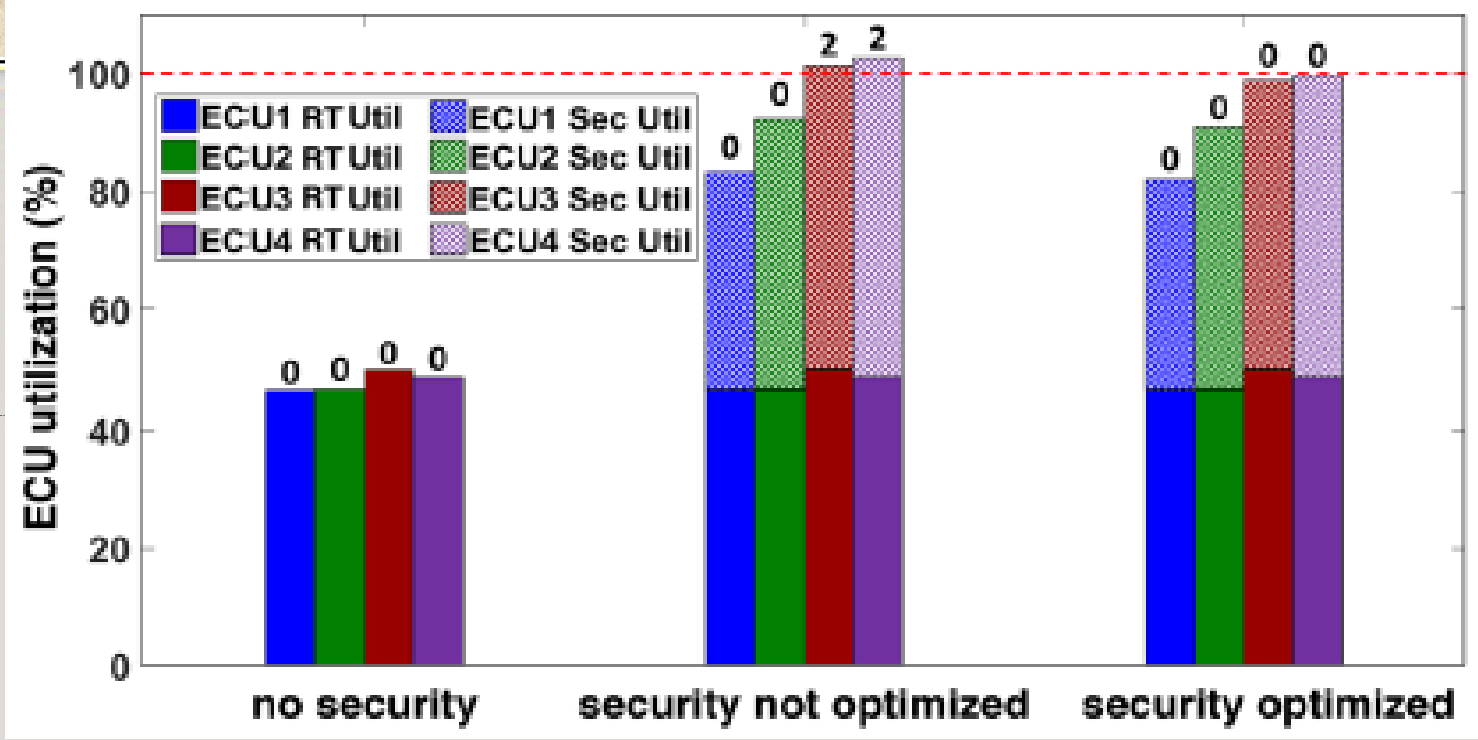
# طرح امنیت محور شبکه های حساس به زمان خودرو

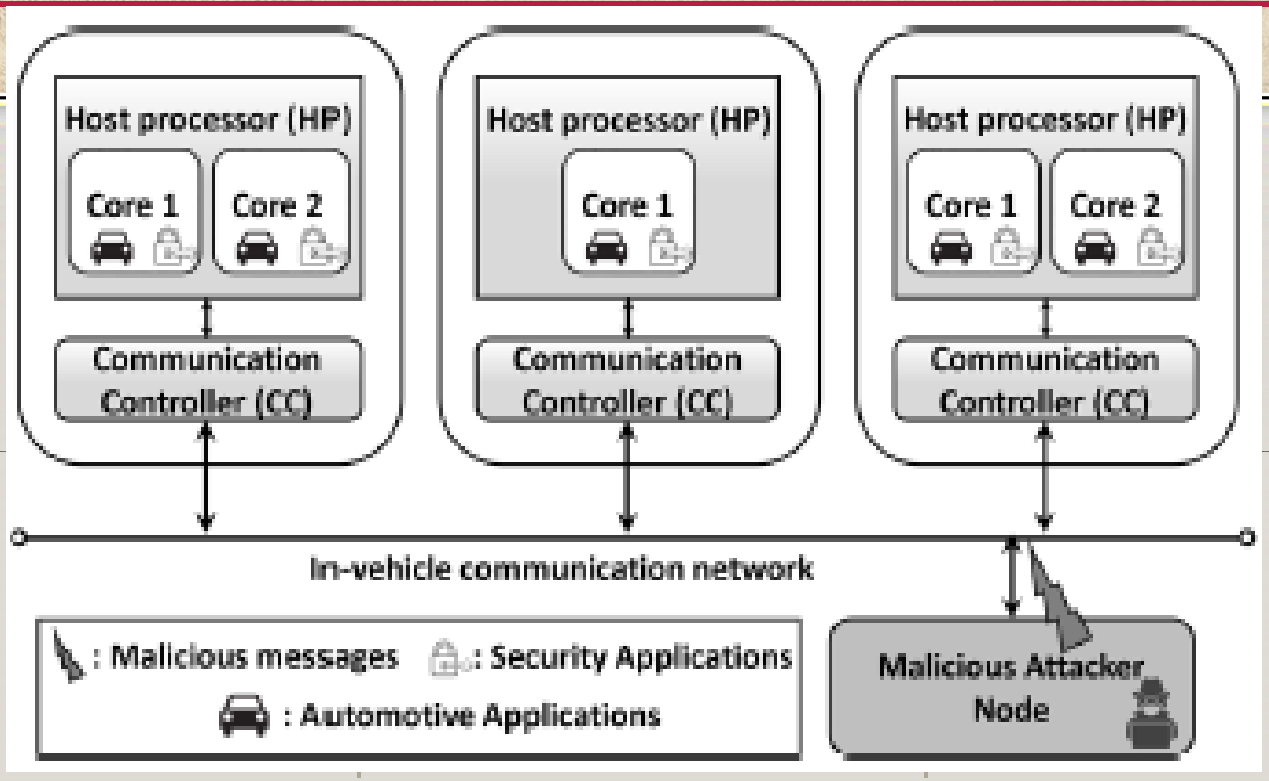
سید محمد رضا جعفری

- خودرو های نوین مجموعه از ECU های به هم متصل هستند که به خاطر افزایش سیستم های مختلف بار پردازشی آن ها دایما رو به افزایش است. این ECU ها لزوما از معماری یا تعداد هسته های پردازشی مشابه برخوردار نیستند. از طرفی نزدیک شدن به پیاده سازی جامع خودرو های خودران باعث افزایش سریع تر تعداد ECU ها شده است.

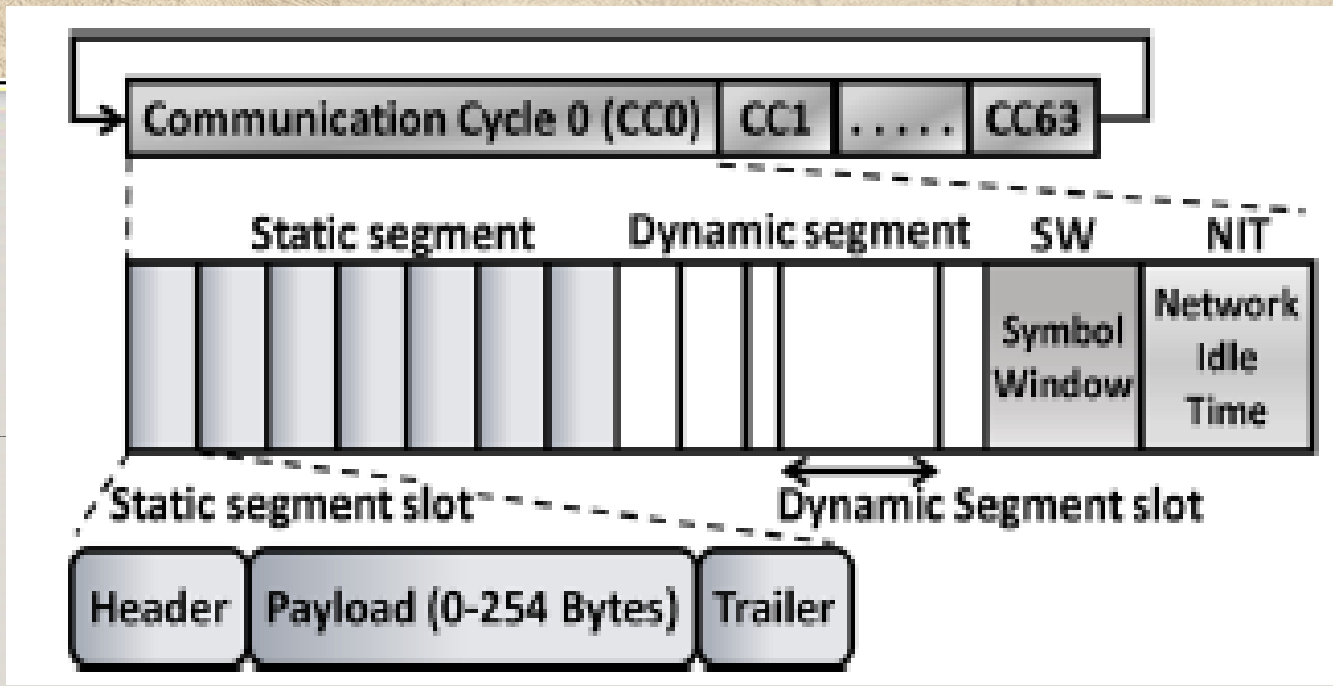
- حال که خودرو ها به طور گسترده تری به شبکه های خارج خودرو متصل اند دغدغه امنیت جدی تر شده است. مکانیزم های امنیتی به بخشی جدا نشدنی از ECU ها تبدیل شده اند، اما این مکانیزم ها خود می توانند بار پردازشی اضافی به همراه داشته باشند و منجر به تاخیر در عملکرد بخش های حساس و حیاتی شوند.


ECU utilization (%)
100
80
60
40
20
0
ECU1 RT Util
ECU2 RT Util
ECU3 RT Util
ECU4 RT Util
ECU1 Sec Util
ECU2 Sec Util
ECU3 Sec Util
ECU4 Sec Util
0 0 0 0
0 0 2 2
0 0 0 0
no security
security not optimized
security optimized

امنیت داده در خودرو ها تا سال های اخیر مورد بی توجهی قرار داشت تا آنکه در سال 2010 گروهی با دسترسی فیزیکی (پورت EBD II) توانستند موفق به تزریق پیام شدند. علاوه بر آن از طریق مهندسی معکوس تعدادی از ECU ها موفق به آپدیت Firmware از طریق شبکه CAN شدند. در سال 2014 عده ای موفق شدند تا از طریق هک سیستم رادیو خودرو Jeep Cherokee به هر دو شبکه CAN این خودرو دست یابند. در سال های اخیر نویسندگانی موفق به ایجاد برنامه تروجانی شدند که با آلوده کردن گوشی هوشمند پس از متصل شدن آن به سیستم تفریحی/اطلاعاتی خودرو به نویسندگان اجازه می داد تا پیام های دستکاری شده خود را در CAN وارد کنند.


Host processor (HP)
Core 1
Core 2
Communication Controller (CC)
Host processor (HP)
Core 1
Communication Controller (CC)
Host processor (HP)
Core 1
Core 2
Communication Controller (CC)
In-vehicle communication network
: Malicious messages
: Security Applications
: Automotive Applications
Malicious Attacker Node

سیستمی کلی که در آن ECU ها متعدد با برنامه های مختلف حساس به زمان وجود دارد. این ECU ها به وسیله ی شبکه باس FlexRay به یکدیگر متصل اند. هرECU از دو بخش اساسی HP و CC تشکیل شده است. HP وظیفه پردازش برنامه های خودرو و امنیتی را دارد و CC به عنوان رابط بین HP و FlexRay حضور دارد.


Communication Cycle 0 (CC0)
CC1
. . . . .
CC63
Static segment
Dynamic segment
SW
NIT
Symbol Window
Network Idle Time
Static segment slot
Dynamic Segment slot
Header
Payload (0-254 Bytes)
Trailer

ساختار پروتکل FlexRay به صورت چرخه ای است. بدین معنا که هر بار این چرخه ها با ساختاری یکسان به ترتیب تکرار میشوند. هر چرخه شامل بخش های ثابت ، پویا ، پنجره نماد و زمان بیکاری شبکه است. بخش های ثابت و بیکاری شبکه غیر قابل اجتناب هستند و بخش های پویا و پنجره نماد لزوما همیشه حضور ندارند.

بخش ثابت دارای Slot های برابر زمانی است( TDMA)که هر اسلات دارای سه بخش Header, Payload, Trailer است و وظیفه جا به جایی پیغام های حساس به زمان را دارد. بخش پویا وظیفه جا به جایی پیغام های حساس به وقایع را دارد و از بخش هایی با اندازه های مختلف تشکیل شده است. در بخش پویا از Flexible TDMA استفاده شده است. بدین معنا که ECU ای که بالاترین اولویت را دارد بر روی گذرگاه قرار میگیرد. پنجره علامت برای نشانه گذاری اولین دوره ارتباط شبکه است و همچنین برای تعمیر و نگه داری شبکه کاربرد دارد. بخش بیکار شبکه برای حفظ هماهنگی می باشد.

در بخش اختصاص Task ها ، SEDAN به سرعت هر Task را به یک ECU ارایه می دهد تا بتواند حالت بهنگام بودن ECU را حفظ کند. در این بخش Task هایی که به هر دلیلی به یک ECU خاص تعلق دارند از این مستثنی هستند. برای هر Taskمصرف بلادرنگ از نسبت زمان اجرا بر دوره Task بدست می آید. مصرف بلادرنگ برای هر ECU از مجموع مصرف بلادرنگ Task هایی که به آن ECU مشخص تخصیص داده شده است بدست می آید.

$$\tilde{U}_{t_q} = \frac{\tilde{e}_q}{\tilde{p}_q}$$

$$\tilde{U}_n = \sum_{q=1}^{G_n} \left( \tilde{U}_{t_{q,n}} \right)$$

تلاش لازم در این بخش متمرکز بر به صفر رساندن مصرف بلادرنگ ECU ها میباشد .

ابتدا لیستی از ECU ها بر اساس مصرف بلادرنگ ECU ها ایجاد میشود، سپس اولین Task تخصیص نیافته به ECU ای که کمترین مصرف بلادرنگ را دارد تخصیص داده میشود و پس از آن مصرف بلادرنگ آن Task به مصرف بلادرنگ ECU اضافه میشود و این رویه برای Task بعدی تکرار میشود تا هیچ Task اختصاص نیافته ای باقی نماند.

$$m_{j,n}^{SV} = m_{j,n}^{AW} * m_{j.n}^{SS}$$

$$Aggregate\ Security\ Value\ (ASV) = \frac{\sum_{n=1}^{N}\sum_{j=1}^{R_n}\left(\psi_{j,n} * m_{j,n}^{SV}\right)}{\sum_{n=1}^{N} R_n}$$

ASV معیاری بسیار مهمی برای تعیین امنیت به ازای تعداد پیغام ها است. از این معیار می توان برای مقایسه امنیت در سیستم های مختلف استفاده کرد. تعریف معادله پایین از ضرب نمره امنیتی در وزن ASIL آن بدست می آید، که به صورت زیر نشان داده میشود و به آن ارزش امنیتی می گویند.

نرخ میزان شکست بنابر ASIL را با خطا در زمان (FIT) نشان می دهند. FIT را به صورت ماکزیمم خطا های قابل پذیرش در 1 میلیارد ساعت استفاده بیان می کنند. بنابر قوانین ASIL نوع A،B،C،D به ترتیب 10FIT،100FIT،100FIT،1000FIT می باشد. بنابر ASILD تعداد خطا ها در یک ساعت باید کمتر از 10^-8 باشد. بنابر Kکلمه موجود در MAC احتمال خطای آن 2 به قوه K می باشد و Pj,n دوره یک پیغام را در میلی ثانیه نشان می دهد.

$$((3600*10^3)/p_{j,n})*2^{-k} \leq 10^{-8}$$

$$\Delta_{j,n}(D) = k \geq \left\lceil Q + \log_2\left(\frac{1}{p_{j,n}}\right)\right\rceil$$

ثابت Q برای ASIL D مقداری برابر 48.35 دارد. مقدار Q برای درجه بندی های C و B و A دارای ارزش 45.04 و45.04 و 41.72 .

مصرف ECU برای انجام رمز نگاری بلوکی برای یک پیام به صورت زیر محاسبه میشود:

$$\overline{U}_{m_{j,n}} = \left( \left\lceil \frac{b_j}{b_{size}} \right\rceil * \frac{T_{encr/decr}}{p_j} \right)$$

در فرمول بالا منظور از b size اندازه بلوکی است که بر روی آن امر رمزنگاری و یا رمزگشایی انجام میشود

$$\overline{U}_{m_{j,n}} = \left( \left\lceil \frac{b_j}{16} \right\rceil * \frac{T_{AES(X)}}{p_j} \right)$$

استفاده میشود می توان معادله اول را به AESاز آن جایی که از صورت بالایی بازنویسی کرد.

برای محاسبه مصرف ایجاد شده توسط بخش امنیت، مصرف ایجاد شده توسط بخش امنیت از تمامی داده های فرستاده شده و دریافت شده را جمع میشود. برای محاسبه مصرف کل یک ECU از جمع مصرف ایجاد شده توسط امنیت و مصرف بلادرنگ استفاده میشود. برای جلوگیری از تاخیر در اجرای هر ECU باید از مصرف کل آن کمتر از 100% باشد.

$$\overline{U}_n = \sum_{j=1}^{R_n} \overline{U}_{m_{j,n}}$$

$$U_n = \widetilde{U}_n + \overline{U}_n$$

در نهایت در جدول بالا مقایسه تعداد اشتباهات ایجاد شده در روش Lin et al که یک روش رقیب برای SEDAN است را نشان میدهد. این تعداد دفعات عدم رعایت امور امنیتی برای بار های پردازشی مختلف را نشان میدهد.

| Framework | Lin et al. 128 | Lin et al. 192 | Lin et al. 256 | SEDAN |
|---|---|---|---|---|
| Low load | 28 | 12 | 0 | 0 |
| Medium load | 45 | 16 | 0 | 0 |
| High load | 96 | 31 | 0 | 0 |