه بی‌سیم به اینترنت. اخذ عوارض یکی از انگیزه‌های مهم برای ارتباطات خودروها با زیر ساخت‌ها است. این اطلاعات آماری از طریق پایگاه جامع اطلاعاتی خودروها قابل دستیابی است و زیرساخت‌های کنار جاده‌ای می‌توانند به وسیله آن کنترل به اعتبار بیمه‌نامه، وضعیت معاینه فنی خودرو، کاربری خودرو و اعتبارسنجی موارد دیگر اقدام کنند. به دلیل این تنوع کار باید یک تحلیل مورد به مورد درباره ملزومات و بهره‌وری صورت گیرد. درباره کاربردهای آماری و تفریحی بایستی این نکته مهم را در نظر گرفت که آیا کاربردهای امنیت ترافیکی و کاربردهای ضروری به خوبی پیاده شده‌اند و آیا می‌توان با استفاده از فناوری شبکه مقایسه‌ای مجزا این موارد را بهتر پیاده کرد.

1-7-1- کاربردهای ایمنی الکترونیکی

این کاربردها بین خودرو با خودرو و یا بین خودرو با تجهیزات کنار جاده‌ای برقرار می‌شود و شامل موارد زیر به صورت خلاصه می‌باشند.

هشدار تخلف ترافیکی، هشدار تخلف از علامت توقف، هشدارهای عمومی داخل وسیله نقلیه، راهنمای گردش به راست، هشدارهای تصادف چهارراه‌ها، اطلاعات در مورد عبور عابران، هشدارهای عبور خودروهای ضروری مانند امداد و آتش‌نشانی، معاینه فنی و گواهی الکترونیکی سالم بودن خودروها، آژیر سبز داخل خودرو به هنگام آسیب دیدن راننده، پی‌گرد خودروی سرقتی، آژیر خرابی خودرو و یا بالا بودن ترمز دستی، سرویس‌های پلیس جاده‌ای، سنسورهای احساس تصادف، ضبط وقایع، هشدار محدوده کاری برای کارگران در جاده، هشدار پیچ در جاده، چراغ ترمز الکترونیکی، هشدار سریع عوض کردن لاین سرعت، هشدار مسیر اشتباه پیمایشی راننده و هشدار وجود ریل راه آهن یا مواردی شبیه آن که در هر مورد هشدارها به صورت بوق یا چراغ یا آژیرهای خاصی به راننده اطلاع رسانی لازم را انجام می‌دهند.

همان‌طور که در شکل زیر ملاحظه می‌شود، سه خودرو زمانی که به تقاطع نزدیک می‌شوند توسط امکانات شبکه‌های بین خودرویی از خطر تصادف در تقاطع مطلع شده و سرعت خود را کاهش می‌دهند.

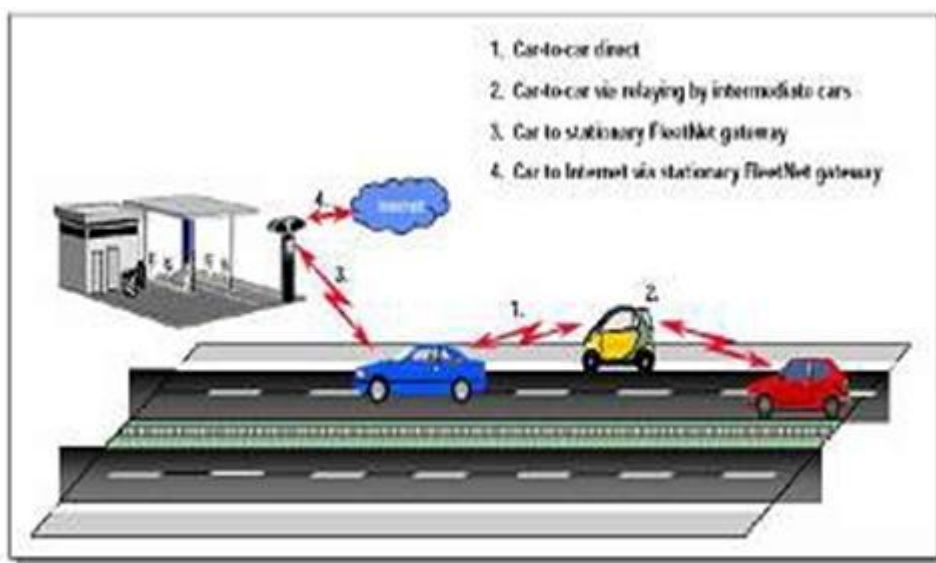


شکل 14- هشدار عبور از علامت توقف

1-7-2- کاربردهای رفاهی

این دسته از کاربردها به منظور بالا بردن میزان راحتی راننده و مسافران و بهبود کیفیت سفرها، مدنظر می‌باشند. نمونه‌ای از این کاربردها که از لحاظ تجاری قابل توجه بوده و در آینده امکان گسترش زیاد دارند عبارتند از: پیدا کردن کوتاه‌ترین مسیر به مقصد، گزارش هوا، اعلان وضعیت قیمت در فروشگاه‌ها، قیمت سوخت در ایستگاه‌های بین راهی، برقراری ارتباط اینترنت برای سرنشینان خودروها و باز کردن فایل‌های چند رسانه‌ای و ...

شکل زیر نمایی از پروژه FleetNet را می‌دهد که هدف آن برقراری ارتباط بین خودروها و درگاه‌های اینترنت کنار جاده‌ای است.



شکل 15- نمونه‌ای از کاربردهای رفاهی در (پروژه FleetNet)

1-7-3- کاربردهای مدیریت ترافیک

این کاربردها مستقیماً به جلوگیری از ترافیک و در نتیجه امنیت خیابان‌ها و جاده‌ها اشاره دارند و شامل موارد زیر هستند:

هشدار ادغام اتوبان، کنترل حرکت تطبیقی (مثلاً مطابق با مسیر اتوبان و بدون انحراف به راست یا چپ)، کنترل گروهی خودروها، مدیریت رانندگی در شرایط بحرانی نظیر مه، باران، ناشی بودن راننده، کنترل ترافیک هوشمند، سنسور کاوشگر در وسیله نقلیه برای بررسی وضعیت سطح جاده، مدیریت تصادفات، بررسی وضعیت مبداء و مقصد راننده، مدیریت سرعت، کنترل دسترسی ناحیه، پرداخت الکترونیکی عوارض، خدمات کرایه خودرو و ردیابی محموله مواد خطرناک که این هشدارها مستقیماً به اطلاع راننده می‌رسند.

1-7-4- کاربردهای نگهداری و تعمیر و خدمات جانبی برای آسایش راننده

این دسته از کاربردها به منظور بالا بردن میزان راحتی راننده و مسافران و بهبود کیفیت سفرها مدنظر می‌باشد. نمونه‌ای از این کاربردها عبارتند از: تعمیرات بلافاصله خودرو، تقویت دید راننده، کاهش تشعشعات آفتاب و استفاده از لامپ‌های خاص به هنگام تابش آفتاب، ردیابی مقصد و مدیریت رانندگی، مدیریت آسایش راننده، تصحیح اتوماتیک GPS، امکانات رد و بدل کردن پیغام بین دو راننده، امکانات استفاده از موبایل و اینترنت و تلویزیون، امکانات دسترسی به بعضی اطلاعات در مورد رانندگان و وسایل نقلیه دیگر.

در شکل زیر نمایی از یک اتومبیل مجهز به تجهیزات شبکه‌های بین خودرویی دیده می‌شود. شرکت ولوو در نظر دارد خودرویی به سیستم اجتناب از تصادف را وارد بازار کند. این سیستم با به کارگیری یک سیستم نوری راداری تا فاصله‌ی 6 متری جلوی خودرو را تحت پوشش قرار خواهد داد اگر خودروی جلویی به صورت ناگهانی ترمز نموده یا بایستد، این سیستم به منظور کمک به راننده به صورت خودکار ترمزها را آماده می‌کند تا وی بتواند با کاهش سرعت یا تغییر مسیر از تصادف پیشگیری کند ولی اگر وقوع تصادف حتمی باشد، سیستم به صورت خودکار ترمزها را فعال خواهد کرد.



شکل 16- نمایی از خودروهای کمک‌یار راننده شرکت ولوو

1-8- مهمترین زیر سیستم‌های مرتبط با پیشگیری از تصادفات و برخی محصولات تجاری

این زیرسیستم‌ها از شبکه‌های بین خودرویی به همراه دوربین و رادار استفاده می‌نمایند و در سه دسته قابل تقسیم‌بندی می‌باشند.

1-8-1- سیستم‌های پیشگیری از تصادفات در چهارراه‌ها و تصادفات جلو به عقب

شاید بتوان گفت هدف غائی بسیاری از تحقیقات انجام شده مرتبط با ترافیک پیشگیری از تصادفات با کاهش شدت آن است.

مسئله پیشگیری از تصادف در مقالات از زوایای مختلف مورد توجه قرار گرفته است.

مهم‌ترین دسته‌بندی از نظر مکان امکان وقوع تصادف اتوبان‌ها، جاده‌ها و تقاطع‌ها و از نظر نوع تصادف شامل تصادفات جلو به

عقب می‌باشند. در این زمینه علاوه بر تحقیقات آکادمیک، شاهد محصولات تجاری مانند MOBILEEYE هستیم که تلاش

اصلی محققین در این زمینه تخمین زمان مانده به برخورد 1(TTC) می‌باشد. شکل زیر یک نمونه از این محصول را نشان می‌دهد

که در هنگام کاهش ناگهانی فاصله با خودرو جلویی با دادن اخطار صوتی و تصویری به راننده وی را از خطر قریب الوقوع آگاه

ساخته است.



شکل 17- محاسبه زمان برخورد توسط MobileEYE

1-8-2- سیستم‌های هشدار انحراف از خط

رانندگی در بین خطوط، اجتناب از ورود به لاین دیگر و خروج از جاده از جمله مهم‌ترین پارامترهای رانندگی مطمئن هستند. 60 درصد تصادفات به علت انحراف غیرعمدی از خط رخ می‌دهند. هدف این سیستم‌ها شناسایی و ردگیری خطوط میانی و کناری جاده و هشدار به راننده جهت برگشت به وضعیت درست می‌باشد.

اخیراً مدل‌هایی از مرسدس، نیسان و سیترون با این توانایی‌ها و کیت‌های تجاری قابل نصب بر روی خودروها به بازار آمده‌اند. عمده کارهای انجام شده در این زمینه مبتنی بر بینایی خودرو می‌باشد. عموماً حسگر مورد استفاده دوربینی است که در پشت آینه شیشه جلوی خودرو نصب می‌گردد. معیار اصلی مورد استفاده در بیشتر مقالات زمان مانده تا برخورد با خط می‌باشد که با به دست آوردن نقاط مشترک مسیر خودرو و مدل خط تخمین زده می‌شود؛ اما محاسبه آن به دلیل مواردی مانند سرعت غیر خطی خودرو، زاویه‌ی خودرو و انحنای جاده بسیار مشکل می‌باشد. در نمونه‌های انجام شده معمولاً پارامتر حساسیت قابل کنترلی در سیستم لحاظ می‌شود که راننده توسط آن می‌تواند شدت حساسیت سیستم را تغییر دهد. در این زمینه شاهد استفاده از محصولاتی مانند MobileYE و ADAS هستیم. برخی از محصولات با استفاده از دوربین‌های دید در شب، توانایی عمل در شب را هم دارند. محصولات تولید شده که عمدتاً قابلیت عمل در شرایط جوی مختلف را دارا می‌باشند، عموماً از یک سیگنال صوتی شبیه به صدای ناشی از حرکت خودرو بر روی خطوط برجسته برای اخطار به راننده بهره می‌برند. شکل زیر رانندگی در شرایط مه‌آلود با

از تجهیزات شبکه‌های بین خودرویی را نشان می‌دهد.

شکل 18- رانندگی در مه توسط تجهیزات شبکه‌های بین خودرویی



1-8-3- سیستم‌های شناسایی موانع

عکس العمل ناگهانی یا دیر هنگام رانندگان در برخورد با یک مانع در جاده علت اصلی بسیاری از تصادفات بوده است. هدف در این مرحله شناسایی موانع موجود در جاده به منظور هشدار زودتر به راننده می‌باشد و به واقع چنین سیستم‌های کمکی، در افزایش توان دید راننده نقش مؤثری ایفا می‌نمایند. نگاهی به مقالات منتشر شده در زمینه شناسایی موانع موجود در جاده، روشن می‌سازد که مؤلفین، سایر وسایل نقلیه، عابر پیاده، علائم ترافیکی، تکه سنگ بزرگ، جعبه و تایلر موجود در سطح یا کنار جاده را به عنوان مانع قلمداد نموده‌اند.

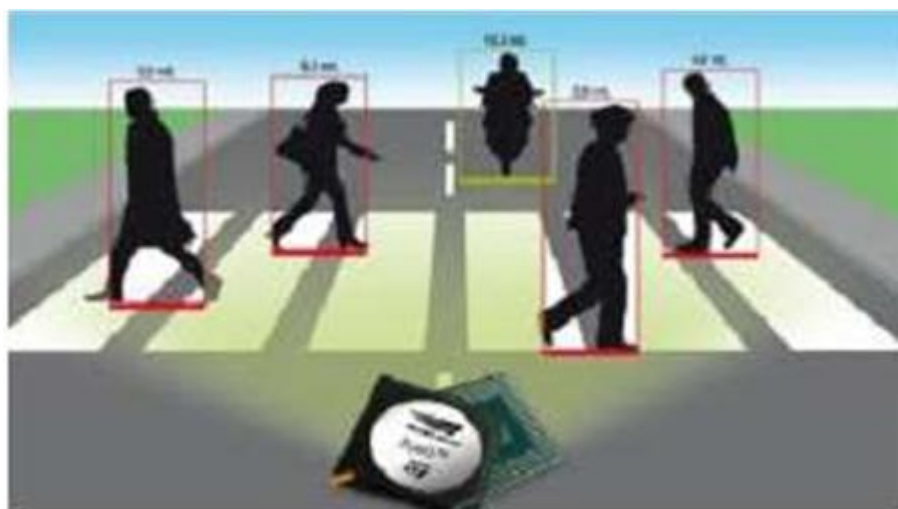
تحقیقات ذکر شده مبتنی بر دید استریو و استفاده از یک و سه دوربین می‌باشند. در دید با یک دوربین مواردی از قبیل اندازه مانع، پارامترهای دوربین و اطلاعاتی از جاده معلوم فرض می‌شوند ولی در دید استریو این موارد به صورت خودکار استخراج می‌شوند. تشخیص اشیاء ثابت مشکلات بیشتری نسبت به اشیاء متحرک دارد. برای اشیاء کوچک در حدود 15 سانتی‌متر ارتفاع و در فواصل دور در حدود 100 متر، رادار مناسب نیست؛ رادار در مواجهه با اجسام غیرفلزی مانند چوب، سیمان و حیوان مشکلاتی دارد. شکل زیر محیط حرکت خودرو را با استفاده از سیستم تشخیص موقع نشان می‌دهد که قسمت‌های مختلف جاده، موانع و

خودروها همگی داخل کادرهای سبزرنگ قرار می‌گیرند و به راننده اطلاع‌رسانی می‌نمایند.



شکل 19- نمای جاده با استفاده از تجهیزات شناسایی موانع

همچنین در شکل نمایی از یک خیابان با استفاده از محصولات MobileYE را نشان می‌دهد که فاصله خودرو با عابران پیاده سنجیده می‌شود و عابران نزدیکتر داخل کادر قرمز و عابران دورتر داخل کادر سبز رنگ قرار می‌گیرند.



شکل 20- نمایی از نحوه محاسبه خودرو تا عابران پیاده

9-1- اجزای شبکه‌های VANET

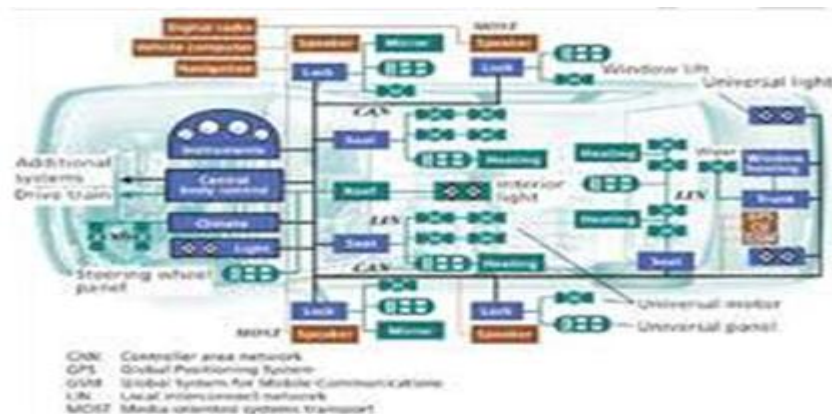
یک خودرو برای اضافه شدن به یک شبکه VANET به یک گیرنده/فرستنده سیگنال‌ها و اطلاعات (همانند کارت شبکه بی‌سیم) و یک دستگاه کنترل کننده شامل یک تراشه مرکزی نیاز دارد. همان‌طور که گفتیم، پروتکل اصلی شبکه بین خودرویی موردی، DSRC و پروتکل ارتباطی 802.11p است. همچنین محدوده پوشش‌دهی این تجهیزات باید از سی صد متر تا چند کیلومتر (در جدیدترین طرح‌ها صحبت از دو الی سه کیلومتر است) باشد.

ایستگاه‌ها و آنتن‌های کنار جاده با اتصال به اینترنت و شبکه ترافیک شهری، اطلاعات را با دستگاه بی‌سیم خودرو رد و بدل می‌کنند. در حقیقت، مهم‌ترین بخش شبکه VANET حسگرهایی هستند که باید در قسمت‌های مختلف خودرو به کار گرفته شوند و وضعیت خودرو و محیط خارجی را به راننده و کنترل کننده گزارش کنند یا به عکس، فرامین راننده یا اطلاعات دریافتی از خودروهای دیگر را اعمال کنند. حسگرها در VANET به دو نوع تقسیم می‌شوند: حسگرهای خود مختار و سنسورهای مشارکت کننده. حسگرهای خودمختار شامل حسگرهای ¹ART برای سنجش محدوده رادیویی و ارتباط خودرو با دیگر نودهای شبکه ²MGT برای سنجش حداکثر سرعتی که راننده می‌تواند داشته باشد و هنوز در شبکه باقی بماند، ³MDT برای تشخیص خودروهایی که به طور فیزیکی در شبکه وجود دارند (این حسگرها برای مقابله با حملات Sybil کاربرد دارد) و حسگرهای دیگری برای شناسایی وضعیت خودرو در نقشه و تعیین فاصله با خودروهای جلویی و عقبی هستند. حسگرهای مشارکت کننده برای اعلام تغییر وضعیت خودروهای همسایه، رسیدن به یک مکان خاص، دریافت اطلاعات مورد نیاز راننده و غیره کاربرد دارند.

¹ Acceptance Range Threshold

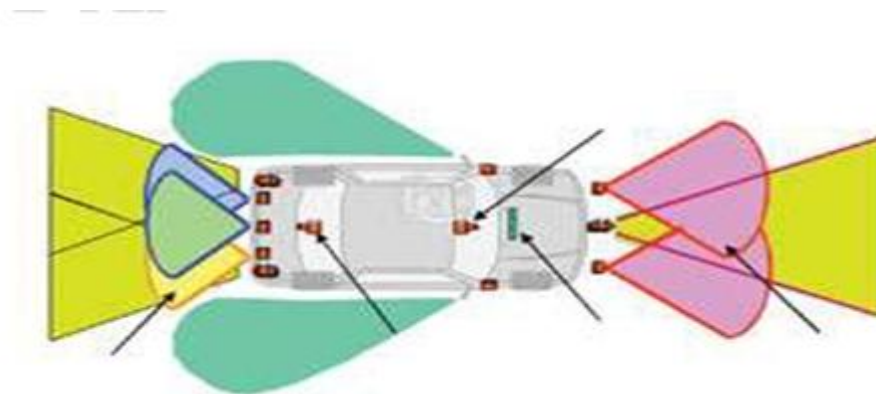
² Mobility Grade Threshold

³ Maximum Density Threshold



شکل 21- نمایی شماتیک از حسگرهای شبکه VANET

شکل 23- محدوده‌های تحت پوشش سنسورهای شبکه‌های VANET



شکل 22- محدوده‌های تحت پوشش سنسورهای شبکه‌های VANET

10-1- چالش‌های شبکه‌های VANET

نخستین و بزرگ‌ترین چالش شبکه‌های بین خودرویی موردی، امنیت آنها است. به راحتی می‌توان تصور کرد که اگر کوچک‌ترین تهدیدی متوجه این گونه شبکه‌ها شود چه عواقب ناگوار جانی و مالی به دنبال خواهد داشت و برخلاف اینترنت یا

وب، سلامت و جان انسان‌ها به طور مستقیم در معرض خطر قرار می‌گیرد. کافی است شبکه VANET اطلاعات دقیقی به راننده ندهد تا شاهد تصادف و واژگونی و ده‌ها رخداد دیگر باشیم.

همچنین کوچک‌ترین اشتباه یا اخلاف در برنامه‌ها یا حسگرهای درون خودرو می‌تواند نتایج خطرناکی به دنبال داشته باشد.

«شبکه‌های «بین خودرویی موردی» می‌توانند بزرگ‌ترین فناوری متحول کننده خودروها در دهه دوم هزاره دوم باشند و امنیت را به رانندگان هدیه کنند.»

مسئله امنیت در شبکه‌های VANET آن‌قدر حساس و بحرانی است که یکی از عوامل اجرایی نشدن این شبکه‌ها در سال‌های گذشته محسوب می‌شود. انواع راه‌کارهای مبتنی بر رمزنگاری اطلاعات بین خودروها، ایزوله کردن شبکه و استفاده از مکانیزم‌های احراز هویت برای خودروهای جدیدی که می‌خواهند وارد شبکه شوند، طراحی برنامه‌های اختصاصی اعتبارسنجی مانند ELP، VPKI و به کارگیری سخت‌افزارهایی با قابلیت اطمینان 99.99 درصد و ده‌ها طرح دیگر، برخی از کارهای صورت گرفته برای امن کردن شبکه‌های VANET است. به غیر از امنیت، مسیریابی اطلاعات و ارتباط میان خودروها با سرعت بالا چالش بعدی است. به علت نبود یک نود مرکزی، یک خودرو برای ارتباط با خودروی دیگری که به طور مستقیم امکان ارسال و دریافت اطلاعات را ندارد، باید از خودروهای میانی استفاده کند و چون سرعت در این شبکه‌ها یک فاکتور بسیار حیاتی است، الگوریتم مسیریابی اهمیت دو چندانی پیدا می‌کند. استفاده از سیگنال‌های چندگانه، مکانیزم‌های تشخیص حضور و محو شدن خودروها در یک شبکه، پشتیبانی شرکت‌های خودروساز از استانداردها و پروتکل‌ها و ارتباط میان حسگرها از دیگر چالش‌های شبکه‌های VANET است.

1-10-1- چالش‌های فنی و مکان‌یابی در VANET

برخی از کاربردهایی که می‌توان برای VANET مجسم کرد در تعدادی از خودروهایی که اخیراً طراحی شده‌اند محقق شده است. بعضی از این کاربردها بدین قرار می‌باشند:

- اختطار تصادفات خودروها
- اختطار فاصله امن
- مشارکت در رانندگی

- مشارکت در کنترل سرعت مناسب اتومبیل
- پخش اطلاعات جاده‌ای
- دستیابی به اینترنت
- پارک خودکار اتومبیل
- خودروهای بدون راننده

تمامی این کاربردها ملزم به بهره‌گیری به یک سری فناوری‌های مکان‌یابی می‌باشند. VANET با ورود به مراحل حساس‌تر هرچه بیشتر متکی به سیستم‌های مکان‌یابی می‌شود. در مسئله مکان‌یابی تعریف سیستم مرجع با مشخصات مکان فیزیکی گره‌ها یا نحوه استقرار فضایی آنها نسبت به همدیگر صورت می‌پذیرد. منظور از مکان فیزیکی طول جغرافیایی و ارتفاع است، به عنوان مثال مکان‌یابی جغرافیایی از طریق سیستم موقعیت‌یاب جهانی (GPS) با استفاده از سیستم اطلاعات جغرافیایی انجام می‌شود. در سیستم‌های اخطار تصادفات خودروها، اطلاعات جغرافیایی با میزان فاصله گره‌ها از همدیگر تلفیق می‌شوند.

با این وجود GPS مشکلات نامطلوبی را از خود نشان داده است، از جمله این مشکلات این است که GPS همواره در دسترس نیست و در برخی کاربردها قدرت لازم را از خود نشان نمی‌دهد. برای فائق آمدن بر محدودیت‌های GPS اخیراً برخی فناوری‌های مکان‌یابی مثل: Dead Reckoning Cellular Localization, image/Video Localization مورد استفاده شده است.

ارتباطات بین خودروها یا خودرو با ساختارهای کنار جاده‌ای از طریق کانال‌های رادیویی همانند شبکه‌های سیار پی سیم است. ساختار شبکه‌های موقت به گونه‌ای است که فاقد هماهنگی کننده ارتباطات مرکزی می‌باشد و این چالش‌های اساسی VANET است. از آنجا که نمی‌توان هیچ هماهنگی کننده مرکزی یا توافق نامه‌ای را فرض نمود؛ بنابراین پردازش پیام ضروری است. از چالش‌های دیگر می‌توان به شبکه‌های نقشه‌یاب سیار مبتنی بر حرکت خودروها و تأثیر محیطی بر روی تکثیر کانال‌های رادیویی نام برد.

1-10-2- چالش‌های VANET از منظر اجتماعی و اقتصادی

معرفی به بازار مشکلات مؤثر VANET است. در کل ارزش افزوده برای هر مشتری بستگی به تعداد مشتریانی دارد که خودروی خود را به فناوری VANET مجهز کرده‌اند. بنابراین مسئله اساسی چگونگی متقاعد کردن استفاده‌کنندگان اولیه برای خرید تجهیزات این فناوری برای خودروهایشان است. راهکارهای متفاوتی از جمله اجبار قانونی، تخفیف در حق بیمه خودرو، فراهم کردن کاربردهای جذاب و راهکارهای دیگر مورد بحث محققان قرار گرفته است. به طور کلی ممکن است برخی از زیرساخت‌های کنار جاده‌ای برای مشتریان اولیه مفید واقع شود. با این حال با توجه به زیرساخت‌های کنار جاده‌ای و مدیریت فناوری اطلاعات، خیلی از جوامع مختلف و گردانندگان جاده‌ای را تحت تأثیر قرار خواهد داد.

البته برقرار کردن تعادل بین امنیت و حریم خصوصی چالش‌های دیگری است و باید گفت وجود چنین اعتمادی با حریم خصوصی فرستنده در تناقض است.

فصل دوم-روش های جلوگیری از تصادف خودروی مبتنی بر VANET

2-1- مقدمه

روزانه حدود 16000 انسان در سرتاسر دنیا در اثر انواع جراحات جان خود را از دست می دهند. دلیل شایع مرگ و دلیل اصلی مرگ در سنین 1-40 سال، آسیب هایی هستند که به طور عمده در تصادفات جاده ای رخ می دهد و مطابق با داده های سازمان بهداشت جهانی، مرگ های جاده ای حدود 25 درصد کل مرگ های ناشی از جراحات ها است. یکی از مهم ترین آمارهای مورد توافق در مورد تصادفات و آسیب ها، نقش 70-90 درصدی عوامل انسانی در کلیه تصادفات است.

اولین بار در سال 1769 میلادی نیکولاس جوزف کاگنات اولین خودرو مکانیکی متحرک به نام «واگن بخار» را ساخت. اولین تصادف در سال 1771 میلادی بود که آقای کاگنات خودروی بخار خود را به یک دیوار آجری کوبید! و نخستین تصادف رانندگی در ایران در سال 1305 شمسی میان اتومبیل مظفرالدین شاه و درشکه درویش خان نوازنده در خیابان سپه تهران اتفاق افتاد.

در دنیا نخستین انسانی که در یک حادثه رانندگی جان خود را از دست داد، یک خانم انگلیسی بود. بریجیت درسکول 44 ساله اولین کسی در دنیا است که در یک سانحه رانندگی جان خود را از دست داده است. وی روز هفدهم آگوست سال 1896 در میدان کریستال پالاس لندن بر اثر تصادف فوت کرد.

میزان بالای تصادفات جاده‌ای در کشورهای مختلف حاکی از حساسیت بسیار زیاد این شیوه‌ی حمل و نقل است. در کشورهای توسعه‌یافته به رغم برنامه‌ریزی‌ها و سرمایه‌گذاری‌های گوناگونی که در جهت کاهش این گونه تصادفات به عمل آمده، بالاترین درصد مرگ و میر و جراحات و ضایعات انسانی متعلق به این بخش است.

طبق گزارشات سال 2004 اداره آمار ایالت متحده، تصادفات جاده‌ای، منجر به 230/6 میلیارد دلار خسارت مالی، 33471 کشته و 2697000 مجروح، شده است. نکته جالب در آمار ارائه شده این است که خسارت مالی به بار آمده به تنهایی 2/3 درصد از کل تولید ناخالصی ملی آمریکا می‌باشد. و طبق گزارش اداره کل معاونت راهنمایی و رانندگی کشور ایران، به عنوان مثال فقط در سال 1385 شمسی حدود 27500 نفر کشته و 1863000 نفر مجروح و در کنار این‌ها باعث 160 میلیارد دلار خسارت مالی ناشی از حوادث جاده‌ای درون‌شهری و برون‌شهری شده است.

شکل شماره 24، عوامل دخیل تصادفات جاده‌ای را نشان می‌دهد؛ این عوامل با تأثیرات متقابل بر یکدیگر در وقوع تصادفات مؤثر می‌باشند و اگر یکی از این عوامل دچار ناپایداری شود، این چرخه دچار تزلزل شده و تشدید این ناپایداری باعث وقوع تصادفات می‌شود.

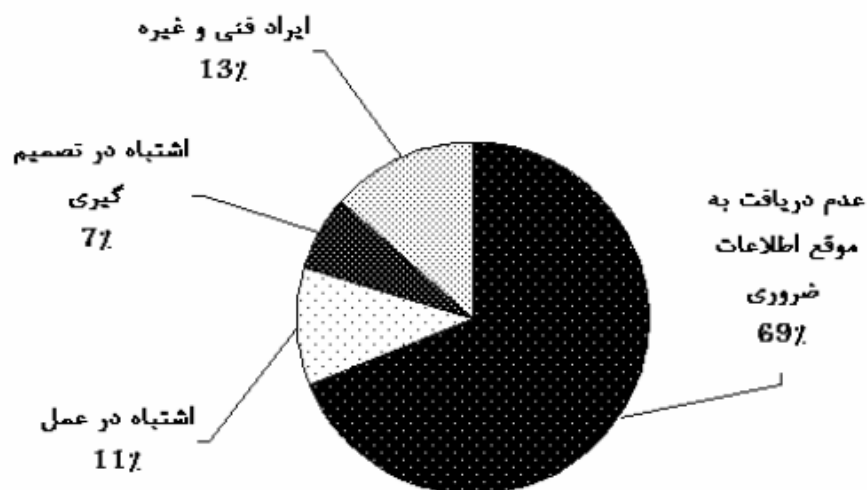


شکل 23- عوامل موثر بر تصادفات

آمار بالای خسارت موجب شده است در مورد مسأله «ایمنی وسایل نقلیه» خودروسازان و مدیران امور حمل و نقل جاده‌ای برای بهبود کیفی محصولات خود، سیستم‌هایی را به آن‌ها اضافه کنند که به طرز چشمگیری آمار کشته‌ها و زخمی‌های ناشی از سوانح رانندگی را کاهش داده است. به طور مثال هنری فورد در سال 1913 میلادی اولین لاین برای اتومبیل‌ها را ساخت و در سال 1927 حدود 15 میلیون لاین ساخته شدند. در 1956 اولین وسایل ایمنی، کمربند ایمنی، برای خودروهای شرکت فورد ساخته شد و در همین 1978 ترمزهای ABS در مرسدس بنز ساخته شد.

همین امر باعث شده است که پروژه‌ها و تحقیقات وسیعی در کشورهای مختلف انجام شود از آن جمله می‌توان کنسرسیوم امنیت حمل و نقل جاده‌ای VSCC در ایالت متحده، کنسرسیوم Internet ITS در ژاپن، C2C – CC در اتحادیه اروپا و ReVENT و OW در آلمان را نام برد.

پس از تحقیقات فراوان در کشورهای مختلف، در مورد عوامل مؤثر در تصادفات، نتایج همگی بر یک عامل به عنوان عامل اصلی تصادفات اتفاق نظر دارند. این عامل همان گونه که در شکل شماره 25 نشان داده شده است، خطای اطلاعاتی می باشد.



شکل 24- عوامل مؤثر در تصادفات با ذکر درجه اهمیت

به بیان دیگر راننده به علت اینکه اطلاعات ضروری را دریافت نکرده و یا دیر دریافت می کند، نمی تواند عکس العمل مناسب را برای جلوگیری از تصادفات اتخاذ نماید. در نتیجه به نظر می رسد اگر بتواند سطح اطلاعات راننده از محیط اطراف و همچنین محدوده اطلاعاتی او را گسترش داد، تحول شگرفی در ایمنی حمل و نقل به وجود می آید.

در همین راستا تلاش فراوانی صورت گرفته است. در سال 1999 میلادی، کمیسیون ارتباطات فدرال ایالات متحده پهنای باند لازم برای ارتباطات بی سیم بین خودرویی و ارتباط خودروها با ایستگاه های ثابت کنار جاده ای را اختصاص داد. تقسیم بندی شبکه های بین خودرویی می تواند براساس زیرساخت شبکه باشد. در این نوع تقسیم بندی سه نوع شبکه کلی به شرح زیر داریم:

- 1) شبکه بین خودرویی با استفاده از زیرساخت های اختصاصی
- 2) شبکه بین خودرویی با استفاده از شبکه های سلولی
- 3) شبکه بین خودرویی با استفاده از ارتباطات مستقیم بین خودرویی

2-2- بررسی چند مورد از جنبه‌های خاص VANET

1) در این شبکه‌ها محدودیت توان وجود ندارد. برخلاف اکثر شبکه‌های متعارف و مخصوصاً شبکه‌های حسگر که محدودیت انرژی دارند، شبکه‌های بین خودرویی، به علت این که متکی به انرژی نامحدود باتری خودرو می‌باشند، چنین محدودیتی ندارند.

2) این شبکه‌ها به صورت بالقوه مقیاس وسیع دارند. معمولاً، شبکه‌های موردی عمومی برای مقیاس کوچک و متوسط بررسی می‌گردند. با این وجود، شبکه‌های بین خودرویی در حالت کلی می‌توانند به بزرگی شبکه جاده‌ای باشند و تعداد زیاد خودروها باعث ایجاد شبکه‌ای در مقیاس وسیع از آنها می‌گردد.

3) شبکه موردی بین خودروها (VANET) دارای قطر شبکه بسیار کمتری نسبت به شبکه‌های عمومی هستند. با توجه به سرعت بالا شکل جغرافیایی این شبکه‌ها، طول مسیرهای انتها به انتهای قابل برقراری، بسیار کوچک و معمولاً در حدود چند گام است.

4) توپولوژی شبکه ارتباط زیادی به رفتار راننده دارد. پروتکل مطرح شده در VANET که سعی در برقراری امنیت مسیریابی دارند، عبارتند از: WTRP, AODV, SRB, DRNS, GVGrid, DOLPHIN. این امر در شبکه موردی عمومی، موضوعیت ندارد. این رفتار باید به نحوی از طریق سیستم‌های داخل خودرو استخراج شده و به خودروهای همسایه ارسال گردد. خاصیت جالب دیگر این است که محتویات پیام‌ها نیز می‌تواند باعث تغییر توپولوژی گردد. در نتیجه این نوع شبکه‌ها به سرعت می‌توانند تغییر توپولوژی داده، انعطاف پذیری زیادی ایجاد کنند.

2-3- کاربردهای VANET

پروژه‌ها و کنسرسیوم‌ها فهرست گسترده‌ای از کاربردهای این فناوری را بررسی کرده‌اند. به طور کلی طبقه‌بندی این کاربردها عبارتند از: امنیت، کارایی حمل و نقل، کاربردهای آماری و تفریحی.

2-3-1- امنیت

در کاربردهای ایمنی، هدف بالا بردن ضریب امنیت مسافران در جاده‌ها است. برای کاربردهای امنیتی، کنسرسیوم ارتباطات امن خودرویی (VSC) هشت کاربرد مهم بالقوه را تعیین کرده است: اخطارهای تخطی از علائم ترافیکی، اخطار سرعت در پیچ‌ها، چراغ الکترونیکی ترمز اضطراری، سنسورهای احساس تصادف، اخطارهای تصادف پیش‌رو، کمک‌کننده گردش به چپ، اخطارهای تغییر مسیر، راهنمای علائم ایست متحرک.

2-3-2- کارایی حمل و نقل

در این مورد از کاربردها، هدف افزایش کیفیت مسافرت‌ها است. کارایی حمل و نقل به طور کلی شامل کاربردهای مدیریت ترافیک و کاربردهای خدمات جانبی برای آسایش راننده می‌شود.

کاربردهای مدیریت ترافیک: این کاربردها مستقیماً به جلوگیری از ترافیک و در نتیجه امنیت خیابان‌ها و جاده‌ها اشاره دارند و شامل موارد زیر هستند:

هشدار ادغام اتوبان، کنترل حرکت تطبیقی (مثلاً مطابق با مسیر اتوبان و بدون انحراف به راست یا چپ)، کنترل گروهی خودروها، مدیریت رانندگی در شرایط بحرانی (نظیر مه، باران و ناشی بودن راننده)، کنترل ترافیک هوشمند، سنسور کاوشگر در وسیله نقلیه برای بررسی وضعیت سطح جاده، مدیریت تصادفات، بررسی وضعیت مبدأ و مقصد راننده، مدیریت سرعت، کنترل دسترسی ناحیه و غیره که هر یک از این موارد به روش خاص خود به اطلاع راننده می‌رسند.

نمونه ای از کاربردهای خدمات جانبی برای آسایش راننده عبارتند از: تقویت دید راننده، کاهش تشعشعات آفتاب و استفاده از لامپ‌های خاص به هنگام تابش آفتاب، تصحیح اتوماتیک GPS، امکانات رد و بدل کردن پیغام بین دو راننده و غیره.

2-3-3- کاربردهای آماری و تفریحی

این کاربردها به منظور بالا بردن میزان راحتی و در اختیار گذاشتن سرویس‌های رفاهی برای راننده و سرنشینان مدنظر می‌باشند.

نمونه‌هایی از این کاربردها که از لحاظ تجاری قابل توجه می‌باشند و در آینده امکان گسترش زیادی دارند عبارتند از: گزارش هوا،

ارتباط اینترنت برای سرنشینان ماشین، بررسی وضعیت امکانات رفاهی پایانه‌های بین شهری، اطلاع‌رسانی قیمت سوخت در ایستگاه‌های بین راهی و بار کردن اطلاعات اینترنتی مانند موزیک‌ها و فیلم‌ها.

2-4- مروری بر تحقیقات انجام گرفته و برخی محصولات تجاری

2-4-1- سیستم پیشگیری از تصادفات

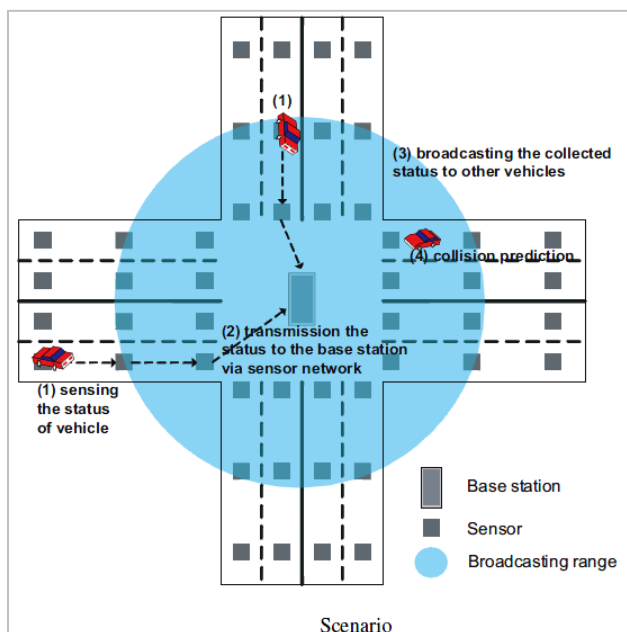
شاید بتوان گفت هدف غائی بسیاری از تحقیقات انجام شده مرتبط با ترافیک، پیشگیری از تصادفات یا کاهش شدت آن می‌باشد. مسأله پیشگیری از تصادف، در مقالات از زوایای مختلفی مورد توجه قرار گرفته است. مهم‌ترین دسته‌بندی‌ها از نظر محل امکان وقوع تصادف، شامل اتوبان‌ها، جاده‌ها و تقاطع‌ها و از نظر تصادف شامل جلو به عقب است.

شایع‌ترین انواع تصادفات جلو به عقب است. بر طبق اطلاعات آماری 60 درصد این تصادفات در صورتی که راننده نیم ثانیه زودتر هشدار دریافت کند و 90 درصد آن در صورتی که راننده 1/5 ثانیه زودتر آگاه شود، قابل پیشگیری هستند. محصول تجاری MobilEye در هنگام کاهش ناگهانی فاصله با ماشین جلویی، با دادن اخطار صوتی و تصویری به راننده، وی را از خطر تصادف آگاه می‌سازد.

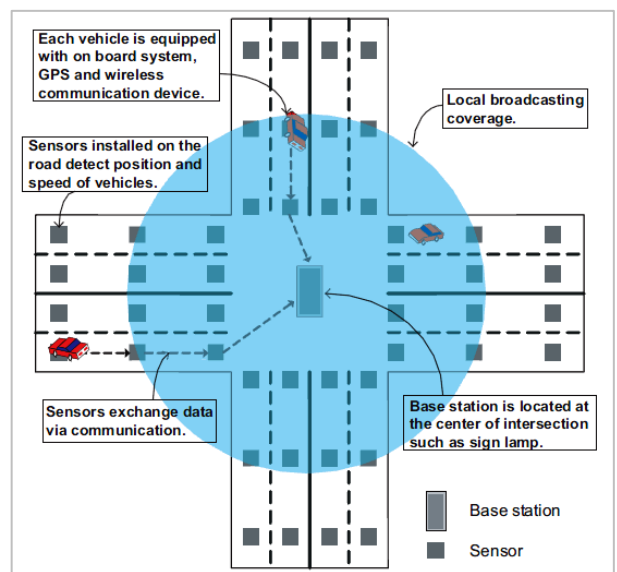


شکل 25- اخطار کاهش فاصله در سیستم MobilEye : 2 ثانیه، 1 ثانیه و 0.6 ثانیه تا برخورد با خودروی جلویی

Kwon و همکاران، در سال 2006، سیستم پیش بینی کننده تصادف برای تقاطع‌ها مبتنی بر شبکه حسگر ارائه داده‌اند.



(ب)



(الف)

شکل 26- (الف) اجزای اصلی سیستم kown. (ب) مراحل اصلی سیستم kown

ایده کلی این سیستم از چهار مرحله تشکیل می‌شود:

(1) موقعیت و سرعت خودروی عبوری، توسط حسگرهای سطح جاده و نزدیک تقاطع مشخص می‌شود.

(2) اطلاعات جمع‌آوری شده توسط حسگر از طریق شبکه حسگر به ایستگاه اصلی منتقل می‌شود.

(3) اطلاعات جمع‌شده در ایستگاه اصلی، از طریق همین ایستگاه به صورت دوره‌ای به خودروهای تحت پوشش ارسال

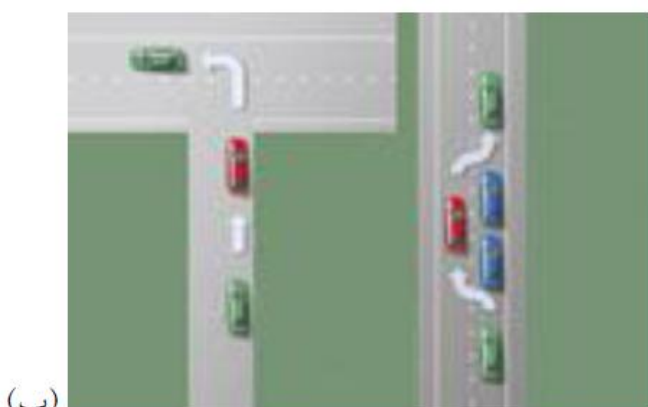
می‌شود.

(4) هر خودرو براساس اطلاعات دریافتی از ایستگاه اصلی الگوریتم «پیش بین تصادف» خود را اجرا می‌کند.

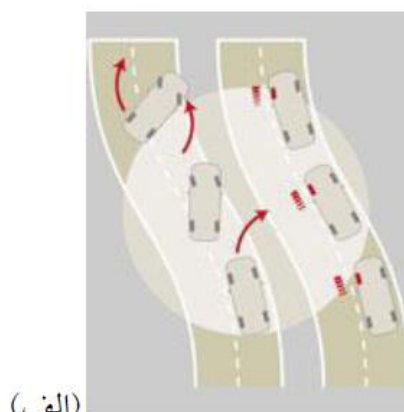
الگوریتم فوق به این معنی است که با داشتن حداقل و حداکثر خودروهای مفروض A, B اگر اشتراک بازه‌های زمانی رسیدن A, B به نقطه تصادف بیشتر از حد خاصی باشد، دو خودرو در آن نقطه، تصادف خواهند نمود. Kown برای تقاطع مورد بحث، هفت نقطه تصادف در نظر گرفته است.

برخی از سازندگان خودرو بر آنند تا سیستم‌های پیشگیری از تصادف را در خودروهای خود تعبیه نمایند. شرکت خودروسازی ولو^۱ در نظر دارد خودروهایی مجهز به سیستم‌های اجتناب از تصادف را وارد بازار کند. سیستم نامبرده تعبیه شده در خودروهای شرکت ولو با پیش‌بینی احتمال تصادف جلو و عقب و در سرعت‌های پایین، قادر به پیشگیری از 50 درصد تصادفات درون‌شهری و ترافیک‌های با سرعت امن خواهد بود. براساس آمار 75 درصد از کل تصادفات، تصادفات مربوط به سرعت‌های پایین (حداکثر 30 کیلومتر در ساعت) است. سیستم ولو با استفاده از یک سیستم نوری - راداری، تا فاصله 6 متری جلوی خودرو را تحت پوشش قرار خواهد داد. اگر خودروی جلویی به صورت ناگهانی ترمز کند، این سیستم به منظور کمک به راننده به صورت خودکار ترمزها را آماده نموده و جریان بنزین را کاهش می‌دهد تا راننده با کاهش سرعت یا تغییر مسیر از تصادفات پیشگیری کند و یا پیامدهای آن را کاهش دهد.

IDIS, DSTC از دیگر تکنولوژی‌های امن‌سازی به کار رفته در محصولات ولو (مثل Volvo S 80) است. عدم توانایی کنترل خودرو و لیز خوردن خودرو در زمین‌های لغزنده از دلایل دیگر تصادفات است. DSTC پایداری راننده در چنین شرایطی، را افزایش می‌دهد. حواس پرتی راننده به علت صدای زنگ تلفن، مخصوصاً در شرایط بحرانی علت دیگری برای وقوع تصادفات است. IDIS با استفاده از یک سیستم مجتمع با تلفن تمام تماس‌های تلفنی را به زمان بعد از انجام شدن یک عمل خطرناک توسط راننده مثل سبقت گرفتن، موکول می‌کند و به تعویق می‌اندازد.



(ب)
VOLVO^۱



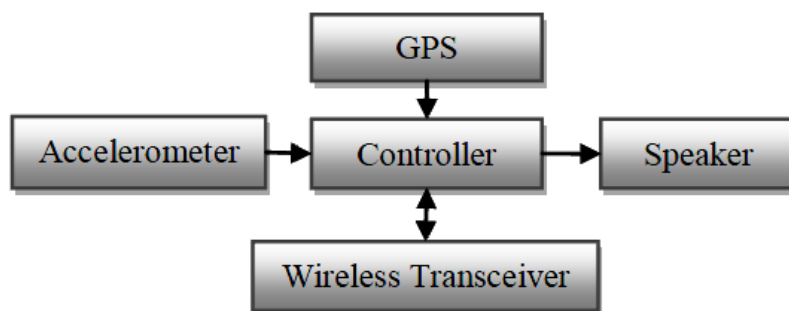
(الف)

شکل 27- (الف) نحوه‌ی حرکت خودرو با DSTC و بدون آن در شرایط لغزنده (ب) برخی از شرایط مورد عمل IDIS در

Volvo S80

فنجی و همکارانش در سال 1387 شمسی، سامانه AutoNet را ارائه کرده‌اند. در مواقعی که راننده دارای دید کافی نیست (مانند تقاطع، سرپیچ‌ها، ورودی تونل‌ها و غیره) و یا حتی مکان‌هایی که مستعد خطرآفرینی هستند، سامانه AutoNet به صورت منطقه‌ای، طی فرایندهایی برخوردار از سیستم‌های خبره و منطق فازی و با استفاده از پارامترهایی از قبیل شرایط جوی و محیطی، احتمال خطرآفرینی یک راننده با توجه به سوابق او، دفعات رخداد تصادف در منطقه حاضر و غیره، به صورت‌های اجتماعی و انفرادی، احتمال تصادف خودرو را محاسبه و به راننده یا رانندگان آن منطقه گزارش می‌کند تا آن‌ها به موقع هوشیاری لازم را به دست آورند.

اسکات ج. وینرت¹، در سال 2010، در مقاله‌ای یک «سیستم هشدار تصادفات» مطرح کرده است. در شکل شماره 29 ساختار سیستم نمایش داده شده است. سیستم دیتاهای مربوط به سرعت را توسط سرعت سنج² نمایش می‌دهد. در مرحله بعد دیتاهای به‌دست آمده، به منظور تعیین و تشخیص تصادف به سوی کنترلر روانه می‌شود. کنترلر تمام پیام‌های تولید شده توسط سایر خودروها را به واسطه یک دریافت کننده بی‌سیم گوش می‌دهد. زمانی که پیامی مبنی بر رخداد یک تصادف پیش رو، دریافت می‌شود، سیستم موقعیت خودرو را توسط GPS به‌دست آورده و به واسطه پیام دریافتی فاصله نسبی از محل تصادف را تشخیص می‌دهد و در نهایت در صورت لزوم کنترل به واسطه بلندگو، هشدار به راننده می‌دهد. هشدار به گونه‌ای که نمایشگر فاصله و شدت تصادف است. اگر همین خودرو دچار تصادف شود سیستم با استفاده از انتقال دهنده بی‌سیم³ موقعیت تصادف را منتشر می‌کند.

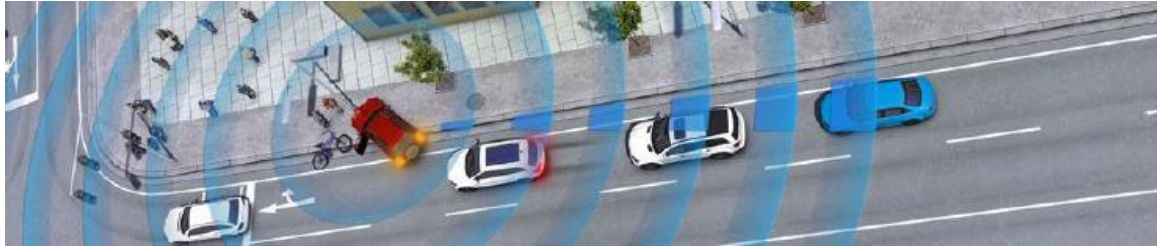


¹ Scott j. Weinrt

² Accelerometer

³ wireless Transceiver

شکل 28- ساختار سیستم هشدار تصادف



شکل 29- عملکرد سیستم هشدار تصادف در VANET

در نمونه‌های، سیستم پیشگیری از تصادف، پیاده‌سازی شده توسط شرکت‌های خودروسازی معرفی گردیده است؛ چندین مدل خودرو موجود هستند که به سیستم شناسایی و جلوگیری از برخورد مجهز هستند. به عنوان نمونه، آئودی A8 نه تنها اگر خودروی دیگری را پیش رو احساس کند ترمز خفیف و نرمی می‌کند، بلکه اگر تصادف قطعی را شناسایی کند با تمام قدرت ترمز خواهد گرفت.

سیستم شناسایی تصادف Acura ZDX از موج رادیویی میلی متری (بالا ترین باند فرکانس رادیویی) استفاده می‌کند که تا صد متر جلوتر را اسکن می‌کند. این ویژگی که سیستم ترمز کاهش تصادف نام دارد، از پاسخ‌دهی راننده برای تعیین چگونگی ترمز استفاده می‌کند. این ویژگی ابتدا مانع را به صورت بی درنگ شناسایی کرده و سپس به صورت بصری و صوتی به راننده اخطار می‌دهد، برای پاسخ صبر می‌کند، ترمز خفیفی می‌گیرد، اخطارهای بیشتری نمایش می‌دهد، سپس ترمز را با تمام قدرت گرفته و کمربندهای ایمنی را فعال می‌کند.

2-4-2- سیستم شناسایی انحراف از خط

رانندگی مطمئن مستلزم رانندگی در بین خطوط، اجتناب از ورود به لاین دیگر و خروج از جاده است. 60 درصد از نرخ تصادفات مربوط به انحراف غیر عمدی از خط است. شناسایی و ردگیری خطوط میانی و کناری جاده و هشدار به راننده جهت برگشت به وضعیت درست از اهداف سیستم‌های هشدار انحراف از خط، است.

بیشترین کارهای انجام شده در این زمینه مبنی بر بینایی ماشین است. و عملکرد آن مبنی بر دوربینی است که در پشت آینه شیشه جلوی خودرو نصب می‌شود. سیستم MobilEye از یک دوربین برای تعیین خطوط جاده و تعیین موقعیت نسبی اتومبیل‌ها استفاده می‌کند و در صورتی که خطوط جاده پاک شده باشد و یا قابل دیدن نباشد متوقف می‌شود و به راننده اخطار می‌دهد.

هزینه‌های چندین میلیون دلاری این محصولات تجاری صرف شده است. سیستم انحراف از خط مطرح شده در سایت Iteris به نام Auto Vue برای کامیون مرسدس به قیمت 2000 دلار عرضه شده است. این سیستم یا به صورت کیت‌های قابل نصب و یا تعبیه شده در ساختار خودرو عرضه می‌شود. ماشین‌های Nissan , Citroen و مرسدس بنز با این توانایی‌ها به بازار آمده‌اند.

برخی از این سیستم‌ها به واسطه دوربین‌های دید در شب، توانایی عمل در شب را هم دارند. و عموماً از یک سیگنال صوتی شبیه صدای تولید شده از حرکت خودرو بر روی خطوط برجسته برای اخطار به راننده، استفاده می‌کنند.

شکل 30- نمایی از محصولات تجاری ADAS و MobileEye در شناسایی خط و انحراف از خط در روز و شب



شکل 30- نمایی از محصولات تجاری ADAS و MobileEye در شناسایی خط و انحراف از خط در روز و شب

همچنین Bertozzi در سال 2005، با استفاده از دید استریو و مادون قرمز عابرین را شناسایی می‌کند. برای این کار، نواحی



گرم بدن انسان شناسایی می‌شوند.

شکل 31- نمونه‌هایی از عملکرد سیستم‌های تشخیص عابر پیاده

2-5- چالش‌های موجود در شبکه‌های بین خودرویی

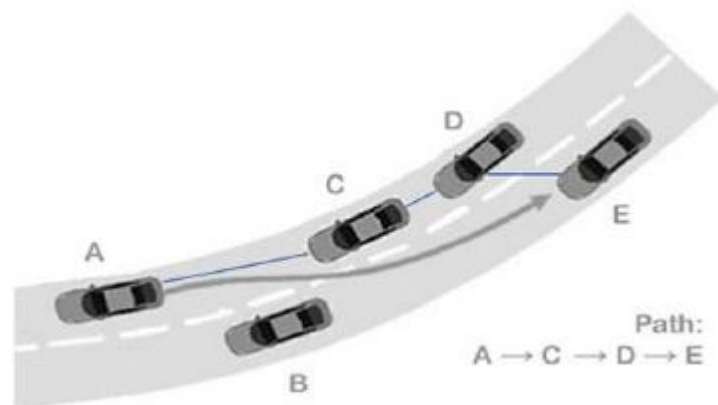
2-5-1- چالش‌های فنی و مکان‌یابی در VANET

برخی از کاربردهای VANET در تعدادی از خودروها محقق شده است. بعضی از این کاربردها عبارتند از: اخطار تصادف خودروها، مشارکت در رانندگی، مشارکت در کنترل سرعت مناسب اتومبیل، پخش اطلاعات جاده‌ای، دست‌یابی به اینترنت، پارک خودکار اتومبیل، خودروهای بدون راننده. تمامی این کاربردها، از یک سری فناوری‌های مکان‌یابی استفاده می‌کنند. با پیشرفت روزافزون VANET شاهد اتکای بیشتر آن به سیستم‌های مکان‌یابی هستیم. با این وجود، استفاده از GPS نیز بدون مشکل نیست. GPS همواره در دسترس نیست و در برخی کاربردها قدرت لازم را از خود نشان نمی‌دهد.

2-5-2- چالش امنیت

در این شبکه‌ها علاوه بر این که تمامی مشکلات موجود در یک شبکه بی‌سیم با زیرساخت با سیم وجود دارد؛ بلکه مشکلات بیشتری نیز دیده می‌شود. به طور مثال، چون تمامی ارتباطات به صورت بی‌سیم انجام می‌شود، می‌توان آن‌ها را شنود کرد و یا تغییر داد. در شبکه‌های بین خودرویی، حمله‌کننده‌ها یا مهاجمان می‌توانند تزریق شوند، جعل شوند، پخش شوند و پیغام را از بین ببرند تا تمامیت و صحت اطلاعات و کارایی سیستم نقض شود. بنابراین راه‌حل‌های امنیتی باید طوری طراحی شوند که به صحت اطلاعات و کاربرد دست یابیم. در این شبکه‌ها تصور یک واحد توزیع کلید و یا زیرساخت کلید عمومی و غیره مشکل است. زیرا این شبکه‌ها اغلب بدون برنامه‌ریزی قبلی ایجاد می‌شوند و برای مدت کوتاهی نیاز به برقراری امنیت دارند.

همچنین با توجه به اینکه خود گره‌ها در عمل مسیریابی شرکت می‌کنند، یک گره متخاصم می‌تواند ماهیت شبکه را نابود کند. برای مثال یک فرستنده می‌تواند در بیان مشاهداتش به خاطر نفع خود سوء استفاده کند.



شکل 32- خود گره‌ها در عمل مسیریابی شرکت می‌کنند.

2-5-3- چالش کانال ارتباطی

با توجه به جدید بودن فناوری VANET واضح است که در سال‌های اولیه برپایی این شبکه‌ها، تعداد خودروهایی که از تجهیزات DSRC در باند 5.9 GHz استفاده خواهند کرد، پایین خواهد بود. در نتیجه در شبکه‌های تشکیل شده، مشکل کمبود

اتصال به وجود خواهد آمد. در این صورت احتمال تکمیل ارسال و دریافت یک پیام امنیتی پایین است و در مقابل زمانی که تعداد خودروهای مجهز به فناوری VANET، افزایش یابد با مشکل دیگری به نام ازدحام در کانال روبرو خواهیم شد. هر چه تعداد گره‌های ارسال‌کننده بیشتر شود، رقابت برای تصاحب کانال بیشتر شده و در نتیجه زمان انتظار هر گره نیز افزایش خواهد یافت.

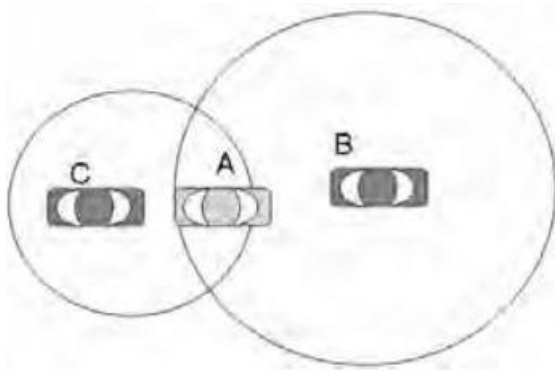
2-5-4- چالش ارسال چند گام

به دلیل برد رادیویی محدود هر گره در شبکه‌های VANET، احتیاج است تا یک پیام پخش‌ی دریافت شده مجدداً برای همسایگان پخش گردد. این نوع ارسال‌ها چند گام¹ نام دارند. گسترش محدوده جغرافیایی یک شبکه باعث می‌شود تا پیام‌ها در تعادل گام‌های متوالی در کل شبکه پخش شوند و همچنین افزایش خودروهای یک شبکه باعث تأخیر در ارسال پیام خواهد شد. در نتیجه، برای ارسال پیام‌های ایمنی به صورت مطمئن، بهتر است خودروهای همسایه خوشه‌بندی (Clustering) شده و ارسال به داخل این خوشه‌ها محدود گردد.

2-5-5- چالش گره پنهان

کلیه اشکال‌های بی سیم با مشکلی به نام گره پنهان مواجه هستند. علت به وجود آمدن این مشکل بُرد رادیویی محدود هر گره است و می‌تواند باعث درصد بالایی از خرابی فریم‌ها (در لایه MAC) شود. در شکل شماره 34 این مشکل به صورت ساده نمایش داده شده است. گره B و گره C به دلیل بُرد محدودی که دارند از حضور یکدیگر در شبکه آگاه نیستند. اگر هر دو گره فریمی را برای A ارسال کنند، این دو فریم در مقصد دچار تمام شده و خراب می‌گردند.

¹ Multi-hop



شکل 33- طرح ساده‌ای از مشکل گره پنهان

2-6- روش پیشنهادی

اگر چه تلاش‌های زیادی سعی در بهینه کردن پهنای باند برای بهبود پوشیدگی پیام دارند ولی QOS به دلایل مختلف هنوز به عنوان یک چالش در VANET باقی مانده است. چالش‌های واقعی QOS نرخ تحول بسته و مدت زمان اتصال و تأخیر می‌باشد به طور مثال در حالت ترافیک سنگین با تعداد زیادی از خودروها مواجه هستیم، هنگامی که هر خودرو پیام‌های دوره‌ای را برای اطلاع یافتن از وضعیت همسایگان رد و بدل می‌کند، ازدحام بالای خودروها و در نهایت حجم زیاد داده‌های تبدلی منجر به افت کارایی پروتکل انتشار می‌شود و در نتیجه داده‌های اضطراری یا گم می‌شوند و یا خیلی دیر عمل می‌کنند و نهایتاً اطلاعات مربوط به وقوع تصادف ممکن است یا دیر برسد یا هرگز نرسد.

بنابراین از آنجایی که کاربردهای ایمنی با حفظ جان مسافران سر و کار دارند و ایمنی حمل و نقل در راستای تبادل اطلاعات اضطراری بین خودروها تأمین می‌شود و انتقال داده‌ها در VANET در بستر پهنای باند کم و برد رادیویی محدود است پس بایستی جریان داده‌ها در VANET چنان مدیریت شود که نرخ تحویل داده‌ها را افزایش و میزان تأخیر آن‌ها را کاهش دهد تا کارایی شبکه VANET، ایمنی حمل و نقل، تضمین گردد.

در روش پیشنهاد شده لازم است هر بسته اطلاعاتی شامل بیت یا بیت‌هایی برای نشان دادن «شماره پیام» و بیت یا بیت‌هایی برای مشخص کردن «نوع پیام» باشد. در این روش قبل از دریافت داده‌های تبدلی، هر خودرو شماره پیام بسته دریافتی را بررسی

می‌نماید در صورتی که قبلاً آن را دریافت کرده، از دریافت مجدد آن صرف‌نظر می‌کند و در نتیجه منجر به بهبود بهره‌وری ارتباط می‌شود.

در مرحله بعد که هر گره مسئول انتقال پیام دریافتی به سایر گره‌هاست، بیت مربوط به نوع پیام را بررسی کرده و پیامی که از نوع اضطراری می‌باشد را در اولویت لیست پیام‌های ارسالی قرار می‌دهد. بدین ترتیب داده‌های حاوی اطلاعات اضطراری به موقع به مقصد می‌رسند و در نهایت با افزایش نرخ تحویل بسته‌ها به خصوص اطلاعات اضطراری مواجه خواهیم بود. این روش کیفیت خدمات سرویس را بهبود داده و می‌تواند به عنوان راه حلی برای چالش ارسال چند گام مطرح گردد.

2-7- نتیجه

VANET به عنوان موضوعی مهم از دهه‌های اخیر در راستای ایمنی و بهبود حمل و نقل جاده‌ای مورد تحقیق و بررسی قرار گرفته است و تا کنون پیشرفت‌های زیادی داشته است و زمانی که در این مسیر صعودی، چالش‌های آن حل و برطرف گردد به عنوان بزرگ‌ترین فناوری قرن حاضر مطرح خواهد شد و مانند کشف دارویی برای پیشگیری از امراض لاعلاج تأثیر خود را بر جاده‌های پر خطر و خودروها و حتی ماهیت رانندگی نشان خواهد داد.

پس لازم است که این امر مهم را جدی گرفته و سرمایه‌گذاری‌های لازم برای رسیدن به امنیت حمل و نقل و جلوگیری از خسارت جانی و مالی جبران ناپذیر آن انجام شود.

فصل سوم - امنیت در MANET

3-1- تحلیل امنیت

طرح امنیتی طراحی شده است تا مقادیر مورد نیاز زیر به دست آید:

- **اعتبارسازی:** از آنجایی که ماشین‌ها باید فقط به پیام‌های قانونی هسته‌ی خودکار عکس‌العمل نشان دهند، لازم است که این پیام‌ها معتبر شوند.
- **تطابق داده‌ها:** به منظور حفاظت در مقابل پیام‌های اشتباه هسته‌ی خودکار که از ماشین‌های قانونی تولید می‌شود (مانند نمونه: نقص فنی تجهیزات یا نرم‌افزار) باید امکان تأیید سازگاری و تطابق پیام‌های هسته‌ی وجود داشته باشد.
- **انکار ناپذیری:** باید امکان داشته باشد تا به طور مطمئن ماشین‌ها را از پیام‌های هسته‌ی خودکار که عبور می‌دهند شناسایی شود که به آن صورت رانندگان نمی‌توانند ماشین‌هایشان را که منبع این پیام‌هاست انکار کنند به بازرسان امکان تعیین مشمولیت قانونی حادثه تصادف داده شود.
- **اختصاصی:** خصوصی بودن رانندگان در مقابل مشاهده گران غیر مجاز باید تضمین شود که از سوء استفاده پیام‌های هسته‌ای خودکار برای ردگیری حرکات ماشین‌ها جلوگیری می‌شود.

- **محدودیت زمان واقعی:** به دلیل زمان‌های کوتاه تماس میان ماشین‌ها (مانند ماشین‌هایی که در مسیرهای مخالف اتوبان عبور می‌کنند) و مدت کوتاه حوادث تصادف (به ویژه نه بیشتر از چند ثانیه)، محدودهای جدی زمان باید تحویل داده شود و پردازشگری پیام‌های هسته‌ای خودکار صورت می‌گیرد.

3-2- امنیت و حریم خصوصی

وقتی اطلاعات در بین اشخاص ناشناس جمع‌آوری و تقسیم می‌شوند نگرانی‌ها در خصوص موثق و قابل اعتماد بودن اطلاعات یک سیستم افزایش می‌یابد، برای مثال یک فرستنده می‌تواند در بیان مشاهدات به خاطر نفع خود سوء استفاده کند؛ مثلاً خودروی A به غلط اعلام می‌کند که جاده مطلوب خودروی B پر ترافیک است و بدین ترتیب دیگران را از خودروی B دور می‌کند و بدین ترتیب مسیر خلوتی برای B ایجاد می‌کند. گزارش‌های شروانه می‌تواند سایر خودروها را به تقلید رفتار همان خودرو یا زیر ساخت‌های کنار جاده برای ناامن کردن جاده وا دارد. خودروها می‌توانند با ایجاد شبکه معتمد، اطلاعات رسیده از فرستندگان نامعتبر را نادیده بگیرند. موفقیت و مقبولیت این فناوری در میان مشتریان نیازمند ایجاد سطح بالایی از قابلیت اعتماد و امنیت است.

3-3- خصوصیات یک ارتباط قابل اعتماد

- فرستنده در نهایت به عنوان یک منبع قابل اعتماد پذیرفته شود.
- پیام فرستنده در حین انتقال دست‌کاری نشود. یک چالش مهم در امنیت VANET فراهم آوردن اعتبارسنجی فرستنده در ارتباطات می‌باشد.

روش‌های گوناگونی برای ارزیابی و اعتبارسنجی فرستنده پیشنهاد شده است که یکی از این راه‌ها راهکار طراحی امضای دیجیتال در خودروها است تا هر پیامی که ارسال می‌شود دارای مشخصه آن امضاء باشد تا در صورت سوء استفاده قابل پیگیری از طریق پلیس باشد. این امر معمولاً از طریق کلید عمومی امضای تعبیه شده در خودرو انجام خواهد گرفت.

3-4- دو چالش عمده در شبکه‌های موردی بین خودرویی

- همبندی شبکه

- انتشار پیام‌های ایمنی دوره‌ای، به‌طور خاص برای ترافیک بزرگراه، به شرح زیر مورد بررسی قرار می‌گیرند. اولاً، برای مواردی که جریان ترافیک جاده‌ای (تعداد خودروهای عبوری در واحد زمان از یک نقطه دلخواه) پایین و سرعت خودروها بالا است. همبندی شبکه ضعیف بوده و به عبارتی ممکن است خودروها نتوانند به دلیل از هم گسیختگی شبکه، با هم ارتباط برقرار نمایند. در این راستا مدلی تحلیل برای مطالعه همبندی در شبکه‌های موردی بین خودرویی ارائه می‌شود. این مدل قادر است اثر عوامل مختلف مؤثر، مانند جریان ترافیک جاده‌ای، توزیع احتمالی سرعت خودروها و محدوده ارسال خودروها را روی همبندی مطالعه نماید. به‌طور خاص، اثر توزیع احتمالی سرعت خودروها، روی همبندی شبکه با استفاده از تکنیک ترتیب تصادفی مطالعه شده است. به علاوه، مدل ارائه شده که براساس نوعی تناظر با سیستم‌های صف با تعداد خدمتگذار نامتناهی است، با استفاده از شبیه‌سازی تأیید شده است. در جریان مطالعه عددی مدل، از آمار و داده‌های موجود در حوزه مهندسی حمل‌ونقل استفاده می‌شود تا درک مناسبی از همبندی در شبکه‌های واقعی بین خودرویی به دست آید. نتایج حاصل از مدل ارائه شده و همچنین نتایج کارهای قبلی موجود در متون، حاکی از این است که همبندی در برخی شرایط خاص ترافیکی به نحو چشمگیری افت می‌یابد. در نتیجه به منظور بهبود سطح همبندی راهکاری را پیشنهاد نموده‌ایم که براساس آن، تعدادی خودروی اضافی به ترافیک بزرگراه تزریق می‌شوند. این خودروی اضافی به ترافیک بزرگراه تزریق می‌شوند. این خودروها علاوه بر بهبود درجه همبندی، می‌توانند سرویس‌های رفاهی مانند تبلیغات، سرگرمی و غیره را به خودروهای در حال عبور ارائه دهند. به این ترتیب وجود آنها از لحاظ اقتصادی نیز قابل توجیه است. همبندی در حضور این گره‌های اضافی متحرک و همچنین گره‌های اضافی ساکن (واحدهای کنار جاده) تحلیل شده و راهکارهایی برای انتخاب پارامترهای دخیل، جهت نیل به همبندی مناسب با در نظر گرفتن محدودیت‌های فنی و اقتصادی پیشنهاد می‌گردد.

ثانیاً، برای حالت ترافیک سنگین (جریان ترافیک بالا)، همبندی شبکه قاعداً در حد قابل قبول بوده ولی هنگامی که پیام‌های دوره‌ای برای اطلاع یافتن از وضعیت همسایگان ردوبدل می‌گردند، ازدحام بالای خودروها منجر به افت کارایی پروتکل انتشار

پیام می‌شوند. این مطلب مورد تأکید قرار گرفته است که چون کاربردهای ایمنی با حفظ جان مسافران سر و کار دارند، ارزیابی کیفیت سرویس آنها نیازمند در نظر گرفتن ملاحظات خاص است. در این راستا، ابتدا با توجه به ویژگی‌های خاص کاربردهای ایمنی مبتنی بر انتشار پیام‌های دوره‌ای، معیار جدیدی به نام محدوده مؤثر، به‌طور خاص، به منظور ارزیابی کارایی این کاربردها پیشنهاد می‌گردد. سپس رابطه بین کیفیت سرویس لایه کاربرد و کیفیت سرویس پروتکل ارتباطی را مدل نموده و براساس آن برای انواع مختلف کاربردهای ایمنی متصور، معیار محدوده مؤثر را با استفاده از شبیه‌سازی استخراج می‌نماییم. نتایج به دست آمده حاکی از این است که با وجود کارایی ضعیف پروتکل انتشار پیام‌های دوره‌ای در ترافیک جاده‌ای سنگین، محدوده مؤثر لایه کاربرد (برای راننده)، قابل قبول بوده و می‌توان به پیاده‌سازی دسته‌ای از کاربردها در آینده نزدیک امیدوار بود.

3-5- شبکه‌های موردی و چالش‌های امنیتی

بهرتر است قبل از پرداختن به شیوه‌های جدید حملات علیه شبکه‌های موردی، کمی درباره چند و چون امنیت و ضعف‌های ساختاری این گونه شبکه‌ها صحبت کنیم. همان‌طور که می‌دانید شبکه‌های بی‌سیم به دو گونه کلی ساختارمند¹ و غیر ساختارمند² تقسیم می‌شوند. بهترین مثال از شبکه‌های ساختارمند، شبکه‌های وایفای و وایمکس هستند. در این گونه شبکه‌ها یک نود یا دستگاه مرکزی مانند اکسس‌پوینت یا روتر وجود دارد که وظیفه مدیریت و مسیریابی و ارتباطات کلی شبکه را عهده‌دار است. اما در شبکه‌های غیر ساختارمند که بهترین نمونه آنها شبکه‌های موردی هستند، هیچ نود مرکزی یا روتر/اکسس‌پوینتی وجود ندارد و نودهای شبکه باید خودشان عملیات مسیریابی و مدیریت ارتباطات و شکل‌دهی توپولوژی شبکه را انجام دهند و به نوعی خودمختار هستند.

بهترین مثال برای شبکه‌های موردی ارتباط دو یا سه گوشی موبایل و نوت از طریق بلوتوث است. شبکه‌های موردی در صنایع نظامی، حوادث طبیعی، شبکه‌های خودرویی، شبکه‌های درون سازمانی و کاربردهای این‌چنینی بسیار مورد استفاده قرار می‌گیرند. حتی با همین اکسس‌پوینت یا روترهای معمولی نیز می‌توان یک شبکه موردی راه اندازی کرد. پس تا اینجا متوجه شدیم که در شبکه‌های موردی هیچ گونه دستگاهی برای مدیریت شبکه و نودها وجود ندارد و هیچ فضای سخت‌افزاری یا فیزیکی برای پشتیبانی و هدایت شبکه در اختیار نداریم. این قابلیت مزیت ویژه شبکه‌های موردی و البته پاشنه آشیل این گونه شبکه‌ها نیز هست. از آنجا

¹ Infrastructure

² Non Infrastructure

که (همبندی توپولوژی) شبکه‌های موردی همیشه در حال تغییر و دگرگونی است و هیچ نودی جای ثابت و مشخصی در شبکه نداشته و خود نودها ارتباطات درون شبکه‌ای را مدیریت و سرویس‌دهی می‌کنند، مشکلات امنیتی زیادی به وجود می‌آید. در این گونه شبکه‌ها نمی‌توان از هیچ سرویس یا دستگاه سخت‌افزاری برای تأمین امنیت و بالا بردن ضریب اطمینان استفاده کرد و فراهم کردن امنیت فیزیکی نسبت به شبکه‌های مبتنی بر کابل یا ایفای سخت‌تر است. کافی است یک مهاجم برای سرقت اطلاعات، جایی در شبکه را برای اقامت پیدا کند. مشکلات امنیتی در شبکه‌های موردی از آن جهت خاص شده و جداگانه مورد بررسی قرار می‌گیرد که در این شبکه‌ها علاوه بر این که تمامی مشکلات موجود در یک شبکه کابلی یا یک شبکه بی‌سیم وجود دارد؛ مشکلات تازه و بیشتری نیز دیده می‌شود. مثلاً از آنجا که تمامی ارتباطات به صورت بی‌سیم انجام می‌شود، می‌توان آنها را شنود کرد و تغییر داد. همچنین از آنجا که خود نودها در عمل مسیریابی شرکت می‌کنند، وجود یک نود متخاصم می‌تواند به نابودی شبکه بیانجامد. همچنین در این شبکه‌ها تصور یک واحد توزیع کلید یا زیرساخت کلید عمومی و غیره مشکل است، زیرا این گونه شبکه‌ها بیشتر بدون برنامه‌ریزی قبلی انجام می‌شوند و برای مدت کوتاهی به برقراری امنیت نیاز دارند و در عین حال هر نود انرژی بسیار کمی دارد. برای جمع‌بندی این بخش باید بگوییم که عمده حملات به شبکه‌های موردی از جانب مسیریابی¹ است و حملات جدید براساس آسیب‌پذیری‌های پروتکل‌ها و الگوریتم‌های مسیریابی به وجود می‌آیند. حملات در VANET را می‌توان به طور وسیع به سه گروه اصلی دسته‌بندی کرد:

1) آن‌هایی که قابلیت استفاده و دسترسی VANET را تهدید می‌کنند.

2) آن‌هایی که اعتبار و صحت VANET را تهدید می‌کنند.

3) آن‌هایی که محرمانگی راننده را تهدید می‌کنند.

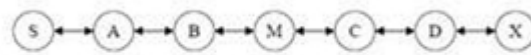
در ادامه یکی از مهم‌ترین حملات جدید کشف و معرفی شده عملی و پژوهشی دنیا در سال‌های 2011 و 2012 را بررسی

می‌کنیم.

¹ Routing

3-6- حمله تغییر در گاه^۱

یکی از مهم‌ترین و کلاسیک‌ترین تهدیدات در شبکه‌های موردی، حملات تغییر^۲ هستند. در این نوع حملات، نود یا نودهای متخاصم سعی می‌کنند با تغییر بسته‌های مسیریابی یا بسته‌های اطلاعاتی، شبکه را هک کنند. این تغییر می‌تواند در بسته‌های



شکل 34- یک شبکه موردی فرضی

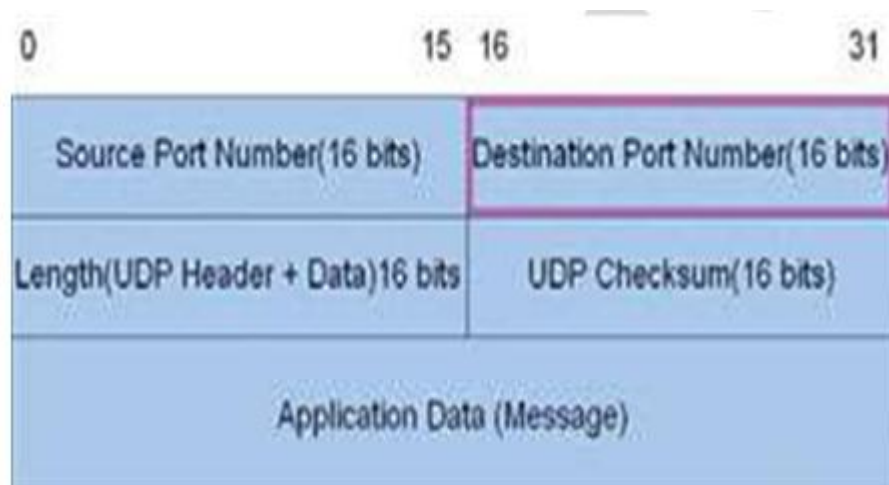
مسیریابی (RREQ بسته‌هایی که برای شناسایی نودهای همسایه صادر می‌شود RREP، بسته‌هایی که در پاسخ به دریافت بسته‌های RREQ برای نود مبدا ارسال می‌شود و RERR بسته‌هایی که برای اعلام قطع شدن یک لینک یا از بین رفتن یک نود در توپولوژی شبکه صادر و برای نودهای همسایه ارسال می‌شود) اعمال شود یا تغییر در آدرس نود مبدا و مقصد بسته‌ها صورت گیرد. شیوه‌های دیگر می‌تواند در فیلد «تعداد هاپ»^۳ (فیلد نگهدارنده تعداد گام‌هایی که یک بسته مسیریابی طی کرده است که همان نودها در طول مسیر است) یا در فیلد آدرس مقصد صورت گیرد که روش آخری موجب بروز حملات DDOS می‌شود. برای تشریح حملات بالا یک مثال را بررسی می‌کنیم. در شکل 35، یک شبکه موردی فرضی ترسیم شده است. در این طرح فرضی نود مبدا S و نود مقصد X است. نود مبدا برای ارتباط با نود X باید از نودهای میانی A، B، ... تا D برای انتقال بسته اطلاعاتی کمک بگیرد. در این شرایط اگر یکی از نودهای میانی یک نود مهاجم یا خرابکار باشد، می‌تواند با تغییر دادن بسته‌های مسیریابی یا اطلاعاتی عبوری از خود در شبکه اختلال ایجاد کند. مثلاً فرض کنید که نود M با دریافت هر بسته مسیریابی و شناسایی نودهای فعال در شبکه، پیغامی به این صورت بسازد که خودش آخرین نود در شبکه است و دیگر نودی برای انتقال بسته مسیریابی وجود ندارد. در این شرایط ارتباط نود S با نود X قطع خواهد شد.

¹ Port Change

² Changing

³ Hop Count

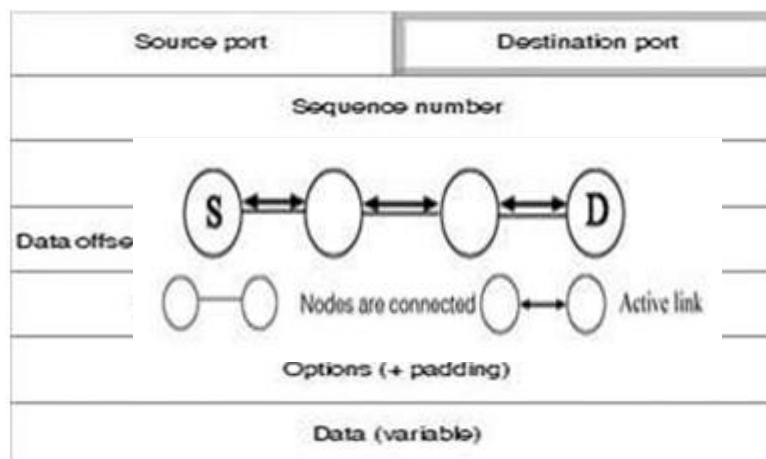
در چند سال اخیر گونه‌های جدیدی از حملات تغییر، تعریف و طراحی شده‌اند و کم و بیش در حال شکل‌گیری و استفاده هستند که یکی از مهم‌ترین آنها حمله تغییر درگاه است که برای نخستین بار توسط محیط جین¹ و همکارانش در سال 2010 مطرح شده است. هدف این حمله، از دسترس خارج کردن یک یا چند گره از شبکه و تغییر کل مسیریابی و ارتباط گره‌های مبدا و مقصد با یکدیگر است. این حمله از آن جهت اهمیت دارد که به راحتی روی شبکه‌های مبتنی بر TCP/IP و پروتکل UDP قابل اجراست. شکل‌های 36 و 37 سرآیند بسته‌های TCP/IP و UDP را برای شبکه‌های بی‌سیم نشان می‌دهد.



شکل 35- سرآیند بسته‌ها در پروتکل TCP/IP

در این سرآیندها برای ارسال یک بسته نیاز به آدرس IP و شماره توالی یا شماره درگاه گره مقصد است (در مسیریابی شبکه‌های موردی همیشه یک جدول آخرین شماره دریافت شده از گره‌ها نگهداری می‌شود که براساس همین شماره نیز مسیریابی جدید صورت می‌گیرد. گره‌های دریافت کننده بسته‌های مسیریابی باید از شماره‌های توالی بزرگ‌تر استفاده کنند). ترکیب آدرس

¹ Mohit Jain



شکل 37- یک شبکه موردی فرضی با نودها و لینک‌های فعال و سالم

ip و شماره درگاه را آدرس سوکت¹ می‌گویند که یک آدرس یکتا برای هر گره ایجاد می‌کند. حمله تغییر درگاه در چهار

مرحله صورت می‌گیرد که طی آنها با تغییر آدرس IP و شماره درگاه، برخی از گره‌های فعال شبکه از فرآیند مسیریابی و

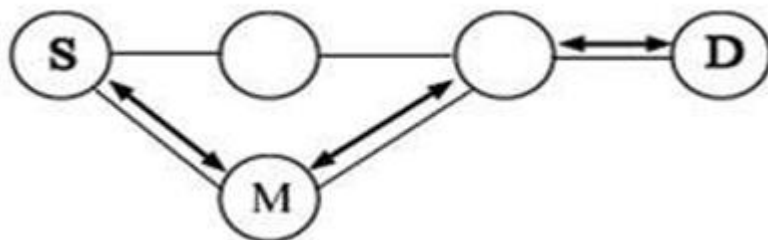
ارتباطات درونی شبکه خارج می‌شوند. شبکه موردی فرضی پیش از شروع حمله در شکل 38 نمایش داده شده است.

گره S می‌خواهد اطلاعاتی را با گره D تبادل کند. در ارتباطات قبلی، دو گره میانی وظیفه رساندن بسته‌ها را به گره‌های S و D بر عهده داشتند و میان این گره‌ها لینک‌های سالم و فعالی برقرار شده است. از آنجا که توپولوژی شبکه موردی به علت تغییر محل فیزیکی گره‌ها دائماً در حال عوض شدن است، گره S برای ارتباطات جدید خود باید ابتدا یک مسیریابی انجام داده و پس از اطمینان از وجود گره‌ها و توپولوژی قبلی شروع به ارسال اطلاعات کند. در این شرایط گره مهاجم M به گره‌های شبکه نزدیک شده و شروع به جستجو و اسکن آدرس IP و شماره درگاه‌های باز گره‌ها می‌کند (معمولاً برای این عملیات نرم‌افزارها و ابزارهای Port Scan وجود دارد).

با داشتن اطلاعات گره مقصد D، وقتی بسته مسیریابی RREQ را از گره S دریافت می‌کند، شماره درگاه آن را تغییر داده و یک شماره بزرگتر از قبلی قرار می‌دهد. با این حرکت می‌خواهد به گره S بفهماند که آخرین ارتباط برقرار شده میان او و گره D از طریق خودش بوده است. سپس بسته مسیریابی RREQ تغییر یافته را برای گره میانی بعدی ارسال و در نهایت به دست گره D

¹ Socket Address

می‌رساند. گره D نیز چون صحت بسته را مطمئن شده و شماره درگاه صحیح است، تأیید می‌کند که آماده دریافت اطلاعات است و مسیر طی شده را دوباره با بسته RREP در اختیار گره S قرار می‌دهد (شکل 39). گره مهاجم M نیز بسته RREP را دوباره تغییر می‌دهد و شماره درگاه بزرگ‌تری درون آن جاسازی می‌کند. به این ترتیب، دوباره گره میانی فعال و سالم از میان خواهد رفت و گره S با دریافت بسته تأیید مسیریابی و تشخیص اینکه آخرین مسیریابی صحیح صورت گرفته از طریق گره M است، شروع به ارسال اطلاعات به گره D می‌کند. در این حمله یک یا چند گره، در حالی که فعال هستند از فرآیند مسیریابی خارج شده و در انتقال بسته‌های اطلاعاتی شرکت نمی‌کنند و گره مهاجم به هدفش که شنود یا سرقت اطلاعات یا از بین بردن لینک فعال میان دو گره است، خواهد رسید.



شکل 38- نود مهاجم M در حالت ایجاد ارتباط میان نود مبدا و مقصد

فصل چهارم - نتیجه گیری و منابع

4-1- نتیجه گیری

با پیشرفت روزافزون علوم و فناوری، جوامع سعی در بهره‌گیری از آن‌ها برای رفع مشکلات و بهینه‌سازی فرآیندها دارند. VANET یکی از این فناوری‌های پیشنهاد شده در شبکه حمل و نقل خودرویی است که می‌تواند کمک شایانی به صنعت حمل‌ونقل، صنعت بیمه خودرو، مدیریت جاده‌ای و بهبود بهره‌وری نهادهای مربوطه داشته باشد. برخلاف مشکلات و محدودیت‌هایی که هنگام استفاده از این شبکه‌ها بوجود می‌آید، همواره می‌توان به استفاده از این شبکه‌ها و دستاوردهای آنان در جلوگیری از تصادف و کاهش آمار مرگ و میر امیدوار بود. برخلاف بسترسازی‌های فرهنگی که گاه سال‌ها به طول می‌انجامد و یا بررسی راهکارهای جدید که هر یک هزینه‌ها و مشکلات خود را به دنبال دارند، بهتر است استفاده از این شبکه‌ها بعنوان دستاورد نویدبخش تامین امنیت و بهترین انتخاب برای آسان نمودن ارتباطات نقلیه‌ای فرهنگ‌سازی شود. تلاش‌های بعدی هم بهتر است در راستای کم کردن محدودیت‌ها و بازبینی مشکلات برپاسازی این شبکه‌ها صورت گیرد. مهندس ترافیک در سیستم حمل و نقل هوشمند با دو مساله تعیین کننده مواجه است. ایمنی ترافیک و کارایی ترافیک. آینده مدیریت و کنترل ترافیک به طور حتم به شکل کنترل دیجیتال و اتوماتیک خواهد بود. بی تردید یکی از مواردی که در آینده نزدیک بیشتر مطرح خواهد شد شبکه اقتضایی بی‌سیم بین خودروهاست. در این شبکه هر خودرو به منزله گره‌ای است که می‌تواند هم بصورت گیرنده و هم

بصورت فرستنده عمل کند و اطلاعات مختلف بدین صورت میان وسایل نقلیه پخش خواهد شد. کاربردهای کلی این سیستم به دو دسته کلی موارد ایمنی و غیر ایمنی (نظیر پیدا کردن پمپ بنزین) تقسیم خواهد شد.

روش‌های مانیتورینگ برای کنترل ترافیک علاوه بر هزینه بر بودن دارای مشکلاتی نظیر تاخیر در رسیدگی و عدم امکان ارسال اطلاعات به سایر رانندگان می‌باشند. لذا استفاده از شبکه اقتضایی یک گام به جلو محسوب می‌شود. در این شبکه ارتباط یا بصورت ارتباط مستقیم میان خودروهاست و یا با ارتباط خودرو با کنارجاده. که در حالت اول نیاز به زیرساخت نیست و خودروها به شکل بی‌سیم با هم ارتباط برقرار می‌کنند بطور کلی این سیستم‌های ارتباطی که دارای کاربرد شخصی یا ایمنی هستند با نام ارتباط بازه کوتاه اختصاصی DSRC شناخته می‌شوند در حالت دوم خودروها شبکه اقتضایی بی‌سیم مشخصی را بوجود می‌آورند که می‌تواند اطلاعات را در یک شبکه همتا انتقال دهد این شبکه اقتضایی بین خودرویی با نام VANET شناخته می‌شود. از جمله کاربردهای تعریف شده برای این فناوری می‌توان به این مورد اشاره کرد:

- کاهش مشکلات ترافیکی
- پیشگیری از حوادث جاده‌ای
- بهبود مدیریت اقدامات لازم پس از حوادث جاده‌ای
- کنترل اعتبار مدارک و کاربردهای آماری و رفاهی دیگر

شبیه‌سازی ترافیکی و شبکه حمل و نقل، پیشرفت‌های نرم‌افزاری قابل توجهی یافته است اما نیاز به همگامی با پیشرفت‌های سخت‌افزاری دارند. به علاوه، شبیه‌سازها برای ایجاد نتایج واقعی‌تر نیازمند در نظر گرفتن پارامترهای مؤثر مربوط است. هرچند VANET با چالش‌های بسیاری مانند چالش‌های اقتصادی، اجتماعی، امنیتی و فنی روبرو است.

کاربران خواستار ایمنی و امنیت در جاده‌ها هستند. امکان وقوع این احتمال در صورت تکمیل امنیت و ایمنی VANET که یک نوع تکنولوژی در حال توسعه است، امکان پذیر می‌باشد. مبحث کاربردهای ایمنی در شبکه‌های موردی بین خودرویی، یک موضوع بین رشته‌ای بوده و لازم است هم ملاحظات شبکه و هم ملاحظات ایمنی جاده‌ای با یکدیگر مد نظر قرار گیرند. در این پروژه تلاش شد تا به توصیف کلی حملات ممکن در VANET پرداخته و برخی از راهکارهای ممکن را بررسی کنیم. همانطور که گفتیم حملات در VANET را می‌توان به طور وسیع به سه گروه اصلی دسته‌بندی کرد که شامل آن‌هایی که

قابلیت استفاده و دسترسی VANET را تهدید می‌کنند، آن‌هایی که اعتبار و صحت VANET را تهدید می‌کنند و آن‌هایی که محرمانگی راننده را تهدید می‌کنند، می‌شود.

VANET ها در محیط‌های نامطمئن و ناامن، گسترش یافته‌اند در نتیجه تصدیق و سندیت یک وسیله در زمان درخواست منابع اطلاعات در شبکه، امری مهم به حساب می‌آید. در این پروژه، دقت تصدیق VANET نیز مورد بحث قرار گرفت و مطالب زیر بنایی و پایه را برای فهم بهتر تصدیق VANET، جهت طراحی مکانیزم‌هایی جدید و کارآمد در تصدیق VANET، شرح داده شد.

همانطور که بیان شد این تکنولوژی، سرزمین و منطقه‌ای غنی برای مهاجمانی است که تلاش به تغییر مضمون کاربردهای امن و ناامن دارند، به حساب می‌آید. در این شبکه‌ها، خودروها اطلاعاتی نظیر وضعیت خود و جاده، موقعیت‌های خطرناک و حادثه ساز و ... را در قالب پیام بین یکدیگر رد و بدل می‌سازند. بدیهی است صحت پیام‌های ارسالی در این شبکه‌ها از اهمیت بالایی برخوردار بوده و انتشار اطلاعات نادرست علاوه بر کاهش کارایی این شبکه‌ها حتی ممکن است خسارات غیر قابل جبرانی به همراه داشته باشد. از این رو توجه بسیاری از مراکز دانشگاهی و نیز صاحبان صنایع به تامین امنیت در این شبکه‌ها معطوف گشته است. یکی از روش‌های امن کردن شبکه‌های بین خودرویی شناسایی خودروهای بدرفتاری است که اقدام به انتشار پیام‌های نادرست می‌نمایند، با شناسایی و خنثی نمودن این گونه حمله‌ها کارایی شبکه بالا می‌رود. این نوع شبکه‌ها تاکنون پیشرفتهای زیرساختی و نرم افزاری زیادی داشته‌اند، اما هنوز چالش‌های جدی پیش رو دارند.

منابع

- [1] فتحی، م. امین طوسی، م. صادقی، م. و امیری، ع. (1385) "مروری بر تحقیقات انجام شده در زمینه پیشگیری از تصادف" هفتمین کنفرانس مهندسی حمل و نقل و ترافیک ایران.
- [2] دوستی، پ. (1390)، "طراحی خودرو و فیزیک امنیت تصادفات"
- [3] مریم کلویی، پ. (1392)، "تحلیل امنیت در شبکه های بین خودرویی"
- [4] محمدی زاده. میثاق، "vanet"، شبکه بین خودرویی موردی"
- [5] موسی پور، مسیح، "امنیت مسیریابی در شبکه های موردی"، سمینار کارشناسی ارشد، دانشگاه امیر کبیر، بهمن 90
- [6] سادات پور، وحید، رحمانی، مسعود، "افزایش ایمنی حمل و نقل با استفاده از ارتباطات مستقیم بین خودرویی"، کنفرانس ملی تصادفات و سوانح جاده ای ایران آذر 88
- [7] یوسفی، صالح، "تحلیل و ارزیابی همبندی و انتشار پیام ایمنی در شبکه بین خودرویی" سمینار حمل و نقل هوشمند دانشگاه علم و صنعت
- [8] اشعری. فرشته، فتحی. محمود، "کاربردهای ایمنی در سیستم های حمل و نقل هوشمند" مجموعه مقالات سومین کنفرانس بین المللی حوادث رانندگی، ۱۳۹۱
- [9] باقری خلیلی. سعید، شیخ السلامی. عبد الرضا، "تحلیلی بر تحقیقات انجام شده در شبکه های وسایل نقلیه، فصل نامه علمی ترویجی راهور، شماره ۱۵، ۱۳۹۰
- [10] شرفی. افسانه، زهره وند. حسین، اکبرپور. رضا، "معرفی شبکه بین خودرویی و انواع چالش های موجود در آن، مجموعه مقالات دومین همایش سراسری فن آوری اطلاعات و ارتباطات، بهمن ۱۳۹۰
- [11] بصیرت. حامد، سریانی. محسن، "دستیابی به ایمنی در خودروها با استفاده از شبکه های ارتباطی بین خودرویی" مجموعه مقالات کنفرانس بین المللی شهر الکترونیک، ۱۳۸۸
- [12] http://en.wikipedia.org/wiki/Vehicular_ad_hoc_network
- [13] www.paperdl.com
- [14] . Raya, M. , Aziz, A. , Hubaux, J.P. (2006), "Efficient Secure Aggregation in VANETs" International Conference on Mobile Computing and Networking, pp.67-75
- [15] Papadimitratos, P., Buttyan, L., Holczer, T., Freudiger, J., Raya, M. Ma, Z. and others
- [16] Kwon. Oje, et. al, "Collision Prediction at Intersection in Sensor Network Environment", Proceedings of the IEEE ITSC 2006, Toronto, Canada, September 17-20, 2006, pp 982-987.
- [17] Weiner. Scott J., " Feasibility of a 802.11 VANET Based Car Accident Alert System", Northeastern University, 2010.

[18] Zeadally. Sherali , Hunt. Ray , Chen. Yuh-Shyan , Irwin. Angela, Hassan. Aamir, " Vehicular ad hoc networks (VANETS): status, results, and challenges", Springer Science+Business Media, LLC 2010.

[19] K. Weniger, “PACMAN: Passive Autoconfiguration for Mobile Ad hoc Networks”, in IEEE Journal on Selected Areas in Communications, vol. 23, Issue 3, pp. 507–519, March 2005

[20] H. Ammari, H. El-Rewini, “Integration of Mobile Ad Hoc Networks and the Internet using Mobile Gateways”, in Proceedings of the 18th International Parallel and Distributed Processing Symposium (IPDPS’04), Santa Fe (Mexico), April 2004.

[21] De Poorter, E., Latré, B., Moerman, I. and Demeester, P. (2008) Symbiotic networks: Towards a new level of cooperation between wireless networks. *Wireless Personal Communications* 45(4), 479–495.