
بسم الله الرحمن الرحيم

دانشکده کامپیوتر و فناوری اطلاعات
گروه هوش مصنوعی
پایان‌نامه کارشناسی ارشد

طراحی یک مدل هوشمند امن برای ارتباطات وسائل نقلیه

مهدیه علی محمدی

استاد راهنما :
دکتر علی اکبر پویان

اساتید مشاور:
دکتر امید رضا معروضی
مهندس میثم یدالله زاده طبری

بهمن ۹۲
دانشگاه شاهرود

دانشکده : کامپیوتر و فناوری اطلاعات

گروه : هوش مصنوعی

پایان نامه کارشناسی ارشد خانم مهدیه علی محمدی

تحت عنوان: طراحی یک مدل هوشمند امن برای ارتباطات وسائل نقلیه

در تاریخ .....۹۲/۱۱/۲۶..... توسط کمیته تخصصی زیر جهت اخذ مدرک کارشناسی ارشد مورد ارزیابی و با درجه .....عالی..... مورد پذیرش قرار گرفت.

عضو هیأت داوران	نام ونام خانوادگی	مرتبهٔ علمی	امضاء
1ـ استادراهنما			
2ـ استاد مشاور			
3ـ نماینده شورای تحصیلات تکمیلی			
4ـ استاد ممتحن			
5 ـ استاد ممتحن			

رئیس دانشکده :

پـیامبر اکرم (ص): هیچ دانش آموزی نیست که به در خانه دانشمندی آمد و شد کند، مگر این که خداوند برای هر گامی که بر می‌دارد عبادت یک سال رقم زند.

تقدیم به هرآنکه به من علم آموخت.

تشکر و قدردانی

سپاس خدای را که سخنوران در ستودن او بمانند و شمارندگان شمردن نعمت‌های او ندانند و کوشندگان، حق او را گزاردن نتوانند. و سلام و درود بر محمّد و خاندان پاک او، طاهران معصوم، هم آنان که وجودمان وامدار وجودشان است؛ و نفرین پیوسته بر دشمنان ایشان تا روز رستاخیز.

برخود لازم می‌دانم از کلیه کسانی که بنده را در تهیه و تدوین این پایان‌نامه یاری نمودند، صمیمانه تشکر و قدردانی نمایم. به خصوص از استاد فرزانه جناب آقای دکتر پویان که در کلیه مراحل انجام این پژوهش با خوشرویی، مرا یاری و راهنمایی نمودند و نیز با نظرات مدبرانه خود شیوه تحقیق آموختند، از استاد فرهیخته جناب آقای دکتر معروضی که مشاوره لازم را در این خصوص ارائه نمودند و مهندس یدالله‌زاده که مرا در نگارش این اثر یاری نمودند و همچنین از دکتر حسن‌پور که با زحمات پیوسته ایشان شیوه تحقیق آموختم، صمیمانه تشکر و قدردانی می‌نمایم.

در انتها از خانواده و تمام اساتید دوران تحصیلم که در پیمودن این راه یاریم نمودند صمیمانه سپاسگزارم.

تعهد نامه

اینجانب مهدیه علی محمدی دانشجوی دوره کارشناسی ارشد رشته هوش مصنوعی دانشکده مهندسی کامپیوتر و فناوری اطلاعات دانشگاه شاهرود نویسنده پایان نامه "طراحی یک مدل هوشمند امن برای ارتباطات وسائل نقلیه" تحت راهنمائی دکتر علی اکبر پویان متعهد می شوم .

- تحقیقات در این پایان نامه توسط اینجانب انجام شده است و از صحت و اصالت برخوردار است .
- در استفاده از نتایج پژوهشهای محققان دیگر به مرجع مورد استفاده استناد شده است.
- مطالب مندرج در پایان نامه تاکنون توسط خود یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ جا ارائه نشده است .
- حقوق معنوی این اثر متعلق به دانشگاه شاهرود می باشد و مقالات مستخرج با نام « دانشگاه شاهرود » و یا « Shahrood University» به چاپ رسیده است.
- حقوق معنوی تمام افرادی که در به دست آمدن نتایج اصلی پایان نامه تأثیرگذار بوده اند در مقالات مستخرج از پایان نامه رعایت گردیده است.
- در کلیه مراحل انجام این پایان نامه ، در مواردی که از موجود زنده (یا بافتهای آنها) استفاده شده است ضوابط و اصول اخلاقی رعایت شده است .
- در کلیه مراحل انجام این پایان نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته یا استفاده شده است اصل رازداری ، ضوابط و اصول اخلاق انسانی رعایت شده است .

تاریخ: ۹۲/۱۱/۲۶

امضای دانشجو

مالکیت نتایج و حق نشر

- کلیه حقوق معنوی این اثر و محصولات آن (مقالات مستخرج ، کتاب ، برنامه های رایانه ای ، نرم افزار ها و تجهیزات ساخته شده است) متعلق به دانشگاه صنعتی شاهرود می باشد . این مطلب باید به نحو مقتضی در تولیدات علمی مربوطه ذکر شود .
- استفاده از اطلاعات و نتایج موجود در پایان نامه بدون ذکر مرجع مجاز نمی باشد.

چکیده

شبکه بین خودرویی امروزه به عنوان طرحی جامع و نوین مطرح شده است که هدف آن، برقراری ایمنی در جاده، مدیریت ترافیک و فراهم‌سازی کاربردهای رفاهی برای رانندگان و مسافران در جاده است.

ارتباطات خودروها در این شبکه به دو صورت خودرو به خودرو و خودرو به زیرساخت (واحدهای کنار جاده) می‌باشد. در این ارتباطات، پیامهای مختلفی حاوی رخدادهای مهم هشداردهنده در مورد وضعیت جاده و خودروها، اطلاعات ترافیکی، اطلاعات شخصی خودروها مثل سرعت و مکان ارسال می‌گردند. متاسفانه ارتباطات بیسیم و همچنین سرعت بالای تعداد زیادی از خودروهای موجود در شبکه، منجر به ایجاد چالشهایی در شبکه می‌شوند که از جمله ارسال اطلاعات نادرست، تغییر و ارسال مجدد پیامهای منتشر شده در شبکه، دورانداختن بسته‌های مسیریابی در شبکه و جعل هویت می‌توانند تاثیرات جبران‌ناپذیری بر زندگی افراد بگذارد. علاوه بر این، کاربران شبکه تمایل دارند که اطلاعات خصوصی آنها که منجر به شناسایی منحصر به فرد آنها در شبکه می‌شوند، حفظ گردند. بنابراین حفظ امنیت و حریم خصوصی دو مسئله بحرانی برای استفاده عملی این شبکه‌ها در زندگی واقعی هستند. بررسی‌ها نشان می‌دهند زیرساخت کلید عمومی راه‌حل مناسبی برای ایمن‌سازی ارتباطات در شبکه خودرویی می‌باشد. بنابراین در این پایان‌نامه به بررسی رخنه‌های موجود در این زیرساخت پرداخته و دو نیاز امنیتی مهم را بررسی کرده‌ایم.

در مسئله اول، مکانیابی در شبکه خودرویی بررسی شده است. برای تعداد زیادی از کاربردهای این شبکه، دریافت اطلاعات صحیح در مورد مکان خودروها یک نیاز اساسی است. به همین منظور به بهبود سیستمی برای مکانیابی پرداخته‌ایم که از واحدهای کنار جاده برای مکانیابی استفاده می‌کند و خطاهای جی.پی.اس را ندارد. در این بهبود نحوه آرایش واحدهای کنار جاده را به گونه‌ای تغییر داده‌ایم که دو مزیت حاصل شود؛ اولا، برای مکانیابی توسط خودروها، سربار ارتباطی با واحدهای کنار جاده کم می‌شود و ثانیا، در کاربرد تایید موقعیت خودروها، فضای حالتی که خودروی بدخواه می‌تواند یک موقعیت نادرست انتخاب کند کاهش می‌یابد.

در مسئله دوم، حمله سایبل[۱] بررسی شده است. در این حمله، خودروی بدخواه خود را به جای چند خودروی دیگر جا می‌زند و یا اینکه موجودیتهای ساختگی در شبکه ایجاد می‌کند. هدف او خلل در کاربردهای مبتنی بر رأی‌گیری، اختلال در مسیریابی و کاهش کارایی شبکه است. در این پایان‌نامه ابتدا حمله سایبل را شبیه‌سازی کرده و تاثیر سوء آن را در سه الگویتم مسیریابی مختلف نشان می‌دهیم. سپس با بررسی روشهای مختلف، بهترین روش مبارزه با این حمله یعنی مکانیزم زیرساخت کلید عمومی را انتخاب کرده و با بررسی یکی از پروتکل‌های پیشنهادی در این زمینه که نرخ شناسایی صددرصد دارد، به اصلاح روش پرداختیم.

کلید واژه: شبکه خودرویی، حمله سایبل، اختلال در مسیریابی، زیرساخت کلید عمومی، مکانیابی.

۱. Sybil

فهرست مقالات اتخاذ شده

- Alimohammadi M., Pouyan A. A.; Vehicular Ad Hoc Networks: Introduction and a proposal for vehicle positioning; ۱۳th International conference on Traffic and Transportation Engineering; ۲۰۱۴, published.
- Alimohammadi M., Pouyan A. A.; Performance Analysis of Cryptography Methods for Secure Message Exchanging in VANET, International Journal of Scientific & Engineering Research; ۵(۲); ۹۱۱-۹۱۷; ۲۰۱۴.
- Pouyan A. A., Alimohammadi M.; Sybil Attack Detection in Vehicular Networks; journal of Computer Science and Information Technology (CSIT); Horizon Research publishing; ۲(٤) , ۱۹۷-۲۰۲, ۲۰۱٤.
- Alimohammadi M., Pouyan A. A.; Defense Mechanisms Against Sybil Attack in Vehicular Ad hoc Networks, John Wiley & Sons, Security and Communication Networks, accepted.
- Hosseinirad S. M., Alimohammadi M., Basu S. K., Pouyan A. A.; An ICA Based LEACH Algorithm for Improving WSN Performance; ۶th Conference on Information and Knowledge Technology; ۲۰۱۴; submitted

فهرست مطالب

فهرست اشکال

فهرست جداول

فهرست علائم اختصاری

Vehicle to Vehicle	V۲V
Vehicle to Infrastructure or Vehicle to RSU	V۲I-V۲R
On Board Units	OBU
Road Side Unit	RSU
Vehicular Ad Hoc Network	VANET
Mobile Ad hoc Network	MANET
Dedicated Short Range Communications	DSRC
Trusted Authority	TA
Public Key Infrastructure	PKI
VANET PKI	VPKI
Certificate Authority	CA
Department of Motor Vehicle	DMV
Global Positioning System	GPS
Geographic Information System	GIS
Vehicle Collision Warning Systems	CWS
Differential GPS	DGPS
Intelligent Transportation System	ITS
Time Of Arrival	TOA

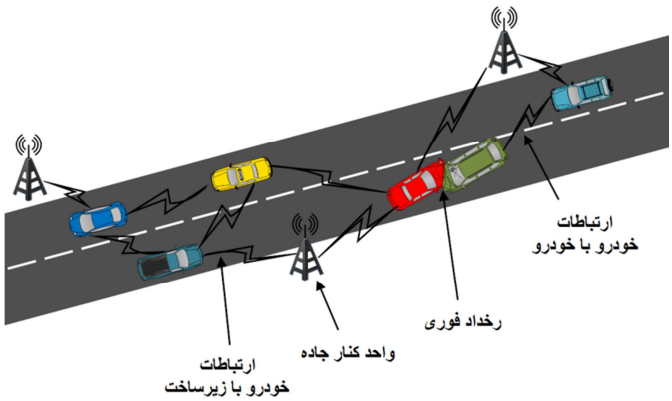
Time Difference Of Arrival	TDOA
Received Signal Strength Indicator	RSSI
Elliptic Curve Cryptography	ECC
Korea Information Security Agency	KISA
Differential cryptanalysis	DC
Linear Cryptanalysis	LC
Advanced Encryption Standard	AES
US National Institute of Standards and Technology	NIST
Data Encryption Standard	DES
Network Simulator ٢	NS٢
Constant Bit Rate	CBR
Ad-hoc On-demand Distance Vector	AODV
Dynamic Source Routing	DSR
Optimized Link State Routing	OLSR
Packet Delivery Factor	PDF

فصل ۱

مقدمه

۱-۱ معرفی شبکه خودرویی

ایده اولیه شبکه‌های بین خودرویی برای نخستین‌بار در سال ۱۹۹۸ توسط یک گروه مهندسی به نام سیستم‌های الکترونیکی Delphi Delco با همکاری شرکت IBM، با هدف استفاده در رنج وسیعی از کاربردها مطرح شد [۱]. شبکه خودرویی با استفاده از امواج رادیویی، انواع ارتباطات خودرو به خودرو [۱] و خودرو به زیرساخت[۲] را ایجاد می‌کند. خودروها به صورت کاملاً خودمختار با یکدیگر ارتباط برقرار کرده و یک شبکه غیرساختارمند بی‌سیم را ایجادمی‌کنند (شکل ۱-۱).



شکل ۱-۱. شمایی کلی از شبکه‌های بین خودرویی موردی

برای برقراری ارتباط، هر خودرو باید مجهز به ابزاری باشد که امکان ارتباطات بیسیم را فراهم سازد. این ابزار ارتباطی، واحد داخل خودرو[۳] نامیده می‌شود که با نصب این ابزار، هر خودرو قادر به ارتباط با خودروهای دیگر و واحدهای کنار جاده[۴] می‌باشد. واحدهای کنار جاده واحدهایی نصب شده در نقاط شاخص کنار جاده هستند که این نقاط شاخص می‌توانند چراغ‌های راهنمایی رانندگی، علائم ترافیکی و

---

۱. Vehicle to Vehicle (V۲V)
۲. Vehicle to Infrastructure (V۲I) یا Vehicle to RSU (V۲R)
۳. OnBoard Units (OBU)
۴. Road Side Units (RSU)

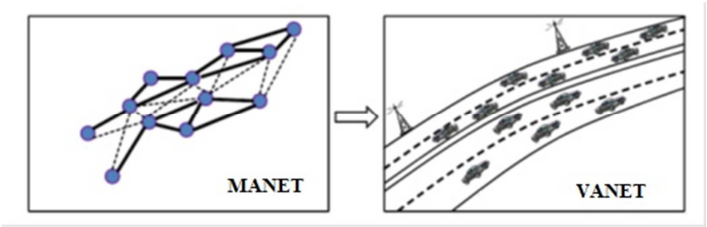
مسیریاب‌های بیسیم باشند که دسترسی به خودروهای روی جاده را فراهم می‌کنند. واحدهای کنار جاده می‌توانند به ستون فقرات اینترنت وصل شده و سرویسهای گوناگونی همچون پروتکلهای کنترل انتقال و کاربردهای زمان واقعی مالتی مدیا را برای کاربران خود فراهم سازند. بدین ترتیب با وجود واحد داخل خودرو و واحدهای کنار جاده، یک شبکه خودسازمان‌یافته می‌تواند ایجاد شود که شبکه‌های بین خودرویی موردی[۱] نامیده می‌شود.

در حقیقت شبکه‌های خودرویی، یک نوع خاص از شبکه‌های سیار موردی [۲] هستند که نودها در این شبکه خودروها هستند. هر خودرو می‌تواند در هر لحظه خودروهای اطرافش را شناسایی‌کرده و با اتصال به آن‌ها یک شبکه تشکیل دهد و ارتباطات لازم را برقرار کند. این خودرو کمی بعدتر با خودروهای جدید اطرافش یک شبکه دیگر ایجاد خواهد کرد. مبنای اصلی شبکه‌های خودرویی غیرساختارمند بودن آن‌ها و استفاده از استاندارد ۸۰۲.۱۱p و مجموعه استانداردهای ارتباطات اختصاصی بردکوتاه [۲] است[۳].

۱-۲- خصوصیات

همانطور که اشاره شد، شبکه بین خودرویی موردی نوع خاصی از شبکه سیار موردی هستند به نحوی که نودهای سیار با خودروهای مجهز به واحد پردازشی داخل خودرو جایگزین شده است (شکل ۱-۱) که در نتیجه خصوصیاتی دارد که متمایز از خصوصیات شبکه‌های سیار موردی می‌باشد. این خصوصیات شامل موارد زیر می‌باشند [۳-۵].

۱. Vehicular Ad Hoc Network (VANET)
۲. Mobile Adhoc Network (MANET)
۳. Dedicated Short Range Communications (DSRC)



شکل ۱-۱ . ارتباط بین شبکه خودرویی موردی و شبکه سیار موردی [۳]

- **تغییر سریع در توپولوژی:** خودروها معمولاً با سرعت نسبی بالا حرکت می نمایند و بنابراین توپولوژی این شبکه‌ها بصورت پویا سریعا در حال تغییر است. برای خودروهایی که در یک جهت حرکت می‌کنند موقعیتهای آنها نسبت به هم تغییراتش آهسته بوده و برای خودروهایی که از مقابل هم حرکت می‌کنند این تغییرات خیلی سریع است.
- **عدم محدودیت توان:** برخلاف لپ‌تاپ‌ها، دستیار دیجیتال شخصی (PDAها) یا سنسورها، که محدودیت باطری دارند؛ شبکه بین خودرویی بدلیل اتکا بر انرژی نامحدود باطری از این محدودیت معاف است.
- **مقیاس وسیع:** شبکه‌های بین خودرویی در حالت کلی می توانند به بزرگی شبکه جاده‌ای باشند و تعداد زیاد خودروها باعث ایجاد شبکه‌ای در مقیاس وسیع از آنها می‌گردد. به گونه‌ای که مرتبه تعداد خودروها در واقعیت در حدود 10^7 می‌باشد. در نتیجه چالش‌های متفاوتی برای این نوع شبکه‌ها بروز می‌کنند.
- **تغییر تراکم خودروها در شبکه:** تعداد خودروهایی که در یک ناحیه مشخص از جاده هستند، در طول روز در حال تغییر است. به این معنا که در ساعات خاصی از روز تردد وسائل نقلیه بیشتر است. این امر از این لحاظ قابل تأمل است که شبکه‌های متراکم و کم تراکم در برخی از موارد ازجمله کنترل توان، کنترل بار و مسیریابی، تفاوت‌هایی زیادی با هم دارند. به عنوان مثال در یک شبکه

متراکم، گره‌ها سعی می‌کنند با کم کردن توان ارسالی از میزان تداخل‌ها و بار شبکه بکاهند، در حالی که در یک شبکه کم تراکم گره‌ها با بالابردن توان خود سعی دارند تا همبندی شبکه را حفظ نمایند.

- **تحرک بالا و در عین حال قابل پیش‌بینی:** سرعت وسائل نقلیه در شهرها معمولا تا ۶۰ کیلومتر بر ساعت است که این سرعت می‌تواند به ۱۲۰ کیلومتر بر ساعت در بزرگراه‌ها برسد. علاوه بر این، تحرک خودروها تصادفی نیست و در نتیجه، الگوی تحرک خودروها بر اثر شکل خاص جاده و محدودیتهای مقرراتی (از قبیل سرعت)، محدود می شود. این امر باعث شده است که عده‌ای از محققان تلاش نمایند که از این قابلیت پیش بینی برای بهبود کارایی الگوریتم‌ها استفاده نمایند. تعدادی از محققان نیز تلاش کرده‌اند که برای بالا بردن دقت شبیه سازی‌ها، مدل‌های تحرک ویژه برای این شبکه‌ها بنیان نهاده و تأثیر محدودیت‌های فوق را در آنها لحاظ نمایند [۶].
- **توپولوژی شبکه ارتباط زیادی به رفتار راننده دارد:** در شبکه خودرویی و بخصوص در کاربردهای ایمنی آن، رفتار راننده باید مد نظر قرار بگیرد. این امر در شبکه‌های 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. مثلاً هنگامی که که پیام مبتنی بر وقوع تصادف ارسال می‌گردد، خودروها با کم کردن سرعت، باعث ایجاد ازدحام و در نتیجه به وجود آمدن شبکه‌ای متراکم می‌شوند [۷].

۱-۳ کاربردهای شبکه خودرویی

کاربردهای شبکه خودرویی به دو دسته تقسیم می‌شوند؛ دسته اول کاربردهایی هستند که باعث افزایش ایمنی در جاده‌ها می‌شوند تحت عنوان کاربردهای ایمنی و دسته دوم کاربردهایی هستند که سرویسهای ارزشمندی را برای خودروها فراهم می‌کنند که از جمله این سرویسها می‌توان به سرویسهای سرگرمی اشاره کرد [۸-۱۰].

۱-۳-۱ کاربردهای ایمنی

کاربردهای ایمنی همانطور که قبلا اشاره شد، شمار تصادفات را تا حد زیادی می‌توانند کاهش دهند، بر حسب مطالعات انجام شده [۱۱]، در صورتیکه نیم ثانیه قبل از لحظه برخورد به راننده هشدار داده شود، ۶۰ درصد از شمار تصادفات کاهش خواهد یافت. سه سناریوی اصلی در کاربردهای ایمنی وجود دارد که شامل:

۱. تصادفات: زمانیکه رانندگان با سرعت بالا در جاده‌های اصلی حرکت می‌کنند و خودرویی در جلوی آنها حرکتی ناخواسته و غیر عادی دارد، زمان برای عکس‌العمل نشان دادن توسط راننده خیلی اندک است همچنین اگر یک تصادف رخ دهد، خودروهای نزدیک به خودروی مورد نظر، اغلب قبل از اینکه توقف کنند به یکدیگر برخورد خواهند کرد. کاربردهای حوزه ایمنی شبکه‌های VANET در اینجا برای اخطار به رانندگان از وقوع یک تصادف در آینده‌ای نزدیک مورد استفاده قرار می‌گیرند و به این ترتیب از یک تصادف زنجیره‌ای در جاده اجتناب خواهد شد. علاوه بر این با دریافت اخطار توسط راننده از تصادف اول نیز می‌توان جلوگیری کرد و به عنوان نمونه با رسیدن به یک پیچ خطرناک به راننده هشدار داد تا از سرعت خود بکاهد و به این ترتیب از هرگونه تصادفی با شرایط آب و هوایی یا جاده‌ای نامناسب تا حد امکان جلوگیری کرد.

۲. تقاطع‌ها: در واقعیت، رانندگی در نزدیکی یا در خود بزرگراهها یکی از چالشهای پیچیدی‌ای است که رانندگان با آن مواجه می‌شوند. زیرا با رسیدن دو یا چند جریان ترافیکی به هم احتمال وقوع تصادف افزایش می‌یابد. در سال ۲۰۰۳ برطبق اعلام وزارت حمل و نقل ایالات متحده آمریکا، برخوردهایی که در تقاطع‌ها اتفاق افتاده بیش از ۴۵ درصد از کل برخوردها و ۲۱ درصد از تصادفاتی است که منجر به فوت شده است. تعداد این تصادفات کشنده ۹۲۱۳ تصادف گزارش شده است [۱۲]. در این شرایط

اگر یک کاربرد مرتبط با ایمنی VANET برخوردهای قریب‌الوقوع را به راننده اطلاع دهد، تعداد تصادفات کاهش چشمگیری خواهد داشت.

۳. ترافیک جاده‌ای: کاربردهای مرتبط با ایمنی برای تعیین بهترین مسیر برای رانندگان به منظور رسیدن به مقصد می‌توانند مورد استفاده قرار بگیرند. با این کار، ترافیک جاده‌ها کاهش می‌یابد و از ایجاد ازدحام در مناطق خاصی از جاده جلوگیری می‌شود و در نتیجه ظرفیت جاده‌ها افزایش یافته جریان ترافیکی نرمی در جاده‌ها برقرار می‌شود. علاوه بر این، برقراری این شرایط تاثیر غیر مستقیمی هم بر کاهش تصادفات خواهد داشت زیرا اتلاف وقت رانندگان کمتر شده و در نتیجه رانندگان تمایل بیشتری به رعایت قوانین ترافیکی از خود نشان خواهند داد.

۱-۳-۲ کاربردهای غیرایمنی

کاربردهای غیر ایمنی فراهم کننده اطلاعات، آگهی‌ها و سرگرمی برای کاربران هستند. نمونه‌هایی از این کاربردها شامل موارد زیر می‌باشند.

۱. اتصال به اینترنت: امروزه دسترسی به اینترنت برای خیلی از افراد به عنوان یک نیاز روزانه مطرح است. بدین منظورواحدهای کنار جاده برای دستیابی به اینترنت می‌توانند به عنوان گذرگاه عمل کرده و امکان دسترسی به اینترنت و نیز آپلود یا دانلود mp۳ یا ویدئوهای با سایز کوچک را برای رانندگان خودروها فراهم نمایند. مسافران داخل خودروها نیز می‌توانند از امکانات دریافت و ارسال ایمیل، گشت و گذار در وب‌سایت‌ها و بازیهای آنلاین استفاده کنند.

۲. کاربردهای نظیر به نظیر: این کاربردها برای رفع خستگی مسافران می‌تواند مفید واقع شوند و امکان به اشتراک‌گذاری موزیک، فیلم و غیره و همچنین چت و بازی با یکدیگر را فراهم می‌کنند.

۳. کاربردهای یاری رسان: واحدهای کنار جاده می‌توانند به رانندگان کمک کنند که مکانهای مورد نظر خود را بیابند. این مکانها از قبیل نزدیکترین رستوران، کافی‌شاپ، منطقه خرید، پمپ بنزین و

پارکینگ می‌باشند. زمانیکه خودروها به یک واحد کنار جاده می‌رسند، درخواستهای خود را به واحد کنار جاده میفرستند؛ سپس واحد کنار جاده در بانک اطلاعاتی خود جستجو کرده و پاسخ درخواستهای آنها را می‌دهد. واحدهای کنار جاده می‌توانند در ورودی پارکینگها نیز قرار گیرند و بدین طریق خودروها قبل از ورود به پارکینگ از وجود فضای خالی در پارکینگ مطلع گردند و در صورت وجود فضای خالی برای پارک خودرو، واحدهای کنار جاده داخل پارکینگ می‌توانند خودروها را برای ورود به منطقه خالی مورد نظر راهنمایی کنند [۱۳]. در یک نمونه از این کار [۱۴]، با بررسی و یافتن نزدیکترین پارکینگ خالی و راهنمایی خودرو به داخل پارکینگ انجام شده است که علاوه بر این مورد امکان سرقت خودرو پارک شده در پارکینگ را نیز بررسی کرده و در صورت سرقت و خروج از پارکینگ امکان ردگیری را توسط درخواستهایی که به طور دوره‌ای توسط خودروهای پارک شده در پارکینگ باید به واحدهای کنار جاده نصب شده در پارکینگ گزارش داده شود فراهم می‌کند و بدین طریق با دریافت این پیامها توسط خودروهای خارج از پارکینگ و واحدهای کنار جاده، خودروی سرقت شده را ردگیری کرد.

۴. کاربردهای تجاری: واحدهای کنار جاده می‌توانند به فروشگاهها کمک کنند که آگهی‌های خود از قبیل پیشنهادهای ویژه آخر هفته، آگهی‌های هفتگی و سهمیه‌های بلیت فیلم را پخش کنند. علاوه بر این رانندگان قادر خواهند بود که در برخی موارد بلیت خود را مستقیما از واحدهای کنار جاده خریداری کنند.

۵. کاربرد در دریافت اطلاعات محیط: VANETها می‌توانند اطلاعات محیطی را از طریق خودروها جمع-آوری کنند. در این راستا سنسورهای نصب شده بر روی خودروها داده‌هایی چون اطلاعات رطوبت و شرایط آب و هوایی را دریافت کرده و این اطلاعات را به واحدهای کنار جاده می‌فرستند. واحدهای کنار جاده نیز اطلاعات تمام خودروها در رنج خود را برای استفاده‌های آتی جمع‌آوری می‌کنند.

۱-۴- امنیت در شبکه بین خودرویی

۱-۴-۱- رفتارهای امنیتی

از آنجا که هم‌بندی (توپولوژی) شبکه‌های موردی همیشه در حال تغییر و دگرگونی است و هیچ نودی جای ثابت و مشخصی در شبکه نداشته و نودها خود ارتباطات درون شبکه‌ای را مدیریت و سرویس‌دهی می‌کنند که در نتیجه مشکلات امنیتی زیادی در این شبکه به وجود می‌آیند. در این‌گونه شبکه‌ها نمی‌توان از هیچ سرویس یا دستگاه سخت‌افزاری برای تأمین امنیت و بالا بردن ضریب اطمینان استفاده کرد و کافی است یک مهاجم برای سرقت اطلاعات، جایی در شبکه را برای اقامت پیدا کند. در این صورت قادر به ارسال مجدد بسته‌ها به منظور اخلال در شبکه، تغییر محتوای بسته‌ها، جعل و تغییر هویت و بدست اوردن اطلاعات خصوصی خودروها همچون مسیر و مکان خودروها خواهد بود. بنابراین قبل از پیاده‌سازی و استفاده از کاربردهای گوناگون شبکه بین خودرویی موردی، دو مسئله مهم امنیت و حفظ حریم شخصی در این شبکه‌ها باید حل شوند [۱۵-۱۷]. 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 واحد به صورت عمومی و غیره مشکل است، زیرا این‌گونه شبکه‌ها بیشتر بدون برنامه‌ریزی قبلی ایجاد می‌شوند و برای مدت کوتاهی به برقراری امنیت نیاز دارند. برای جمع‌بندی این بخش باید بگوییم که عمده حملات به شبکه‌های موردی از جانب مسیریابی (Routing) است و حملات جدید براساس آسیب‌پذیری‌های پروتکل‌ها و الگوریتم‌های مسیریابی به وجود می‌آیند.

پذیرش یک نوع پروتکل IEEE ۸۰۲.۱۱ توسط کارخانه‌های وسائل نقلیه، کار مهاجم را در شبکه‌های VANET راحت‌تر می‌کند. اگر امنیت در این شبکه‌ها در نظر گرفته نشود، این شبکه‌ها مانند یک شمشیر دو لبه عمل می‌کنند بنابراین با لحاظ کردن امنیت در این شبکه‌ها رفتارهای امنیتی در VANET را به صورت زیر دسته‌بندی می‌کنیم [۳].

۱. پارازیت: یک حمله‌کننده عمدا تعداد زیادی از پیامهای جعلی را تولید کرده تا با شلوغ کردن کانال ارتباطی مانع ارتباطات نرمال سایر خودروها شود.

۲. جعل پیام و سندسازی: یک حمله‌کننده با نیات بدخواهانه می‌تواند یک حمله سندسازی را راه بیاندازد که این کار بصورت بالقوه باعث بروز تصادفات می‌شود. بنابراین تازگی و صحت پیامهای انتقال یافته در ارتباطات بین خودروها (V۲V) برای اطمینان از عدم جعل پیامهای دریافت شده مهم هستند.

۳. دستکاری ترافیک در انتقال بسته: در این نوع حمله، یک حمله کننده به صورت عمدی باعث تاخیر، حذف، خرابی یا تغییر در پیامها می‌شود تا به ارتباطات نرمال V۲V در شبکه آسیب بزند.

۴. جعل هویت: در این حمله هدف حمله کننده اینست که برای پیاده‌سازی اهداف خود دیگران را متقاعد کند که یک وسیله قانونی در شبکه است. مثلا با این کار ادعا می‌کند که یک خودروی اورژانس است و وسائل نقلیه‌ای که در جلویش هستند را برای عبور خود کنار می‌زند.

۵. شکستن حریم خصوصی: در VANETها، جمع‌آوری اطلاعات خصوصی وسیله نقلیه از سربار ارتباطات خودروها کار آسانی است و بنابراین اگر یک حمله کننده پیامهای کافی را بتواند از خودروها جمع‌آوری کند، با استنتاج روی اطلاعات شخصی خودروی مورد نظر، حریم شخصی خودرو شکسته شده و اطلاعات خصوصیش فاش خواهد شد.

۶. دستکاری روی خودرو: علاوه بر سوءاستفاده از پروتکلهای ارتباطی، ممکن است حمله‌کننده دیتا را در همان مبدا دستکاری کند. دستکاری دیتا در مبدا، هم با دستکاری حسگرهای نصب شده بر روی

خودرو می‌تواند باشد و هم با بکارگیری سخت افزارهایی خاص. به عنوان نمونه حمله کننده می‌تواند سنسوری را از کار بیاندازد یا مقداری یخ در اطراف سنسور بگذارد تا سنسور پیام جعلی هشدار مبنی بر جاده یخی را برای خودروهای دیگر ارسال کند.

۱-۴-۲- نیازمندی‌های امنیتی

۱. **اعتبارسنجی**[۱]: اعتبارسنجی توانایی ثابت‌کردن اینست که یک کاربر همان شخصی است که ادعا می‌کند. اعتبارسنجی پیام یک نیاز حیاتی در VANET است چون این اطمینان را فراهم می‌کند که پیام دریافت شده در شبکه از طرف یک خودرو قانونی وتعیین اعتبار شده در شبکه ارسال شده است.

۲. **یکپارچگی**[۲]: اطمینان از اینکه پیام‌های مبادله شده بین خودروها در معرض تغییر، اضافه یا حذف قرار نگرفته‌اند. در واقع این ویژگی در صورت برقراری، این اطمینان را فراهم می‌کند که همه پیام‌های فرستاده شده توسط خودروها باید بدون تغییر تحویل داده شوند.

۳. **عدم انکار**[۳]: جلوگیری از اینکه یک وسیله وجود و یا محتوای پیام ارسال شده توسط خود را انکار کند. این ویژگی یک خصوصیت بحرانی در VANET است چون اینگونه یک مهاجم از انکار حملاتی که خود راه انداخته است خودداری می‌کند.

۴. **کنترل دسترسی**[۴]: نیاز برای تامین عملیات ایمن و قابل اطمینان یک سیستم را کنترل دسترسی گویند. در VANET هر موجودیت با رفتار سوء باید از شبکه طرد شود که از امنیت موجودیت‌های غیر قانونی شبکه محافظت کنیم. علاوه بر این هر عملی که از سوی آن موجودیت مورد نظر با رفتار سوء دریافت شده باید کنسل گردد.

---

۱. Authentication
۲. Integrity
۳. Non-repudiation
۴. Access control

۵. **حریم خصوصی**[۱]: توانایی حفاظت از اطلاعات خصوصی، از یک گروه تصدیق نشده در شبکه را حریم خصوصی گویند. در VANET شناسه واقعی هر خودروی شخصی تنها برای خودروهای دیگر و واحدهای کنار جاده پنهان است. این شناسه باید برای تصدیق کننده قابل اطمینان[۲] یا واحد TA آشکار باشد. علاوه بر شناسه هر خودرو موقعیت و مکان خودرو نیز باید برای خودروهای دیگر مخفی بماند و به این ترتیب مسیر خودرو قابل ردگیری نباشد.

۱-۵ هدف و رویکرد پژوهش

هدف از این پژوهش این است که با بررسی ویژگیهای این شبکه و ضرورت مسئله امنیت، رخنه‌ها و مشکلات را در برخی مدلهای امنیتی موجود پیدا کرده و به منظور برطرف نمودن آنها راه‌حلهای کارایی پیشنهاد و یا ارائه دهیم. دو مشکل امنیتی مهمی که در این زمینه مورد بحث و بررسی قرار می‌گیرند شامل: ۱. ارسال موقعیت نادرست توسط خودروی بدخواه در ارسال دوره‌ای پیامهای حاوی اطلاعات مکانی و ۲. راه‌اندازی حمله سایبل برای افت کارایی شبکه و حفظ منافع حمله‌کننده است.

اطلاعات موقعیت برای کاربردهای زیادی در شبکه خودرویی مورد استفاده قرار می‌گیرد، از جمله مسیریابی، مدیریت ترافیک، عبور کور از تقاطع (عبور از تقاطع‌های بدون چراغ)، اصلاح دید راننده، پارک خودکار و کاربردهایی که خودروها با همکاری با یکدیگر هدف خاصی را مثل عبور ایمن از تقاطع برآورده می‌کنند. بنابراین با توجه به اهمیت صحیح بودن اطلاعات مکانی خودروها، تایید موقعیت خودرو به عنوان یک نیاز امنیتی در این زمینه مطرح شده است [۱۹,۱۸]. پس می‌توان مدلی برای تایید موقعیت در این شبکه‌ها مورد استفاده قرار داد که خودروهای بدخواه در شبکه شناسایی شوند. در واقع اگر خودروها در ارسال موقعیت نادرست محدودتر باشند و این امکان وجود داشته باشد که از همان ابتدا خودرو نتواند اطلاعات اشتباه ارسال کند، این نیت بدخواهانه خودروی بدخواه با مکانیزمهای ساده‌تر، بدون مبادلات

---

۱. Privacy
۲. Trusted Authority (TA)

پیامهای اضافی در شبکه، خنثی می‌شود. این امر در این پژوهش با بررسی یکی از روشهای مکانیابی مبتنی بر واحدهای کنار جاده، که معایب روش مکانیابی متداول جی.پی.اس را ندارد، ممکن شده است. در واقع باید راهی وجود داشته باشد که خودروی بدخواه فضای حالت کمتری برای انتخاب یک موقعیت نادرستی داشته باشد که توسط واحدهای کنار جاده قابل شناسایی نباشد. با بررسیهای انجام شده تغییر آرایش واحدهای کنار جاده تاثیر زیادی در برآوردن این هدف دارد که در این پژوهش بررسی می‌شود.

راه‌اندازی حمله سایبل در شبکه خودرویی، با اهداف مختلفی صورت می‌گیرد. این اهداف شامل مواردی چون: افت کارایی الگوریتمهای مسیریابی، عدم تحویل بسته‌های حاوی پیام هشدار به سایر خودروها و در نتیجه اختلال در کاربردهای مدیریت ترافیک و همچنین رسیدن به منافع خودروی بدخواه با اختلال در کاربردهای مبتنی بر سیستم رأی‌گیری می‌باشد. بنابراین شناسایی موجودیتهای سایبل و خودروی بدخواه به عنوان یک نیاز امنیتی در این شبکه تعریف شده است. اما برای سنجش اهمیت پرداختن به این موضوع به عنوان یک بحث مجزا، بهتر است میزان اختلال این حمله حداقل در یکی از کاربردهای مهم شبکه خودرویی، که این حمله در آن تاثیرگذار است، بررسی گردد. این بررسی در این پژوهش بر روی کاربرد مسیریابی در شبکه خودرویی، با روشهای متداولی که پاسخ بهتری در شبکه خودرویی می‌دهند، انجام می‌شود. پس از تعریف اهمیت پرداختن به این حمله، باشبیه‌سازی حمله در کاربرد مسیریابی، حال باید روش مناسبی برای دفاع انتخاب کرد. با بررسی راهکارهای مختلف در این زمینه بدلیل تنوع و کثرت تعداد کارهای انجام شده، ابتدا باید ذهنیتی روشن در مورد میزان کارایی هر یک پیدا کرد که بهترین کار در این راستا دسته‌بندی روشهای موجود است تا بتوان به سراغ مجموعه‌ای رفت که هم اهداف کلی ما را برآورده نماید و هم اینکه از نظر هزینه با بودجه اختصاص یافته مطابقت داشته باشد. پس از انتخاب مجموعه راهکارهای مناسب، باید به بررسی نواقص و مشکلات پرداخت. در این پژوهش با بررسی موارد متعدد، این حملات دسته‌بندی می‌شوند و به دلیل مزایای سیستمهای مبتنی بر

رمزنگاری و احراز هویت در ارتباطات امن خودرویی، این دسته می‌تواند به عنوان بهترین راهکار انتخاب شود. بعد از این، روشی باید انتخاب شود که نرخ شناسایی بالایی داشته باشد و زمان پردازش زیادی به واحد کنار جاده تحمیل نکند. چون این امر باعث می‌شود واحد کنار جاده مقیاس‌پذیری کمی داشته باشد و قادر نباشد همه خودروهایی که در رنج رادیویی او هستند سرویس‌دهی کند. روش مناسبی در این پایان‌نامه انتخاب می‌شود که این ویژگیهای اصلی را داراست. در این پژوهش به اصلاح این روش و بررسی آن از نظر امکان پیاده‌سازی و بار محاسباتی تحمیل شده به واحدهای کنار جاده می‌پردازیم.

۱-۶ مشکلات پژوهش و نیازها

این پژوهش در راستای بررسی راهکارهای ایمنی و پروتکلهای امنیتی در شبکه خودرویی می‌باشد. بنابراین یکی از مواردی که در اکثر پروتکلهای امنیتی در سطح بالا مطرح می‌شود (پروتکلهایی که خیلی از نیازهای ایمنی را تامین می‌کنند و دیدگاه امنیتی دارند)، نیاز به استفاده از الگوریتمهای رمزنگاری متقارن و نامتقارن و همچنین امضای دیجیتال است. برخی از روشهای رمزنگاری متقارن به طور کلی در تعدادی از کارهای پژوهشی بررسی شده‌اند، اما مقایسه‌ای بین روشهای متداول و برخی دیگر از روشهای خاص دیگر که از نظر ایمنی مناسب هستند و اما کاربرد خاص منظوره دارند، در حوزه رمزنگاری متقارن انجام نشده است. همچنین در موارد بررسی شده، مقایسه‌ای بین روشهای رمز نامتقارن با هدف رمزنگاری کلید عمومی با طول کلیدهای مختلف و بررسی طول پیام به طور جامع انجام نشده است تا بتوان روشی را انتخاب کرد که با شرایط پیش‌رو و اندازه پیامهای مختلف کاراتر و قابل استفاده باشد. دو فاکتور اساسی برای انتخاب روشهای رمزنگاری در شبکه خودرویی، ایمنی کافی و زمان اجرای کم هستند. بنابراین نیاز است که این بررسی به طور مجزا انجام گیرد تا انتخاب ما را در مورد الگوریتمهای رمزنگاری مورد نیاز هدفمند کرده و زمان اجرای پروتکل تحت پیاده‌سازی را بهینه نماید. این امر به طور مجزا در این پژوهش انجام می‌شود.

۱-۷ ساختار پایان‌نامه

در فصل دوم برای فهمیدن نقاط ضعف و فهم کلیت موضوع، به طور خلاصه به بررسی برخی پژوهش-های انجام شده در این زمینه می‌پردازیم.

در فصل سوم از این پایان‌نامه، یکی از موارد پرکاربرد در شبکه خودرویی یعنی مکانیابی در شبکه را بررسی کرده و با بیان نقص‌های سیستم موقعیت‌یاب جهانی که کاربرد زیادی برای مکانیابی در این شبکه دارد، به بررسی مدلی برای مکانیابی خودروها می‌پردازیم که از واحدهای کنار جاده برای موقعیت‌یابی استفاده می‌کند. این مدل را با رویکرد توجه به مسئله امنیتی تایید موقعیت خودروها، تحلیل کرده و سپس با بررسی این مدل در زمینه پاسخ به این نیاز امنیتی، به بهبود آرایش واحدهای کنار جاده برای کاهش امکان ارسال موقعیت نادرست توسط خودروهای بدخواه در شبکه می‌پردازیم.

در فصل چهارم، یک مجموعه از الگوریتمهای رمزنگاری را از نظر ایمنی و زمان اجرا که دو فاکتور کلیدی در کاربردهای شبکه خودرویی هستند، تحلیل می‌کنیم. برای انتخاب بهترین روش برای پیاده-سازی در پروتکلهای امنیتی شبکه خودرویی، این روشها را پیاده‌سازی می‌کنیم و پس از ارزیابی روشها، بهترین روش را از نظر ایمنی و زمان اجرا پیشنهاد می‌دهیم.

در فصل پنجم، به بررسی یکی از حملات رایج، حمله سایبل، در این شبکه می‌پردازیم و با شبیه‌سازی این حمله تاثیر منفی و اختلال آن را در یکی از موارد پرکاربرد شبکه یعنی مسیریابی، نشان می‌دهیم. سپس یکی از روشهای پیشنهادی در این زمینه را برای شناسایی حمله، اصلاح کرده و پیاده‌سازی می-کنیم تا مقیاس‌پذیری و امکان پیاده‌سازی عملی آن را بررسی نماییم.

در فصل ششم، نتایج و جمع‌بندی پژوهش‌های انجام شده را ارائه می‌دهیم و در پایان موضوعاتی برای تحقیق در آینده پیشنهاد می‌گردند.

فصل ۲

مروری بر کارهای گذشته

۲-۱- مقدمه

در کل برای حفظ ایمنی و ناشناخته ماندن خودروها در شبکه باید از مکانیزم‌های رمزنگاری و تصدیق هویت استفاده کرد. چون تنها با استفاده از این روش است که انتقال محرمانه اطلاعات شخصی و همچنین حفظ حریم شخصی هر دو امکان‌پذیر است. علاوه بر این، این روشها در طرح مدلی برای مقابله با حملات مختلف از جمله حمله سایبل می‌توانند مورد استفاده قرار بگیرند. در ابتدای این بخش برخی از کارهای انجام شده در زمینه تامین امنیت و حفظ حریم خصوصی در شبکه بین خودرویی را بیان می‌کنیم.

در کنار ایمن‌سازی ارتباطات در شبکه باید از حملات مختلف که در مدل امن ارتباطات خودرویی امکان‌پذیر است جلوگیری کرد. به همین دلیل در بخش دوم از این فصل، یکی از حمله های مرسوم به نام حمله سایبل را که در شبکه‌های سنسوری و شبکه‌های موردی مورد بحث است، بررسی می‌کنیم. در این راستا، راهکارهای مناسب جهت شناسایی حمله را به سه دسته تقسیم نموده و سپس به ارائه برخی روشهای کارا در هر دسته می‌پردازیم.

۲-۲- مدل امن ارتباط خودرو با خودرو[۱] و خودرو با زیرساخت[۲]

موضوع امنیت و حریم خصوصی از سال ۲۰۰۴ تاکنون در حوزه صنعتی و پژوهشی به طور خاص مورد بررسی قرار گرفته است. در [۲۱,۲۰] اولین موضوع مورد بحث در حوزه برقراری امنیت و حفظ حریم شخصی در شبکه خودرویی، بکارگیری یک زیرساخت کلید عمومی مناسب برای حفاظت از اطلاعات مبادله شده و اعتبارسنجی متقابل افراد موجود در شبکه بیان شده است و برای حفظ حریم شخصی پیشنهاد شده است که از اسم مستعار استفاده شود تا به این ترتیب خودروها در شبکه گمنام باشند و حریم آنها فاش نشود.

---

[۱] . Vehicle to Vehicle (V۲V)

[۲] . Vehicle to Infrastructure (V۲I) - Vehicle to RSU (V۲R)

برای رسیدن به دو هدف اعتبارسنجی پیام و گمنامی در شبکه، Raya و همکاران در [۲۲,۱۵] پیشنهاد داده‌اند که هر خودرو از قبل با تعداد زیادی از جفت کلید عمومی و خصوصی و نیز گواهینامه‌های کلید عمومی متناظر با آنها، بارگذاری شود. در این کار همه پیام‌های ترافیکی با یک مدل بر مبنای کلید عمومی امضا می‌شوند و برای رسیدن به هدف حفظ حریم شخصی نیز هر جفت کلید عمومی و خصوصی در یک دوره زمانی کوتاه استفاده شده و یک شماره شناسایی ساختگی یا شبه شناسه[۱] در هر گواهینامه کلید عمومی استفاده شده است. علاوه بر این، یک بازه زمانی امن محاسبه شده است که به این ترتیب هر خودرو باید شماره شناسایی ساختگی خود را حداقل یکبار در این بازه تغییر دهد و با این کار دو شماره شناسایی متوالی از یک خودرو نمی‌توانند توسط یک دشمن متصل شده (دشمن نمی‌تواند بفهمد که دو شماره متعلق به یک خودرو هستند) و اطلاعات خودرو فاش شود. خصیصه حریم شخصی با این کار حفظ می‌شود و این شیوه، متد کارایی است اما در این متد برای اینکه بتوان این اطلاعات امنیتی را در هر خودرو ذخیره کرد به ظرفیت ذخیره‌سازی زیادی نیاز است. علاوه بر این در سمت واحد اعتبارسنجی رکورد همه شماره‌های شناسایی ساختگی و جفت کلید متناظر با آنها را برای همه خودروها باید نگه‌داری کرد. در نتیجه این متد هم برای واحد اعتبارسنجی دشوار است که شناسه واقعی یک خودروی بدخواه را بیابد و هم اینکه مدیریت این شماره‌های شناسایی ساختگی دشوار خواهد بود.

به منظور غلبه بر ضعف‌هایی که در کار پیشین بیان شد، Lin و همکاران در [۲۳] یک مدل امضای گروهی را توسعه داد که در این مدل، دیگر نیازی به شناسایی منحصر به فرد خودروها نیست و همه خودروهایی که در یک گروه هستند یک کلید عمومی واحد را به اشتراک می‌گذارند در حالیکه هرکدام کلید خصوصی مربوط به خود را دارند که متناظر با کلید عمومی گروه است. زمانیکه یک خودرو یک پیام امضا شده را دریافت می‌کند، این پیام را با کلید عمومی گروه تصدیق می‌کند و با این کار فقط می‌فهمد

[۱]. Pseudo ID

که آیا پیام توسط یک کاربر قانونی عضو گروه ارسال شده است یا خیر. اما در مورد اینکه چه کسی از اعضای گروه این پیام را ارسال کرده است اطلاعاتی ندارد. بنابراین با این شیوه حریم خصوصی کاربر کاملا حفظ می‌شود و شماره شناسایی و اطلاعات کاربر توسط گیرنده قابل برداشت نیست. اما در شرایطی که درگیری و مشکلی در شبکه پیش بیاید، واحد اعتبارسنجی به عنوان مدیر گروه این توانایی را دارد که شناسه واقعی فرستنده را با کلید محرمانه مربوط به خود ردگیری کرده و بیابد. این روش، روش مناسبی به نظر می‌رسد اما معایبی هم دارد که یک عیب آن در موردی بروز می‌کند که بخواهیم گواهینامه یک فرد از گروه را فسخ کنیم. در این شرایط واحد اعتبارسنجی برای حذف کلید خصوصی یک فرد از گروه، باید کلیدهای امنیتی کل گروه را تغییر داده و به روز کند. عیب دیگر این روش اینست که با وجود اینکه این روش حریم خصوصی افراد را در شرایط عادی حفظ می‌کند، اما هزینه محاسباتی تصدیق یک امضای گروهی در مقایسه با مدل امضای سنتی برمبنای زیرساخت کلید عمومی[۱] بالاست که در نتیجه در سناریوهایی که تراکم ترافیک بالاست تا حد زیادی پیامها از دست می‌روند. در نتیجه در روشی که در نظر می‌گیریم کم بودن میزان محاسبات و کاهش زمان تصدیق یک موضوع بحرانی است.

به منظور کاهش سربار محاسباتی روش امضای گروهی Calandriello و همکاران در [۲۴] یک مدل هیبرید معرفی می‌کنند که مدل زیرساخت کلید عمومی سنتی و مدل امضای گروهی را ترکیب می‌کند. در این مدل مشابه با مدل امضای گروهی گفته شده، به هر خودرو یک کلید عمومی گروهی و یک کلید خصوصی اختصاص داده می‌شود. کلید عمومی برای همه اعضای گروه مشترک است و کلید خصوصی برای هر یک منحصر به فرد است. اختلاف این مدل با مدل قبلی در اینجاست که کلید خصوصی برای امضای پیام استفاده نمی‌شود بلکه از این کلید برای تولید گواهینامه‌های کلید عمومی موقت استفاده می‌شود. در واقع هر خودرو چند جفت کلید خصوصی و عمومی تولید کرده که یک گواهینامه کلید عمومی شامل یک

[۱] . Public key infrastructure (PKI)

شناسه ساختگی، طول عمر و همچنین یک امضاء متناظر با هر جفت کلید تولید می‌شود. امضای موجود در گواهینامه بجای واحد اعتبارسنجی، با کلید خصوصی خود خودروی مورد نظر امضا می‌شود. گزینه طول عمر در گواهینامه نشان می‌دهد که چه مدت گواهینامه معتبر است. این طول عمر باید کوتاه باشد به گونه‌ای که یک دشمن نتواند دو شناسه ساختگی مجزا را اتصال دهد. جفت کلید عمومی و خصوصی موقت کارکردشان همانند کارکرد ذکر شده در [۱۵] است و این کلیدها برای امضای پیامهای ترافیکی مورد استفاده قرار می‌گیرند. فرآیند فسخ نیز مانند روال گفته شده در [۲۳] است. اگر یک درگیری بوجود بیاید واحد اعتبارسنجی می‌تواند شناسه واقعی مهاجم را از طریق گواهینامه کلید عمومی ردگیری کند. چون گواهینامه توسط خودروها با استفاده از کلید خصوصی گروهی آنها امضا شده است. بنابراین این مدل هیبرید طراحی شده یک توازن بین زیرساخت کلید عمومی و امضای گروهی برقرار می‌کند و با وجود اینکه سربار محاسباتی کمتری از مدل امضای گروهی دارد، اما نسبت به زیرساخت کلید عمومی هنوز هم سربار محاسباتی آن بالاست. در این مدل، عمل حذف یک خودروی بدخواه از گروه همانند مدل قبلی نیاز به تعویض کلید مشترک گروه و کلیدهای اعضای گروه دارد که این امر بر بار این مدل می‌افزاید. پس این مدل هنوز نمی‌تواند موضوع مقیاس‌پذیری را پوشش دهد.

وجود واحدهای کنار جاده، یکی از خصوصیات منحصر به فرد شبکه‌های خودرویی است که در برخی از پژوهش‌ها بکارگیری این واحدها برای حفظ حریم خصوصی افراد پیشنهاد شده است.

Freudiger و همکاران در [۲۵] یک مدل منطقه مشترک[۱] را معرفی می‌کنند که حریم خصوصی افراد در این مدل حفظ می‌شود. در این کار، یک واحد کنار جاده یک منطقه مشترک را مدیریت می‌کند و شماره شناسایی ساختگی و کلیدهای عمومی متناظر نیز توسط خود خودروها تغییر می‌کنند. یک دشمن نمی‌تواند دو شماره شناسه ساختگی از یک خودرو را زمانیکه خودرو از یک منطقه مشترک در حال عبور

[۱]. Mix-Zone model

است لینک کند. فرض بر اینست که واحدهای کنار جاده در تقاطع‌ها قرار گرفته‌اند و خودروهایی که از یک تقاطع عبور می‌کنند، ابتدا اعتبارسنجی متقابل با واحد کنار جاده دارند و سپس یک کلید محرمانه از واحد کنار جاده دریافت می‌کنند. تمام خودروهای قانونی همان کلید محرمانه را به طور مشترک استفاه می‌کنند. زمانیکه خودروهای یک تقاطع، پیام‌های محرمانه را ارسال می‌کنند، ابتدا این پیامها را با کلید-های عمومی موقت خود امضا می‌کنند و سپس کل پیام را با کلیدهای محرمانه رمز می‌کنند. در این شرایط، یک دشمن بدون کلید محرمانه نمی‌تواند محتوای پیام را که گواهینامه‌های کلید عمومی استفاده شده را نیز شامل می‌شود ببیند و بدین ترتیب قادر نیست دو شماره شناسه ساختگی استفاده شده را قبل و بعد از اینکه یک خودرو از منطقه مشترک عبور کند، لینک کند. اما یک خودروی قانونی در این منطقه که کلید محرمانه را در اختیار دارد، می‌تواند دو شماره شناسایی را لینک کند. بنابراین این مدل قادر به خنثی کردن یک حمله داخلی نیست.

یکی از چالش‌هایی که در کارهای انجام شده وجود دارد در زمینه فسخ گواهینامه خودروهایی است که به عنوان خودروهای معاند در شبکه شناسایی می‌شوند که همانطور که اشاره شد عمل ردگیری و فسخ گواهینامه آنان از سوی واحدهای قابل اعتماد یا همان واحدهای اعتبارسنجی انجام می‌شود. در این عمل به محض مشخص شدن سوءرفتار از جانب یک کاربر شبکه توسط مدیر امنیتی سیستم، عمل ردگیری و حذف این کاربر انجام می‌شود.

۲-۳- مقابله با حمله سایبل

چند نوع از حملات شبکه‌های بین خودرویی تنها در حد آشنایی در فصل ۲ معرفی شدند. در اینجا حمله سایبل بیشتر مورد مطالعه و بررسی قرار می‌گیرد که در ابتدا تعریفی از آن بیان می‌گردد. همچنین یکی دیگر از مسائل مهم که در فرضیات شبکه و تبادل پیام در این شبکه‌ها مورد بحث قرار می‌گیرد و

نحوه شناسایی این حمله نباید خللی در آن ایجاد نماید، حفظ حریم خصوصی افراد است که شامل حفظ موقعیت خودروها و شماره شناسه آنها است.

حملات سایبل تهدیدی جدی برای شبکه‌های حسگر بیسیم به شمار می‌آیند. در چنین حملاتی، یک گره مخرب چندین هویت جعلی برای خود ایجاد کرده و گره‌های شبکه را گمراه می‌کند این حملات می-توانند در عملیاتی مثل مسیریابی، رأی‌گیری، تجمیع‌سازی داده‌ها، ارزیابی اعتبار گره‌ها، تخصیص عادلانه منابع و تشخیص بدرفتاری اختلال ایجاد کنند. در این حمله مکانیزم‌هایی که مبتنی بر رأی‌گیری هستند کارایی خود را از دست می‌دهند. چون برخی گره‌ها جعلی هستند و نمی توان به اطلاعات به دست آمده از آنها اعتماد کرد و همچنین با ایجاد هویتهای جعلی توسط خودروی بدخواه، در صورت هدایت بسته‌ها به این مکان‌های جعلی و دورانداختن بسته‌ها بجای هدایت آنها به مقصد، در مسیریابی بسته‌ها اختلال ایجاد می‌شود. راه حل‌های متنوعی برای تشخیص این حمله و حذف آن از بستر شبکه پیشنهاد شده است که در این قسمت، راه‌حل‌های موجود را به صورت زیر طبقه‌بندی می‌کنیم:

- روشهای تست منبع.
- روشهای مبتنی بر رمزنگاری و احراز هویت.
- روشهای مبتنی بر مکان‌یابی.

۲-۳-۱- روش تست منبع

این روش شامل منابعی چون منبع رادیویی، منابع محاسباتی و حافظه و همچنین منبع شناسه خودروها می‌باشد. در این روش، کشف و شناسایی موجودیت سایبل براساس بررسی منابعی است که توسط خودروها مورد استفاده قرار می‌گیرند. خودروی بدخواه و کلیه موجودیت‌های سایبل از منابع مشترک استفاده می‌نمایند. این منابع شامل حافظه و وسایل ذخیره‌سازی جانبی، پردازشگر حافظه و منابع محاسباتی، کانالهای ارتباطی و گیرنده و فرستنده سیگنال می‌باشند. با ردیابی پیامها و همچنین

مانیتور کردن خودروها و پی‌بردن به این موضوع که کدام خودروها از منابع مشترک جهت ارسال پیام و نیز پردازش سیگنالهای دریافتی استفاده می‌کنند می‌توان خودروهای بدرفتار را کشف کرد. این روش مستلزم وجود ابزارهای خاص جهت مانیتور کردن شبکه و ردیابی پیامها است.

در مورد منابع محاسباتی، همانطور که در [۲۶] بیان شده، خودروهایی که در حل یک پازل مشخص شکست می‌خورند، به عنوان خودروی ساختگی شناخته می‌شوند. در بررسی که در [۲۷] انجام شده، ادعا شده است که متد پیشنهادی در [۲۶] در شبکه‌های ادهاک عملی نیست و متدهای دیگری چون تست منبع رادیویی، ثبت خودروها و تایید موقعیت خودرو برای شناسایی حمله سایبل پیشنهاد شده است.

در روش تست منبع رادیویی [۲۸,۲۷]، فرض بر اینست که هر نود (در اینجا نود همان خودرو است) یک موجودیت فیزیکی است که شامل یک منبع رادیویی می‌باشد. هر منبع رادیویی در هر زمان فقط می-تواند بر روی یک کانال رادیویی به انتقال اطلاعات بپردازد. فرض کنید نودی می‌خواهد همسایگانخود را چک کند که سایبل هستند یا خیر. برای این منظور نود چک کننده پیامی را برای n نود همسایه خود از طریق n کانال مختلف پخش همگانی می‌کند و سپس یک کانال را به صورت تصادفی انتخاب کرده و برای دریافت پیام پاسخ نود موردنظر در این کانال، منتظر می‌ماند. در این شرایط اگر نودی که این کانال به او تخصیص یافته بود قانونی باشد، پیام را شنیده و پیام پاسخ را در همان کانال ارسال می‌کند در غیر اینصورت اگر نود غیر قانونی و بدخواه باشد قادر نیست که به طور همزمان در کانالهای مختلف، برای هویتهای مختلفش پیام را شنیده و پیام پاسخ را ارسال کند و بدین ترتیب نود سایبل شناسایی می‌شود. این متد در شبکه‌های سنسوری کاراست اما در شبکه‌های خودرویی قابل استفاده نیست. زیرا در این روش فرض بر اینست که یک نود قادر نیست در یک زمان بیش از یک کانال را برای ارسال و دریافت خود بکار گیرد. در صورتیکه چنین فرضی در شبکه‌های خودرویی ممکن نیست و یک خودرو قادر است بیش از یک کانال را برای ارسال و دریافت خود بکار بگیرد.

در مورد منبع شناسه، باید یک کنترل کننده از توزیع کلیه خودروها در شبکه مطلع باشد و شناسه خودروها را قبلا ثبت کرده باشد و در صورت مبادله پیام، اگر آدرس MAC و IP خودرویی در لیست قبلا ثبت نشده باشد، به عنوان خودروی جعلی شناخته می‌شود [۲۹]. در این متد برای حفظ حریم شخصی باید اطلاعات خودروها شامل شناسه خودروها به صورت امن در شبکه مبادله شود به گونه‌ای که این اطلاعات برای خودروهای دیگر قابل رؤیت نباشد. این مکانیزم هم در شبکه‌های خودرویی قابل بکارگیری نیست زیرا اولا برای ارسال پیامها باید شناسه یکه و واقعی خودروها در پیامها درج شود که حریم خصوصی نقض می‌شود و ثانیا نیاز به ثبت اولیه خودروها همراه با تصدیق فیزیکی جهت جلوگیری از ثبت خودروهای جعلی است که این امر در مراحل اولیه بکارگیری شبکه خودرویی که هنوز تمام مناطق و خودروها مجهز نیستند و همچنین در مورد خودروهایی که بین کشورها رفت و آمد دارند در صورت نبود زیرساخت یا مکانیزم واحد در دو کشور قابل استفاده نیست.

۲-۳-۲- روشهای مبتنی بر رمزنگاری و احراز هویت

در روشهای مبتنی بر رمزنگاری و احراز هویت که نمونه‌ای از آنها در [۳۲-۳۰,۲۷] بررسی شده است، مقابله با حمله سایبل با مکانیزم تصدیق هویت و رمزنگاری کلید عمومی بررسی شده است. در این پژوهش‌ها استفاده از زیرساخت کلید عمومی برای شبکه خودروی موردی[۱] پیشنهاد شده است و توزیع کلید، مسئله امنیت ارتباطات خودروها و همچنین حفظ حریم خصوصی رانندگان به طور کامل مورد بررسی قرار گرفته است. علاوه بر این برای فسخ گواهینامه که یکی از موضوعات چالش برانگیز در حفظ امنیت و کاهش سربار در ارتباطات بین خودرویی است راه‌حلی پیشنهاد شده است که از حمایت ایستگاه-های پایه برای ارسال پیامهای فسخ استفاده می‌کند. در این مکانیزم، همانطور که هر خودرو با رمزنگاری کلید عمومی اعتبارسنجی می‌شود، حمله سایبل نیز در جریان این اعتبارسنجی می‌تواند شناسایی شود

[۱]. VPKI

[۳۳]. روش شناسایی براساس رمزنگاری می‌تواند عملکرد خوبی برای شناسایی موجودیت‌های سایبل در شبکه داشته باشد و حریم خصوصی رانندگان را نیز حفظ نماید اما عیب این روش اینست که بکارگیری مکانیزم زیرساخت کلید عمومی و رمزنگاری با کلید عمومی یا تایید هویت پیام، پردازش بیشتری داشته و در نتیجه زمان بیشتری می‌برد و اندازه پیام نیز تا حدی افزایش می‌یابد. اما سیستم‌های کلید متقارن در مقایسه با سیستمهای کلید عمومی حافظه کمتری مصرف می‌کنند و مصرف انرژی و پهنای باند را کاهش می‌دهند و بهمین دلیل بیشتر سعی می‌شود در مواردی که امکان‌پذیر باشد از کلید متقارن استفاده کرد. در سیستم‌های کلید متقارن نیز توزیع کلید یک مسئله چالش برانگیز است [۳۴] که در این مورد معمولا از روش تبادل کلید دیفی هلمن استفاده می‌شود.

با وجود سربار افزایش زمان پردازش پیام، مصرف حافظه و افزایش پهنای باند در اثر استفاده از روشهای رمزنگاری و امضای دیجیتال، پژوهش‌های اخیر نشان داده‌اند که برای تبادل امن پیامها در شبکه خودرویی بکارگیری روش امضای دیجیتال یک امر رایج و لازم است و این مزیت را دارد که علاوه بر جلوگیری از حمله سایبل، ایمنی پیامها را تضمین می‌کند و پیام از حملاتی چون دستکاری و جعل محفوظ می‌ماند. همچنین با این روش قادر به حفظ حریم خصوصی رانندگان هستیم و تبادل پیامهای گروهی نیز امکان پذیر است. بنابراین با در نظر گرفتن کلیه نیازهای ایمنی که در این شبکه‌ها باید برقرار شوند در کنار شناسایی حمله سایبل، بکارگیری روشهای مبتنی بر احراز هویت با توجه به آسیب‌پذیر بودن روشهای با پیچیدگی محاسباتی و فضایی کمتر، مزیت بیشتری دارند.

از جمله روشهایی که از گواهینامه دیجیتال برای اثبات واقعی بودن خودرو استفاده شده است یک مدل شناسایی حمله سایبل بنام Footprint [۳۵] است که در این مدل از مسیر خودروها برای شناسایی استفاده می‌شود و حریم خصوصی خودروها شامل مکان خودروها در شبکه فاش نمی‌شود. عملکرد این مدل به این شکل است که با مواجه شدن خودرو با واحد کنار جاده به محض درخواست خودرو،

گواهینامه‌ای از سوی واحد کنار جاده صادر می‌شود که به این ترتیب حضور خودرو در زمان مشخص شده در محدوده این واحد کنار جاده اثبات می‌شود. برای شناسایی منحصر به فرد خودرو در شبکه، یک خودرو مجموعه‌ای از پیامهای تصدیق شده از واحدهای کنار جاده متوالی که بهم زنجیر شده را جمع‌آوری کرده و بدین ترتیب دنباله‌ای از این پیامها یک مسیر با اختفای مکان برای این خودرو شکل می‌دهند. با جمع-آوری گواهینامه‌های دریافتی توسط یک خودرو می‌توان مسیر آن را شناسایی و آن را ردیابی کرد و از مسیر خودرو آگاه شد که به همین دلیل در اینجا برای حفظ حریم خصوصی خودرو، واحد کنار جاده‌ای که این گواهینامه را امضا می‌کند هویتش آشکار نیست و از پیام امضا شده نمی‌توان فهمید کدام واحد کنار جاده در کدام مکان این گواهینامه را امضا کرده است. از طرفی پیامهای تصدیق شده نه به صورت دائم بلکه به صورت موقت قابل لینک هستند یعنی دو پیام صادر شده از یک واحد کنار جاده اگر و تنها اگر در همان دوره زمانی صادر شده باشند قابل شناسایی هستند. این هدف تنها برای این منظور است که استفاده از پیامهای تصدیق شده برای شناسایی خودروها به گمنام ماندنشان برای حفظ حریم خصوصی صدمه‌ای نزند. چون گاها حتی بدون دانستن اینکه کدام واحد کنار جاده پیام را امضا کرده، از جمع‌آوری پیامهای تصدیق شده در طول زمان برای شناسایی مسیر خودروها می‌توان استفاده کرد که با این محدودیت روی لینک پذیری دو پیام امضا شده، پیامهای تصدیق شده نمی‌توانند برای شناسایی طولانی مدت مورد استفاده قرار بگیرند. برای شناسایی حمله، در طی یک محاوره که توسط خودرو یا واحد کنار جاده مقداردهی اولیه شده است و برگزار کننده محاوره[1] نامیده می‌شود، خودروهایی که شرکت دارند باید مسیر خود را برای تایید به آن ارائه دهند. با ارسال مسیر همه خودروهایی که شرکت دارند، برگزار کننده محاوره می‌تواند شناسایی حمله را با تشکیل گراف متشکل از مسیرها و بررسی شباهت هریک از جفت مسیرها، به صورت آنلاین هدایت کند. در این مدل خودروهای بدخواه هم می‌توانند مسیرهای مختلف

[1] . Conversation holder

برای هویت‌های ساختگی خود بسازند. اما این مسیرهای ساخته شده باید شامل امضای واحدهای کنار جاده باشند که در زمان و مکان خاصی صادر شده است. این امر باعث می‌شود که خودروی بدخواه در ساخت مسیرهای گوناگون محدودیت داشته باشد و این مسیرها ناگزیر مشابه هستند و بر طبق معیار شباهت تعریف شده می‌توان دو مسیر را مقایسه و در صورت شباهت زیاد به عنوان سایبل تشخیص داد و حذف کرد. نرخ شناسایی در این مدل در یک سناریوی شهری بررسی شده ۹۸ درصد است. مزیتهای این متد شامل:

- در این پروتکل نیاز به شناسایی خودروها و آشکار شدن هویتشان نیست (ناشناخته ماندن خودروها).
- تنها نیاز است که خودروها مجهز به چیپ دریافت کننده جی.پی.اس و ماژول ارتباطات وایرلس DSRC باشند.
- شناسایی حمله سایبل می‌تواند به صورت آنلاین و مستقل، توسط یک برگزارکننده محاوره (یک خودرو مخصوص یا واحد کنار جاده) انجام شود.

اما محدودیت‌های این پروتکل شامل:

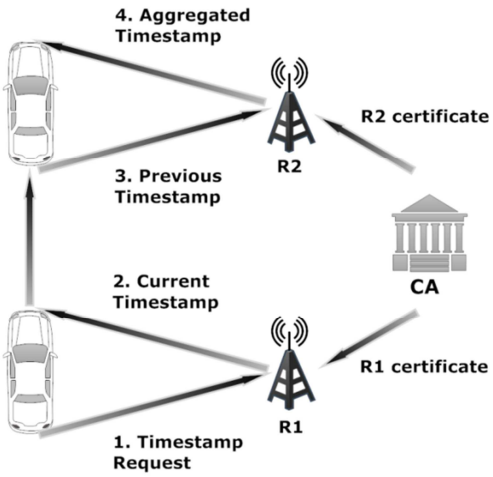
۱. شناسایی گراف کامل در گراف متشکل از مسیرها پیچیدگی نمایی دارد.
۲. در صورتیکه خودروهای بدخواه تحرک زیادی داشته باشند و سرعتشان بالاتر باشد می‌توانند مسیرهای طولانی‌تری ایجاد کنند. در نتیجه سایبلهایی که تشکیل می‌دهد شناسایی نمی‌شوند.
۳. این روش در صورتی که تعدادی واحد کنار جاده سازش شده وجود داشته باشد، آسیب‌پذیر است و باعث می‌شوند خودروهای بدخواه هر تعداد گواهینامه دریافت کنند به طوریکه مسیرهای متمایز ایجاد کنند که تشخیص‌پذیر نباشد.

۴. بکارگیری این پروتکل در بزرگراهها و مسیرهای بین شهری، به دلیل یکسان بودن مسیر برای اکثر خودروها و شباهت بین مسیرها، احتمال خطا را در مواردی که مسیرها متعلق به خودروهای قانونی هستند بالا می‌برد و آنها را به عنوان سایبل شناسایی می‌کند.

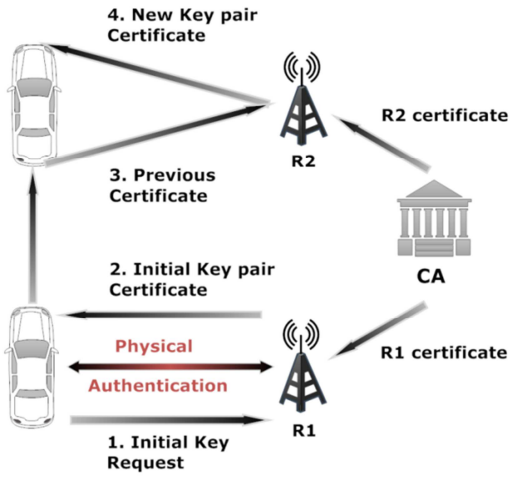
پروتکل دیگری نیز وجود دارد که این پروتکل نیز از مسیرهای ساخته شده برای شناسایی موجودیت-های سایبل استفاده می‌کند و به زیرساخت کلید عمومی نیازی ندارد [۳۶]. چون اولا در مراحل اولیه شکل‌گیری شبکه خودرویی تنها درصد کمی از خودروهای روی جاده هوشمند بوده و می‌توانند بخشی از این شبکه باشند و در نتیجه امکان دفاع در برابر حمله با کمک خودروهای مجاور ممکن است عملی نباشد؛ ثانیا در مراحل اولیه تنها مولفه‌های زیرساخت ضروری در شبکه موجودند و بکارگیری زیرساخت کلید عمومی اختصاصی خودرویی برای تایید خودروها احتمالا زمان‌بر است و ثالثا منابع موثق ثبت نام خودرو در میان چندین کشور نیاز است که روی یک مدل واحد برای گواهینامه توافق کنند. در نتیجه در اینکار دو هدف برای دو دیدگاه مبتنی بر گواهینامه موقت، مد نظر قرار گرفته شده که یک هدف مینیمم کردن نیازهای معماری سیستم و هزینه های محاسباتی برای مدیریت گواهینامه است و دیگری توانایی گسترش در یک مرحله اولیه از شبکه خودرویی است. در این مدل برای تصدیق خودروها، واحدهای کنار جاده تنها مولفه‌هایی هستند که گواهینامه صادر می‌کنند که این گواهینامه با عبور خودرو از کنار هر واحد کنار جاده بدست می‌آید. در این دیدگاه مشابه با Footprint، گرفتن گواهینامه مهر زمانی[۱] از واحد کنار جاده، متناظر با اثبات حضور خودرو در حیطه این واحد کنار جاده در زمان مشخص شده است. در اینجا با بهره‌گیری از همبستگی زمانی و مکانی بین خودروها و واحدهای کنار جاده می‌توان حمله سایبل را با چک کردن شباهت سری‌های گواهینامه مهر زمانی، بررسی کرد. علت استفاده از گواهینامه موقت اینست که گواهینامه طولانی مدت هم مشکلات حریم خصوصی دارد و هم مشکلات مدیریتی در صدور،

[۱] . Timestamp

توزیع، ذخیره و فسخ آن. در این دیدگاه فقط واحدهای کنار جاده هستند که توسط مرجع صدور گواهی دیجیتال[1] مدیریت و تایید می‌شوند. دو مدل معماری در اینکار بررسی شده که در نوع گواهینامه صادر شده از واحدهای کنار جاده متفاوتند. شکل (۲-۱) و (۲-۲) شمایی از دو روش استفاده شده در این مقاله هستند.



شکل ۲-۱. دیدگاه مبتنی بر گواهینامه آنی [۳۶]



شکل ۲-۲. دیدگاه مبتنی بر گواهینامه مهر زمانی [۳۶]

در مدل اول و دیدگاه گواهینامه مهر زمانی، خودروهای در حال رانندگی از مقابل واحدهای کنار جاده یک سری گواهینامه مهر زمانی دریافت می‌کنند که مجموعه گواهینامه‌های دریافت شده از تعداد محدودی واحد کنار جاده مجاور، مسیر در حال رانندگی اخیرشان و زمان را نشان می‌دهند. به دلیل تنوع الگوهای حرکتی خودروها احتمال عبور دو خودرو از چند واحد کنار جاده در همان زمان خیلی کم است. بدین ترتیب اگر دو پیام ترافیکی الگوهای گواهینامه مهر زمانی مشابهی داشته باشند احتمالا سایبل هستند و بدین ترتیب شناسایی حمله در این مدل با توجه به همین شباهت مسیرها انجام می‌شود.

[1] . Certificate authority (CA)

در دیدگاه دوم یعنی گواهینامه آنی[1]، هر واحد کنار جاده جفت کلید موقت و گواهینامه‌ای را صادر می‌کند که تنها برای یک منطقه محلی ویژه پوشیده شده توسط واحد کنار جاده، برای یک زمان محدود، صحیح هستند. برای بدست آوردن اولین گواهینامه نیاز است که خودرو یک واحد کنار جاده مجهز به دوربین یا وسیله‌های دیگری را برای اینکه تصدیق فیزیکی انجام شود بیابد. به محض اینکه خودرو اولین کلید و گواهینامه موقت خود را بدست آورد جفت کلید و گواهینامه خود را با واحدهای کنار جاده بعدی بروز کرده و به صورت یک گواهینامه زنجیر شده جدید در می‌آورد. در این پروتکل، گواهی دریافت شده از واحد کنار جاده جاری به مقدار درهم شده گواهینامه‌های قبلی به صورت یک زنجیره پیوند می‌خورد و گواهینامه موقت جدید را می‌سازد. هر خودرو تنها از یک گواهینامه موقت برای یک بازه مکانی واحد می-تواند استفاده کند و منحصر به فرد بودن گواهینامه و تصدیق فیزیکی اولیه، از حمله سایبل جلوگیری می-کند.

در مقایسه این دو پروتکل: مزیت دیدگاه مبتنی بر دنباله‌های مهر زمانی اینست که حریم خصوصی را حفظ می‌کند و نیاز به تصدیق اولیه واحدهای کنار جاده به صورت فیزیکی نیست. اما از معایب این روش اینست که نیاز به یک آرایش دقیق از واحدهای کنار جاده دارد طوری که ثابت شده است که برای جلوگیری از سوء استفاده و تشکیل یک مسیر ثانویه برای یک خودرو، نیاز است که در هر مسیری که منتهی به یک تقاطع می‌شود یک واحد کنار جاده نصب شده باشد در صورتیکه اینکار در مناطق شهری باعث افزایش هزینه می‌شود. در این مدل نیز همانند مدل بیان شده در Footprint، سناریوی شهری بررسی شده در صورتیکه استفاده از این روش در بزرگراهها احتمال شباهت مسیرها را بالا می‌برد. اشکال دیگر روش مبتنی بر مهر زمانی اینست که پیام ترافیکی می‌تواند طولانی باشد و تصدیق پیام ممکن است زمانبر شود. شناسایی حمله سایبل در این روش بر روی احتمال توزیع خودرو متکی است. اما مزیت اصلی

[1] . Temporary

دیدگاه گواهینامه آنی اینست که حمله سایبل در هر صورت می‌تواند شناسایی شود که این امر به دلیل انتساب یکه گواهینامه موقت به هر خودرو است و همچنین سایز پیام ترافیکی کوتاهتر از دیدگاه اول است. اما اشکال اساسی این روش نیاز اولیه برخی از واحدهای کنار جاده به تصدیق فیزیکی اولیه است که گواهینامه اولیه تا زمانی که خودرو یک واحد کنار جاده مجهز به دوربین را ملاقات نکند صادر نمی‌شود و بکارگیری دوربین در واحدهای کنار جاده برای این هدف هزینه بر است.

پروتکل دیگر برای مقابله با حمله سایبل ، پروتکلی تحت عنوان P^2DAP است [۳۷] که در این پروتکل تعداد زیادی شبه شناسه به هر خودرو اختصاص می‌یابد. این شناسه‌ها برای کل خودروها در ابتدا قبل از اختصاص به خودروها گروه بندی می‌شوند به گونه‌ای که مقدار درهم[۱] محاسبه شده شبه شناسه-های هر گروه مقدار واحدی می‌شود که با مقدار گروه دیگر متفاوت است. کلید درهم‌سازی در این حالت در اختیار واحدهای کنار جاده نیز قرار می‌گیرد. علاوه بر این در سطح دیگر شبه شناسه‌های متعلق به هر گروه با کلیدی که فقط در اختیار یک سازمان مرکزی است (سازمان وسائل نقلیه موتوری[۲] که در حکم همان مرجع صدور گواهی دیجیتال است) درهم‌سازی می‌شوند و این دو مقدار درهم محاسبه شده از یک شبه شناسه به عنوان پلاک منحصر به فرد خودرو در نظر گرفته می‌شود و کلیه شبه شناسه‌ها با همان مقدار درهم محاسبه شده در سطح اول و دوم به یک خودرو اختصاص می‌یابند. در اینکار برای حفظ حریم خصوصی از شبه شناسه استفاده شده که می‌تواند پس از طی مدتی معین از سوی سازمان مرکزی تغییر کند. همچنین برای امنیت بیشتر حریم خصوصی هر خودرو، واحد کنار جاده نمی‌تواند خودروی خاصی را در گروه مورد نظر شناسایی کند که اینکار به این دلیل است که در صورت سازش واحد کنار جاده با یک خودروی بدخواه، اطلاعات خودروها (ذخیره شده در واحد کنار جاده) در اختیار خودروی بدخواه قرار نگیرد. علاوه بر این کلیدی که برای درهم در اختیار واحد کنار جاده قرار دارد موقت بوده و به صورت

---

۱. Hash
۲. Department of Motor Vehicle (DMV)

دوره‌ای عوض می‌شود. برای امنیت بهتر در اینکار پروتکل باز هم بهبود یافته و در نسخه ای دیگر از چند سطح درهم بجای یک سطح استفاده شده که امکان شناسایی خودرو را از جانب خودروی بدخواهی که با یک واحد کنار جاده سازش کرده از بین ببرد. در شناسایی حمله سایبل، واحد کنار جاده شبه شناسه‌های متناظر با هر رخداد گزارش شده از جانب خودروهایی که همان رخداد را گزارش کرده‌اند در یک لیست قرار می‌دهد و سپس با بررسی مقدار درهم سطح اول (یا درهم دانه درشت[۱]) تمام شبه شناسه‌هایی که این مقدار درهم برای آنها یکسان است را در یک گزارش به سازمان مرکزی می‌فرستد. سازمان مرکزی با محاسبه مقدار درهم سطح دوم (یا درهم دانه ریز[۲]) این شبه شناسه‌ها آنهایی را که مقدار درهم دوم آنها برابر است را به عنوان سایبل فسخ می‌کند (چون متعلق به یک خودرو هستند) و آنهایی که برابر نیستند را به عنوان اخطار اشتباه[۳] رد می‌کند. این روش در حالت بهینه و اولیه آن می‌تواند همه سایبلها را به درستی تشخیص دهد. اما هزینه بر است و مقداری از بار محاسباتی بر روی واحد مرکزی است که این امر باعث افزایش ایمنی و احتمال شناسایی بالای حمله شده و اما منجر به ایجاد تاخیر و گلوگاه برای واحد مرکزی می‌شود. به همین منظور در اینکار یک رابطه سبک و سنگینی بین میزان شناسایی موجودیتهای سایبل و بار محاسباتی تحمیل شده به واحد مرکزی ایجاد می‌شود و با کاهش نرخ شناسایی بار تحمیل شده به واحد مرکزی کاهش می‌یابد که در نتیجه مقیاس‌پذیری شبکه افزایش می‌یابد. استفاده از این مدل یک حالت ایده‌آل است که زیرساخت شبکه کاملا برقرار بوده و همه خودروها برای ارسال و دریافت اطلاعات ایمنی باید قبلا در واحد مرکزی ثبت نام شده باشند و شبه‌شناسه‌های خود را از واحد مرکزی دریافت کنند که این امر استفاده از این مدل را در مراحل اولیه بکارگیری شبکه خودرویی در شهرها دشوار می‌کند. مشکل دیگر روش اینست که سازمان مرکزی برای شرایطی با ترافیک سنگین زراحی نشده است و ارتباطات اضافی منجر به ایجاد گلوگاه برای آن می‌شود [۳۷]. در این روش یک خودرو نمی-

---

۱. Coarse grained
۲. Fine grained
۳. False alarm

تواند موجودیتهای جدید در شبکه ایجاد کند چون این موجودیتها در سازمان مرکزی قبلا ثبت نام نشده-اند و همچنین خودروها نمی‌توانند همان رخداد خاصی که در شبکه پخش می‌کنند را با تعدادی از شبه شناسه‌های اختصاصی خود بفرستند (بجای یک شبه شناسه)؛ اما این امکان وجود دارد که شبه شناسه‌ها را از پیامهای دیگری که توسط خودروهای دیگر در شبکه مبادله می‌شوند برداشته و قبل از اینکه این شبه شناسه‌ها دور انداخته شوند، به عنوان سایبل مورد استفاده قرار دهند. این مسئله در شهرها با تعداد تقاطعات زیاد و جاده‌های دو طرفه احتمال بیشتری دارد.

۲-۳-۳- روشهای مبتنی بر مکان‌یابی

در روش مقابله با حمله سایبل با روش تایید موقعیت خودروها، موقعیت فیزیکی هر خودرو در شبکه تایید شده و این اطمینان حاصل می‌گردد که هر خودرو تنها به یک شناسه و در نتیجه یک هویت محدود می‌شود. در توجیه بکارگیری این روش برای تشخیص حمله سایبل می‌توان گفت در اکثر موارد پیامهای کمکی و ایمنی ترافیکی به اطلاعات مکانی وابستگی زیادی دارند. به عنوان مثال گزارش وضعیت ترافیک، اجتناب از برخورد، هشدارهای اضطراری، همیاری در رانندگی یا دسترسی به منابع که به طور مستقیم وابسته به اطلاعات موقعیت خودروها هستند. بنابراین کسب دقیق اطلاعات مربوط به موقعیت، دارای کاربردها و اهمیت زیادی است. این اطلاعات برای حفظ حریم خصوصی رانندگان باید از دسترسی عموم حفاظت شوند تا خودرویی قادر به ردیابی و کشف مسیر خودروهای دیگر نباشد. تکنیکهایی برای تایید موقعیت یا فاصله در شبکه‌های سیار پیشنهاد شده‌اند که برخی از این تکنیکها برای کاربردهای داخلی[۱] طراحی شده‌اند، برخی مبتنی بر ایستگاههای ثابت هستند و برخی نیز بر پایه سخت‌افزار خاصی کار می-کنند و هیچ‌یک از این روشها برای شبکه‌هایی چون شبکه‌های خودرویی با این اندازه پویایی، مناسب نمی-باشند [۳۲].

[۱] . Indoor

برای جلوگیری از اکثر حملات مبتنی بر موقعیت و حمله سایبل، Yan و همکارانش [۳۸]، راه حل جدیدی را پیشنهاد کرده‌اند که مبنای آن ضرب‌المثل "دیدن باور" است می‌باشد. در این دیدگاه از یک رادار به عنوان چشم مجازی خودرو استفاده می‌شود. گرچه این بینایی به دلیل رنج انتقال نسبتا کم رادار محدود است اما خودرو با این رادار می‌تواند خودروهای اطراف را ببیند و گزارشات آنها که شامل مختصات جی.پی.اس خودروها است می‌تواند بشنود. با مقایسه آنچه که خودرو دیده است با چیزی که شنیده، قادر خواهد بود موقعیت واقعی همسایگان را تایید و اثبات نماید و بدین طریق خودروهای مهاجم را از سایر خودروها جدا نماید که امنیت محلی را برای خود بدست آورد. برای جلوگیری از برخی از انواع حملات سایبل در این پژوهش راهی پیشنهاد شده که اگر یک رادار چنان کار کند که وجود فیزیکی یک خودرو را بتواند تشخیص دهد، این اطلاعات فیزیکی می‌تواند برای بهبود اطلاعات کلی در مورد خودرو استفاده شود. در این کار شباهت بین ۳ نوع داده محاسبه می‌شود: موارد شناسایی شده توسط رادار، گزارشات ترافیکی و گزارشات همسایگان. برای محاسبه میانگین این شباهتها، به هریک از شباهتها یک وزن اختصاص داده می‌شود به گونه‌ای که وقتی رادار کار می‌کند موارد شناسایی شده توسط رادار مطمئن‌ترین داده بوده و دارای بیشترین وزن هستند و زمانی که رادار کار نمی‌کند، گزارشات همسایگان دارای بیشترین وزن هستند. در این شرایط بعد از محاسبه شباهت، اگر میزان شباهتها نزدیک به یکدیگر باشند متوسط سرعت و موقعیت خودرو محاسبه می‌شود و تاریخچه‌ای از نقشه جاده با ذخیره مقادیر سرعت و موقعیت متوسط در طول یک دوره زمانی نگه‌داری می‌شود. اما اولین اشکال این روش اینست که نیاز به یک سخت افزار اضافی دارد که هزینه‌بر است، دومین مشکل اینست که در این پژوهش تکنیک جدیدی برای تایید موقعیت ادعا شده خودروها معرفی شده که با استفاده از یک سیستم رادار که در هر جهتی قادر است عمل کند کار می‌کند در صورتیکه چنین وسیله‌ای هنوز موجود نیست [۳۹]. سومین مشکل اینست که نمی‌توان جلوی برخی حملات را به صورت رضایت بخش گرفت. به عنوان مثال شرایطی که

یک خودرو ادعا می‌کند در موقعیت خودرویی دیگری است که آن خودرو واقعا وجود فیزیکی دارد [۳۹]. چهارمین مشکل این روش، نگاه‌داری اطلاعات مکانی خودرو در سایر خودروها است که این امر باعث نقض حریم خصوصی رانندگان می‌شود. یکی دیگر از اشکالات بیان شده در این روش اینست که اگر خودرویی خارج از رنج دریافت رادار باشد بکارگیری این روش غیر عملی است [۴۰]. در صورتی که در [۴۱] در توجیه چنین حالتی بیان شده است که رنج دریافت رادار در اینکار ثابت بوده و در صورت خارج بودن یک خودروی هدف از دامنه دریافت یا دید رادار، از خودروهای واسطه استفاده می‌شود که در این صورت برای حفظ امنیت بیشتر لازم است که از چند خودرو واسطه بجای یک خودرو برای دریافت اطلاعات مکان خودروی هدف استفاده شود. اما این روش باز از نظر امنیتی و زمان لازم برای تایید موقعیت خودروها مشکل دارد. چون خودروهای واسط ممکن است اکثرا موجودیتهای سایبل باشند و خودروی مورد نظر را که قصد تایید قانونی بودن خودروی صادر کننده پیام را دارد، فریب دهند. از طرفی گرفتن واسطه برای دریافت اطلاعات مکانی خودروی صادر کننده پیام، باعث تاخیر و افزایش زمان پاسخ خواهد شد و در شبکه‌های بین خودرویی این تاخیر به دلیل حساسیت مسئله زمان در ارسال اطلاعات ایمنی، می‌تواند عواقب نامطلوبی داشته باشد.

برای حل مشکل اخیر یعنی حفظ امنیت در شرایطی که خودروی مورد نظر خارج از رنج رادار باشد و همچنین کاهش زمان پاسخ روش پیشنهادی توسط Yan، در [۴۱] روشی پیشنهاد شده که از راداری استفاده می‌شود که به صورت پویا قابل تنظیم است. در این متد در صورتیکه خودروهای همسایه دورتر از رنج رادار باشند، رنج رادار تا حدی می‌تواند افزایش یابد و بجای تایید موقعیت از راه دور و با واسطه، خودرو تا جای ممکن، مستقیما موقعیت خودروی هدف را با افزایش رنج رادار به صورت پویا، دریافت می-کند. در این روش علاوه بر افزایش ایمنی در محدوده محلی خودرو، کارایی سیستم نیز در تعیین موقعیت خودروها بهبود یافته است. با این وجود در صورتی که فاصله اعلان شده، از رنج افزایش‌یافته رادار باز هم

بیشتر باشد، مانند روش قبل در متد اولیه Yan، باید تایید موقعیت خودروی هدف با کمک همسایگان انجام پذیرد. پس این روش نیز فقط تاحدی مشکل روش Yan را برطرف می‌سازد و مشکلات دیگر همچنان باقی است.

در کار دیگری که توسط Xiao و همکارانش انجام شده [۴۲] و به طور مفصل‌تر در [۳۲] بررسی شده است، متدی با سربار کم به منظور شناسایی و مکان‌یابی موجودیت‌های سایبل در شبکه خودرویی پیشنهاد شده است. شناسایی این روش بصورت محلی در اطراف هر خودرو و به صورت توزیع شده با تایید موقعیت ادعا شده هر خودرو انجام می‌شود. در اینکار ابتدا مدل ساده‌ای پیشنهاد شده که خودروی تایید کننده از خودروهای اطراف خودروی هدف برای اطمینان از صحت ادعای خودروی هدف استفاده می‌کند. بدین ترتیب قدرت سیگنال دریافتی حاصل از پیام ارسالی خودروی هدف توسط خودروهای همسایه اندازه‌گیری شده و موقعیت خودروی هدف با دریافت اطلاعات قدرت سیگنال از همسایگان، توسط خودروی تایید کننده محاسبه و تایید می‌شود. این روش ساده و با سربار کم، دقت پایینی دارد و با محدوده خطای ۱۰ متر موقعیت خودرو را تعیین می‌کند و در صورت نزدیکی زیاد خودروها در جاده روش مناسبی نیست و همچنین در برابر اندازه‌گیری‌های ساختگی قدرت سیگنال توسط موجودیت‌های سایبل آسیب‌پذیر است و حتما باید خودروهای اطراف موجودیت‌های سایبل نباشند که این روش بتواند با دقت مناسبی عمل کند. به همین منظور بهبودی در این روش انجام شده که در مدل پیشنهادی یک خودروی تایید کننده قصد تایید موقعیت یک خودروی ادعا کننده‌ای را دارد که اطلاعات موقعیت و شناسه خود را به صورت دوره‌ای پخش می‌کند. این کار با کمک یک مجموعه خودرو با نام خودروهای شاهد انجام می-شود. برای شاهد گرفتن خودروهای قابل اطمینان، از الگوی ترافیک و حمایت ایستگاه کنار جاده استفاده می‌شود. تمام خودروها با عبور از هر ایستگاه کنار جاده، گواهینامه‌ای را دریافت می‌کنند که به صورت دوره‌ای توسط ایستگاه پخش می‌شود و هدف از این گواهینامه فقط این است که خودرو ادعای خود را که

از کنار ایستگاه مورد نظر عبور کرده ثابت کند پس تنها شامل اطلاعات ایستگاه کنار جاده است. در این مدل خودروهای شاهد فقط از میان خودروهایی انتخاب می‌شوند که در سمت مخالف خودروی ادعا کننده در حال حرکت هستند. بنابراین موقعیت موجودیتهای سایبلی که توسط یک خودروی مهاجم تولید شده-اند اثبات نمی‌شود زیرا از خودروهای سایبلی که همجهت با خودروی ادعاکننده هستند که نمی‌توان به عنوان شاهد استفاده کرد و همچنین برای اثبات موقعیت خودروی ادعا کننده‌ای که خود سایبل است از موجودیت‌های سایبلی که در سمت مخالف جاده فرض شده نیز نمی‌توان به عنوان شاهد استفاده کرد. زیرا بدلیل عدم وجود فیزیکی، گواهینامه‌ای برای اثبات عبور خود از واحدهای کنار جاده در سمت مخالف جاده ندارند. از مزایای این مدل پراکندگی در گسترش واحدهای کنار جاده و پردازش توزیع شده و همچنین عدم نیاز به سخت افزار اضافی است و از معایب آن شامل عدم دقت کافی بدلیل شناسایی موقعیت خودرو از روی قدرت سیگنال دریافتی، عدم استفاده از خودروهای همسو با جهت حرکت خودروی ادعاکننده که نیاز به حضور خودروهای کافی در سمت مقابل جاده دارد (سمت عکس حرکت ادعا کننده) و بکارگیری این روش را در جاده‌های یک طرفه غیر عملی می‌سازد و همچنین حریم خصوصی افراد با پخش و تایید موقعیت و شناسه واقعی توسط خودروها نقض می‌شود.

روشهای مختلف مکانیابی خودروها در صورتیکه حریم خصوصی خودروها را حفظ نمایند و شرایط لازم را برای تصدیق موقعیت داشته باشند، می‌توانند برای شناسایی حمله سایبل مورد استفاده قرار بگیرند. به عنوان نمونه در [۴۳] روشی برای مکانیابی خودروها بدون استفاده از جی.پی.اس پیشنهاد شده است که هدف از بکارگیری این سیستم، مکانیابی با دقت بیشتر و از بین رفتن معایبی چون اختلال و یا مسدود شدن سیگنالهای جی.پی.اس با موانعی چون ساختمانها و کوهها می‌باشد. در این دیدگاه برای مکانیابی هر خودرو، نیاز به یک آرایش خاص از واحدهای کنار جاده است و یک جفت واحد کنار جاده در دو سمت جاده باید در فاصله‌های معین نصب شوند. فاصله هر جفت واحد کنار جاده از جفت واحد بعدی دو برابر

شعاع رادیویی واحدهای کنار جاده است. هر جفت واحد بصورت پریودیک و همزمان پیامهایی را صادر می‌کنند که خودرو با دریافت این پیامها می‌تواند فاصله خود را از دو واحد تخمین بزند و به این ترتیب مکان خود را محاسبه نماید. در نتیجه محاسبه دو مکان ممکن برای خودرو بدست می‌آید که مکان درست خودرو با دریافت دومین پیام از جانب جفت واحدهای کنار جاده تعیین می‌گردد. این روش دقت مکانیابی مناسبی دارد و مکان هر خودرو توسط خود خودرو محاسبه می‌گردد. اما برای اینکه این روش برای شناسایی حمله نیز قابل استفاده باشد، باید مکانیابی خودرو توسط تایید کننده موقعیت نیز قابل انجام باشد. در اینجا واحدهای کنار جاده فقط می‌توانند این مسئولیت را به عهده بگیرند و برعکس روال گفته شده در این روش، ابتدا پیامهای شامل اطلاعات موقعیت توسط خودرو بصورت پریودیک پخش می‌شوند و سپس هر جفت واحد کنار جاده مکان خودرو را با توجه به فاصله تخمین زده شده تا خودرو، با همکاری یکدیگر، تایید می‌نمایند. استفاده از این روش مشکلاتی را برای حریم خصوصی خودروها ایجاد می‌کند که با تغییر آرایش واحدهای کنار جاده تا حد زیادی این مشکل برطرف می‌شود. در این پایان‌نامه این راهکار پیشنهادی را بررسی خواهیم کرد.

۲-۴- نتیجه‌گیری

در این فصل چند نمونه از مدلهای حفظ امنیت و حریم شخصی بررسی شدند. مدلهایی که در بخش اول از این بررسیها در نظر گرفته شده‌اند، می‌توانند در مدل شناسایی حمله سایبل نیز کارا باشند. در بخش دوم، به بررسی مدلهایی پرداختیم که منحصرا برای شناسایی حملات سایبل مورد استفاده قرار می-گیرند. دو دسته روشهای مبتنی بر مکانیابی و روشهای مبتنی بر رمزنگاری و امضای دیجیتال برای شبکه-های خودرویی مناسب‌تر بوده و قابل بکارگیری هستند. برخی روشهای مبتنی بر مکانیابی، که دقت بالایی در محاسبه مکان خودرو دارند، علاوه بر شناسایی حملات سایبل در نیاز امنیتی تایید موقعیت ارسالی توسط خودروها نیز قابل بکارگیری هستند. تایید موقعیت به این شیوه می‌تواند انجام پذیرد که خودرو در پیامهای دوره‌ای که باید موقعیتش را ارسال کند، موقعیت خود را که از روشهای مختلف محاسبه شده، مثل گیرنده‌های جی.پی.اس، برای تایید کننده یا واحد کنار جاده ارسال می‌کند و واحد کنار جاده خود موقعیت بسته ارسالی را با روشهای مختلف مثل محاسبه سیگنال دریافتی یا زاویه دریافت، محاسبه می-کند و با مقایسه آن با موقعیت ارسالی از طرف خودرو، موقعیتش را تایید را رد می‌کند.

روشهای مبتنی بر مکانیابی حریم خصوصی خودروها را حفظ نمی‌کنند و همچنین در برخی از روشهای دقیقتر تعداد مبادلات در شبکه افزایش می‌یابد و در نتیجه سربار اضافی در شبکه ایجاد می‌کنند. بهمین با وجود محاسبات بیشتر در روشهای مبتنی بر رمزنگاری، این روشها کارایی بیشتری در شناسایی حمله و همچنین مبادلات ایمن پیامها بدون دستکاری و جعل پیامها توسط شخص ثالث دارند. بهمین منظور با انتخاب این روش مقابله، در فصل ۶ به اصلاح یکی از این روشها که نرخ شناسایی بالایی برای شناسایی حمله دارد می‌پردازیم.

فصل ۳

مکانیابی و تایید موقعیت خودروها

۳-۱- مقدمه

یکی از مهمترین داده‌ها برای اهداف و کاربردهای مختلف در شبکه خودرویی اطلاعات مکان خودروها می‌باشد. به گونه‌ای که اکثر کاربردها در شبکه خودرویی از اطلاعات مکان استفاده می‌کنند یا اینکه می-توانند از اطلاعات بدست آمده از برخی از این تکنیک‌های مکانیابی برای عملکرد بهتر خود استفاده کنند. در مسئله مکانیابی، تعریف یک سیستم مرجع برای مکانیابی در میان نودها، با شناسایی مکان فیزیکی آنها (برای مثال طول، عرض و ارتفاع جغرافیایی) یا توزیع فضایی آنها در ارتباط با یکدیگر صورت می‌گیرد. به عنوان مثال نقشه مکان[۱] معمولا با استفاده از سیستم تعیین موقعیت جهانی[۲] به همراه یک سیستم اطلاعات جغرافیایی[۳] تعیین می‌شود، در حالیکه سیستمهای هشدار برخورد[۴] در خودروها می‌توانند با مقایسه فاصله بین مکان خودروها همراه با انتشار اطلاعات جغرافیایی، پیاده‌سازی شوند. بنابراین دقت مورد نیاز برای مکانیابی در کاربردهای مختلف متفاوت است. به عنوان مثال در جدول (۳-۱) دقت موردنیاز در برخی از کاربردهای اساسی شبکه خودرویی آورده شده است [۴۴].

در شبکه خودرویی، علاوه بر کاربردهایی که مستقیما نیاز به اطلاعات مکان خودروها دارند، برخی کاربردها هستند که به منظور جلوگیری از حملات موجود در شبکه، این اطلاعات را مورد استفاده قرار می‌دهند. همانطور که در فصل ۲ نیز اشاره گردید، یکی از این موارد شناسایی حمله سایبل است که خودرو می‌تواند با مقایسه آنچه از خودروها دریافت کرده با آنچه خود اندازه‌گیری کرده موقعیت خودرو را تایید کرده و مطمئن شود موجودیت جعلی این پیام را ارسال نکرده است

---

۱. Map location
۲. Global Positioning System (GPS)
۳. Geographic Information System (GIS)
۴. Vehicle Collision Warning Systems (CWS)

جدول ۳-۱. دقت مکانیابی مورد نیاز در برخی از کاربردهای شبکه بین خودرویی موردی [۴۴].

تکنیک	دقت مکانیابی		
	بالا (۱-۰ متر)	متوسط (۱۰-۱ متر)	پایین (۲۰-۱۰ متر)
مسیریابی	---	---	√
انتشار داده	---	---	√
مکانیابی نقشه[۱]	---	---	√
کنترل کروز به صورت تطبیقی مشارکتی[۲]	---	√	---
ایمنی تقاطع به صورت مشارکتی[۳]	---	√	---
عبور کور[۴]	---	√	---
حرکت گروهی[۵]	---	√	---
سیستم هشدار برخورد[۶]	√	---	---
اصلاح دید[۷]	√	---	---
پارک خودکار خودرو	√	---	---

[۱]. نشان دادن موقعیت جاری خودرو بر روی نقشه.

[۲]. کروز کنترل در واقع ابزاری برای ثابت نگه داشتن سرعت خودرو در حین رانندگی در سطح جاده‌ها، بزرگراه‌ها و اتوبان‌هاست. کروز کنترل تطبیقی مشارکتی، با همکاری و مشارکت خودروها همراه است که این سرعت را به صورت تطبیقی تنظیم می‌کند.

[۳]. خودروهایی که به تقاطع وارد می‌شوند پیامهای را برای عبور ایمن از تقاطع با یکدیگر مبادله می‌کنند.

[۴]. در تقاطع‌های فاقد چراغ، امکان عبور ایمن خودروها را با همکاری و ارتباط با یکدیگر فراهم می‌کند.

[۵]. این تکنیک زمانی استفاده می‌شود که چند خودرو (یک یا بیشتر)، یک خودروی سردسته را دنبال می‌کنند یا به عبارتی دیگر چند خودرو در حال سفر به یک مکان هستند. در اینصورت مینیمم فاصله بین خودروها باید رعایت گردد و خودروها باید موقعیت خودروی جلوی خود را با دقت مناسبی ردگیری کنند.

[۶]. یکی از کاربردهای شبکه خودرویی است به عنوان دستیار راننده. یکی از قسمتهای این سیستم، سیستم هشدار فاصله ایمن است. زمانی که فاصله از مقدار مینیمم کمتر می‌شود به راننده هشدار داده و یا به صورت اورژانسی ترمز می‌گیرد. قسمت دیگر این سیستم‌ها مربوط به هشدار برخورد به خودروهای نزدیک محل برخورد است.

[۷]. دید بهتری به رانندگان در مورد خودروها و موانع می‌دهد. این سیستم در شرایطی چون مه غلیظ و وجود خودروهای مخفی بدلیل وجود موانع، ساختمانها و خودروهای دیگر کاربرد دارد.

یکی دیگر از این حملات، ارسال موقعیت نادرست توسط یک خودرو است که خودرو با این کار می-تواند در کلیه کاربردهایی که از اطلاعات مکان استفاده می‌کنند، اختلال ایجاد کند و به عنوان مثال در مسیریابی بسته‌ها، بسته‌های پیام دریافتی را دورانداخته و یا اشتباها فوروارد نماید.

بنابراین با توجه به قدرت اختلال در این حمله، در این فصل یکی از روشهای مکانیابی که برطرف کننده معایب جی.پی.اس است را بیان کرده و به بررسی روش در زمینه استفاده از آن برای کاربرد تایید موقعیت خودروها می‌پردازیم و با تغییر آرایش واحدهای کنار جاده، فضای حالت انتخاب را برای خودرو بدخواه کاهش می‌دهیم و بدین ترتیب از همین روش مکانیابی برای تایید موقعیت خودروها نیز می‌توان استفاده کرد.

۳-۲- روشهای متداول مکانیابی در شبکه خودرویی

یکی از روشهای بسیار متداول و مورد استفاده در کاربردهای شبکه‌های بین خودرویی با دقت متوسط یا پایین‌تر، استفاده از گیرنده‌های جی.پی.اس در خودروها است. سیستم تعیین موقعیت جهانی یا جی.پی.اس یک سیستم ناوبری رادیوئی ماهواره‌ای است که توسط ارتش ایالات متحده آمریکا طراحی و ایجاد شده است. این سیستم اساساً یک سیستم نظامی است و کاربردهای غیرنظامی آن دارای محدودیت-های خاصی است. تکنیک‌های مختلف تعیین موقعیت جی.پی.اس دارای کاربری‌ها و دقت‌های مختلفی هستند، به گونه‌ای که حیطه کاربردهای سیستم را از تعیین موقعیت بسیار دقیق ژئودتیک تا ناوبری هوائی و دریایی گسترش داده‌اند. این سیستم در ابتدا برای مصارف نظامی تهیه شد ولی از سال ۱۹۸۰ استفاده عمومی آن آزاد و آغاز شد و سرانجام در سال ۱۹۹۴ شبکه‌ای شامل۲۴ ماهواره تشکیل گردید (۲۱ ماهواره فعال و ۳ ماهواره فعال یدکی)، به گونه‌ای که تمام سطح زمین را پوشش دهند. از این ۲۴ ماهواره، هر چهار ماهواره در یکی از شش مدار تعیین شده استقرار دارند. حرکت و استقرار ماهواره‌ها به گونه‌ای است که در هر نقطه از سطح زمین در آن واحد حداقل شش ماهواره در دید گیرنده باشند. امروزه

تعداد ماهواره‌ها به عدد ۲۸ عدد رسیده است. امواج در طیفی از امواج الکترومغناطیس ارسال می‌شوند که تحت هر شرایط جوی قابل دسترسی باشند. برای تعیین موقعیت طول و عرض جغرافیایی، حداقل باید سه ماهواره در آسمان محل باشند. در صورتی که مقدار ارتفاع را نیز بخواهیم، باید از چهار ماهواره استفاده کرد. هرچه تعداد ماهواره‌های قابل مشاهده بیشتر شود، معادلات اساسی تعیین موقعیت بیشتر خواهند شد و بنابراین زمان لازم برای تعیین موقعیت یک نقطه، کاهش یافته و دقت تعیین موقعیت نیز افزایش خواهد یافت.

بخش کنترل زمینی جی.پی.اس شامل ایستگاه‌های زمینی است که دارای مختصات معلومی هستند. این ایستگاه‌ها موقعیت ماهواره‌ها را نسبت به یک سامانه مختصات ژئودتیک ژئوسنتریک (مبدا سامانه مختصات تقریبا در مرکز زمین قرار دارد) محاسبه می‌نمایند. تعداد این ایستگاه‌های زمینی پنج عدد است که ایستگاه اصلی با نام کلرادواسپرینگ در آمریکا قرار دارد و چهار ایستگاه فرعی دیگر در هاوایی، کوآجالین، دیگوگارسیا و آسنشن مستقر هستند. کاربران جی.پی.اس به طور کلی، گیرنده‌های جی.پی.اس هستند که از آنتن، تنظیم‌کننده فرکانس دریافتی، پردازشگر داده‌ها و ساعت بسیار دقیق (اغلب از نوع نوسانگر کریستالی) تشکیل شده‌اند. البته این‌گونه گیرنده‌ها دارای یک نمایشگر جهت ارائه اطلاعات از قبیل موقعیت مکانی، سرعت حرکت گیرنده و غیره به کاربران هستند. معمولاً نوع گیرنده‌ها با تعداد کانال‌های آنها مشخص می‌شود که هر سال با افزایش تعداد ماهواره‌ها نیز تعداد کانال‌ها افزایش می‌یابد[۱]. جی.پی.اس دو دسته کاربرد دارد، کاربرد نظامی و کاربرد غیر نظامی. دقت سیگنال جی.پی.اس در هر دو کاربرد یکسان است و اما در کاربردهای غیر نظامی از یک فرکانس استفاده می‌شود در حالیکه کاربردهای نظامی از دو فرکانس بهره می‌برند. این امر بدین معناست که کاربران نظامی می‌توانند تصحیح یونسفریک[۲] انجام دهند و بدین ترتیب کاهش انرژی رادیویی سبب شده توسط اتمسفر زمین را کاهش دهند. تنزل

[۱] . http://www.noojum.com/article/۱۲٤-all/۱۱۸٤-۲۰۰۹-۰٤-۰۹-۰۱-۰۸-۲۵.html
[۲] . ionospheric correction

کمتر موج رادیویی در کاربردهای نظامی منجر به دقت بالاتر آنها نسبت به کاربردهای غیرنظامی می‌شود[1].
برخی از عوامل کلی موثر بر دقت جی.پی.اس شامل موارد زیر می‌باشند:

۱. **هندسه ماهواره:** شکل قرار گرفتن ماهواره‌ها نسبت به یکدیگر می‌باشد که اگر چهار ماهواره در آسمان محل وجود داشته باشد و هر چهار ماهواره در شمال و شرق گیرنده جی.پی.اس باشند طرح و هندسه این ماهوارها برای این جی.پی.اس بسیار ضعیف می‌باشد و شاید جی.پی.اس قادر نباشد مکان-یابی نماید. زیرا تمام اندازه‌گیری‌های فاصله در یک جهت عمومی قرار دارند. مثلث سازی ضعیف است و ناحیه مشترک بدست آمده از اشتراک این مسافت‌سنجی‌ها وسیع می‌باشد. در این موقعیت‌ها حتی اگر جی.پی.اس مکان‌یابی را انجام دهد و موقعیتی را گزارش نماید، دقت آن نمی‌تواند زیاد خوب باشد (کمتر از۵۰۰-۳۰۰ فوت). اگر همین چهار ماهواره در چهار جهت (شمال ، جنوب ، شرق ، غرب) و با زوایای ۹۰ درجه قرارداشته باشند، طرح این چهار ماهواره برای جی.پی.اس مزبور بهترین حالت می‌باشد. عوارض زمینی، تداخل امواج الکترونیکی و یا حتی شاخ و برگ متراکم درختان می توانند مانع دریافت سیگنال شوند که باعث ایجاد خطا در تعیین موقعیت و گاهی مانع قرائت موقعیت می‌شود. بنابراین طرح و هندسه قرار گرفتن ماهواره‌ها هنگامی که جی.پی.اس نزدیکی ساختمانهای بلند، قلل کوهها، دره‌های عمیق و یا در وسایل نقلیه قرار گرفته باشد، به مسأله مهمتری تبدیل می‌گردد. اگر مانعی در رسیدن سیگنالهای بعضی از ماهواره‌ها وجود داشته باشد، جی.پی.اس می‌تواند از بقیه ماهواره‌ها بـــرای مکان‌یابی خود استفاده نماید. هرچه این موانع بیشتر و شدیدتر شوند مکان یابی نیز مشکل‌تر می‌گردد [۴۵].

۲. **خطای سیگنال چند مسیری:** این خطا زمانی رخ می دهد که سیگنالهای جی.پی.اس قبل از آنکه به دستگاه گیرنده برسند، بوسیلهٔ موانع طبیعی و مصنوعی موجود در طبیعت مانند ساختمان های بلند و یا سطوح صخره های بزرگ بازتابیده شده باشند. این اتفاق سبب افزایش زمان حرکت سیگنال می

[1] . http://www.gps.gov/systems/gps/performance/accuracy/

شود و خطایی رخ می‌دهد که هم بر روی کد تأثیر می‌گذارد و هم بر روی فاز (مثلاً از سقف شیروانی یک ساختمان). این خطا در کاربردهای استاتیک باعث کاهش دقت در اندازه‌گیری فاصله تا ۱۰ متر برای حالت شبه فاصله و تا چند سانتیمتر در اندازه‌گیری فاز موج حامل می‌شود. اما در کاربردهای کینماتیک اثر این خطا باعث قطع ارتباط بین گیرنده و ماهواره می‌شود. راه‌های حذف آن عبارتند از: ۱. حتی‌المقدور اطراف ایستگاه سطوح منعکس کننده وجود نداشته باشد، ۲. استفاده از صفحه زمینی (Ground Plate) که با استفاده از این صفحه انعکاس‌های زمینی به آنتن نمی‌رسد، ۳. استفاده از میانگین‌گیری زمانی مشاهدات و تعریف یک زاویه مناسب (Cut of Angle) برای آنتن برای دریافت امواج. این زاویه در واقع حداقل زاویه‌ای است که جهت دریافت و مشاهده ماهواره‌ها به دستگاه معرفی می‌گردد، ۴. استفاده از آنتن های مخصوص موسوم به Chock Ring که برای کارهای دقیق از این آنتن استفاده می‌شود و دارای مزایای: ۱) در برابر چند مسیری مقاوم است، ۲) تغییرات مرکز فاز نخواهیم داشت، ۳) در مقابل خطای نویز و Jam خیلی مقاوم است[۱].

۳. **خطای پارازیت**[۲]: در شرایطی بوجود می‌آید که گیرنده تحت تأثیر میدان مغناطیسی باشد. مثلا " در نزدیکی دکل‌های فشار قوی، ایستگاه‌های فرستنده رادیوئی و ماکروویو. راه‌های مقابله این است که یا محل ایستگاه را با دقت انتخاب کنیم یا اینکه از آنتن Chock Ring استفاده کنیم.

۴. **خطای نویز:** این خطا در حد میلیمتر است و نمی‌توان با مدلسازی آن را حذف کرد.

برای افزایش دقت جی.پی.اس روشهای گوناگونی وجود دارد. از جمله این روشها استفاده از جی.پی.اس تفاضلی[۳] است که با در نظر گرفتن ایستگاه‌های ثابت، موقعیت واقعی این ایستگاه‌ها با موقعیت بدست آمده با سیستم جی.پی.اس مقایسه شده و اطلاعات خطا (شامل میزان خطا) در موقعیت‌یابی محاسبه می-

---

۱. http://survey۲۰۱۲.blogfa.com/post/۹
۲. Jam
۳. Differential GPS (DGPS)

شود و تصحیحات لازم همراه با پیامهای هشدار، برای کاربران سیستم در منطقه تحت پوشش، جهت بهبود دقت و صحت سیستم جی.پی.اس ارسال می‌گردند. ایستگاه‌های مرجع جی.پی.اس تفاضلی که موقعیت دقیقشان معلوم است، برای تولید تصحیحات می‌توانند به دو صورت عمل کنند. حالت اول بصورت تک مرجعی است که مستقل از هم تصحیحات را انجام می‌دهند و حالت دوم چند مرجعی است که مشاهدات چند ایستگاه که با هم ارتباط داخلی دارند، با هم برای تولید تصحیحات استفاده می‌شوند [۴۷]. استفاده از جی.پی.اس تفاضلی نیاز به سخت افزار اضافی دارد و بهمین دلیل در همه جا نمی‌توان از آن استفاده نمود.

با استفاده از سیستم WAAS نیز دقت گیرنده‌های جی.پی.اس به بهتر از سه متر نیز می‌رسد. در این سیستم (WAAS) ایستگاه‌های زمینی سیگنالهای تصحیح شده جی.پی.اس را تامین کرده و دقت بیشتری در تعیین موقعیت می‌دهند. این سیستم شامل ۲۵ ایستگاه مرجع زمینی است که در سرتاسر ایالات متحده قرار دارند، دو ایستگاه اصلی در سواحل واقع شده و دو ماهواره ثابت در نزدیکی خط استوا هستند. ایستگاههای مرجع با دریافت سیگنال‌های جی.پی.اس پیام تصحیح را به ایستگاههای اصلی ارسال می‌کنند. ایستگاههای اصلی اطلاعات ایستگاه‌های مرجع زمینی را جمع آوری کرده و پیام‌های مربوط به تصحیحات جی.پی.اس را تهیه می‌کنند. با اینکار خطای مداری ماهواره، انحراف ساعت و تاخیرات سیگنال ماهواره کاهش می‌یابد. سپس پیام اصلاح شده از طریق یکی از دو ماهواره ثابت واقع در طول خط استوا، به صورت یک سیگنال استاندارد جی.پی.اس، برای دریافت‌کننده‌های مجهز به تکنولوژی WAAS پخش می‌شود. تمام جی.پی.اس های دارای سیستم WAAS قادر به دریافت این اطلاعات می‌باشند. در حال حاضر WAAS تنها در آمریکای شمالی موجود است و فردی که خارج از آمریکای شمالی است می‌تواند از جی.پی.اس مجهز به WAAS استفاده کند اما داده تصحیح نمی‌شود [۴۸]. پس بکارگیری این تکنولوژی

در کشورما نیز مقدور نیست. دقت جی.پی.اس در سه حالت عادی، استفاده از جی.پی.اس تفاضلی و WAAS در جدول (۳-۲) بیان شده است.

جدول ۳-۲. دقت مکانیابی سیستم‌های مختلف [۴۸]

دریافت کننده	دقت
سیستم جی.پی.اس	۱۵-۱۰ متر
جی.پی.اس تفاضلی	۵-۳ متر
WAAS	۳-۲ متر

همانگونه که تکنولوژیهای ITS[۱] و شبکه بین خودرویی، بسمت کاربردهای بحرانی‌تر مثل سیستم هشدار برخورد و خودروهای بدون سرنشین پیش می‌روند، به سیستم‌های مکانیابی قوی و با دسترس-پذیری بالاتری هم نیاز خواهد بود. متاسفانه دریافت کننده‌های جی.پی.اس در این موارد بهترین راه‌حل نیستند. چون دقت جی.پی.اس، در یک منطقه باز با خط دید بدون مانع، برای سیگنالهای دریافت‌شده از تعداد کافی ماهواره، به طور متوسط ۱۰ متر است [۴۳] و همچنین این دریافت‌کننده‌ها در محیط‌های بسته (مثل تونل) یا مناطق با تراکم بالا در شهرها به درستی کار نمی‌کنند. چون در این مکانها معمولا دید مستقیمی به ماهواره برای دریافت سیگنال و محاسبه موقعیت، وجود ندارد. از طرفی تصحیح سیگنال با روشی چون جی.پی.اس تفاضلی، دقتی تا ۳ متر را حاصل می‌کند. اما در عمل همانطور که در عوامل کاهش دقت جی.پی.اس بیان کردیم، سیگنالهای جی.پی.اس به سادگی توسط موانعی همچون ساختمانها، صخره‌ها یا کوهها و شاخ و برگ درختان مختل می‌شوند. در نتیجه یک خودروی در حال عبور از میان کوهها، نواحی پرشاخ و برگ و یا مناطق شهری با ساختمانهای بلند، ممکن است از این اختلالات و مکانیابی نادرست توسط جی.پی.اس رنج ببرد. برای جلوگیری از این مشکل، تاکنون پیشنهاداتی برای

[۱]. Intelligent Transportation System

افزایش دقت سیستمهای مبتنی بر جی.پی.اس پیشنهاد شده است که کارایی مکانیابی با ارتباطات خودرو با خودرو افزایش پیدا می‌کند [۴۹-۵۱]. بطور مشابه تکنیک‌های مسافت‌یابی با کارایی بهبود یافته نسبت به روش پایه آن، پیشنهاد شده‌اند [۵۲-۵۴]. اما این تکنیک‌ها حداقل به سه خودروی مجهز به جی.پی.اس در اطراف هر خودرو نیاز دارند تا بتوانند مکان خودروی مورد نظر را تخمین بزنند. یعنی این مدلها برای شبکه خودرویی متراکم مناسب هستند. با توجه به اشکالات متدهای موجود، متدی توسط OU در [۴۳] پیشنهاد شده است که از اطلاعات واحدهای کنار جاده برای مکانیابی خودروها استفاده می-کند. یعنی متدی که وابسته به سیگنالهای ارسالی توسط ماهواه و یا خودروها اطراف خود نیست. در ادامه این متد انتخاب و بررسی می‌گردد.

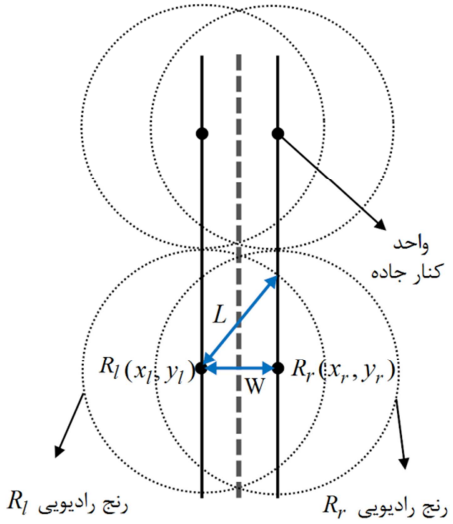
۳-۳- مکانیابی با کمک واحدهای کنار جاده

۳-۳-۱- نحوه مکانیابی با روش OU

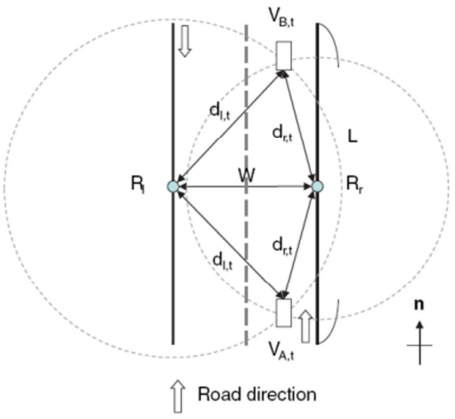
واحدهای کنار جاده در این روش به گونه‌ای هستند که در هر قسمت باید دو واحد در دو سمت جاده روبروی یکدیگر قرار بگیرند. نمونه‌ای از آرایش واحدها با توجه به فرضیات شبیه‌سازی در [۴۳]، در شکل (۳-۱) آورده شده است. این واحدها با خودروها ارتباط برقرار می‌کنند و هر خودرو با دریافت پیامهایی که به صورت دوره‌ای توسط دو واحد کنار جاده در دو سمت جاده صادر می‌شوند، فاصله خود را از دو واحد کنار جاده تخمین می‌زند. این تخمین فاصله را می‌توان با تکنیک‌های مسافت‌سنجی مختلفی چون زمان ورود[۱]، اختلاف زمان ورود[۲] و قدرت سیگنال دریافتی[۳] در گیرنده بدست آورد که تکنیک اختلاف زمان ورود دقیق‌تر و بهتر عمل می‌کند. در این تکنیک اختلاف زمان لازم برای ارسال و دریافت بسته‌های پیام محاسبه شده و با مشخص بودن سرعت نور و لحاظ کردن تاخیر ارسال و دریافت بسته، فاصله واحد کنار

[۱] . Time Of Arrival (TOA)
[۲] . Time Difference Of Arrival (TDOA)
[۳] . Received Signal Strength Indicator (RSSI)

جاده تا خودرو با کمی خطا قابل محاسبه است. بعد از محاسبه فاصله‌های $d_{l,t}$ و $d_{r,t}$ بین خودرو و دو واحد کنار جاده R_r و R_l، دو دایره متقاطع همانند شکل (۳-۲) بدست می‌آیند.



شکل ۳-۱. نمونه‌ای از آرایش واحدهای کنار جاده با توجه به فرضیات پیاده‌سازی در [۴۳]

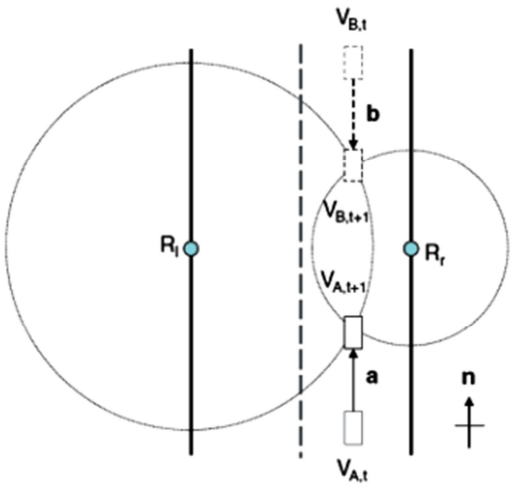


شکل ۳-۲. نحوه محاسبه موقعیت در [۴۳]

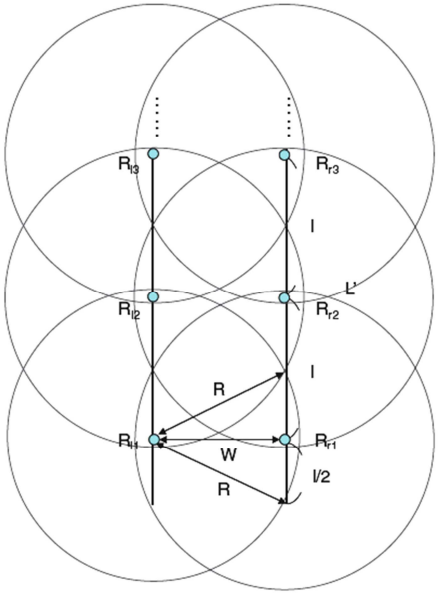
سپس با استفاده از مفهوم دو دایره متقاطع (دو دایره به مرکز دو واحد کنار جاده و به شعاع فاصله خودرو تا هر یک از واحدها) دو مکان ممکن $V_{A,t}$ و $V_{B,t}$ برای خودرو بدست می‌آید. اینکه کدام مکان موقعیت واقعی خودرو است با توجه به دریافت دومین مجموعه از پیامهای صادر شده توسط واحدها بدست می‌آید. با دریافت دومین مجموعه از پیامها و تخمین مجدد فاصله از دو واحد کنار جاده R_r و R_l دو موقعیت جدید $V_{A,t+1}$ و $V_{B,t+1}$ برای خودرو بدست می‌آیند. و سپس دو بردار حرکت از $V_{A,t}$ به $V_{A,t+1}$ و از $V_{B,t}$ به $V_{B,t+1}$ طبق شکل (۳-۳) بدست آمده و موقعیت واقعی خودرو با مقایسه زاویه بین دو بردار حرکت و جهت جاده تعیین می‌شود، به گونه‌ای که بردار حرکت صحیح و جهت جاده باید زاویه کمتر از ۹۰ درجه داشته باشد. در این روش مطالعات بیشتری بر روی تاثیر آرایش واحدهای کنار جاده و امکان شکست برخی واحدها در ارسال پیامهای دوره‌ای به خودروها انجام شده که مزایای روش را بهتر نشان می‌دهد. با بررسی این روش مزایای کلیدی زیر را می‌توان بیان کرد:

- نسبت به تراکم ترافیک و تعداد خودروها پایدار است.
- نسبت به سرعت خودروها پایدار است و سرعت خودرو تاثیری در دقت مکانیابی ندارد.
- دقت مکانیابی نسبتا بالایی دارد و رنج خطای مکانیابی از ۰.۵ تا ۳ است.
- نیاز به تجهیزات سخت‌افزاری خاصی برای خودرو نیست و هزینه اضافی برای خودرو ندارد.

اما این آرایش از واحدهای کنار جاده کل جاده را پوشش نمی‌دهد و برای همین منظور برای پوشش کامل جاده و در نتیجه افزایش دقت مکانیابی، آرایش شکل (۳-۴) در اینکار فقط پیشنهاد شده است که به تعداد خیلی بیشتری واحد کنار جاده نیاز دارد و خیلی پرهزینه‌تر است.



شکل ۳-۳. بردارهای حرکت و تخمین موقعیت صحیح خودرو با دریافت اولین و دومین مجموعه از پیامهای واحدهای کنار جاده [۴۳]



شکل ۳-۴. آرایش بهبود یافته واحدهای کنار جاده [۴۳]

۳-۳-۲- مشکلات روش مکانیابی OU

مشکل اول در روش مکانیابی OU در شکل (۳-۱) عدم پوشش کامل جاده است و مشکل دوم که یک مسئله مهم در کاربردهای مربوط به مکانیابی در شبکه‌های خودرویی تایید موقعیت خودروها است که در روش OU در [۴۳] بررسی نشده است.

تایید موقعیت به این دلیل نیاز است که خودروی بدخواه می‌تواند موقعیت خود را به اشتباه گزارش دهد و بدین ترتیب در کاربردهایی چون کنترل ترافیک، تنظیم فاصله با خودروهای اطراف، جلوگیری از برخورد و غیره خلل ایجاد کند و باعث تصادف یا تراکم در جاده‌ها شود. آرایش شکل (۳-۱) ایمنی لازم را در مقابل ارسال موقعیت نادرست توسط خودروی بدخواه ندارد و از طرفی در آرایش شکل (۳-۴) صرف نظر از هزینه زیاد، اگر واحدهای کنار جاده با هم ارتباط برقرار کنند، امکان تایید موقعیت خودرو را با دقت بالا فراهم می‌کنند. در اینصورت تایید موقعیت باید توسط واحدهای کنار جاده، با دریافت سیگنال ارسالی خودرو انجام شود.

تایید موقعیت می‌تواند از دو راه انجام شود: ۱. مقایسه موقعیت ارسالی توسط خودرو و موقعیتی که واحدهای کنار جاده با دریافت پیام از طرف خودرو تخمین می‌زنند. در این روش خودرو پیامی حاوی موقعیت خود در پاسخ به پیامی که توسط واحدهای کنار جاده به آنها ارسال می‌کنند می‌فرستد (این پیام برای محاسبه موقعیت خودرو به صورت دوره‌ای به خودرو ارسال می‌شود). واحدهای کنار جاده با لحاظ کردن تاخیر ارسال پاسخ، با توجه به سرعت خودرو، موقعیت گزارش شده را دقیق‌تر در نظر گرفته و از طرفی خود واحدها با دریافت سیگنال پیام ارسالی توسط خودرو موقعیتش را بدست آورده و این دو مقدار را مقایسه می‌کنند. در صورتیکه تقریبا برابر باشند خودرو صادق است وگرنه بدخواه است. این مورد مواقعی کاربرد دارد که خودرو رخدادی را همراه با موقعیت خود باید گزارش دهد. ۲. از همان ابتدا نیازی به مقایسه با موقعیت گزارش شده در پیام پاسخ از جانب خودرو نیست و خود واحدهای کنار جاده موقعیت خودرو را با پیامهای دوره‌ای که حاوی اطلاعات موقعیت هم نیستند و توسط خودروها پخش می‌شوند، محاسبه می‌کنند. این مورد زمانی کاربرد داد که پیامهایی حاوی اطلاعات موقعیتی خودرو به صورت پریودیک برای کاربردهایی چون ارزیابی ترافیک توسط خودرو پخش می‌شوند که در شرایطی که خود

واحدها می‌توانند مکان را محاسبه کنند نیازی به پخش اطلاعاتی که حریم خصوصی خودروها را به خطر می‌اندازد نیست.

در نحوه آرایش واحدهای کنار جاده در شکل (۳-۴)، در نواحی تحت پوشش سه یا چهار واحد کنار جاده، امکان فریب توسط خودروی بدخواه خیلی پایین است و بدیهی است که هرچه تعداد واحدها زیادتر می‌شود، با وجود افزایش هزینه پیاده‌سازی، دقت مکانیابی افزایش یافته و امکان ارسال موقعیت اشتباه از جانب خودروی بدخواه از بین می‌رود. در آرایش شکل (۳-۴)، علت نیاز به تعداد زیادی از واحدها برای پوشش قسمت زیادی از جاده توسط بیش از دو واحد کنار جاده، نحوه قرارگیری واحدها در دو سمت جاده است که دو واحد با عرض جغرافیایی یکسان در دو سمت جاده قرار دارند. بنابراین می‌توان نحوه آرایش واحدها در اینکار را به گونه‌ای تغییر داد که دقت مکانیابی تقریبا یکسان باشد و اهداف زیر را نیز برآورده نماید:

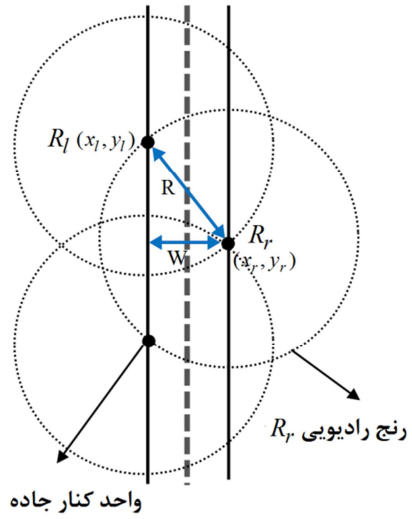
- همه جاده توسط دو یا سه واحد کنار جاده پوشش داده شود.
- تعداد واحدهای کنار جاده کمتر از آرایش شکل (۳-۴) است.
- فضای حالت برای انتخاب اطلاعات موقعیت نادرست توسط خودروی بدخواه خیلی کمتر و یا ناچیز باشد.
- در بسیاری از موارد نیاز به دریافت پیام دوم از جانب واحدهای کنار جاده برای انتخاب موقعیت صحیح خودرو از بین دو نقطه از مکان برخورد دایره‌های متقاطع نمی‌باشد (در بخش محاسبه موقعیت توسط خودرو).
- دقت مکانیابی در نقاط تحت پوشش دو واحد، یکسان با مدل مطرح شده در [۴۳] است و در نقاط تحت پوشش سه واحد، این دقت بیشتر است.

۳-۳-۳- حل مشکلات روش OU با تغییر آرایش واحدهای کنار جاده

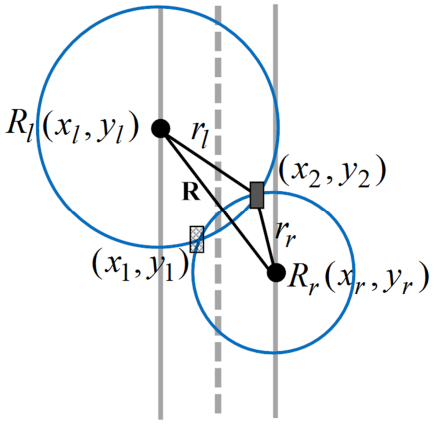
مدل پیشنهادی با اهداف ذکر شده، در شکل (۳-۵) نشان داده شده است. فاصله دو واحد کنار جاده می‌تواند بیشتر یا مساوی با شعاع رادیویی واحد کنار جاده در نظر گرفته شود و این مقدار از عرض جاده بیشتر است. همانطور که در این شکل ملاحظه می‌شود، برخی نواحی تحت پوشش دو واحد کنار جاده و برخی تحت پوشش سه واحد قرار دارند. در نواحی تحت پوشش سه واحد کنار جاده، موقعیت‌یابی دقیق‌تر می‌تواند انجام شود و اما در نواحی تحت پوشش دو واحد، دقت موقعیت‌یابی همانند مدل نشان داده شده در شکل (۳-۱) است.

در مدل شکل (۳-۱)، برای محاسبه موقعیت بعد از محاسبه فاصله بین خودرو و جفت واحدهای کنار جاده با روش اختلاف زمان ارسال و دریافت پیام ارسالی توسط واحدهای کنار جاده، دو دایره متداخل با مرکزیت دو واحد کنار جاده و به شعاع فاصله واحدها تا خودروی مزبور بدست می‌آیند که نقاط تقاطع در متد OU با ایجاد دستگاه معادلات دو دایره بدست می‌آید که برای امکان حل دستگاه، عرض جغرافیایی مختصات جفت واحدهای کنار جاده، برابر در نظر گرفته شده‌اند. اما با تغییر آرایش واحدها در مدل پیشنهادی، عرض جغرافیایی یکسان نیست و در نتیجه محاسبات یافتن دو نقطه تقاطع را باید به گونه‌ای دیگر انجام دهیم. همانطور که در شکل (۳-۶) مشاهده می‌کنیم، در بسیاری از موارد دو نقطه تقاطع در دو سمت جاده و یا یکی از نقاط در خارج از محدوده جاده قرار می‌گیرد که ابهام اینکه کدامیک از دو نقطه موقعیت صحیح خودرو است را از بین می‌برد و بنابراین نیاز به دریافت مجموعه پیام دوم از جانب جفت واحد کنار جاده به خودرو نیست. احتمال اینکه دو نقطه در یک طرف جاده بیفتند به ندرت است زیرا همانطور که گفته شد، موقعیت و فاصله دو واحد کنار جاده در آرایش جدید نسبت به عرض جاده بیشتر است و این امر این احتمال را کمتر می‌کند.

برای محاسبه موقعیت شکل (۴-۶) را در نظر می‌گیریم. دو واحد کنار جاده $R_r(x_r,y_r)$ و $R_l(x_l,y_l)$ دارای موقعیت معلوم هستند و خودرو نیز فاصله خود را تا دو واحد کنار جاده به صورت r_r و r_l تعیین کرده است. با رسم دایره‌های متقاطع، دو نقطه تقاطع (x_1,y_1) و (x_2,y_2) بدست می‌آیند.



شکل ۳-۵. آرایش پیشنهادی واحدهای کنار جاده



شکل ۳-۶. محاسبه موقعیت خودرو در آرایش پیشنهادی واحدهای کنار جاده

معادلات دو دایره متقاطع به صورت معادله (۳-۱) داده شده‌اند:

$$\begin{aligned}(x-x_l)^2+(y-y_l)^2&=r_l^2\\(x-x_r)^2+(y-y_r)^2&=r_r^2\end{aligned} \qquad (۱-۳)$$

شروط لازم برای داشتن نقاط تقاطع بین دو دایره که فاصله مرکز آنها از یکدیگر R است بصورت معادلات (۳-۲) و (۳-۳) هستند:

$$R=\sqrt{(x_r-x_l)^2+(y_r-y_l)^2} \qquad (۲-۳)$$

$$|r_r-r_l|<R<r_l+r_r \qquad (۳-۳)$$

پس از بدست آوردن معادلات خط گذرنده از مبدأ دو دایره و خط عمود بر این خط و گذرنده از دو نقطه تقاطع، نقاط تقاطع دو دایره به صورت معادله (۳-۴) محاسبه می‌گردند:

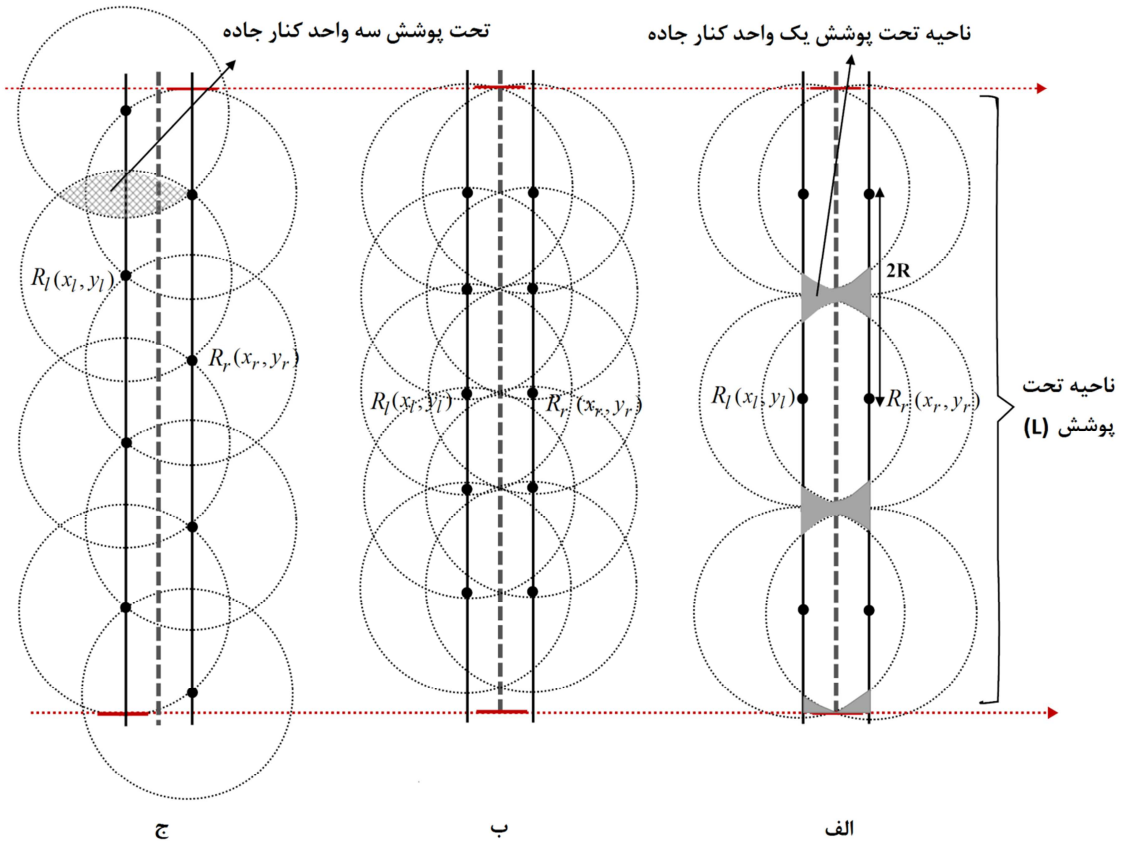
$$x_1, x_2 = \frac{x_l + x_r}{2} + \frac{(x_r - x_l)(r_l^2 - r_r^2)}{2R^2} \pm 2\frac{y_l - y_r}{R^2}A$$
$$y_1, y_2 = \frac{y_l + y_r}{2} + \frac{(y_r - y_l)(r_l^2 - r_r^2)}{2R^2} \mp 2\frac{x_l - x_r}{R^2}A \qquad (۴-۳)$$

ناحیه A در فرمول (۳-۴)، ناحیه مثلثی فرم یافته توسط دو مرکز دایره و یکی از نقاط تقاطع است (شکل (۳-۶)) و به صورت زیر محاسبه می‌گردد:

$$A = \frac{1}{4}\sqrt{(R + r_l + r_r)(R + r_l - r_r)(R - r_l + r_r)(-R + r_l + r_r)} \qquad (۵-۳)$$

بدین ترتیب دو نقطه تقاطع در دایره‌های شکل (۳-۶) محاسبه می‌شوند. اما اینکه کدام نقطه مختصات واقعی است با توجه به مشخص بودن عرض جاده و جهت حرکت خودرو قابل تعیین است. زیرا اگر خارج از حیطه جاده باشد با توجه به عرض جاده (نقاط شروع و انتهای جاده با توجه به عرض، مشخص است) قابل برداشت است و اگر در سمت دیگر جاده باشد با توجه به جهت حرکت قابل برداشت است.

برای مقایسه تعداد واحدهای کنار جاده مورد نیاز، مدل پیشنهادی همراه با مدل پایه که در [۴۳] بررسی و شبیه‌سازی شده است و همچنین مدل بهبود یافته که در [۴۳] فقط پیشنهاد داده شده است، در شکل (۳-۷) نشان داده شده‌اند. همانطور که در این شکل ملاحظه می‌گردد، مدلی که در شکل (ب) برای بهبود (الف) پیشنهاد شده به تعداد زیادی از واحدهای کنار جاده نیاز دارد که هزینه پیاده‌سازی را خیلی بالا می‌برد. اما مدل شکل (ج) با بهبود مدل (الف)، به تعداد کمتری از واحدهای کنار جاده نیاز دارد.



شکل ۳-۷. آرایش واحدهای کنار جاده – الف) آرایش پایه بررسی و شبیه‌سازی شده توسط OU در [۴۳]. ب) آرایش پیشنهاد شده در [۴۳]. ج) آرایش پیشنهاد شده در این فصل

طبق بررسی انجام شده، اگر طول کل جاده که با نماد A نشان می‌دهیم، مضربی از ناحیه تحت پوشش L در شکل (۳-۷) باشد و R شعاع رادیویی واحدهای کنار جاده باشد، داریم:

$$A = mL, \quad (m = 1, 2, ...) \qquad (۵-۳)$$

اگر طبق مدل پایه در شکل (۳-۷ الف) $L = 6R$ باشد (R شعاع رادیویی واحد کنار جاده است)، رابطه بین تعداد واحدهای کنار جاده در این سه مدل به صورت زیر است:

- مدل (الف): $n = 6m$،

- مدل (ب): $n > 10m$ یا $n \approx ۱۱m$ (چون واحدهای دور دوم یا طول ۲L در ادامه مدل، به اندازه R با دور جاری همپوشانی دارند)
- مدل (ج): $n = 8m$.

یعنی اگر فرضا شعاع رادیویی هر واحد کنار جاده ۵۰۰ متر و طول جاده ۱۰ کیلومتر باشد، m=۲۰ بوده و تعداد واحدهای کنار جاده مورد نیاز در شکل (۳-۷) طبق مدل (الف) ۱۲۰، طبق مدل (ب) بیش از ۲۰۰ (حدود ۲۲۰) و طبق مدل (ج) ۱۶۰ واحد است. بعد از بررسی تعداد واحدهای کنار جاده مورد نیاز، به بررسی تایید موقعیت و فضای نمونه‌ای که خودروی بدخواه می‌تواند از آن فضا موقعیت نادرست خود را انتخاب کند می‌پردازیم.

برای بیان آسیب‌پذیری شبکه در صورت ارسال موقعیت نادرست توسط یک خودرو، یکی از کاربردهای مهم موقعیت‌یابی و اشکالی که ممکن است در آن ایجاد شود را بیان می‌کنیم. همانطورکه قبلا اشاره کردیم، یکی از کاربردهای مهم سیستم موقعیت‌یابی، مسیریابی در شبکه است. روش مسیریابی جغرافیایی[۱] بدلیل ویژگیهای شبکه‌های خودرویی همچون پویایی زیاد شبکه، تغییر سریع توپولوژی، اندازه بزرگ شبکه و نیز وجود کاربردهای ایمنی در شبکه خودرویی که این کاربردها از نظر زمان بحرانی بوده و به اطلاعات موقعیت قابل اطمینان وابسته هستند، یک انتخاب بجا و مناسب برای مسیریابی در شبکه است و این روش مخصوصا از مسیریابی مبتنی بر توپولوژی بهتر است [۵۵,۱۹]. در مسیریابی حریصانه[۲] از نوع مسیریابی جغرافیایی، نودی به عنوان نود بعدی در مسیریابی برای دریافت بسته انتخاب می‌شود که نسبت به موقعیت نود جاری به نود مقصد نزدیک‌تر باشد. بنابراین یک نود باید در مورد همه همسایگان خود آگاهی داشته باشد و موقعیت آنها را بداند. برای نیل به این هدف، لازم است که همه نودها موقعیتشان را به صورت دوره‌ای پخش کنند. بدین ترتیب هر نود می‌تواند یک جدول همسایگی بسازد و

[۱]. Geographic routing protocol
[۲]. Greedy based routing

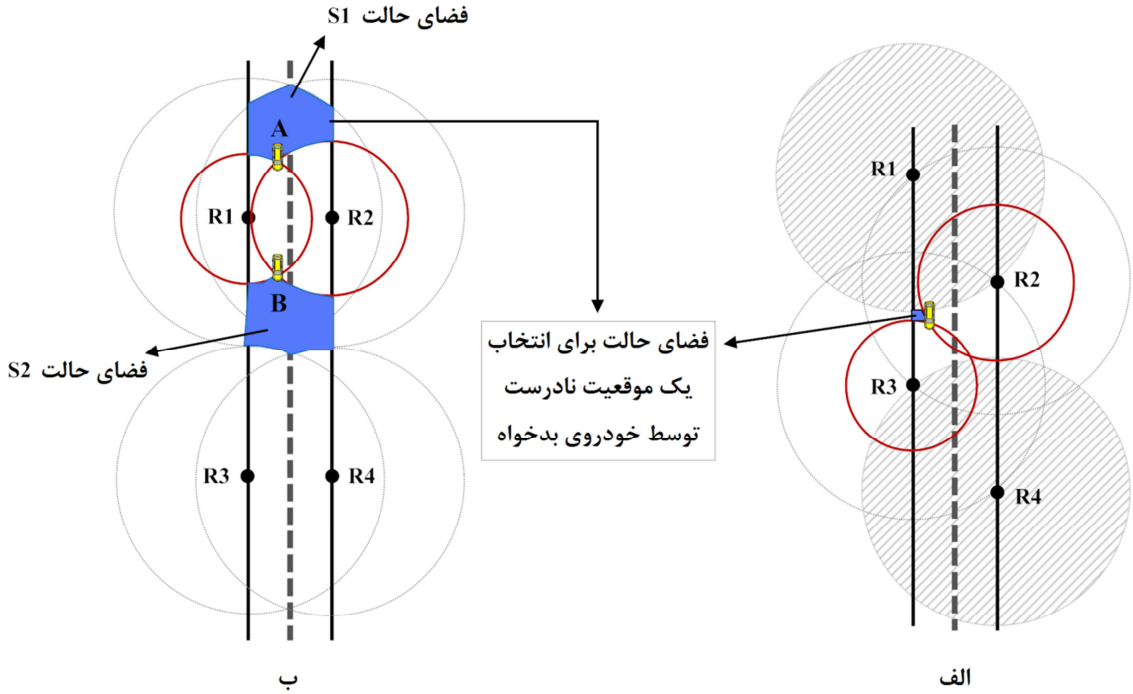
تصمیمات ارسال به نود بعدی از روی این جدول در نود مورد نظر گرفته شوند. این مکانیزم مسیریابی در برابر تحرک زیاد نودها (خودروها) پایدار است اما یک مسئله امنیتی برای مسیریابی مبتنی بر موقعیت یا مسیریابی جغرافیایی وجود دارد. برخی خودروها ممکن است بدخواه بوده و موقعیت‌های نادرست را در پیامهای دوره‌ای خود ارسال کنند. این حمله تاثیر بزرگی بر روی پروتکل‌های مسیریابی دارد، چون منجر به تغییر توپولوژی و بنابراین افت کارایی شبکه می‌شود. موقعیتهای نادرست می‌توانند نرخ تحویل داده را تا ۳۰٪ در پروتکل‌های مسیریابی جغرافیایی کاهش دهند [۱۸]. دریافت موقعیت نادرست علاوه بر ارسال موقعیت اشتباه از طرف خودروی بدخواه، ممکن است ناشی از عدم کارکرد صحیح یک سیستم تعیین موقعیت مانند دریافت‌کننده جی.پی.اس یا محاسبات نادرست در اثر شرایط دریافت بد نیز باشد [۱۹]. در هر صورت در اینجا نیاز به یک مکانیزم امنیتی مناسب برای پیشگیری از این حمله است. آرایش پیشنهادی برای واحدهای کنار جاده این مزیت را داراست که فضای حالت را برای انتخاب موقعیت نادرست توسط خودروی بدخواه کاهش می‌دهد. در متدهای مربوط به فاصله‌یابی، اگر یک تاییدکننده موقعیت (خودرو یا واحد کنار جاده)، بخواهد فاصله خود را تا خودروی ادعاکننده V بیابد، می‌تواند پیامی را برای V بفرستد. فرض می‌شود خودروی V بعد از دریافت پیام فوراً به تاییدکننده پاسخ می‌دهد. اگر همه این ارتباطات در لینک‌های رادیویی انجام شوند، سیگنالها باید با سرعت نور حرکت کنند. خودروی تاییدکننده می‌تواند فاصله خود را تا V با اندازه‌گیری بازه زمانی از انتقال پیام تا دریافت پاسخ تخمین بزند. مقدار تاخیری که برای ارسال پیام پاسخ وجود دارد در محاسبات لحاظ می‌شود تا بدین ترتیب دقت فاصله تخمینی را به واقعیت نزدیک نماید. مقدار فاصله تخمین زده شده دو برابر فاصله V از تاییدکننده است بنابراین این فاصله بر دو تقسیم می‌شود تا فاصله تاییدکننده از V بدست آید. این محاسبه فاصله توسط حداقل دو واحد کنار جاده با دریافت پیام دوره‌ای که توسط V ارسال می‌شود (پیامی حاوی موقعیت V)، انجام می‌شود. بعد از این طبق متد مکانیابی که در شکل (۳-۶) بیان شد، مکان خودروی V

این‌بار توسط واحدهای کنار جاده محاسبه می‌شود. با مقایسه مقدار محاسبه شده با مقدار دریافتی در پیام ارسالی توسط V، خودروی بدخواه در صورت ارسال مکان نادرست شناسایی می‌شود.

در این متد در صورتی‌که بتوان پیام پاسخ را از جانب V دیرتر یا زودتر ارسال کرد، خودروی بدخواه می‌تواند تاییدکننده را فریب دهد و وانمود کند که به تاییدکننده دورتر یا نزدیکتر از فاصله واقعی آن است. بنابراین این سوال مطرح می‌شود که آیا امکان ارسال زودتر و یا دیرتر پیام پاسخ از طرف V به تاییدکننده وجود دارد؟

هیچ چیز نمی‌تواند تندتر از سرعت نور حرکت کند، بنابراین برای خودروی ادعاکننده V امکان‌پذیر نیست که ادعا کند نزدیک‌تر از فاصله واقعی خود به تاییدکننده است. اما برای خودروی ادعاکننده این امر امکان‌پذیر است که ادعا کند دورتر از فاصله واقعی خود به تاییدکننده است. اینکار با تاخیر در ارسال پیام پاسخ انجام می‌شود. در مدل بررسی شده OU برای واحدهای کنار جاده، در شکل (۳-۸ ب)، فضای حالتی که خودروی V می‌تواند موقعیت نادرست خود را از آن انتخاب کند و طبق همان موقعیت در ارسال پیام پاسخ تاخیر بیندازد (فضای حالت S۱ یا S۲)، خیلی بیشتر از آرایش پیشنهادی در شکل (۳-۸ الف) است. در شکل (۳-۸ ب)، اگر خودروی V در موقعیت واقعی A باشد، می‌تواند یک موقعیت اشتباه را از فضای حالت S۱ انتخاب کرده و با توجه به آن در ارسال پیام پاسخ خود تاخیر بیندازد تا تاییدکننده را با اطلاعات مکانی اشتباه فریب دهد. اگر موقعیت واقعی خودرو موقعیت B باشد، می‌تواند از فضای S۲ یک موقعیت نادرست را انتخاب کند. فضای حالت S۱ از یک طرف به واحدهای کنار جاده R۱ و R۲ محدود است، چون نمی‌تواند ادعا کند نزدیکتر از موقعیت واقعی خود به آنها است و از طرف دیگر هم چون هر دو واحد R۱ و R۲ سیگنال خودرو را دریافت می‌کنند، باید محدود به مرز ناحیه تحت پوشش رنج رادیویی هر دو واحد R۱ و R۲ باشد و نمی‌تواند وارد حوزه واحدهای کنار جاده دیگر شود. در شکل (۳-۸ الف)، فضای حالت خیلی محدودتر از مدل شکل (۳-۸ ب) است. در این حالت، در برخی موارد نیز فضای حالت برای

انتخاب موقعیت نادرست توسط خودروی بدخواه V نزدیک به صفر است. چون رنج رادیویی واحدهای کنار جاده همپوشانی دارند و این نحوه آرایش برای واحدهای کنار جاده با مصرف تعداد کمتری واحد کنار جاده نسبت به مدل بهبود پیشنهاد شده توسط OU در شکل (۳-۷ ب)، همپوشانی مناسبی دارد و در ضمن فضای حالت را برای انتخاب موقعیت نادرست برای خودروی بدخواه خیلی کم می‌کند.



شکل ۳-۸. فضای حالت برای انتخاب موقعیت نادرست توسط خودروی ادعاکننده V به گونه‌ای که تاییدکننده قادر به تشخیص نباشد-الف) با توجه به آرایش پیشنهادی، ب) با توجه به آرایش مدل OU در [۴۳].

۳-۴- نتیجه‌گیری

اطلاعات مکان یکی از مهمترین داده‌های مورد نیاز برای کاربردهای مختلف در شبکه خودرویی است و اکثر کاربردها در این شبکه از این اطلاعات برای اهداف گوناگون استفاده می‌کنند. به همین منظور در ابتدای این فصل سیستم‌های موقعیت‌یابی گوناگون در شبکه خودرویی را مورد بررسی قرار دادیم که نتیجه این بررسی‌ها استفاده از روش مکانیابی OU است که برای رفع خطاهای دریافت‌کننده‌های جی.پی.اس، در نقاطی که خط دید مستقیم تا ماهواره وجود ندارد، مناسب است. این روش دقت مناسبی در کاربردهایی دارد که نیاز به دقت مکانیابی نسبتا دقیقی (کمتر از ۵ متر) دارند.

یکی از موارد کاربرد این روش مکانیابی، که در این فصل پیشنهاد شد، جلوگیری از حملات ارسال موقعیت نادرست توسط یک خودروی بدخواه در شبکه است. اطلاعات موقعیت نادرست، می‌تواند منجر به ایجاد ازدحام، تصادف و افت کارایی سیستم‌های مدیریت ترافیک گردد. برای استفاده از این روش در تایید موقعیت خودروها، یکی از مشکلات این روش نحوه آرایش واحدهای کنار جاده است که فضای انتخاب زیادی را برای خودروی بدخواه به منظور ارسال موقعیت نادرست فراهم می‌کند. به همین منظور در این فصل آرایشی را پیشنهاد دادیم که کل جاده را پوشش می‌دهد، فضای حالت برای انتخاب اطلاعات موقعیت نادرست توسط خودروی بدخواه را تاحد زیادی کاهش می‌دهد، در بسیاری از موارد نیاز به دریافت پیام دوم از جانب واحدهای کنار جاده برای انتخاب موقعیت صحیح خودرو از بین دو نقطه از مکان برخورد دایره‌های متقاطع نمی‌باشد و در نتیجه سربار مبادله پیام را در شبکه برای تعیین موقعیت توسط خودروها کاهش می‌دهد و دقت مکانیابی در نقاط تحت پوشش دو واحد، یکسان با مدل مطرح شده در [۴۳] است و در نقاط تحت پوشش سه واحد، این دقت بیشتر است. نتایج این بررسیها به صورت شماتیک در این فصل تشریح شدند.

فصل ۴

مقایسه امنیت و زمان اجرا در الگوریتم‌های رمزنگاری مختلف برای استفاده در پروتکل‌های امنیتی شبکه خودرویی

۴-۱- مقدمه

شبکه خودرویی کاربردهای زیادی از رانندگی ایمن گرفته تا دستیار راننده و دستیابی به اینترنت برای کاربردهای رفاهی را فراهم می‌کند. بنابراین در این شبکه، پیامهای مختلف با سطح ایمنی مختلف مبادله می‌شوند و پروتکلهای ارتباطی باید امنیت کافی را در مقابل کلیه پیامهایی که مبادله می‌شوند دارا باشند. برای همین منظور سیستمهای مبتنی بر رمزنگاری برای جلوگیری از حمله‌های مختلف و حفظ حریم شخصی در تبادل برخی اطلاعات حساس و مهم (مکان خودروها و اطلاعات شناسه منحصر به فرد خودروها مثل پلاک خودروها) به عنوان یک ضرورت مطرح می‌شوند. برخی مکانیزمهای رمزنگاری سربار محاسباتی بیشتری دارند که منجر به زمان پاسخ بیشتر و در نتیجه افت کارایی شبکه می‌شوند (مقیاس-پذیری شبکه کم می‌شود). بنابراین برای استفاده از این روشها و کارایی بهتر پروتکلهای ارتباطی تعریف شده، نیاز است که کارکرد این روشها بررسی شود تا یک مکانیزم ایمن، با زمان پردازش کم و طول پیام کافی تولید نماییم. برای ایمن‌سازی ارتباطات شبکه به هر دو نوع رمزنگاری کلید متقارن و رمزنگاری کلید نامتقارن نیاز داریم. در نتیجه در این فصل روشهای متداول در هر دو مکانیزم رمزنگاری متقارن و نامتقارن را پیاده‌سازی و بررسی کرده، تا بهترین روش را از لحاظ ایمنی، زمان اجرا و طول کلید برای پروتکلهای ارتباطی در شبکه خودرویی انتخاب نماییم. برنامه‌های پیاده‌سازی شده در این فصل با استفاده از کتابخانه Openssl و زبان C و تحت سیستم عامل اوبونتو ۱۲.۰۴ بر روی سیستمی با امکانات پردازشگر دو هسته-ای ۲.۶۶ گیگاهرتز و رم ۴ گیگ پیاده‌سازی شده‌اند.

۴-۲- علل نیاز به مکانیزمهای رمزنگاری

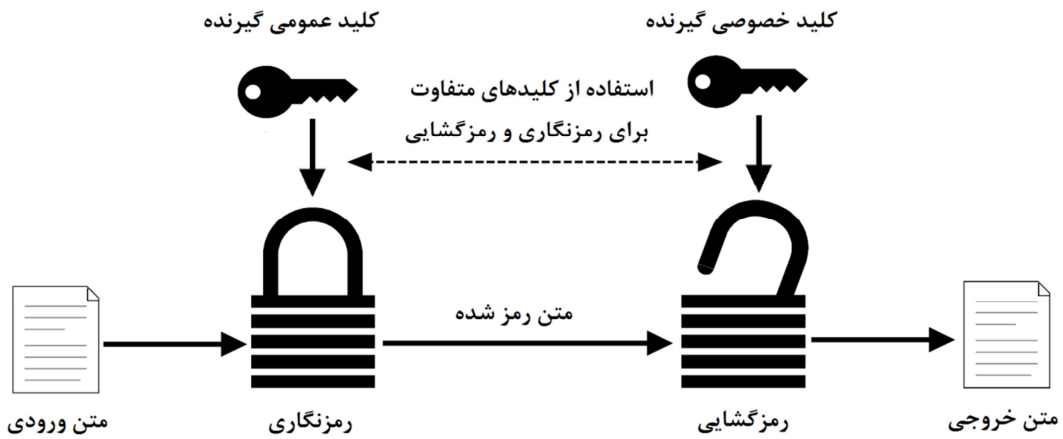
تعداد زیادی از پروتکلهای ارتباطی در شبکه خودرویی برای جلوگیری از حملات مختلف علیه ایمنی پیامها و حریم خصوصی رانندگان، نیاز به استفاده از روشهای رمزنگاری دارند. حمله‌کننده‌ها در این شبکه در دو دسته جای می‌گیرند: ۱. حمله‌کننده‌های داخلی که موجودیتهای مورد اعتماد در شبکه هستند و ۲. حمله‌کننده‌های خارجی که توسط سایر اعضا قابل شناسایی و اعتماد نیستند. تعداد زیادی از حملاتی که توسط حمله‌کننده‌های داخلی یا خارجی شبکه به وقوع می‌پیوندند، می‌توانند توسط روشهای مبتنی بر رمزنگاری شناسایی و یا پیش‌گیری شوند [۵۷,۵۶,۳۶,۳۵,۵,۳]. برخی از این حملات شامل:

- **استراق سمع پیام:** این امر به منظور دریافت اطلاعات خصوصی خودروی دیگر و سپس ردگیری و جعل هویتش انجام می‌پذیرد. این حمله، حریم خصوصی رانندگان را نقض می‌کند. برای حل این مشکل از روشهای رمزنگاری و امضای دیجیتال باید استفاده کرد. یک راه‌حل رمزنگاری پیامهایی است که شامل اطلاعات مهمی چون شناسه و مکان خودرو هستند.
- **دستکاری پیام:** این کار برای منافع حمله کننده و ایجاد ترافیک صورت می‌گیرد. امضای دیجیتال توسط فرستنده، گیرنده را از صحت و درستی پیام و عدم دستکاری مطمئن می‌کند.
- **حمله سایبل:** جعل شناسه خودروهای مختلف در شبکه و یا ساخت شناسه توسط خودروی بدخواه برای کاهش کارایی و اختلال در مسیریابی. مکانیزم‌های مختلفی برای شناسایی حمله وجود دارند که روشهای مبتنی بر رمزنگاری به دلیل نرخ شناسایی بالا و حفظ حریم خصوصی مناسب هستند.
- **ارسال پیامهای نادرست در شبکه:** با وجود زیرساخت کلید عمومی، خودروی بدخواهی که اقدام به ارسال اطلاعات نادرست می‌کند، با گزارش خودروهای دیگر، می‌تواند به راحتی ردگیری و فسخ شود.
- **ارسال مجدد بسته‌ها:** با درج تاریخ اعتبار پیام (دوره‌ای کوتاه مدت) و امضای آن امکان ارسال مجدد در دوره محدود تعیین شده از بین می‌رود.

معمولا برای حفظ ایمنی پیامها، از هر دو روش رمزنگاری کلید عمومی/نامتقارن و رمزنگاری متقارن (کلید مشترک) استفاده می‌کنیم. در ادامه به بیان ویژگیها و مقایسه الگوریتم‌های مختلف می‌پردازیم.

۴-۳- روش رمزنگاری کلید عمومی/ نامتقارن

روش رمزنگاری کلید عمومی از جفت کلید عمومی و خصوصی برای رمز استفاده می‌کند که کلید خصوصی نزد مالک جفت کلید به صورت امن نگه‌داری می‌شود و کلید عمومی برای رمزنگاری در اختیار خودروهای دیگر شبکه قرار می‌گیرد. این روش رمزنگاری، برای سه هدف ۱. رمزگذاری/ رمزگشایی (برای حفظ محرمانگی)، ۲. امضاء رقمی (برای حفظ اصالت پیام و معین نمودن فرستنده پیام) و ۳. توزیع کلید (برای توافق طرفین روی کلید نشست مخفی) می‌تواند مورد استفاده قرار بگیرد. در مورد رمزنگاری نامتقارن پیامها، همانطور که در شکل (۴-۱) نشان داده شده است، پیام مورد نظر با استفاده از کلید عمومی گیرنده که قبلا با روشی مطمئن در شبکه توزیع شده است، رمز می‌شود و پس از ارسال، توسط کلید خصوصی گیرنده رمزگشایی می‌شود.



شکل ۴-۱- رمزنگاری نامتقارن/کلید عمومی

توزیع کلیدهای عمومی خودروها در شبکه، برای اطمینان از هویت واقعی آنها، باید همراه با گواهینامه دریافتی از یک واحد معتبر و شناخته شده باشد.

در مورد امضای دیجیتال، ابتدا چکیده پیام با یکی از روشهای درهم‌سازی در سمت فرستنده تولید شده و سپس با کلید خصوصی فرستنده پیام رمز می‌شود و همراه با پیام ارسال می‌گردد. گیرنده با دریافت پیام، ابتدا خود چکیده آن را تولید می‌کند و سپس با کلید عمومی فرستنده چکیده رمزشده پیام که توسط گیرنده تولید شده رمزگشایی کرده و دو چکیده را مقایسه می‌کند. در صورت یکی بودن آنها مطمئن می‌شود که پیام از جانب فرستنده‌ای که ادعا می‌کند پیام از طرف او فرستاده شده، ارسال شده است. بدین ترتیب هویت فرستنده ثابت می‌شود. رمزنگاری کلید عمومی مبتنی بر توابع ریاضی و محاسبات پیچیده است که این امر باعث می‌شود این روش برای دستگاههای کوچک مناسب نباشد. مزایای الگوریتمهای رمز نامتقارن را به صورت زیر بیان می‌کنیم:

۱. **راحتی:** این الگوریتمها مشکل توزیع کلید ندارند. هر خودرو جفت کلید عمومی و خصوصی خود را دریافت کرده و به این ترتیب پیامهای خود را در شبکه بدون نیاز به انتقال کلید مشترک به طور ایمن، انتقال می‌دهد.

۲. **مدیریت آسان کلید:** با استفاده از کلید عمومی، نیاز نیست برای هر کاربر یک کلید توافقی ایجاد کرد. بلکه می‌توان از یک جفت کلید برای ارتباط با کل کاربران شبکه استفاده کرد.

۳. **امکان امضای پیام برای تصدیق هویت فرستنده:** روشهای رمزنگاری کلید عمومی برای امضای دیجیتال و تصدیق هویت فرستنده قابل استفاده است.

معایب الگوریتمهای رمزنگاری کلید عمومی را می‌توان به صورت زیر بیان کرد:

۱. **گواهینامه کلید عمومی:** کلیدهای عمومی نمی‌توانند به راحتی در شبکه مورد استفاده قرار بگیرند و برای اطمینان گیرنده، باید توسط یک واحد معتبر تایید شده باشند. گواهینامه دریافتی برای هر کلید عمومی تعلق واقعی این کلید به خودرو را نشان می‌دهد.

۲. **سرعت پایین:** این روش رمزنگاری در مقایسه با روش کلید متقارن سرعت خیلی کمتری دارد.

۳. **اندازه کلید:** اندازه کلید در مقایسه با روشهای رمز متقارن بزرگتر است.

۴. **منابع محاسباتی:** در مقایسه با روشهای متقارن منابع محاسباتی بیشتری نیاز دارند.

۵. **مقاومت:** این روش از روشهایی است که شکستن رمز را برای تحلیلگر با توجه به تکنولوژیهای موجود و در زمان محدود غیرممکن سازد. هرچه قدرت محاسبات بیشتر شود، احتمال شکست روشهایی که طول کلید کوتاهتر دارند بیشتر می‌شود.

پیامها در صورت کوتاه بودن، با روش کلید عمومی رمز می‌شوند. از نظر کاربردی، رمزگذاری با کلید عمومی بیش از آنکه جایگزینی برای رمزگذاری سنتی (رمز متقارن) باشد، نقش مکمل آنرا برای حل مشکلات توزیع کلید بازی می‌کند. معمولا کلید مشترک مربوط به رمزنگاری متقارن با رمزنگاری نامتقارن رمز می‌شود و بعد از ارسال کلید، کلیه پیامهای بین فرستنده و گیرنده در زمان تعریف شده برای مدت اعتبار کلید مشترک (یا طول عمر کلید)، با رمزنگاری کلید متقارن رمز می‌شوند که سربار محاسباتی کمتر و در نتیجه زمان اجرای خیلی کمتری دارند. روشهای مختلف رمزنگاری کلید عمومی، که در اکثر کاربردها مورد استفاده قرار می‌گیرند، محدود هستند و در اکثر موارد روش RSA و برخی نیز از روش مبتنی بر منحنی بیضوی برای رمزنگاری کلید عمومی استفاده می‌کنند. یکی از مزایای این دو روش اینست که هر دو روش RSA و منحنی بیضوی در هر سه مقوله رمزنگاری نامتقارن، امضای دیجیتال و توزیع کلید مشترک کاربرد دارند. به همین منظور دو روش متداول RSA و روش مبتنی بر منحنی بیضوی (ECC[۱]) را در ادامه بیان می‌کنیم.

RSA: یکی از پرکاربردترین و مشهورترین الگوریتمهای رمز نامتقارن است که توسط Rivest، Shamir و Adleman درسال ۱۹۷۷ توسعه داده شد [۵۸]. نام این روش برگرفته از توسعه‌دهندگان آن است. این

[۱] Elliptic Curve Cryptography

روش مبتنی بر توان رسانی ماژولی و استفاده از اعداد طبیعی خیلی بزرگ است. معمولا برای امنیت کافی در این روش طول کلید حداقل ۱۰۲۴ بیت در نظر گرفته می‌شود.

در این روش حمله جستجوی جامع کلید در صورتی که اندازه فضای کلید بزرگ باشد امکان‌پذیر نیست. در مقابل حملات ریاضی نیز، امنیت این روش ناشی از دشوار بودن تجزیه اعداد بزرگ به دو عامل اول است که شکستن این روش را در زمانی قابل قبول غیرممکن می‌کند. حملات زمانی، مبتنی بر استخراج تغییرات زمانی در عملیات و یا زمان رمزگذاری/رمزگشایی مثلاً ضرب کردن با اعداد کوچک در مقابل اعداد بزرگ یا بدست آوردن اندازه عملوندها برحسب زمانی که طول می کشد، می‌باشند که البته معمولاً پیاده‌سازی‌های این الگوریتم، تغییرات زمانی شدید ندارند. با این وجود، راه حل این حمله شامل: ۱. استفاده از زمان ثابت برای عمل توان رسانی (هرچند کارایی را کاهش می دهد)، ۲. اضافه کردن تأخیرهای تصادفی (برای گیج کردن حمله کننده) و ۳. ضرب کردن متن رمز در یک عدد تصادفی قبل از عمل توان رسانی است.

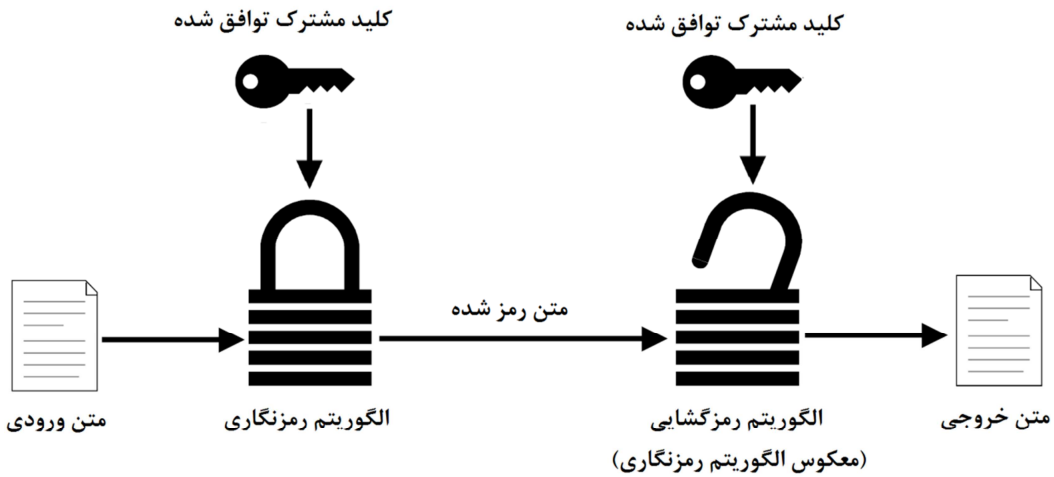
رمزنگاری مبتنی بر منحنی بیضوی (ECC): نوعی رمزنگاری کلید عمومی می‌باشد، که براساس ساختاری جبری منحنی‌های بیضوی بر روی زمینه‌های محدود طراحی شده است. استفاده از منحنی‌های بیضوی در رمزنگاری به طور جداگانه توسط Neal Koblitz و Victor S. Miller در سال ۱۹۸۵ پیشنهاد شد. این روش با طول کلید کوتاهتر از RSA و امنیت یکسان، جایگزین مناسبی برای آن به نظر می‌رسد. این مزیت برای وسایلی که از نظر حافظه و ظرفیت پردازش محدود هستند، مانند کارتهای هوشمند، اهمیت زیادی دارد. امنیت روشهای مبتنی بر منحنی بیضوی وابسته به تابع لگاریتم گسسته است.

در شبکه خودرویی به روشهای کلید عمومی برای هر دو هدف رمزنگاری کلید عمومی و همچنین امضای دیجیتال نیاز داریم. اما بررسی نسبتا کاملی در مورد امضای دیجیتال با کمک دو روش RSA و منحنی بیضوی در [۵۹] بیان شده است. بنابراین در این بخش بررسی خود را محدود به رمزنگاری کلید

عمومی می‌کنیم و در ادامه این دو روش را برای انتخاب روشی مناسب جهت بکارگیری در مدلهای ارتباطی ایمن در شبکه خودرویی مورد مقایسه قرار می‌دهیم.

۴-۴- رمزنگاری کلید متقارن

روشهای مبتنی بر کلید نامتقارن به دلیل افزایش طول کلید، افزایش محاسبات و در نتیجه افزایش زمان اجرا برای امضای پیامهای بزرگ مناسب نمی‌باشند. برای همین منظور، معمولا از روش کلید متقارن برای رمزنگاری پیام اصلی استفاده می‌شود. در این روش رمزنگاری همانطور که در شکل (۴-۲) نشان داده شده است از یک کلید مشترک استفاده می‌شود که رمزنگاری و رمزگشایی هردو با این کلید انجام می-شوند.



شکل ۴-۲. رمزنگاری متقارن

از مزایای روشهای رمزنگاری متقارن می‌توان به موارد زیر اشاره کرد:

۱. **سادگی:** این روش رمزنگاری ساده‌تر از روش رمز نامتقارن است.

۲. **سرعت:** این روش سریعتر از روشهای رمزنگاری کلید عمومی هستند.

۳. **منابع محاسباتی:** این روشها منابع محاسباتی زیادی برای رمزنگاری و رمزگشایی نیاز ندارند.

۴. **طول کلید:** طول کوتاه کلید از مزایای این روش رمزنگاری می‌باشد.

از معایب روشهای رمزنگاری متقارن شامل:

۱. **تبادل کلید:** برای تبادل ایمن کلید مشترک، یک کانال امن باید وجود داشته باشد یا از روشهای ایمن برای انتقال کلید استفاده شود.

۲. **تعداد کلیدها:** برای ارتباط با هر خودرو در شبکه یک کلید مشترک جدید باید توافق شود. مدیریت و نگه‌داری این کلیدها خود یک مشکل است.

۳. **تصدیق هویت:** سندیت پیام با این روش اثبات نمی‌شود. چون فرستنده و گیرنده هر دو از یک کلید مشترک استفاده می‌کنند، بنابراین نمی‌توان تایید کرد که پیام از یک فرستنده منحصر به فرد و خاص می‌آید.

تولید رمز متقارن با روشهای مختلف انجام می‌پذیرد که شامل رمز قطعه‌ای و رمز دنباله‌ای است. در رمز دنباله‌ای پردازش پیامها بصورت پیوسته انجام می‌گیرد و در رمز قطعه‌ای پردازش پیامها بصورت قطعه قطعه است که اندازه قطعات متفاوت است (سایز متعارف قطعات ۶۴، ۱۲۸ یا ۲۵۶ بیت است). اکثر روشهای رمز متقارن مبتنی بر قطعه هستند و هر قطعه متن اولیه با نگاشتی برگشت‌پذیر به متن رمزشده تبدیل شده است. الگوریتم قطعات ورودی را در چند مرحله ساده و متوالی به نام دور پردازش می‌کند که هر دور مبتنی بر اعمال ساده‌ای چون جایگزینی و جایگشت است.

قدرت رمزنگاری کلید متقارن بستگی به طول کلید دارد. برای یک الگوریتم رمزنگاری هرچه اندازه کلید بزرگتر باشد شکستن رمز سخت‌تر است. تعداد دور الگوریتم نیز هرچه بیشتر باشد، حمله را سخت‌تر می‌کند. در این بخش به ارزیابی ۶ الگوریتم مختلف برای رمزنگاری متقارن می‌پردازیم. الگوریتمی برای ارتباط پیامهای ایمن در شبکه خودرویی مناسب‌تر است که هم سطح ایمنی قابل قبولی در مدت چرخه طول عمر کلید داشته باشد و هم اینکه زمان رمزنگاری کمتری داشته باشد. در این بررسی که برای شبکه

خودرویی انجام می‌گیرد، چون از نظر باطری محدودیتی نداریم، منابع مصرفی را در مقایسات منظور نمی-کنیم. به منظور مقایسه و انتخاب روشی مناسب برای رمزنگاری، به بررسی روشهای متداول رمزنگاری متقارن پرداخته‌ایم که در جدول (۴-۱) روشهای انتخابی و ویژگیهای هریک را بیان کرده‌ایم. در این روشها اندازه بزرگ بلوک داده باعث مقاوم‌تر شدن در برابر حمله روز تولد می‌شود و بزرگتر شدن اندازه کلید از حمله جستجوی جامع[۱] جلوگیری می‌کند [۶۰]. بنابراین این دو خصوصیت مهم را در مقایسه خود در این جدول لحاظ کرده‌ایم.

جدول ۴-۱. مقایسه ویژگیهای الگوریتمهای متداول رمز متقارن

	DES	AES	Blowfish	Camellia	CAST-۱۲۸	SEED
طول کلید (بیت)	۵۶	{۱۲۸، ۱۹۲ یا ۲۵۶}	۳۲ تا ۴۴۸	{۱۲۸، ۱۹۲ یا ۲۵۶}	۴۰ تا ۱۲۸ (واحد افزایش ۸)	۱۲۸
طول بلوک داده (بیت)	۶۴	۱۲۸	۶۴	۱۲۸	۶۴	۱۲۸
تعداد دور	۱۶	{۱۰، ۱۲ یا ۱۴} متناسب با هر کلید	۱۶	۱۸ (کلید ۱۲۸ بیت) یا ۲۴ (کلید ۱۹۲ یا ۲۵۶)	۱۲ یا ۱۶ (۱۶ برای کلید بزرگتر از ۸۰ بیت)	۱۶

SEED: روش رمزنگاری بلوکی که توسط آژانس امنیت اطلاعات کره[۲] از سال ۱۹۹۸ توسعه داده شد و بعنوان الگوریتم رمزنگاری استاندارد ملی در کره جنوبی پذیرفته شده است. این روش در برابر حمله‌های شناخته شده شامل تحلیل تفاضلی[۳]، تحلیل خطی[۴] و حمله‌های مبتنی بر کلید مقاوم است. هیچ مشکل امنیتی در این روش آشکار نشده و تنها حمله ممکن جستجوی جامع کلید بیان شده است [۶۱].

۱. Brute force
۲. Korea Information Security Agency (KISA)
۳. Differential cryptanalysis (DC)
۴. Linear cryptanalysis (LC)

Camellia: الگوریتم رمز بلوکی که در سال ۲۰۰۰ به طور مشترک توسط شرکت تلگراف و تلفن Nippon و شرکت الکتریکی Mitsubishi توسعه داده شد. سطح ایمنی و پردازش این روش همانند روش AES است. این روش در نرم‌افزار و سخت‌افزار هردو کاربرد دارد. هدف از طراحی این روش سطح ایمنی بالا و کارایی روی چند پلتفرم مختلف است. کاربرد Camellia در IPsec در استاندارد RFC ۳۷۱۳ و در OpenPGP در استاندارد RFC ۴۳۱۲ بیان شده است.

CAST-۱۲۸: یک الگوریتم رمز با متد جایگشت و جانشینی مشابه با DES است که در استاندارد RFC ۲۱۴۴ توصیف شده است. این روش در سال ۱۹۹۶ توسط Carlisle Adams و Stafford Tavares ایجاد شده است (نام CAST برگرفته از نام توسعه دهندگان آن است). از خصوصیات مثبت این روش ایمنی در مقابل تحلیل تفاضلی و تحلیل خطی است. این روش در برخی نسخه‌های GPG و به عنوان روش پیش-فرض استفاده شده است.

Blowfish: در سال ۱۹۹۳ توسط Bruce Schneier طراحی شد. این روش نرخ رمزنگاری خوبی را برای نرم‌افزار فراهم کرده است. سرعت، بهم پیوستگی و رمزنگاری بلوکی آسان با طول کلیدهای مختلف که انتخاب این کلیدهای مختلف یک سبک سنگینی بین دو ویژگی سرعت و امنیت است، از ویژگیهای مثبت این روش است. این روش رمز در معرض حملات ناشی از انتخاب کلید ضعیف است [۶۳,۶۲]. کلاسی از کلیدها به عنوان کلیدهای ضعیف وجود دارد که کاربران باید با دقت کامل کلید را انتخاب کنند به گونه‌ای که در این کلاس نباشد. با وجود مسئله کلیدهای ضعیف، هیچ حمله موفقیت‌آمیزی تاکنون علیه این روش رمزنگاری گزارش نشده است. در این روش، حمله‌های آشکارسازی کلید نیز در صورتیکه کلید مناسبی انتخاب شود و طول کلید بزرگتر از ۱۲۸ باشد، به هیچ وجه ممکن نخواهد بود.

AES[1]: این الگوریتم یک روش رمز بلوکی است که توسط Joan Daemon و Vincent Rijmen اختراع شده و توسط موسسه ملی تکنولوژی و استانداردهای ایالت متحده[2] توسعه داده شده است. این الگوریتم در یک رقابت متشکل از صدها رمزنگار در طی چندین سال انتخاب شده است. به دلیل اندازه بزرگ کلید، امنیت این روش در مقابل حمله جستجوی جامع نسبت به DES خیلی بیشتر است. در مقابل حمله‌های آماری آزمایشات زیادی برای تحلیل آماری متن رمزشده انجام شده که شکست خورده‌اند و در مقابل تحلیل تفاضلی و تحلیل خطی حمله‌ای تاکنون گزارش نشده است.

DES[3]: این روش اولین استاندارد رمزنگاری توسط موسسه ملی تکنولوژی و استانداردهای ایالت متحده است. DES به دلیل کوچک بودن اندازه کلید، امنیت مناسبی ندارد و به همین دلیل روش AES جایگزین این استاندارد شده است. کوچک بودن کلید و همچنین خصوصیت مکمل بودن کلیدها (نیمی از کلیدها در فضای حالت کلیدهای ممکن، مکمل نیمی دیگر هستند بنابراین تنها با تست کردن نیمی از کلیدها قادر به یافتن کلید هستیم) دو خصوصیت عمده‌ای هستند که احتمال حمله جستجوی جامع را بیشتر می‌کنند [۶۴]. این روش در مقابل تحلیل تفاضلی ایمن است و طراحی الگوریتم به گونه‌ای انجام شده که در مقابل این حمله مقاوم است. اما در مورد تحلیل خطی مقاومت کافی را ندارد.

۴-۵- مقایسه و نتایج حاصل از پیاده‌سازی

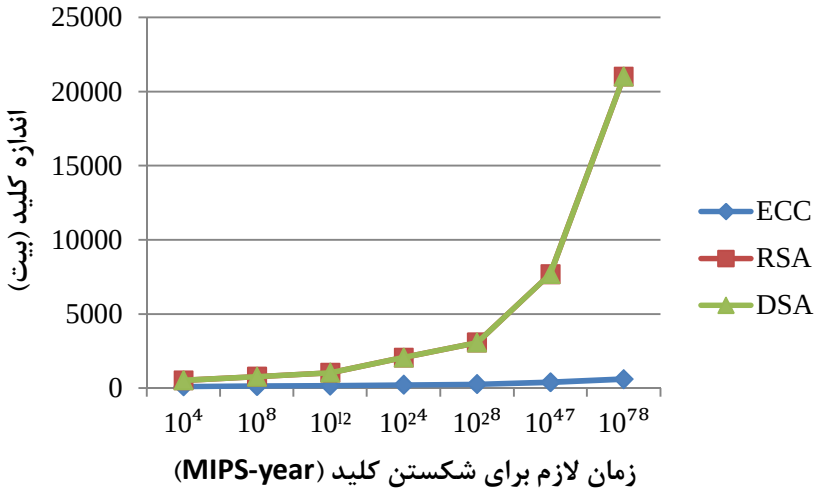
۴-۵-۱- روشهای کلید عمومی: مقایسه سطح ایمنی

در شکل (۴-۳) مقایسه سطح امنیتی کلید عمومی برای سه روش رمزنگاری RSA، روش مبتنی بر منحنی بیضوی (ECC) و روش DSA را بر اساس داده‌های گزارش شده در [۶۶,۶۵] مشاهده می‌کنیم. در این شکل یک MIPS-year زمان محاسباتی یک سال را نشان می‌دهد که در این یک سال، یک ماشین

---

[1] . Advanced Encryption Standard (AES)
[2] . US National Institute of Standards and Technology (NIST)
[3] . Data Encryption Standard (DES)

یک میلیون دستورالعمل را در هر ثانیه انجام می‌دهد. روش RSA معمولا برای رمزنگاری کلید عمومی، روش DSA فقط برای امضای دیجیتال و روش مبتنی بر منحنی بیضوی برای هردو منظور مورد استفاده قرار می‌گیرند.



شکل ۴-۳- مقایسه ایمنی کلید برای سه روش رمزنگاری کلید عمومی

طول کلید در دو روش RSA و DSA یکسان است. همانطور که در این شکل ملاحظه می‌شود، روش مبتنی بر منحنی بیضوی با طول کلید خیلی کوتاهتر در مقابل حملات مبتنی بر کلید در مقایسه با دو روش دیگر مقاوم‌تر است. در یک بررسی دقیق‌تر، با توجه به آمار گزارش شده در [۶۶]، در جدول (۴-۲) ملاحظه می‌کنیم که در روش منحنی بیضوی با طول کلید کوتاهتر می‌توان به همان سطح ایمنی در روشهای نامتقارن RSA و DSA رسید. کوتاه بودن طول کلید در سیستمهای رمزنگاری اهمیت زیادی دارد و سبب کاهش توان مصرفی سیستم، پهنای باند، میزان پردازش و حافظه مورد نیاز می‌شود. در سیستمهای سیار مثل تلفن‌های همراه، کارتهای هوشمند و خودروهای هوشمند (به دلیل اهمیت زیاد زمان پاسخ سیستم) که محدودیتهایی در استفاده از الگوریتمهای رمزنگاری وجود دارد، وجود سیستمهای رمزنگاری مبتنی بر منحنی بیضوی به عنوان راهکاری مناسب مطرح می‌شود. البته یکی از مشکلات این

روش زمانبر بودن محاسبات آن بدلیل پیچیدگی بالای عملیات آن می‌باشد که در این زمینه نیز راهکارهایی برای سرعت بخشیدن به محاسبات پیشنهاد شده است [۶۸,۶۷].

جدول ۴-۲. مقایسه طول کلید در دو روش RSA و ECC

سطح ایمنی	طول متناظر برای کلید متقارن (بیت)	طول کلید در روش ECC (بیت)	طول کلید در RSA و DSA	نرخ اندازه کلید ECC به RSA
2^{80}	۸۰	۱۶۰	۱۰۲۴	۱/۶
2^{112}	۱۱۲	۲۲۴	۲۰۴۸	۱/۹
2^{128}	۱۲۸	۲۵۶	۳۰۷۳	۱/۱۲
2^{192}	۱۹۲	۳۸۴	۷۶۸۰	۱/۲۰
2^{256}	۲۵۶	۵۱۲	۱۵۳۶۰	۱/۳۰

برای الگوریتم RSA دو دلیل برای افزایش طول کلید وجود دارد: ۱. برای امنیت بالاتر و ۲. هرچه اندازه پیامها بزرگتر می‌شود باید طول کلید را افزایش دهیم چون برای رمزنگاری در این روش، طول پیام باید از طول کلید ۴۲ بایت کوتاه‌تر باشد. پس افزایش طول کلید، کمک زیادی به افزایش ایمنی پیام می-کند. اما باید در نظر بگیریم که افزایش طول کلید افزایش محاسبات و زمان اجرا را با خود دارد که در نتیجه طول کلیدی انتخاب می‌شود که ایمنی قابل قبولی را برای ما فراهم کند. در منابع مختلف، طول کلید ۱۰۲۴ پیشنهاد شده که تاکنون با منابع محاسباتی موجود حمله‌ای در مقابل آن در زمان محدود گزارش نشده است. در روش منحنی بیضوی هدف از افزایش طول کلید افزایش سطح ایمنی است. در این روش محدودیتی برای طول پیام با توجه به طول کلید وجود ندارد و ایمنی مورد نیاز تعیین کننده طول کلید است.

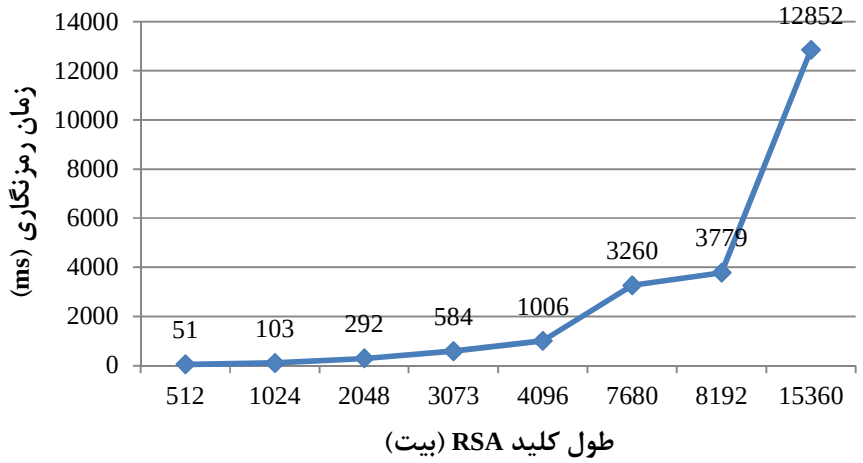
۴-۵-۲- روشهای کلید عمومی: مقایسه زمان اجرا

با روش RSA، برای اینکه بتوانیم پیامهای طولانی‌تر را رمز کنیم سه راه وجود دارد: ۱. اندازه کلید را افزایش دهیم، ۲. رمزکردن پیامهای طولانی با همان روشی که در روشهای بلاکی انجام می‌شود. یعنی پیامها را در بلاکهای با اندازه مناسب رمز کنیم و سپس آنها را با یک روش زنجیرسازی معین که در الگوریتمهای متقارن وجود دارند، بهم وصل کنیم و ۳. از رمزنگاری هیبرید استفاده کنیم. یعنی ابتدا یک کلید تصادفی تولید شود و این کلید که یک کلید رمز متقارن (کلید مشترک توافقی) است، با روش RSA رمز کنیم و پیام اصلی را با روش رمز متقارن و همین کلید مشترک رمزنگاری کرده و ارسال کنیم.

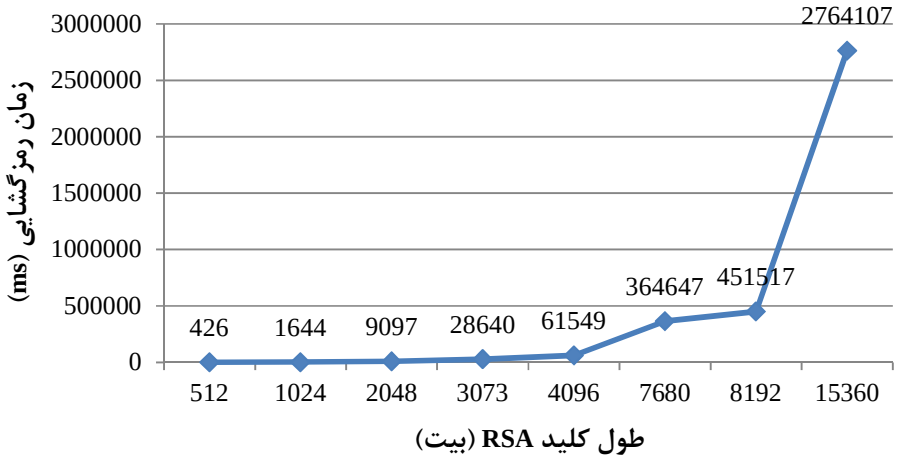
در شبکه خودرویی برای انتخاب بهترین روش، مهمترین فاکتورها، فاکتور زمان و سطح ایمنی الگوریتم انتخابی است. از طرفی پیامهایی که در شبکه بین خودروها و بین خودرو با زیرساخت جاده، مبادله می-شوند اکثرا پیامهای کوتاهی نیستند. این پیامها معمولا حاوی یک پیام نسبتا کوتاه به همراه فاکتورهای ایمنی مثل امضای دیجیتال، کلیدهای عمومی و گواهینامه‌ها هستند. بنابراین در صورت استفاده از RSA و لحاظ کردن روش اول (استفاده از کلید بزرگتر) برای رمزکردن کلیه پیامهای ایمن (پیامهایی که نباید محتوای آنها در شبکه آشکار شود)، زمان رمزنگاری و بخصوص رمزگشایی خیلی افزایش می‌یابد. از طرفی شبکه خودرویی نیاز به زمان پاسخ خیلی کوتاه دارد چون هم زمان عکس‌العمل راننده بعد از دریافت پیامهای ایمنی هشدار به راننده باید خیلی کوتاه باشد و هم مقیاس‌پذیری شبکه (تعداد خودروهایی که پیام را در مدت زمانی معین دریافت می‌کنند که این مدت زمان معمولا مدتی است که خودروها در رنج رادیویی خودروهای دیگر یا واحد کنار جاده هستند) باید به اندازه‌ای باشد که کل خودروها را سرویس دهد. بنابراین این روش مناسب نیست. استفاده از روش دوم برای رمزنگاری پیامهای طولانی نیز روش معمولی نیست و استفاده از آن توصیه نشده است. در کتابخانه‌های رمزنگاری موجود نیز هیچ حمایتی

برای بلوک‌بندی پیام، رمزنگاری با روش RSA و سپس اتصال بلوکها وجود ندارد. اما استفاده از روش سوم و منتقل کردن کلید با روش RSA در اکثر موارد، روش مناسبی است.

طول پیام در زمان رمز تاثیر زیادی ندارد و تنها فاکتوری که نقش خیلی زیادی در زمان پردازش RSA دارد اندازه کلید است. بنابراین برای درک بهتر کارکرد الگوریتم RSA، زمان رمزنگاری و رمزگشایی در این روش را با طول کلیدهای مختلف به ترتیب در شکل‌های (۴-۴) و (۴-۵) نشان داده‌ایم.

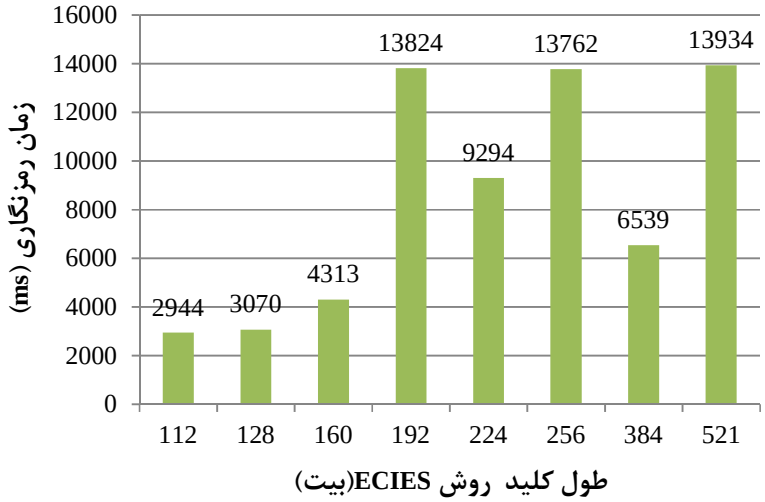


شکل ۴-۴. زمان رمزنگاری برحسب طول کلید در روش رمزنگاری RSA

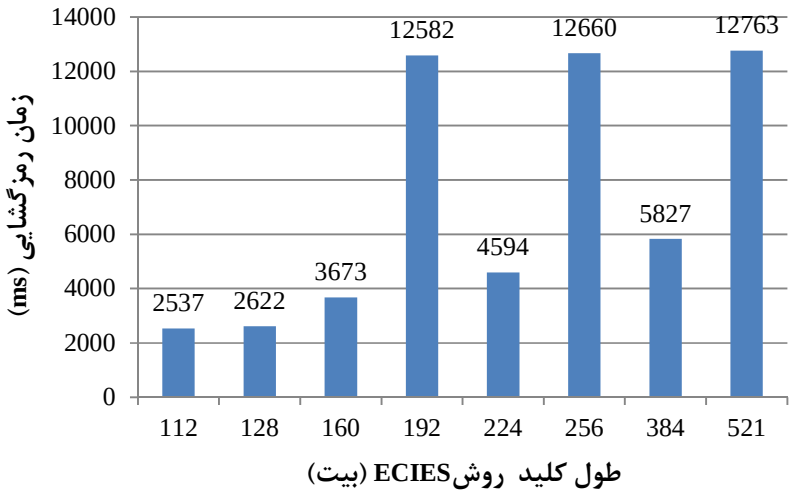


شکل ۴-۵. زمان رمزگشایی برحسب طول کلید در روش رمزنگاری RSA

در بررسی زمان اجرای الگوریتم رمزنگاری کلید عمومی با روش منحنی بیضوی (ECIES)، همانند روش RSA، طول پیام در زمان رمز تاثیر زیادی ندارد و تنها فاکتوری که در زمان پردازش آن تاثیر دارد، اندازه کلید است. بنابراین برای درک بهتر کارکرد این روش، زمان رمزنگاری و رمزگشایی در این روش را با طول کلیدهای مختلف به ترتیب در شکل‌های (۴-۶) و (۴-۷) نشان داده‌ایم.



شکل ۴-۶. زمان اجرای رمزنگاری برای طول کلیدهای مختلف در الگوریتم رمز ECIES



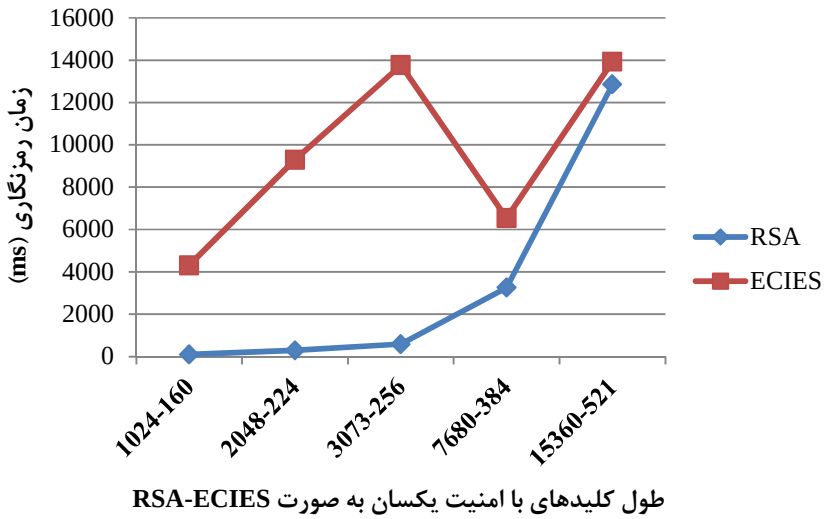
شکل ۴-۷. زمان اجرای رمزگشایی برای طول کلیدهای مختلف در الگوریتم رمز ECIES

همانطور که اشاره شد، در روش ECIES اندازه پیام وابسته به طول کلید نیست. اما در حالت پایه رمزنگاری با روش RSA، طول پیام کمتر از طول کلید است. بنابراین در جدول (۴-۳) اندازه پیام رمزشده را برای طول کلیدهای مختلف نشان داده‌ایم.

جدول ۴-۳. طول پیام تولید شده در روش رمزنگاری نامتقارن RSA برحسب طول کلید

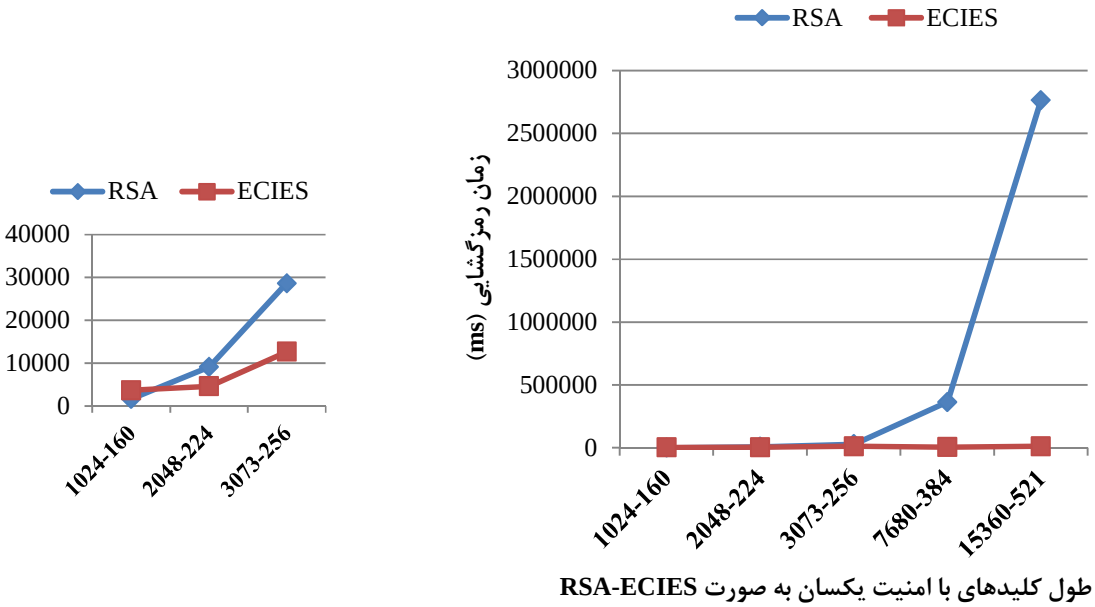
طول کلید (بیت)	۱۰۲۴	۲۰۴۸	۳۰۷۳	۴۰۹۶	۷۶۸۰	۸۱۹۲	۱۵۳۶۰	۱۶۳۸۴
اندازه پیام (بیت)	۶۸۸	۱۷۱۲	۲۷۴۴	۳۷۶۰	۷۳۴۴	۷۸۵۶	۱۵۰۲۴	۱۶۰۴۸

در شکل (۴-۸) و (۴-۹) مقایسه دو روش RSA و ECIES را از نظر زمان رمزنگاری و رمزگشایی ملاحظه می‌کنیم.



شکل ۴-۸. مقایسه زمان اجرا برای رمزنگاری با دو روش RSA و ECIES

با توجه به کلیدهای با امنیت یکسان در دو روش در جدول (۴-۲).



شکل ۴-۹. مقایسه زمان اجرای رمزگشایی دو روش RSA و ECIES

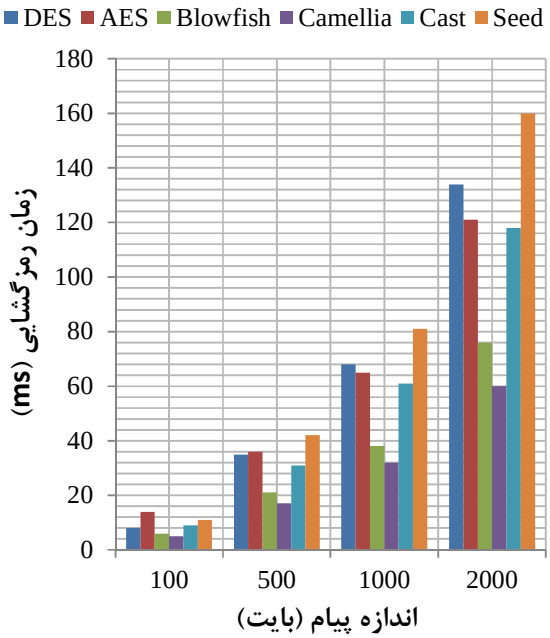
با توجه به کلیدهای با امنیت یکسان در دو روش در جدول (۴-۲).

طبق بررسی روش RSA در شکل (۴-۴)، زمان رمزنگاری برای الگوریتم RSA برای طول کلید ۱۰۲۴ بیت و حتی بزرگتر از آن پایین است و در مقایسه با روش منحنی بیضوی (ECIES) در شکل ۴-۸، زمان پردازش کمتری نیاز دارد. اما در مورد زمان رمزگشایی، همانطور که در شکل (۴-۵) ملاحظه می‌کنیم، با افزایش طول کلید زمان رمزگشایی RSA به شدت افزایش می‌یابد. به گونه‌ای که برای طول کلید بزرگتر از ۲۰۴۸ بیت، استفاده از این روش رمزنگاری دیگر مناسب نیست. در روش مبتنی بر منحنی بیضوی (ECIES)، در شکل (۴-۹)، در اثر افزایش طول کلید از مقدار ۱۹۲ بیت به بعد، زمان رمزگشایی در یک رنج باقی مانده و یا حتی کاهش می‌یابد. همانطور که در این شکل ملاحظه می‌کنیم، تنها برای طول کلید ۱۰۲۴ بیت در روش RSA، هردو زمان رمزنگاری و رمزگشایی نسبت به روش دیگر با طول کلید متناظر (۱۶۰ بیت) کمتر است و در بقیه موارد، رمزگشایی با روش ECIES از نظر زمانی بهتر از RSA است و تفاوت زیادی با آن دارد.

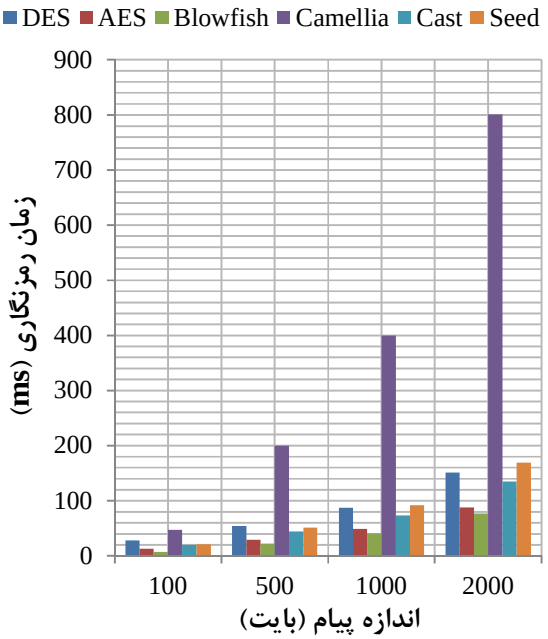
در شبکه خودرویی، در صورت نیاز، معمولا پیام از جانب یک خودروی فرستنده رمز شده و در شبکه پخش می‌شود. مخاطب این پیام می‌تواند سایر خودروهایی که در رنج رادیویی این خودرو هستند باشند و یا واحد کنار جاده باشد. رمزنگاری کلید عمومی برای این ارتباطات در صورتی استفاده می‌شود که یا پیام حامل اطلاعات خصوصی خودرو باشد (مثل شناسه یا پلاک) و یا قرار است پیام را گروه خاصی از خودروها دریافت کنند که در اینصورت قبل از ارسال و دریافت پیام در این گروه خاص باید خودروهای موردنظر با دریافت کلید خصوصی منحصر به خود و کلید عمومی مشترک با بقیه اعضای گروه، به عضویت گروه درآیند. در هر صورت اگر مخاطب پیام یک نفر باشد (خودرو یا واحد کنار جاده) بسته به اهمیت پیام از یکی از دو روش رمزنگاری می‌توان استفاده کرد. به گونه‌ای که اگر از روش RSA استفاده کنیم، بهتر است اندازه پیام طولانی نباشد تا از طول کلید کمتر از ۲۰۴۸ بتوان استفاده کرد و زمان رمزنگاری و رمزگشایی قابل قبولی داشت. اگر مخاطب پیام یک گروه از خودروها باشند، در اینصورت پیام قرار است یکبار رمز شود و چندبار رمزگشایی شود. علاوه بر این با دریافت پیام، خودروهای دیگر اقدام به فوروارد پیام به سایر خودروها می‌کنند که در این صورت زمان رمزگشایی توسط خودروها باید حتی‌المکان حداقل باشد. در اینصورت اگر طول پیام بیش از ۱۷۱۲ بیت (جدول ۴-۳) باشد، استفاده از روش ECIES مناسب‌تر است. بخصوص اینکه در این روش می‌توان سطح امنیتی بالاتری با افزایش بیشتر طول کلید داشت.

۴-۵-۳- مقایسه زمان اجرا در روشهای رمزنگاری متقارن

با توجه به مزایا و نقاط ضعف گفته شده در این روشها، در شبکه خودرویی معمولا طول عمر کلید مشترک خیلی کم است (معمولا از این روش برای ارتباطات اصلی با واحدهای کنار جاده یا واحد مرکزی استفاده می‌شود) و بنابراین امکان حمله و تحلیل برای یافتن مقدار کلید مشترک در اینگونه موارد، از بین می‌رود. به همین منظور همانطور که در شکل‌های (۴-۱۰) و (۴-۱۱) ملاحظه می‌شود، همه روشهای گفته شده را در مقایسه لحاظ کرده تا از نظر زمانی بهترین الگوریتم رمزنگاری متقارن را انتخاب نماییم.



شکل ۴-۱۰. مقایسه زمان رمزگشایی در روشهای مختلف رمز متقارن برحسب اندازه پیام و زمان رمزنگاری



شکل ۴-۱۱. مقایسه زمان رمزنگاری در روشهای مختلف رمز متقارن برحسب اندازه پیام و زمان رمزنگاری

پیامهای مبادله شده در این روش حداکثر ۲۰۰۰ بایت در نظر گرفته شده‌اند. علت استفاده از این داده این است که در شبکه خودرویی طول پیام‌های ایمنی که مبادله می‌شوند، بیشتر از این مقدار نخواهند شد. در این مقایسه از نظر رمزنگاری، روش Camellia بیشترین زمان اجرا را داراست و روش رمزنگاری Blowfish کمترین زمان اجرا را دارد. در رمزگشایی پیام، الگوریتم Seed معمولا بیشترین زمان اجرا را دارد و الگوریتم Camellia کمترین زمان اجرا را داراست. از طرفی، الگوریتم Blowfish که بهترین روش از نظر زمان اجرا در رمزنگاری پیام است، بعد از روش Camellia، بهترین انتخاب برای رمزگشایی است. بنابراین با توجه به زمان مناسب روش Blowfish در هر دو عمل رمزنگاری و رمزگشایی و همچنین ایمنی کافی روش در صورت انتخاب مناسب کلید، این روش برای رمزنگاری متقارن در شبکه خودرویی بهترین انتخاب است.

۴-۶- نتیجه‌گیری

با توجه به حساسیت زمان اجرا در کاربردهای شبکه خودرویی، باید در پیاده‌سازی مکانیزمهای رمزنگاری روشهایی انتخاب شوند که از نظر کارایی یا امنیت در سطح قابل قبولی باشند و زمان کمتری برای عملیات رمزنگاری و رمزگشایی مصرف نمایند. بنابراین در این فصل به بررسی برخی روشهای متداول و روشهای غیر متداول با کارکرد مناسب در رمزنگاری متقارن و همچنین روشهای پر استفاده و رایج در رمزنگاری نامتقارن پرداخته‌ایم. با پیاده‌سازی و مقایسه این روشها، روش Blowfish در رمزنگاری متقارن بهترین گزینه برای انتخاب است. در رمزنگاری نامتقارن، روش RSA در صورت کوتاه بودن پیام (کمتر یا مساوی ۲۰۴۸ بیت) بهترین انتخاب است چون در هر دو مورد رمزنگاری و رمزگشایی زمان کمتری مصرف می‌کند و امنیت خوبی دارد و روش ECIES در صورتی که طول پیام بزرگتر از ۲۰۴۸ بیت باشد، بهترین گزینه است؛ زیرا زمان رمزگشایی در الگوریتم RSA با زیادشدن طول پیام بشدت افزایش می‌یابد.

فصل ۵

بررسی آسیب در حمله سایبل

و

راه کار مقابله در شبکه خودرویی

۵-۱- مقدمه

حمله سایبل توسط دوسر [۲۶] در سال ۲۰۰۲ مطرح شده است. این حمله تهدیدی جدی در شبکه بین خودرویی است و حمله‌کننده شناسه‌های اضافی برای ارتباط با شبکه در نظر می‌گیرد. این شناسه‌های اضافی از دو طریق به حمله‌کننده اختصاص می‌یابد: ۱. خودروی بدخواه یک مجموعه شناسه جعلی را در محدوده شناسه‌های شبکه می‌سازد و ۲. خودروی بدخواه از شناسه سایر خودروهای موجود در شبکه به عنوان شناسه خود در پیام ارسالی، استفاده می‌کند. خودروی بدخواه از این شناسه‌ها به نفع خود استفاده کرده و با هریک از موجودیتهای خود وانمود می‌کند که چند خودروی متفاوت است. هدف او تغییر در نتیجه سیستم رأی‌گیری، ارسال رخدادهای هشداردهنده دلخواه و در نتیجه ایجاد ترافیک و احتمالا تصادف و کلا هر عملی است که به نفع حمله‌کننده است. در شبکه خودرویی باید پیامها به موقع تحویل داده شوند، مکانیابی خودروها دقیق باشد، یکپارچگی پیامها حفظ شود، خودروها تصدیق شوند و ویژگی عدم انکار برقرار باشد و همچنین حریم خصوصی رانندگان حفظ شود. به همین منظور، هرگونه مکانیزم امنیتی که برای شبکه خودرویی طراحی می‌شود باید این اطمینان را حاصل کند که اطلاعات بحرانی و رخدادهایی که به صورت پیام در شبکه مبادله می‌شوند، نمی‌توانند توسط حمله کننده تولید شده، ارسال مجدد شوند و یا تغییر داده شوند. حمله سایبل یکی از اختلالاتی است که توسط خودروی بدخواه جهت رسیدن به اهدافی خاص و یا افت کارایی شبکه صورت می‌گیرد. خودروی سایبل با ایجاد موجودیتهای اضافی قادر است پیامهای ساختگی در شبکه ارسال کند، مانع از ارسال پیام به خودروهای دیگر شود و یا اینکه در مسیریابی خلل ایجاد کند. به همین منظور در این فصل به بررسی این حمله و تاثیر منفی آن در افت کارایی شبکه در سه نمونه از پرکاربردترین الگوریتم‌های مسیریابی می‌پردازیم. سپس راه‌حل کارایی را در جهت رفع این حمله در کاربردهای عملی پیشنهاد می‌دهیم.

۵-۲- بررسی آسیب در حمله سایبل

۵-۲-۱- معرفی حمله

برای شناخت بهتر این حمله و بررسی تاثیر آن در شبکه خودرویی، این حمله را با توجه به طریقه ساخت موجودیتهای سایبل توسط خودروی بدخواه، نحوه ارتباط و همچنین مشارکت موجودیتهای سایبل دسته‌بندی می‌کنیم [۶۹]. بنابراین به سه روش می‌توان حملات سایبل را دسته بندی کرد:

۱. **ارتباط مستقیم یا غیر مستقیم:** ارتباط با موجودیتهای سایبل (ارسال یا دریافت پیام) می‌تواند مستقیم یا غیر مستقیم باشد. در ارتباط مستقیم، موجودیتهای سایبل ایجاد شده توسط خودروی بدخواه با خودروهای قانونی مستقیما ارتباط دارند. در ارتباط غیر مستقیم، ارتباط خودروهای قانونی از طریق خودروهای بدخواه به موجودیتهای سایبل آن هدایت می‌شوند (مثلا در مسیریابی، خودروی بدخواه پس از دریافت بسته پیام، برای معرفی نزدیکترین خودرو به خودروی هدف که بسته مسیریابی را تحویل دهد، یکی از موجودیتهای سایبل خود را معرفی می‌کند).

۲. **شناسه موجودیتهای سایبل:** خودروی بدخواه برای تخصیص شناسه به موجودیتهای سایبل خود از شناسه‌های ساختگی در دامنه معین شده استفاده می‌کند یا اینکه شناسه سایر خودروها را از طریق استراق سمع پیامهای مبادلاتی که در شبکه پخش می‌شوند دریافت کرده و به آنها تخصیص می‌دهد.

۳. **نحوه شرکت دادن موجودیتهای سایبل در حمله سایبل:** موجودیتهای سایبل می‌توانند همزمان در حمله شرکت کنند یا اینکه حمله‌کننده می‌تواند آنها را یکی‌یکی حاضر کند. تعداد شناسه‌های استفاده شده توسط حمله‌کننده کمتر یا مساوی تعداد موجودیتهای فیزیکی در شبکه است.

دو آسیب مهمی که توسط موجودیت سایبل می‌تواند صورت بگیرد عبارتند از:

- **اختلال در مسیریابی:** دو مکانیزم مسیریابی آسیب‌پذیر به حمله سایبل مسیریابی چندگانه[1] و مسیریابی جغرافیایی هستند. علاوه براین حمله سایبل می‌تواند مکانیزم انتخاب سرگروه را در پروتکلهای مختلف مسیریابی مبتنی بر کلاستر مختل کند [۷۰]. در مسیریابی چندگانه، یک مجموعه از مسیرهایی که جدا به نظر می‌رسند ممکن است به موجودیتهای سایبلی ختم شوند که برای یک خودروی بدخواه است. در مسیریابی جغرافیایی، خودروهای بدخواه می‌توانند (با داشتن هویتهای مختلف) همزمان در بیش از یک مکان حاضر شوند [۷۱].
- **سیستمهای مبتنی بر رأی‌گیری:** مکانیزم رأی‌گیری برای جمع‌آوری و یا تایید برخی اطلاعات مهم برای خیلی از کاربردها در شبکه خودرویی مهم است. موجودیتهای سایبل می‌توانند نتیجه رأی را به نفع خودروی بدخواه و یا برای اخلال در شبکه تغییر دهند. شناسایی و گزارش سوءرفتار یک خودرو، تایید موقعیت خودرو، تایید یک رخداد خاص (مثل ترافیک یا وضعیت آب و هوا) که نیاز است توسط چند خودرو در شبکه گزارش شوند تا مورد تایید قرار بگیرد و کلا هر کاربردی که از اطلاعات چند خودرو استفاده می‌کند، نمونه‌هایی از کاربردهای سیستم رأی‌گیری هستند.
- **ارسال پیامهای ساختگی یا تغییر و بروز رسانی پیامهای دریافتی**: اینکار برای اخلال در ترافیک، ایجاد تراکم، باز کردن راه برای عبور خود و ایجاد تصادف توسط خودروی بدخواه و موجودیتهای سایبل در شبکه است.

۵-۲-۲- شبیه‌سازی حمله

یکی از آسیب‌های این حمله، همانطور که اشاره شد، اختلال در مسیریابی است. اینکار با فوروارد نکردن بسته حاوی پیام هشدار برای خودروهای دیگر و یا عدم فوروارد بسته‌ای است که بسوی یک خودروی خاص مسیریابی می‌شود. در این بخش، این اختلال را بر روی سه پروتکل مسیریابی خاص که در

[1] . Multi-path

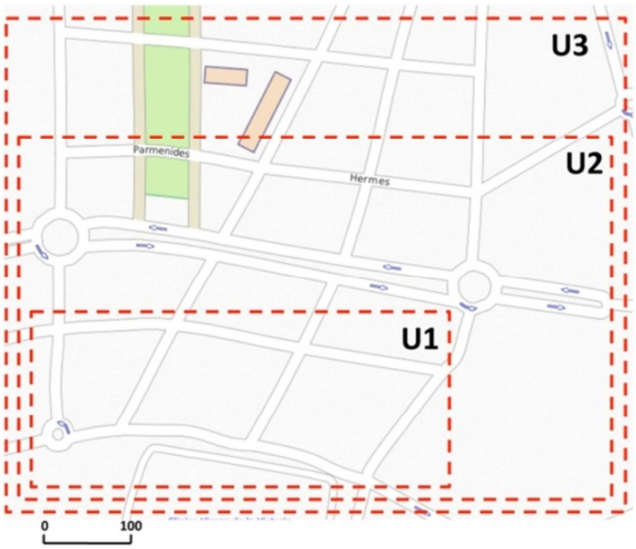
شبکه‌های سیار پرکاربرد هستند و طبق بررسی‌های انجام شده در بین پژوهش‌های مختلف، [۷۲-۷۴] ، کارایی و عملکرد بهتری نسبت به بقیه دارند، بررسی کرده‌ایم. برای این منظور به دلیل کاربرد زیاد و کارکرد مناسب شبیه‌ساز NS۲[۱]، از این شبیه‌ساز برای شبیه‌سازی‌های خود استفاده کرده‌ایم. پارامترهای شبیه‌سازی را در اینکار به صورت جدول (۵-۱) تنظیم کرده‌ایم.

جدول ۵-۱. پارامترهای شبیه‌سازی حمله سایبل

پارامتر	مقدار
نوع ترافیک	CBR[۲]
مدل اتلاف مسیر[۳]	Two ray ground
منطقه شبیه‌سازی	نقشه مالاگا - اسپانیا
اندازه ناحیه	۱۲۰۰ × ۱۲۰۰ متر مربع
تعداد خودروها	۲۰، ۳۰ و ۴۰
سرعت خودروها	بین ۱۰ تا ۵۰ km/h
الگوریتمهای مسیریابی	AODV[۴] ، DSR[۵] و OLSR[۶]
سایز بسته	۵۱۲ بایت
تعداد موجودیتهای سایبل	۴
زمان شبیه‌سازی	۱۸۰ ثانیه

منطقه انتخابی نقشه واقعی منطقه‌ای از مالاگا، واقع در اسپانیا است که به صورت منطقه U۲ در شکل (۵-۱) نشان داده شده است.

۱. Network Simulator ۲
۲. Constant Bit Rate
۳. Path loss model
۴. Ad-hoc On-demand Distance Vector
۵. Dynamic Source Routing
۶. Optimized Link State Routing

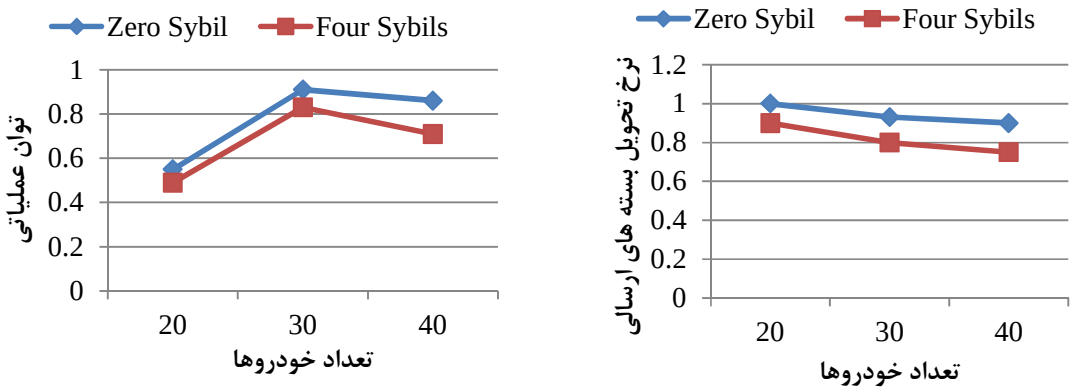


شکل ۵-۱. منطقه شبیه‌سازی شده U۲ واقع در شهر مالاگا، کشور اسپانیا

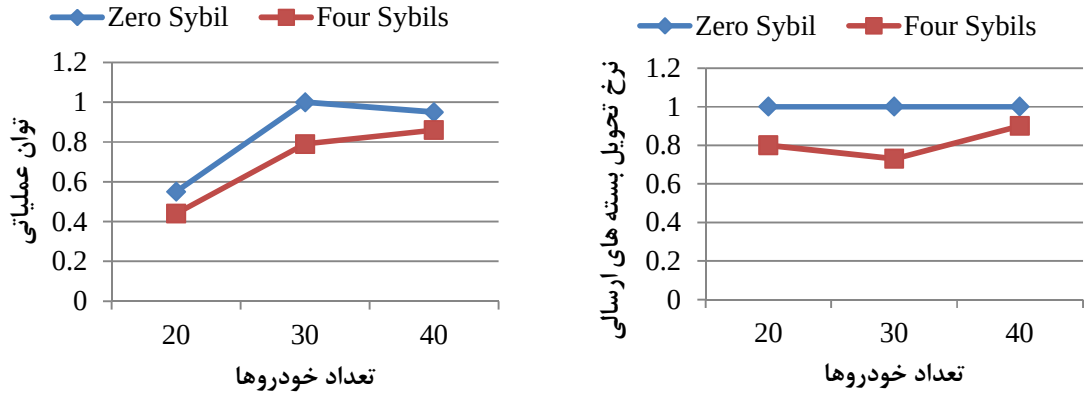
برای این منظور موجودیت سایبل را به هر سه پروتکل مسیریابی اضافه کرده و اختلالی که در شبکه ایجاد می‌کنند را دریافت بسته‌های داده (بسته‌های کنترلی و یا بسته‌های درخواست و پاسخ مسیریابی بدون مشکل منتقل می‌شوند) و عدم تحویل به نود بعدی در شبکه تعریف کرده‌ایم [۶۹]. این بررسی را در سه نمونه با تعداد خودروی ۲۰، ۳۰ و ۴۰، با ۴ موجودیت تعریف شده سایبل در شبکه، در مدت ۱۸۰ ثانیه شبیه‌سازی کرده‌ایم. تحرک خودروها در این مدل برگرفته از نرم‌افزار شبیه‌ساز ترافیک SUMO است. خروجی این شبیه‌ساز فایل ردگیری حرکت خودروها است که توسط نرم‌افزار NS۲ قابل استفاده می‌باشد. مزیت استفاده از نرم‌افزارهای شبیه‌ساز ترافیکی مثل SUMO، این است که می‌توانند از محیط-های حرکت واقعی در شبکه خودرویی، با انتخاب مناطق واقعی کشورها از نقشه‌های دیجیتال رایگان (OpenStreetMap[۱])، استفاده کنند و جهت جاده، چراغها و علائم راهنمایی را تولید نمایند. کارایی شبکه را با دو پارامتر بررسی کرده‌ایم: ۱. نرخ بسته‌هایی که تحویل داده می‌شوند که برابر است با تعداد بسته‌های دریافت شده به تعداد ارسال شده، این پارامتر تحت عنوان PDF[۲] در شبکه‌های سیار معرفی شده است و

۱. http://www.openstreetmap.org/
۲. Packet Delivery Factor

۲. توان عملیاتی[۱] که برابر است با تعداد بیت‌های انتقال داده شده به طول مدت زمان شبیه‌سازی (با واحد kbps). در زیر نتایج این بررسی را مشاهده می‌کنیم. در این شبیه‌سازی هر دو پارامتر را از داده‌های حاصل از شبیه‌سازی، در فایل ردیابی[۲] با اسکریپت‌نویسی awk بدست آوردیم.

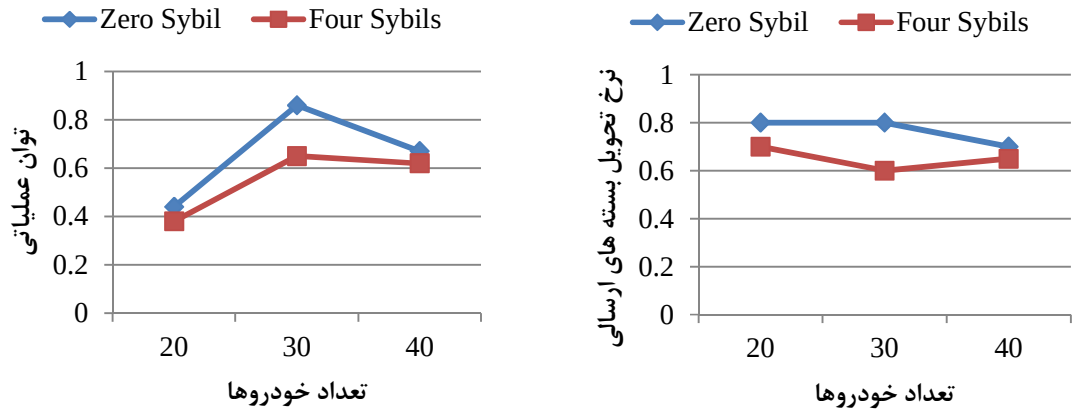


شکل ۵-۲. میزان توان عملیاتی و نرخ تحویل بسته‌ها در پروتکل مسیریابی AODV، با توجه به تعداد خودروهای مختلف و وجود ۴ نود سایبل در شبکه



شکل ۵-۳. میزان توان عملیاتی و نرخ تحویل بسته‌ها در پروتکل مسیریابی DSR، با توجه به تعداد خودروهای مختلف و وجود ۴ نود سایبل در شبکه

۱. Throughput
۲. Trace file



شکل ۵-۴. میزان توان عملیاتی و نرخ تحویل بسته‌ها در پروتکل مسیریابی OLSR، با توجه به تعداد خودروهای مختلف و وجود ۴ نود سایبل در شبکه

توان عملیاتی و نرخ تحویل بسته‌ها دو پارامتری هستند که نشانگر میزان انتقال بسته‌ها در لایه انتقال هستند. تعداد بیتهای داده منتقل شده در طول دوره انتقال بسته داده (بازه‌ی زمانی در این دوره کوچکتر یا مساوی با زمان شبیه‌سازی است) بیانگر پارامتر توان عملیاتی است. در مورد توان عملیاتی، تنها بسته-های داده لحاظ شده‌اند و بسته‌های کنترلی در نظر گرفته نمی‌شوند. نرخ تحویل بسته‌ها، کلیه بسته‌های تحویل داده شده (بسته داده و کنترلی) به تعداد ارسال شده را نشان می‌دهد. در شبیه‌سازی‌های انجام شده، همانطور که انتظار می‌رود، در حالتی که موجودیت سایبل در شبکه وجود نداشته باشد، این دو پارامتر برای همه پروتکلهای مسیریابی مقدار بیشتری دارند و با در نظرگرفتن موجودیتهای سایبل، این مقدار بسته به پروتکل شبیه‌سازی طبق شکل‌های (۵-۲) تا (۵-۴) تغییر می‌کند. همانطور که در این شکلها ملاحظه می‌شود، پروتکل‌های مسیریابی AODV و DSR کارایی بهتری نسبت به پروتکل OLSR در نرخ تحویل بسته‌ها و توان عملیاتی دارند و پروتکل AODV کمتر تحت تاثیر این حمله قرار گرفته است.

۵-۳- روشهای مختلف مبارزه با حمله سایبل و انتخاب بهترین

۵-۳-۱- انتخاب روش مناسب برای شناسایی حمله

شناسایی حمله سایبل همانطور که در کارهای بررسی شده در فصل ۲ اشاره گردید، به سه دسته روشهای تست منبع، روشهای مبتنی بر رمزنگاری و احراز هویت و روشهای مبتنی بر مکان یابی تقسیم می‌شوند. انتخاب روش مناسب برای پیاده‌سازی، بستگی به هزینه‌های اختصاص یافته، سیاستهای هر کشور و خصوصیات متدهای موجود در هر دسته دارد. اینکه به طور قاطع بتوان گفت کدام روش بهتر است، امکان‌پذیر نیست. در واقع روشی مناسب است که بسته به نیاز، خصوصیات زیر را برآورده نماید:

۱. نرخ شناسایی بالایی داشته باشد و با شناسایی به موقع، منجر به عدم آسیب شبکه شود.
۲. زمان شناسایی موجودیتهای سایبل فاکتور مهمی است که به دلیل تحرک‌پذیری بالای خودروها و نیاز به زمان پاسخ کوتاه، باید تا حد ممکن مینیمم باشد.
۳. حریم خصوصی رانندگان را حفظ نماید.
۴. نیاز به سخت‌افزار اضافی، بالاخص برای هدف شناسایی این حمله نداشته باشد.
۵. حتی‌الامکان پیامهای مبادلاتی را در شبکه افزایش ندهد.
۶. مقیاس‌پذیری لازم را داشته باشد و امکان شناسایی برای تعداد خودروهای موجود در ناحیه خاص وجود داشته باشد.

انتخاب روشی مناسب که همه این ویژگیها را دارا باشد، امری دشوار است و بنابراین روشی انتخاب می‌شود که با سبک و سنگین کردن ویژگیهای موجود فاکتورهای کلیدی خاص را داشته باشد. شناسایی حمله با روش تست منبع برای پیاده‌سازی پیشنهاد نمی‌شود؛ چون این روش هم دقت مناسبی ندارد و هم پیاده‌سازی آن در شبکه خودرویی چندان کارا و مناسب نیست.

روشهای مبتنی بر مکانیابی اکثرا ساده هستند، پیچیدگی محاسباتی چندانی ندارند، معمولا نحوه شناسایی آنها توزیع شده است و بنابراین مقیاس‌پذیری بالایی دارند و برخی از این روشها که دقت و نرخ شناسایی بالایی دارند برای هدف تایید موقعیت ارسالی توسط خودرو نیز مناسب هستند. اما در این روشها، واحدهای کنار جاده کاملا مورد اعتماد فرض شده‌اند و معمولا حریم خصوصی خودروها در شبکه نقض می‌شود. علت نقض حریم خصوصی اینست که در این روشها یا اطلاعات مکانی خودروها در شبکه توزیع می‌شوند و یا اینکه میزان فاصله هر خودرو تا خودروهای همسایه بدست آمده و برای شناسایی حمله توسط سایر خودروها، در شبکه ارسال می‌گردند. علاوه بر این در این روش، پردازش توزیع شده توسط خودروها منجر به ایجاد سربار در مبادله پیام و افزایش تعداد مبادلات پیام در شبکه می‌شود.

متدهای مبتنی بر رمزنگاری و تصدیق پیام نیاز به زیرساختی جهت توزیع کلید، ارسال گواهینامه و فسخ آن دارند. زیرساخت در این حیطه به معنای نظارت، اعتبارسنجی و بررسی واحدها توسط یک واحد مرکزی است. این زیرساخت علاوه بر کاربرد در شناسایی حمله سایبل، برای خیلی از کاربردها مثل مبادله ایمن پیام، ارتباطات گروهی خودروها و حفظ حریم خصوصی رانندگان کاربرد دارد. گرچه روشهای مبتنی بر تصدیق و رمزنگاری پیچیدگی بیشتری دارند و معمولا مقیاس‌پذیری کمتری نسبت به روشهای ساده‌تر در دسته روشهای مبتنی بر مکانیابی دارند، اما دقت شناسایی بالا، حفظ حریم خصوصی رانندگان، جلوگیری از دستکاری پیام، عدم انکار پیام توسط فرستنده و تبادل ایمن پیامهای حاوی اطلاعات شخصی مثل مکان و شناسه خودروها، ویژگیهای مثبت این روش‌ها هستند.

۵-۳-۲- پروتکل تحت بررسی و بهبود

پروتکل تحت بررسی تحت عنوان گواهینامه آنی[۱] در [۳۶] مطرح شده است. ویژگیها و دلایل پیشنهاد این روش در [۳۶] بررسی شده است. اما در این پایان نامه به دو دلیل اصلی این پروتکل را انتخاب کردیم:

[۱] . Temporary

۱. شناسایی صد در صد حمله سایبل که با توجه به کارهای انجام شده در این زمینه، تاکنون در موارد کمی شناسایی این حمله با نرخ صد در صد گزارش شده است.

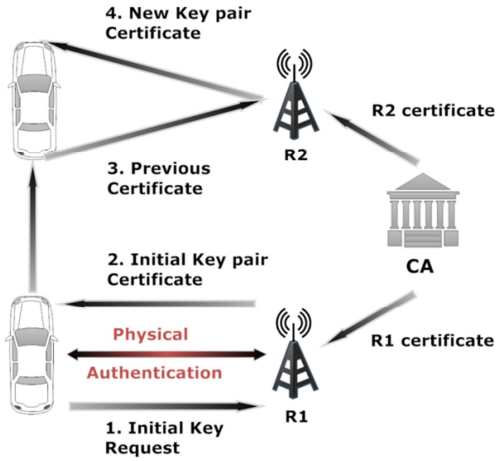
۲. عدم نیاز به پردازش مرکزی برای تصدیق و شناسایی حمله. زیرا پروتکل بررسی شده در [۳۷] که در فصل ۲ بررسی شد، نرخ شناسایی صد در صد دارد اما به دلیل اینکه اولا نیاز به ثبت نام اولیه خودروها در واحد مرکزی است و ثانیا در موارد مشکوک به حمله، بخشی از پردازش باید در واحد مرکزی انجام شود، روش مناسبی برای پیاده‌سازی عملی برای ارتباطات خودرویی نیست و سربار زیادی برای واحد مرکزی دارد.

در دیدگاه انتخابی، هر واحد کنار جاده جفت کلید موقت و گواهینامه‌ای را برای هر خودرو صادر می-کند که تنها برای یک منطقه محلی ویژه، تحت پوشش همان واحد کنار جاده، برای یک زمان محدود، قابل استفاده است. در این پروتکل، دریافت اولین گواهینامه به منزله تصدیق فیزیکی خودرو است که تصدیق خودرو برای مراحل بعدی با توجه به این تصدیق اولیه صورت می‌گیرد. بنابراین باید از راهی مطمئن این تصدیق انجام پذیرد. برای این منظور در [۳۶] شیوه‌های مختلفی چون استفاده از دوربین یا استخراج ویژگیهای خودروها مثل رنگ، نوع خودرو، لاین عبوری خودرو و غیره پیشنهاد شده که این ویژگیها خودرو را در بین مجموعه خودروها بصورت یکه شناسایی می‌نماید. مسئله مهمی که وجود دارد این است که در ایران تعداد خودروهای از یک نوع مثل پراید و از یک رنگ در بین مجموعه خودروها خیلی زیاد است. بنابراین برای تصدیق فیزیکی اولیه که نیاز به یک روش دقیق داریم، روش انتخاب ویژگی روش مناسبی نیست و استفاده از دوربین‌ها به دو دلیل مناسب‌تر هستند:

۱. استفاده از دوربین‌ها در حال حاضر در جاده‌های پرخطر به منظور کنترل سرعت و شناسایی خودروهای متخلف، از راه شناسایی پلاک، متداول است.

۲. دقت بالا و زمان پردازش مناسبی برای شناسایی پلاک خودروها دارند. به عنوان نمونه روشی که در [۷۵] برای شناسایی پلاک خودروها پیشنهاد شده است، برای فاصله‌های مختلف هدف تا دوربین به طور اتوماتیک تنظیم می‌شود و شرایط انعکاس نور را در نظر گرفته است. این روش دقتی برابر با ۹۴٪ و زمانی معادل با ۴.۵ میلی ثانیه دارد که برای این منظور مناسب به نظر می‌رسد. روشهای مختلف شناسایی پلاک به صورت آکادمیک یا کاربردی برای شناسایی پلاک خودروها، در [۷۶] بررسی شده‌اند که حداکثر دقت آنها در یک مورد، در [۷۶] ۹۸.۸۲٪ گزارش شده که زمان شناسایی آن گزارش نشده است.

بنابراین برای بدست آوردن اولین گواهینامه و تصدیق فیزیکی، هر خودرو باید یک واحد کنار جاده مجهز به دوربین را ملاقات نماید. همانطور که در [۳۶] پیشنهاد شده است، برای کاهش هزینه بهتر است که تنها بخشی از واحدهای کنار جاده مجهز به دوربین باشند. اما برای اینکه همه خودروها بتوانند اولین گواهینامه خود را به موقع دریافت کنند، پیشنهاد می‌کنیم واحدهای مجهز به دوربین در ورودیهای هر شهر و مکانهای پرتردد مثل پمپ بنزین‌ها تعبیه شود. پس از تصدیق فیزیکی اولیه و دریافت اولین کلید و گواهینامه موقت توسط خودرو، از واحد کنار جاده مجهز به دوربین، خودرو جفت کلید و گواهینامه خود را با عبور از واحدهای کنار جاده بعدی بروز کرده و به صورت یک گواهینامه زنجیر شده جدید در می‌آورد. در این پروتکل، گواهی‌نامه دریافت شده از واحد کنار جاده جاری به مقدار درهم شده گواهینامه‌های قبلی به صورت یک زنجیره پیوند می‌خورد و گواهینامه موقت جدید را می‌سازد. هر خودرو تنها از یک گواهینامه موقت برای یک بازه مکانی واحد می‌تواند استفاده کند و منحصر به فرد بودن گواهینامه و تصدیق فیزیکی اولیه، از حمله سایبل جلوگیری می‌کند. شکل (۵-۵) روال کلی این پروتکل را به طور کامل نشان می‌دهد.



شکل ۵-۵. دیدگاه مبتنی بر گواهینامه آنی [۳۶]

در [۳۶]، پروتکل گواهینامه آنی، تنها به عنوان یک مدل شناسایی در کنار روش اصلی مطرح شده در مقاله، یعنی دیدگاه مبتنی بر گواهینامه سری زمانی[۱] مطرح شده است. در این پایان‌نامه این مدل را به طور دقیق‌تر و با رفع نقایص آن، بررسی کرده و پیاده‌سازی می‌کنیم چون برای کاربرد عملی آن حتما نیاز به پیاده‌سازی و بررسی معایب آن داریم. در واقع این پروتکل با وجود عملکرد منطقی و شناسایی ۱۰۰٪ حمله سایبل، به دلیل نیاز به رمزنگاری کلید عمومی و همچنین شناسایی اولیه خودروها به صورت فیزیکی، منطقا زمان زیادی مصرف می‌کند. پس مهمترین فاکتوری که ممکن است آن را برای پیاده‌سازی عملی در جاده‌ها منسوخ نماید، زمان پردازش یا بار تحمیلی به واحد کنار جاده است. چون افزایش زمان صدور و یا تایید گواهینامه برای یک خودرو، مقیاس‌پذیری را در شبکه کاهش می‌دهد. بنابراین، هر مدلی که در این زمینه مطرح می‌شود، علاوه بر شناسایی حمله با نرخ بالا، دو نیاز مهم را باید در نظر بگیرد؛ یک نیاز حفظ حریم خصوصی خودروها است و نیاز دیگر امکان پیاده‌سازی عملی روش می‌باشد. بنابراین ما در این بخش برآنیم مقیاس‌پذیری این پروتکل را بررسی کرده و راهکارهایی برای افزایش ایمنی در حفظ حریم خصوصی خودروها ارائه دهیم. بهمین منظور این پروتکل را کامل و امکان‌سنجی کرده‌ایم.

[۱]. Timestamp

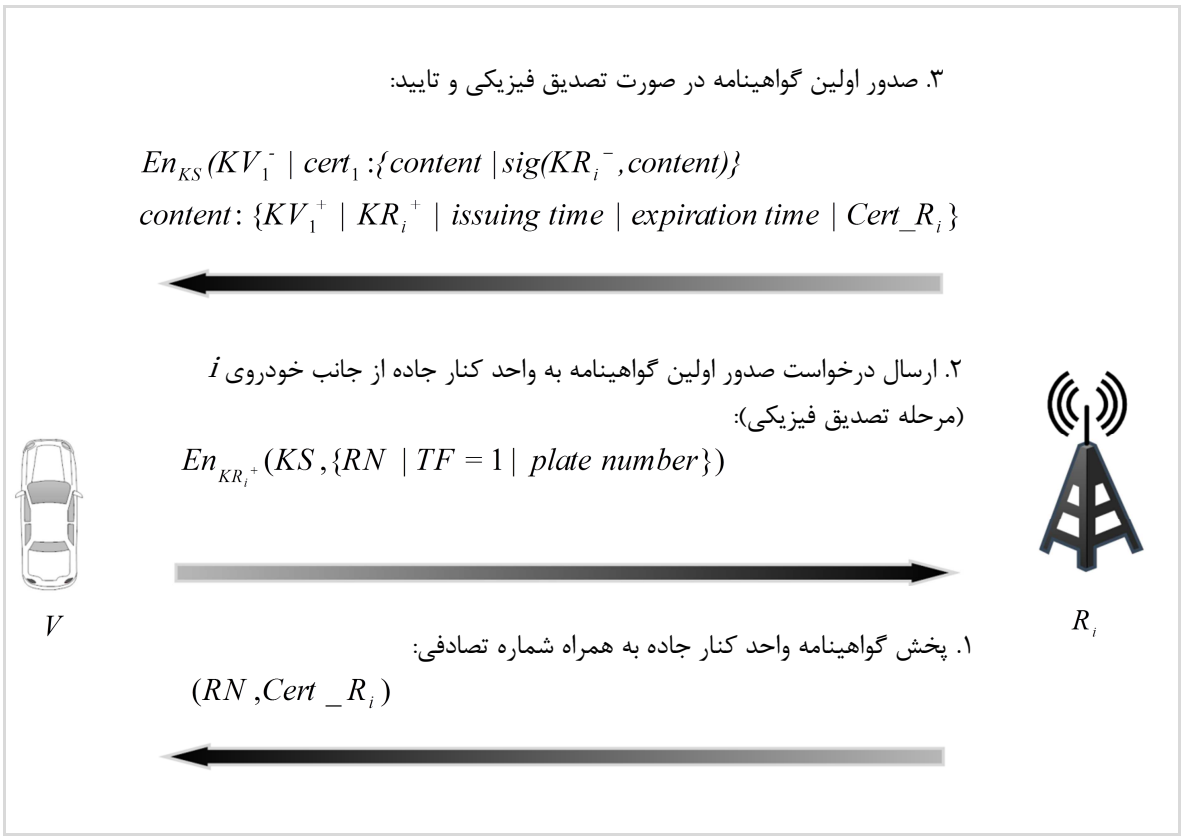
۵-۳-۲-۱- مدل اصلاح شده گواهی‌نامه آنی

در ابتدا برای پیاده‌سازی پروتکل گواهینامه آنی در [۳۶] مواردی را در این روش اصلاح کردیم. پارامترهای اضافی آن را حذف و برای کارکرد صحیح و امکان تایید گواهینامه هر خودرو توسط سایر خودروها، گواهینامه کلید عمومی واحد کنار جاده را به گواهینامه صادر شده برای هر خودرو افزودیم. قبل از بیان نحوه کارکرد روش، ابتدا پارامترهای پروتکل اصلاح شده در جدول (۵-۲) بیان شده‌اند.

جدول ۵-۲. پارامترهای پروتکل اصلاح شده

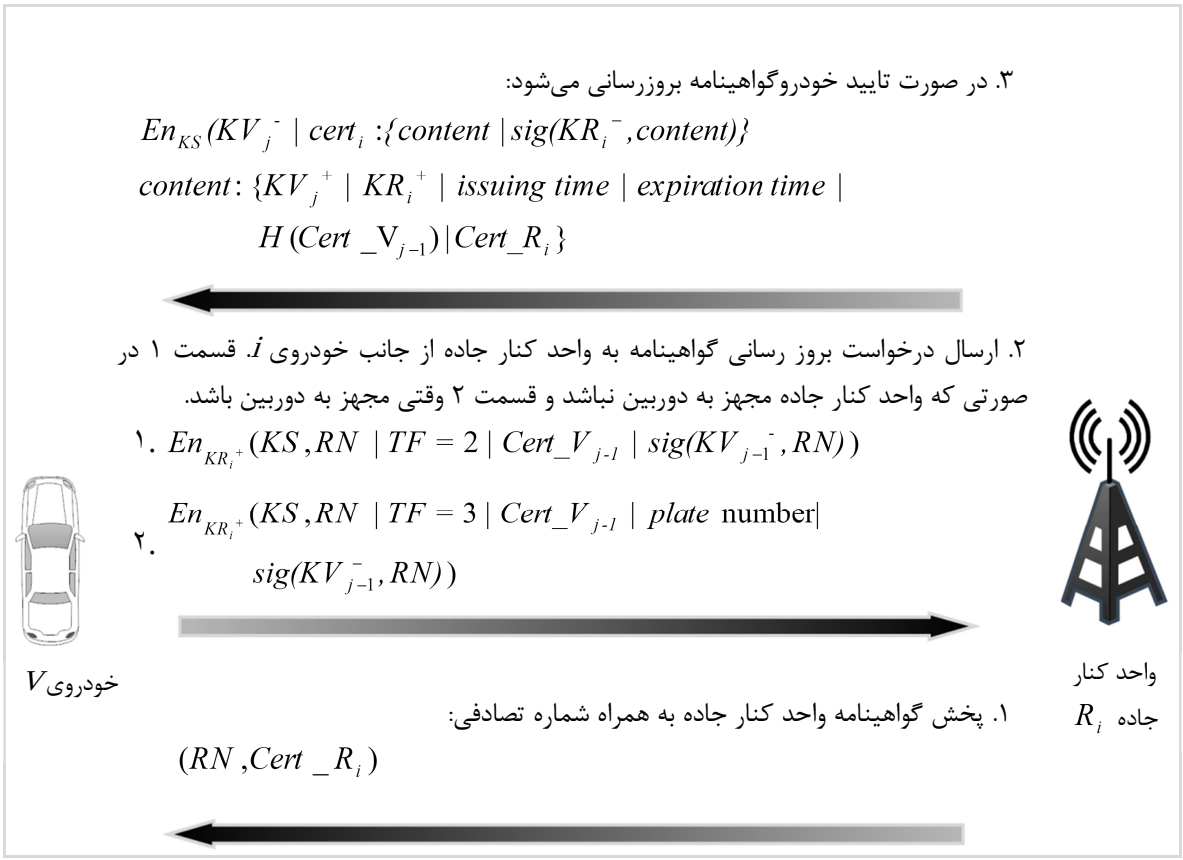
پارامتر	تعریف
KR_i^+, KR_i^-	کلید عمومی وکلید خصوصی واحد کنار جاده iام
KV_j^+, KV_j^-	کلید عمومی وکلید خصوصی خودروی V در ارتباط با jامین واحد کنار جاده
KS	کلید مشترک برای رمزنگاری متقارن
$H(\ )$	تابع درهم‌ساز یک‌طرفه
$sig(\mathrm{K}, \mathrm{M})$	امضای پیام M با کلید خصوصی K
$Cert\_R_i$	گواهینامه i امین واحد کنار جاده که قبلا از طرف واحد مرکزی صادر و امضا شده است.
$Cert\_\mathrm{V}_j$	گواهینامه خودروی V دریافت شده از jامین واحد کنار جاده‌ای که از آن عبور می‌کند، که با درخواست خودرو صادر و امضا می‌شود.
$En_{KR_i^+}$	رمزنگاری نامتقارن با کلید عمومی واحد کنار جاده
En_{KS}	رمزنگاری متقارن با کلید مشترک KS توافق شده بین خودرو و واحد کنار جاده
RN	شماره تصادفی تولید شده از جانب واحد کنار جاده به منظور عدم ارسال مجدد همان درخواست توسط خودرو
TF	پرچم نوع که مشخص کننده نوع پیام است. (۰: درخواست صدور اولین گواهینامه از واحد کنار جاده مجهز به دوربین، ۱: درخواست بروزرسانی گواهینامه از واحد مجهز به دوربین و ۳: درخواست بروز رسانی از واحد غیر مجهز به دوربین)

پروتکل اصلاح شده به ترتیب برای صدور اولین گواهینامه موقت و بروز رسانی گواهینامه در شکل (۵-۶) و (۵-۷) نشان داده شده است.



شکل ۵-۶. تصدیق اولیه و صدور اولین گواهینامه توسط واحد کنار جاده R_i برای خودروی V

در صدور اولین گواهینامه، خودرو با ملاقات با اولین واحد کنار جاده، گواهینامه آن و یک عدد تصادفی را دریافت می‌کند. گواهینامه واحد کنار جاده توسط یک واحد مرکزی شناخته شده برای کل خودروهای جاده صادر شده است و شماره تصادفی برای جلوگیری از ارسال مجدد پیام مرحله ۲ به واحد کنار جاده است. در گام دوم، واحد کنار جاده پیام رمزشده خودرو را که شامل شماره پلاک، نوع پیام ($TF=1$ مشخص کننده اولین درخواست خودرو برای تصدیق اولیه است) و یک کلید مشترک که برای رمزنگاری متقارن در گام ۳ است را دریافت کرده و در گام ۳ جفت کلید موقت و گواهینامه آن را برای خودرو ارسال می‌کند. بروزرسانی گواهینامه در شکل (۵-۷) نشان داده شده است.



شکل ۵-۷. بروزرسانی گواهینامه توسط واحد کنار جاده R_i برای خودروی V

در این پروتکل، در مرحله دوم یک کلید مشترک برای رمزنگاری متقارن (رمزنگاری با سربار کم) همراه با ارسال گواهینامه، توسط خودرو به واحد کنار جاده فرستاده می‌شود. هدف از این کار اینست که واحد کنار جاده کلید خصوصی و گواهینامه خودرو را با سرباری کمتر (با همان درجه امنیت) برای خودرو ارسال کند. در واقع در این روش از یکی از کاربردهای کلید عمومی که در فصل قبل اشاره گردید، یعنی مبادله کلید مشترک استفاده شد تا پیامها در زمان کمتری مبادله شوند. گواهینامه تولید شده از طرف واحد کنار جاده در مرحله ۳، حاوی مقدار درهم شده گواهینامه قبلی است. بدین ترتیب وقتی پیامی از جانب خودرو همراه با ارسال گواهینامه آن در شبکه پخش می‌شود، امکان شناسایی حمله سایبل با مقایسه و بررسی شباهت دو گواهینامه و مقدار درهم شده گواهینامه‌های قبلی فراهم می‌شود. در این مرحله مقدار گواهینامه واحد کنار جاده، در گواهینامه ارسال شده برای خودرو، برای اثبات هویت واقعی

واحد کنار جاده‌ای که این گواهینامه را صادر کرده (در مبادله پیام و ارتباط با سایر خودروها) بکار گرفته خواهد شد. هر گواهینامه دارای زمان شروع و انقضا است که بعد از آن این گواهینامه اعتبار نخواهد داشت و باید توسط واحد کنار جاده بعدی بروزرسانی شود تا بدین ترتیب با مجبور شدن خودرو به تعویض گواهینامه، خودرو قابل ردگیری نبوده و حریم خصوصی خودرو حفظ شود.

خیلی از کاربردها متکی بر اطلاعات دوره‌ای هستند که توسط خودروها در شبکه پخش می‌شوند. به عنوان مثال اطلاعات مکان خودروها می‌توانند برای آشکارسازی و اجتناب از برخورد و مسیریابی جغرافیایی پیام به منظور انتشار پیامهای هشدار استفاده گردد. علاوه بر این، این اطلاعات برای ردگیری حدود تقریبی خودرو در شبکه قابل استفاده است. بنابراین نقض حریم خصوصی در این شبکه ممکن است مانع از گسترش و استفاده همه جانبه از این تکنولوژی بشود. این جفت کلید برای خودرو نقش شبه شناسه[۱] دارد که استفاده مدام از یک شناسه، برای خودرو خطر ردگیری را دارد. یک راه‌حل برای این مشکل تغییر پی‌درپی شبه‌شناسه‌ها در ارسال پیامهای گوناگون در شبکه است که بعنوان راه‌حل اولیه برای حفظ حریم خصوصی پیشنهاد می‌شود [۷۷]. پژوهشهای زیادی بر روی حفظ حریم خصوصی و نحوه تغییر شبه‌شناسه‌ها انجام شده است. نحوه تغییر شبه‌شناسه‌ها در شبکه نحوی باید باشد که خودروی بدخواه قادر نباشد بفهمد خودروی مورد نظر چه زمانی شبه‌شناسه خود را تغییر می‌دهد. اگر برای خودروی بدخواه زمان تغییر شبه‌شناسه مشخص باشد قادر به ردگیری خودرو خواهد بود. برای همین منظور شاید منطقی‌ترین راه‌حلی که به نظر می‌رسد، تغییر شبه‌شناسه‌ها در نواحی شلوغ و یا نواحی است که خودروها در آن مناطق هرگونه ارسال و دریافت پیام را متوقف کرده و فقط می‌توانند شناسه خود را عوض کنند. در این شرایط، بدلیل اینکه همه خودروها تغییر شناسه می‌دهند خودروی مورد نظر حمله کننده (خودرویی که توسط حمله‌کننده در حال ردگیری است)، در میان خودروها گم شده و دیگر قابل

---

۱. pseudonym

ردگیری نخواهد بود. این نواحی را منطقه مخلوط[1] می‌نامند. این روش کارایی مناسبی در حفظ حریم خصوصی دارد [۷۹,۷۸]. در واقع این امر باعث می‌شود که خودرویی که در حال شنود پیامهای شبکه است، به خصوص پیامهای دوره‌ای که توسط خودروها در شبکه مبادله می‌شوند، نتواند خودرو را ردگیری کند. بهمین منظور پیشنهاد می‌شود که در دیدگاه مبتنی بر گواهینامه آنی طول دوره اعتبار گواهینامه‌ها به نحوی تعریف گردد که شناسه خودروها یا بعبارتی جفت کلید موقت در نواحی خاصی مثل تقاطع‌ها تعویض گردد که امکان شناسایی خودروها از بین برود.

۵-۳-۲-۲- فرضیات پیاده‌سازی

فرضیات پیاده‌سازی مدل اصلاح شده در جدول (۵-۳) بیان شده است.

جدول ۵-۳. فرضیات پیاده‌سازی برای مدل مقابله با حمله سایبل

پارامتر	مقدار
تعداد خودروهای بررسی شده	۱۰
سرعت خودرو	۱۰۰km/h
الگوریتم رمز نامتقارن	ECIES با کلید ۱۶۰ بیت
الگوریتم امضای دیجیتال	ECDSA با کلید ۱۶۰ بیت
الگوریتم رمز متقارن	Blowfish با کلید ۱۲۸ بیت
روش درهم‌سازی	SHA۱
حداکثر طول پیام داده	۶۸۷ بایت

تمام درخواستهای تصدیق فیزیکی اولیه با ارتباط واحدها با هم، چک می‌شوند. اگر قبلا خودرو درخواست گواهینامه اولیه داشته است و پلاک آن ثبت شده باشد یعنی گواهینامه دریافت کرده باشد، گواهینامه اولیه مجدد برایش صادر نمی‌شود. در غیر اینصورت امکان دریافت مجدد گواهینامه وجود دارد. بنابراین باید واحدهای کنار جاده با هم ارتباط داشته باشند.

[1] . Mix zone

هر خودرودر مواجهه با واحد کنار جاده مجهز به دوربین، باید شماره پلاکش را ارائه دهد تا از دوبار درخواست جلوگیری شود.

وجود گواهینامه‌های درهم شده که توسط واحدهای کنار جاده قبلی صادر شده‌اند، از ارسال مجدد درخواست جلوگیری می‌کنند. هرگاه یکی از این مقادیر در دو درخواست یکسان باشند، یعنی توسط یک خودرو صادر شده‌اند و این موضوع از حمله سایبل پیشگیری می‌کند.

هرگاه خودرو در رنج بیش از یک واحد کنار جاده باشد، بهتر است از نزدیکترین واحد کنار جاده درخواست گواهینامه کند. در این شرایط می‌تواند از هر دو واحد کنار جاده هم گواهینامه درخواست کند که البته در واحدهای کنار جاده بعدی به دلیل شباهت در مقدار درهم شده گواهینامه‌های قبلی، شناسایی خواهد شد.

نتایج حاصل از پیاده‌سازی این پروتکل در سیستمی با امکانات پردازشی متوسط، با متوسط‌گیری از زمان پردازش برای ۱۰ خودرو، در جدول (۵-۴) آورده شده است. اگر جاده‌ای با تراکم زیاد خودروها را در نظر بگیریم و فرض کنیم: رنج رادیویی هر واحد کنار جاده به شعاع ۵۰۰ متر است، سرعت خودروها ۱۰۰ کیلومتر بر ساعت، عرض جاده ۲۰ متر و مساحت هر خودرو با در نظر گرفتن فاصله آن با خودروهای اطرافش ۱۵ متر است. هر خودرو به مدت یک ثانیه، حدود ۲۷.۷۷ متر را طی می‌کند و بنابراین ۱ کیلومتر را (قطر دایره حاصل از محدوده رادیویی واحد کنار جاده) در مدت حدود ۳۶ ثانیه طی خواهد کرد. پس هر خودرو در حدود ۳۶ ثانیه طول می‌کشد تا از رنج رادیویی واحد کنار جاده خارج شود. در این ۳۶ ثانیه با توجه به نتیجه پیاده‌سازی مدل مطرح شده در جدول (۵-۳)، حدود ۲۳۲۲ خودرو می‌توانند تا زمانی که در رنج رادیویی واحد کنار جاده باشند، گواهینامه خود را در واحد مزبور بروز رسانی کنند یا بعبارتی با فرض سرعت ۱۰۰ کیلومتر بر ساعت برای خودروها و شعاع ۵۰۰ متر برای واحدها، ظرفیت سرویس‌دهی برای بروز رسانی گواهینامه در هر واحد کنار جاده تا ۲۳۲۲ خودرو خواهد بود. از طرفی

تعداد خودروها در این محدوده مکانی از جاده که مساحتی در حدود ۱۰۰۰۰ متر دارد، در حدود ۶۶۷ خودرو است. بنابراین همه خودروهایی که در این محدوده هستند به راحتی می‌توانند از خدمات واحد کنار جاده برای صدور و بروز رسانی گواهینامه خود با توجه به مدل اصلاح شده پروتکل گواهینامه آنی استفاده نمایند.

جدول ۵-۴. پیاده سازی و بررسی بار محاسباتی بر روی واحدهای کنار جاده به منظور امکان سنجی مدل برای پیاده‌سازی واقعی

مدل دریافت گواهینامه	متوسط زمان پردازش در هر واحد کنار جاده (ثانیه)	زمان لازم برای شناسایی پلاک (ثانیه) طبق [۷۵]	تعداد خودروهای قابل سرویس‌دهی در هر ثانیه
مدل اصلاح شده [۳۶]	۰.۰۱۱	۰.۰۰۴۵	۶۴.۵

۶-۴- نتیجه‌گیری

حمله سایبل یکی از اختلالاتی است که توسط خودروی بدخواه جهت صورت گرفته و منجر به افت کارایی شبکه می‌شود. در این فصل تاثیر این حمله را بر روی یکی از مهمترین کاربردهای شبکه خودرویی یعنی مسیریابی بسته‌ها نشان دادیم و مشاهده کردیم که ایجاد موجودیت سایبل توسط خودروی بدخواه منجر به کاهش تعداد بسته‌های تحویلی و توان عملیاتی در شبکه خودرویی خواهد شد. پس از بررسی آسیب در شبکه، با بررسی روشهای مختلف که در فصل ۳ انجام شد، راه‌حل کارایی را در جهت رفع این حمله در کاربردهای عملی بر مبنای رمزنگاری و احراز هویت و تصدیق فیزیکی خودرو انتخاب کردیم و با اصلاح آن، کارایی این روش در شبکه خودرویی مورد بررسی قرار گرفت که با نتایج بدست آمده ثابت شد که با وجود مقیاس‌پذیری کافی، امکان پیاده‌سازی این روش در عمل وجود دارد.

فصل ۶

نتیجه‌گیری و پیشنهادات

۶-۱- نتیجه‌گیری

به دلیل افزایش تعداد خودروها و ترافیک جاده‌ای، میزان تصادفات در ایران افزایش چشمگیری یافته است. علت عمده تصادفات خطاهای انسانی است که اکثرا به دلیل خطاهای اطلاعاتی رخ می‌دهند و در نتیجه راننده نمی‌تواند عکس‌العمل مناسبی را برای جلوگیری از تصادف اتخاذ نماید. بهمین منظور سیستم هوشمند خودرویی با در اختیار قرار دادن اطلاعات محیط اطراف و افزایش سطح آگاهی راننده، تحول شگرفی در ایمنی حمل و نقل و کاهش آمار تصادف ایجاد می‌کند. کاربردهای زیاد این شبکه در زمینه ایمنی خودروها و جلوگیری از تصادف و همچنین کنترل ترافیک مهندسان شرکت‌های خودروسازی و مخابراتی را بر آن داشت تا به ساخت و طراحی خودروهایی بپردازند که بتوانند با سیستم نقلیه هوشمند حرکت کنند.

در این پایان نامه به بررسی شبکه هوشمند خودرویی در حوزه حفظ امنیت شبکه در مقابل خودروهای بدخواه پرداختیم. یکی از مسائل ایمنی ترافیک، دریافت اطلاعات صحیح مکان از طرف خودروها برای مدیریت ترافیک و حفظ ایمنی خودروها در جاده است. خودروی بدخواه با ارسال موقعیت نادرست می‌تواند موجب اختلال در کاربردهای مدیریت ترافیک و حتی راه‌اندازی حمله سایبل در شبکه شود. چون یکی از مواردی که خودرو می‌تواند موجودیتهای ساختگی برای خود در شبکه ایجاد کند، امکان ارسال موقعیتهای اشتباهی است که توسط هیچیک از موجودیتهای داخل شبکه قابل شناسایی نیست. بنابراین در این پایان‌نامه به بررسی روش مکانیابی خودروها با رویکرد امکان ارسال موقعیتهای صحیح در شبکه خودرویی پرداختیم. در راهکار ارائه شده، با تغییر آرایش واحدهای کنار جاده و محاسبه موقعیت خودرو با مفهوم دایره‌های متداخل، به بهبود مدل شناسایی موقعیت با کمک واحدهای کنار جاده پرداختیم. در این شرایط فضای حالت انتخاب موقعیت نادرست برای خودروی بدخواه، به گونه‌ای که موجودیتهای شبکه

قادر به شناسایی آن نباشند کاهش یافت و علاوه بر این، تعداد پیامهایی که برای دریافت موقعیت توسط خودرو در شبکه ارسال می‌شود در اکثر موارد کاهش یافت.

در بررسی دیگر برای حفظ ایمنی در شبکه، به بررسی حمله سایبل در شبکه خودرویی پرداختیم. در این حمله خودروی بدخواه با ایجاد موجودیتهای اضافی قصد فریب خودروهای دیگر را دارد. با بررسی جامعی که در کارهای مروری انجام شد، کلیه مکانیزمهای دفاعی را در برابر این حمله به سه دسته تقسیم کرده و بهترین روش مقابله را روشهای مبتنی بر احراز هویت و رمزنگاری یافتیم. به همین منظور برای مقابله با حمله، پروتکلی انتخاب شد که نرخ شناسایی صددرصد دارد و اما به دلیل شناسایی فیزیکی اولیه و استفاده از مکانیزمهای رمزنگاری زمان پردازش زیادی نیاز دارد. بهمین منظور برای بررسی و امکان سنجی آن برای پیاده‌سازی عملی، به اصلاح و پیاده‌سازی این روش و بررسی زمان پردازش و بار محاسباتی تحمیل شده بر روی واحد کنار جاده پرداختیم که با توجه به نتایج حاصل شده، این روش را به عنوان یکی از روشهای کارا با مقیاس‌پذیری بالا یافتیم به نحوی که قادر است کل خودروهای اطراف خود را تا زمانی که در رنج رادیویی واحد کنار جاده مزبور هستند، پوشش داده و برای صدور و یا بروز رسانی گواهینامه سرویس دهد.

۶-۲- پیشنهادات

۱. مکانیابی بر اساس واحدهای کنار جاده در مقیاس کم با روش فاصله‌سنجی اختلاف زمان ورود سیگنال یا TDOA پیاده‌سازی شده است. بررسی روشهای فاصله سنجی مختلف و استفاده از روشی که دقت بالایی در یافتن فاصله خودرو از واحدهای کنار جاده داشته باشد، می‌تواند تاثیر زیادی در افزایش دقت این روش داشته باشد.

۲. دیدگاه اصلاح شده برای شناسایی حمله سایبل از نظر عملی قابل پیاده‌سازی است. اما برای بررسی بیشتر می‌توان آن را در مقیاس وسیع‌تر پیاده‌سازی کرد. علاوه بر این، در این دیدگاه با دریافت

جفت کلید موقت در یک بازه زمانی تعریف شده برای اعتبار گواهینامه، حریم خصوصی رانندگان تا حدی حفظ می‌شود. به خصوص اگر این بازه کوچکتر باشد امکان ردگیری خودرو کمتر می‌شود. اما می‌توان این پروتکل را به شیوه‌ای پیاده‌سازی کرد که ایمنی بیشتری را برای حریم خصوصی کاربران فراهم سازد. اینکار با تعویض حساب شده گواهینامه‌ها در مناطق خاص امکان‌پذیر خواهد بود. در واقع، یکی از اشکالات عمده این پروتکل این است که جفت کلید موقتی که خودرو از هر واحد کنار جاده دریافت می‌کند، تا زمانی که خودرو گواهینامه بعدی را دریافت نماید، در ارسال پیام‌های دوره‌ای یا ارسال پیامهای هشدار مورد استفاده قرار می‌گیرد.

مراجع

[۱] Lind, R., Schumacher, R., Reger, R., Olney, R., Yen, H., Laur, M., & Freeman, R. (۱۹۹۹). The Network Vehicle-a glimpse into the future of mobile multi-media.*Aerospace and Electronic Systems Magazine, IEEE*, ۱٤(۹), ۲۷-۳۲.

[۲] ASTM E۲۲۱۳-۰۳, July ۲۰۰۳, "Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems — ٥ GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer PHY) Specifications", *ASTM International*.

[۳] Lu, R. (۲۰۱۲). Doctoral dissertation, *Security and Privacy Preservation in Vehicular Social Networks* , University of Waterloo.

[۴] یوسفی ص ، اسفند ماه ۱۳۸۶، رساله دکتری، "تحلیل و ارزیابی همبندی و انتشار پیامهای ایمنی در شبکه های موردی بین خودرویی" ، دانشکده کامپیوتر، دانشگاه علم و صنعت ایران.

[٥] Zhang, C. (۲۰۱۰). Doctoral dissertation, *On Achieving Secure Message Authentication for Vehicular Communications*, University of Waterloo.

[٦] Gupta, P., & Kumar, P. R. (۱۹۹۸). Critical power for asymptotic connectivity. In*Decision and Control, ۱۹۹۸. Proceedings of the ۳۷th IEEE Conference on* (Vol. ۱, pp. ۱۱۰٦-۱۱۱۰). IEEE.

[۷] Lochert, C., Barthels, A., Cervantes, A., Mauve, M., & Caliskan, M. (۲۰۰٥, September). Multiple simulator interlinking environment for IVC. In *Proceedings of the ۳nd ACM international workshop on Vehicular ad hoc networks* (pp. ۸۷-۸۸). ACM.

[۸] Toor, Y., Muhlethaler, P., & Laouiti, A. (۲۰۰۸). Vehicle ad hoc networks: Applications and related technical issues. *Communications Surveys & Tutorials, IEEE*, ۱۰(۳), ۷٤-۸۸.

[۹] Zhu, H., Lu, R., Shen, X., & Lin, X. (۲۰۰۹). Security in service-oriented vehicular networks. *Wireless Communications, IEEE*, ۱٦(٤), ۱٦-۲۲.

[۱۰] Lin, X., Lu, R., Zhang, C., Zhu, H., Ho, P. H., & Shen, X. (۲۰۰۸). Security in vehicular ad hoc networks. *Communications Magazine, IEEE*, ٤٦(٤), ۸۸-۹٥.

[۱۱] Wang, C. D., & Thompson, J. P. (۱۹۹۷). *U.S. Patent No. ٥,٦۱۳,۰۳۹*. Washington, DC: U.S. Patent and Trademark Office.

[۱۲] "U.S. department of transportation," http://safety.fhwa.dot.gov/facts/road factsheet. htm.

[۱۳] Hartenstein, H., & Laberteaux, K. P. (۲۰۰۸). A tutorial survey on vehicular ad hoc networks. *Communications Magazine, IEEE*, ٤٦(٦), ۱٦٤-۱۷۱.

[۱٤] Lu, R., Lin, X., Zhu, H., & Shen, X. (۲۰۱۰). An intelligent secure and privacy-preserving parking scheme through vehicular communications. *Vehicular Technology, IEEE Transactions on*, ٥۹(٦), ۲۷۷۲-۲۷۸٥.

[۱٥] Raya, M., & Hubaux, J. P. (۲۰۰۷). Securing vehicular ad hoc networks. *Journal of Computer Security*, ۱٥(۱), ۳۹-٦۸.

[۱٦] Papadimitratos, P., Hubaux, J., ۲۰۱۱, "Secure vehicular communication systems," in Encyclopedia of Cryptography and Security (۲nd Ed.), pp. ۱۱٤۰–۱۱٤۳.

[۱۷] Moore, T., Raya, M., Clulow, J., Papadimitratos, P., Anderson, R., & Hubaux, J. P. (۲۰۰۸, June). Fast exclusion of errant devices from vehicular networks. In*Sensor, Mesh and Ad Hoc Communications and Networks, ۲۰۰۸. SECON'۰۸. ٥th Annual IEEE Communications Society Conference on* (pp. ۱۳٥-۱٤۳). IEEE.

[۱۸] T. Leinm¨uller, E. Schoch, F. Kargl, and C. Maih¨ofer, “Influence of falsified position data on geographic ad-hoc routing,” in *In Proceedings of the second European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS*, ۲۰۰۵, pp. ۱۰۲–۱۱۲.

[۱۹] T. Leinm¨uller, E. Schoch, and F. Kargl. Position Verification Approaches for Vehicular Ad Hoc Networks. IEEE Wireless Communication Magazine, ۱۳(۵):۱۶–۲۱, October ۲۰۰۶.

[۲۰] Raya, M., & Hubaux, J. P. (۲۰۰۵, March). Security aspects of inter-vehicle communications. In *Swiss Transport Research Conference (STRC)*.

[۲۱] Hubaux, J. P., Capkun, S., & Luo, J. (۲۰۰۴). The security and privacy of smart vehicles. *Security & Privacy, IEEE*, ۲(۳), ۴۹-۵۵.

[۲۲] Raya, M., Hubaux, J. P., (۲۰۰۵, November), “The security of vehicular ad hoc networks”, *Proceedings of the ۳rd ACM workshop on Security of ad hoc and sensor networks*, Alexandria, VA, USA .

[۲۳] Lin, X., Sun, X., Ho, P. H., & Shen, X. (۲۰۰۷). GSIS: a secure and privacy-preserving protocol for vehicular communications. *Vehicular Technology, IEEE Transactions on*, ۵۶(۶), ۳۴۴۲-۳۴۵۶.

[۲۴] Calandriello, G., Papadimitratos, P., Hubaux, J. P., & Lioy, A. (۲۰۰۷, September). Efficient and robust pseudonymous authentication in VANET. In*Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks* (pp. ۱۹-۲۸). ACM.

[۲۵] Freudiger, J., Raya, M., Félegyházi, M., & Papadimitratos, P. (۲۰۰۷). Mix-zones for location privacy in vehicular networks. In *Proceedings of the First International Workshop on Wireless Networking for Intelligent Transportation Systems (Win-ITS)*.

[۲۶] J. Douceur, the Sybil attack, in: Lecture Notes in Computer Science: Revised Papers from the First International Workshop on Peer-to-Peer Systems, vol. ۲۴۲۹, Fig. ۱۸. Average time to detect malicious vehicles. ۲۰۰۲, pp. ۲۵۱–۲۶۰

[۲۷] Newsome, J., Shi, E., Song, D., & Perrig, A. (۲۰۰۴, April). The ۱۱۲ybil attack in sensor networks: analysis & defenses. In *Proceedings of the ۳rd international symposium on Information processing in sensor networks* (pp. ۲۵۹-۲۶۸). ACM.

[۲۸] P. Golle, D. Greene, J. Staddon, Detecting and correcting malicious data in VANETs, in: Proceedings of the ACM Workshop on Vehicular Ad Hoc Networks (VANET), Philadelphia, PA, ۲۰۰۴, pp. ۲۹–۳۷.

[۲۹] Yan, G., Olariu, S., & Weigle, M. C. Providing VANET security through active position detection. Computer Communications ۲۰۰۸; ۳۱(۱۲): ۲۸۸۳-۲۸۹۷, DOI: ۱۰.۱۰۱۶/j.comcom.۲۰۰۸.۰۱.۰۰۹.

[۳۰] شهرزاد گلستانی نجف آبادی، حمید رضا ناجی، علی ماهانی، ۱۳۹۱، " مروری بر روشهای تشخیص حملات سیبیل در شبکه های حسگر بیسیم"، اولین کنفرانس ملی ایده‌های نو در مهندسی برق، دانشگاه آزاد واحد خوراسگان- اصفهان

[۳۱] مجتبی دهقانی فیروز آبادی، الهام راستگو، اسفند ۹۰، بررسی روش تست منبع رادیویی برای دفاع در برابر حملات Sybil، دومین کنفرانس ملی محاسبات نرم و فناوری اطلاعات، دانشگاه آزاد واحد ماهشهر.

[۳۲] Yu, B., Xu, C. Z., & Xiao, B. “Detecting Sybil attacks in VANETs.”*Journal of Parallel and Distributed Computing* (۲۰۱۳)..

[۳۳] Raya, M., Papadimitratos, P., & Hubaux, J. P. (۲۰۰۶). Securing vehicular communications. *Wireless Communications, IEEE*, ۱۳(۵), ۸-۱۵..

[۳٤] Bouassida, M. S., Guette, G., Shawky, M., & Ducourthial, B. “Sybil nodes detection based on received signal strength variations within vanet.” *International Journal of Network Security* ۹, no. ۱ (۲۰۰۹): ۲۲-۳۲.
[۳٥] Chang, S., Qi, Y., Zhu, H., Zhao, J., & Shen, X. (۲۰۱۲). Footprint: Detecting Sybil Attacks in Urban Vehicular Networks. *Parallel and Distributed Systems, IEEE Transactions on*, ۲۳(٦), ۱۱۰۳-۱۱۱٤.
[۳٦] Park, S., Aslam, B., Turgut, D., & Zou, C. C. Defense against Sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support. Security and Communication Networks ۲۰۱۳; ٦(٤): ٥۲۳–٥۳۸.
[۳۷] Zhou, Tong, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty. “P۲DAP—Sybil Attacks Detection in Vehicular Ad Hoc Networks.” *Selected Areas in Communications, IEEE Journal on* ۲۹, no. ۳ (۲۰۱۱): ٥۸۲-٥۹٤
[۳۸] Isaac, J. T., Zeadally, S., & Camara, J. S. (۲۰۱۰). Security attacks and solutions for vehicular ad hoc networks. *Communications, IET*, ٤(۷), ۸۹٤-۹۰۳.
[۳۹] Ibrahim, K. (۲۰۱۱). *Data aggregation and dissemination in vehicular ad-hoc networks* (Doctoral dissertation, Old Dominion University).
[٤۰] Shen, P. Y. (۲۰۱۱). An efficient public key management regime for vehicular ad hoc networks (VANETS).
[٤۱] Yan, G., Yang, W., Li, J., & Ashok, V. G. (۲۰۱۰, November). Active position security through dynamically tunable radar. In *Mobile Adhoc and Sensor Systems (MASS), ۲۰۱۰ IEEE ۷th International Conference on* (pp. ۷۳۳-۷۳۸). IEEE.
[٤۲] Xiao, B., Yu, B., & Gao, C. (۲۰۰٦, September). Detection and localization of ۱۱۳ybil nodes in VANETs. In *International Conference on Mobile Computing and Networking: Proceedings of the ۲۰۰٦ workshop on Dependability issues in wireless ad hoc networks and sensor networks* (Vol. ۲٦, No. ۲٦, pp. ۱-۸).
[٤۳] Ou, C.-H. A roadside unit based localization scheme for vehicular ad hoc networks. Int. J of Communication Systems, Wiley, ۲۰۱۲; ٥۱: ۱۲۳-۱۳۰. DOI: ۱۰.۱۰۰۲/dac.۲۳٥۲.
[٤٤] Boukerche, A., Oliveira, H. A., Nakamura, E. F., & Loureiro, A. A. (۲۰۰۸). Vehicular ad hoc networks: A new challenge for localization-based systems. *Computer communications*, ۳۱(۱۲), ۲۸۳۸-۲۸٤۹.
[۴۵] قاضی شهنی زاده، پوران، سامانه موقعیت یاب جهانی (جی.پی.اس) و کاربردهای آن، وزارت جهاد کشاورزی معاونت برنامه ریزی و اقتصادی دفتر آمار و فناوری اطلاعات.
[۴۶] آزموده اردلان، علیرضا,باعث، مرضیه، مدلسازی خطای یونسفری با استفاده از تصحیح مولفه های مختصات و بردار موقعیت، دانشکده فنی دانشگاه تهران اسفند ۱۳۸۳; ۳۸(۶):۸۲۳-۸۳۰
[۴۷] نجات داوود,وثوقی بهزاد، روش های تولید تصحیح و بهبود دقت در سیستم تعیین موقعیت آنیDGPS ، دانشکده فنی دانشگاه تبریز زمستان ۱۳۸۷; ۳۸(۳ (پیاپی ۵۶) ویژه مهندسی عمران):۲۳-۳۴.
[٤۸] Ben Meadows TechInfo Article, WAAS and GPS Accuracy, document number ۳۰۰, http://www.benmeadows.com/refinfo/techfacts/Default.htm.
[٤۹] Benslimane A. Localization in vehicular ad hoc networks. *Proceedings of Systems Communications*, ۲۰۰٥; ۱۹–۲٥.
[٥۰] Kukshya V, Krishnan H, Kellum C. Design of a system solution for relative positioning of vehicles using vehicle-tovehicle radio communications during GPS

outages. *Proceedings of IEEE Vehicular Technology Conference (VTC)*, ۲۰۰۵; ۱۳۱۳–۱۳۱۷.

[۵۱] Parker R, Valaee S. Vehicular node localization using received-signal-strength indicator. *IEEE Transactions on Vehicular Technology* Nov ۲۰۰۷; ۵٦(٦):۳۳۷۱–۳۳۸۰.

[۵۲] Caffery J, Stüer GL. Overview of radiolocation in CDMA cellular systems. *IEEE Transactions on Vehicular Technology* Apr ۱۹۹۸; ۳٦(٤):۳۸–٤۵.

[۵۳] Alam MS, Alsharif S, Haq N. Efficient CDMA wireless, position, location system using TDOA method. *Nternational Journal of Communication Systems* Sept ۲۰۱۱; ۲٤(۹):۱۲۳۰–۱۲٤۲.

[۵٤] Sharawi MS, Aloi DN. Characterizing the performance of single-channel pseudo-doppler direction finding systems at ۹۱۵ MHz for vehicle localization. *International Journal of Communication Systems* Jan ۲۰۱۱; ۲٤(۱):۲۷–۳۹.

[۵۵] Z. Ren, W. Li, and Q. Yang, "Location verification for VANETs routing," in *Proc. IEEE Int. Conf. Wireless Mobile Comput., Netw. Commun.*, ۲۰۰۹, pp. ۱٤۱–۱٤٦.

[۵٦] Chim, T. W., Yiu, S. M., Hui, L. C. K., & Li, V. O. K. Grouping-enabled and privacy-enhancing. *Information Systems Security*, *۱۷*(۱), ٦۰-۹٦, ۲۰۱۱.

[۵۷] M. Rahbari, M. A. J. Jamali, "Efficient detection of ۱۱٤ybil attack based on cryptography in VANET", International journal of network security & its applications (IJNSA), pp.۱۸۵-۱۹۵, ۲۰۱۱.

[۵۸] W. Stallings, Cryptography and Network Security, chapter ۹, Fourth Edition.

[۵۹] N. Jansma and B. Arredondo, "Performance Comparison of Elliptic Curve and RSA Digital Signatures" Technical Report, University of Michigan College of Engineering, ۲۰۰٤ .

[٦۰] Glossary for the Linux FreeS/WAN project available on: http://www.freeswan.org/freeswan_trees/freeswan-۲.۰۱/doc/glossary.html

[٦۱] Information-technology Promotion Agency (IPA), Japan, CRYPTREC. SEED Evaluation Report", February, ۲۰۰۲, http://www.kisa.or.kr/seed/seed_eng.html

[٦۲] T. Gonzalez, A Reflection Attack on Blowfish, JOURNAL OF LATEX CLASS FILES, vol. ٦, no. ۱, ۲۰۰۷.

[٦۳] O. Kara and C. Manap, "A New Class of Weak Keys for Blowfish", In Alex Biryukov, editor, *Fast softeare Encryption, ۱٤th International Workshop*, FSE ۲۰۰۷, vol. ٤۵۹۳ of *Lecture Notes in Computer Science*, pages ۱٦۷-۱۸۰. Spring-Verlag, ۲۰۰۷.

[٦٤] Quantum Information and Network Security Laboratory, Lecture note on: http://islab.csie.ncku.edu.tw/course/slide/ch_۰٦.ppt

[٦۵] H. Pietilainen, "Elliptic Curve Cryptography on Smart Cards", Masters Thesis, Faculty of Information Technology, University of Helsinki, ۲۰۰۰.

[۶۶] H.-Y. Lin and T.-C. Chiang. Cooperative secure data aggregation in sensor networks using elliptic curve based cryptosystems. In Yuhua Luo, editor, CDVE, volume ۵۷۳۸ of Lecture Notes in Computer Science, pages ۳۸٤–۳۸۷. Springer, ۲۰۰۹

[۶۷] زهرا میرمحمدی، سعادت پورمظفری، بهبود الگوریتم رمز منحنی‌های بیضوی با استفاده از کدگذاری داده، هفتمین کنفرانس انجمن رمز ایران، ۱۳۸۹.

[۶۸] عبدالحسین رضایی، پرویز کشاورزی، بهبود سرعت الگوریتم ضرب اسکالر در سیستمهای رمزنگاری منحنی بیضوی، هفتمین کنفرانس انجمن رمز ایران، ۱۳۸۹.

[٦٩] Grover, J., Kumar, D., Sargurunathan, M., Gaur, M.S., Laxmi, V.: Performance Evaluation and Detection of Sybil Attacks in Vehicular Ad-Hoc Networks. In: Meghanathan, N., Boumerdassi, S., Chaki, N., Nagamalai, D. (eds.) CNSA ٢٠١٠. CCIS, vol. ٨٩, pp. ٤٧٣–٤٨٢. Springer, Heidelberg (٢٠١٠).
[٧٠] Sood, M., & Vasudeva, A., Perspectives of Sybil Attack in Routing Protocols of Mobile Ad Hoc Network. In *Computer Networks & Communications (NetCom)*, Vol. ١٣١, ٣-١٣, ٢٠١٣.
[٧١] Karlof, C., Wagner, D., Secure routing in wireless sensor networks: Attacks and countermeasures, *Ad hoc Networks Journal (Elsevier,)* vol. ١, ٢٩٣ -٣١٥, ٢٠٠٣.
[٧٢] T. Clausen, P. Jacquet, L. Viennot, "Comparative Study of Routing Protocols for Mobile Ad-hoc Networks", in *١st IFIP MedHocNet Conference*, ٢٠٠٢.
[٧٣] S. Baraković, S. Kasapović, and J. Baraković. Comparison of MANET Routing Protocols in Different Traffic and Mobility Models. Telfor Journal, ٢(١):٨-١٠, ٢٠١٠.
[٧٤] Upadhyay, A., & Phatak, R. (٢٠١٣). Performance Evaluation of AODV DSDV and OLSR Routing Protocols with Varying FTP Connections in MANET. *IJRCCT*, ٢(٨), ٥٣١-٥٣٥.
[٧٥] Sarfraz, M.S., Shahzad, A., Elahi, M.A., Fraz, M., "Real-Time automatic license plate recognition for CCTV forensic applications," *Journal of Real-Time Image Processing-Springer Berlin/Heidelberg*, vol. ٨, no. ٣, pp. ٢٨٥-٢٩٥, ٢٠١٣.
[٧٦] C. Patel, D. Shah and A. Patel, Automatic Number Plate Recognition System (ANPR): A Survey, *International Journal of Computer Applications, vol.* ٦٩, no. ٩, pp. ٢١-٣٣, ٢٠١٣.
[٧٧] M. Gerlach and F. G¨uttler. Privacy in VANETs using Changing Pseudonyms - Ideal and Real. In VTC٢٠٠٧-Spring, pages ٥٢١–٢٥٢٥, ٢٠٠٧.
[٧٨] Buttyán, L., Holczer, T., Vajda, I.: On the effectiveness of changing pseudonyms to provide location privacy in VANETs. In: Stajano, F., Meadows, C., Capkun, S., Moore, T. (eds.) ESAS ٢٠٠٧. LNCS, vol. ٤٥٧٢, pp. ١٢٩–١٤١. Springer, Heidelberg (٢٠٠٧)
[٧٩] Freudiger, J., Shokri, R., Hubaux, J.-P.: On the Optimal Placement of Mix Zones. In: Goldberg, I., Atallah, M.J. (eds.) PETS ٢٠٠٩. LNCS, vol. ٥٦٧٢, pp. ٢١٦–٢٣٤. Springer, Heidelberg (٢٠٠٩)

Abstract

Nowadays, vehicular ad hoc network has been proposed as a comprehensive and new plan, which aims to provide road safety, traffic management and convenience applications for drivers and passengers on the road.
In this network, communications are in two ways: vehicle to vehicle and vehicle to Infrastructure (road side unit). Different messages containing events warning about road and traffic conditions, traffic information, private information of vehicles such as speed and location are exchanged in these communications. Unfortunately, wireless communications and the high-speed mobility of a large number of vehicles pose many challenges in VANETs.

It is evident that any malicious behavior of users (vehicles), such as injecting false information, modifying and replaying the disseminated messages, discarding routing packets in the network and impersonation has irreversible effects on people's lives. In addition, users show prime interest in protecting their private information leading to unique identification in the network. So, it is clear that security and privacy preservation are two critical challenges for VANET deployment in real world. Studies have shown that Public Key Infrastructure (PKI) is a well-recognized solution for secure VANET communications. Consequently, in this thesis, we explore the breaches addressed in this infrastructure and examine two important security requirements.

In the first problem, positioning is investigated. Valid information about the location of the vehicle is a basic requirement for a large number of VANET applications. Disseminating fake position information generated by malicious vehicle or malfunctions of vehicles location finding system (e.g. GPS), can disrupt traffic management applications and so cause to congestion and road accidents. Therefore, we have tried to improve a localization scheme based upon the information provided by road side units that have not limitations of the GPS-based systems. In this improvement, we change road side unit deployment such that has two advantages: first, location finding now involves less communication overhead, second, in validating a vehicle's location the large state space due to malicious vehicle now gets significantly smaller.

In the second problem the Sybil attack is discussed. In such attack, the malicious vehicle impersonates other vehicles or introduces fake identities in the network. Its mission is to interrupt a voting system, routing method and reducing efficiency. In this dissertation we first simulate the Sybil attack on three different routing algorithms, and then by analyzing various defensive approaches we select the best one that has the public key infrastructure. Finally using a suggested protocol for this matter which has a ١٠٠٪ detection rate, firstly we reform this approach and then simulate it, in terms of scalability and practical implementation.

Key words: VANET, Sybil attack, routing disruption, PKI, localization.

Shahrood University
Computer engineering and information technology
M.Sc. thesis

Designing an intelligent secure schema for vehicular communication

By:
Mahdiyeh Alimohammadi

Supervisor:
Dr Ali Akbar Pouyan

Advisors:
Dr Omid Reza Maruzi
Meisam Yadollahzadeh Tabari

February ۲۰۱۴