تجزیه و تحلیل طرح امنیتی احراز هویت وسیله نقلیه توسط RSU ها در VANET

چکیده

شبکه بین خودرویی VANET، شبکه ای برای ارائه ارتباط بین V2V نزدیک (وسیله نقلیه با وسیله نقلیه) و V2I (وسیله نقلیه با زیرسازه) می باشد. جهت افزایش بازده شبکه، شبکه باید دارای پایداری انتقال و امنیت قابلیت اطمینان باشد. در این مقاله، طرح امنیت احرازهویت وسیله نقلیه جدیدی VASS پیشنهاد می دهیم که براساس طرح احرازهویت مبتنی بر ID و با استفاده از کارت hi-pass (بلیط گذر از شاهراه) و شماره پلاک مجوز، RSU امن به OBU در VANET را تضمین می کند. اثربخشی و فایده VASS را بعد از تحلیل آن توسط شبکه پتری نشان می دهیم.

واژه های کلیدی: احراز هویت مبنی بر ID، OBU، شبکه های پتری، RSU، امنیت، VANET، VASS، احراز هویت وسیله نقلیه

1. مقدمه

شبکه بین خودرویی VANET شامل ارتباط بین وسایل نقلیه و ارتباط با واحدهای کنارجاده ای RSU نصب شده در مناطق اصلی است. بویژه، داده هایی همچون محل وسیله نقلیه، زمان جریان، جهت، سرعت، حجم ترافیک، شتاب و عدم شتاب، به وسیله واحدهای OBU در VANET توزیع می شود. براساس چنین داده هایی، VANET نقش دستکاری کننده در حجم ترافیک جاده ای، از طریق کنترل جریان ترافیک، اقدامات جلوگیری از تصادف، راه حلی برای حجم پیچیده ترافیک و اعلام جاده های جایگزین را بازی می کند.

در VANET، یکی از مهمترین مسائل وسایل نقلیه ای است که احراز هویت موفقی داشته اند. Raya همکارانی، روش تایید شده ای را با استفاده از تعداد زیادی جفتهای کلیدی خصوصی و عمومی ناشناس پیشنهاد دادند، اما این اثر نیازمند هزینه محاسباتی بالا و هزینه ذخیره بالا می باشد. Lu و همکارانش به معرفی پروتکل ECPP (حفظ حریم خصوصی شرطی موثر) برای VANETها پرداختند که سه سطح حریم خصوصی کاربر را برای دستیابی به احراز هویت، گمنامی و قابلیت ردیابی دارد. RSUها در ECPP مسئول صدور گواهیهای کلیدی

عمومی و موقت برای وسایل نقلیه می باشند. با این حال، ECPP از گواهیهای کلیدی عمومی و امضاء درهر پیام استفاده می کند که به هزینه محاسباتی بالا برای تایید پیام منجر می شود. Zhang و همکارانش، روش RAISE (طرح احراز هویت پیام به کمک RSU) با استفاده از کد احراز هویت پیام هش کلیدی متقارن HMAC را جهت کاهش هزینه امضاء پیشنهاد دادند. در [8]، PPAS (طرح احراز هویت با حفظ حریم خصوصی) برای محیط های ارتباط V2I پیشنهاد شد که احراز هویت سبکی دارد. همانگونه که در بالا ذکر شد [8-11]، ما دریافتیم که طراحی طرح احراز هویت با حفظ حریم خصوصی و امنیت، با تاخیر محاسباتی و احراز هویت پایین در VANET، چالش اصلی است.

این تحقیق، بر مسئله احراز هویت درهر وسیله نقلیه، در ارتباط بین وسایل نقلیه در شاهراه تاکید دارد. بعبارت دیگر، احراز هویت قطعی در وسایل نقلیه، در حالت ارتباط بین وسایل نقلیه، نه تنها از تصادف جلوگیری می کند بلکه بعنوان داده اصلی در موضوعات مسئولیت بعد از تصادف نیز استفاده می شود. ضروری است که در ارتباط بین وسایل نقلیه، هویت ها (ID) مجزا شوند، در رابط فرستنده و گیرنده مداخله ای نشود و محرمانه بودن پیام ارتباطی بین ماهیت ها تضمین شود. جهت نمایش بازده ایمنی، مکانیسم امنیتی جدیدی برای VANET پیشنهاد شده است و با مدلسازی شبکه پتری، اثربخشی و مزیت آن تایید شده است.

شبکه های پتری به عنوان ابزار ریاضی و گرافیکی، محیط یکنواختی برای مدلسازی، تحلیل و کنترل سیستم های پیچیده می باشند. مدلسازی شبکه های پتری، خطاها و معایر طرح امنیتی را شناسایی کرده و صحت پروتکل ایمنی را بهبود می بخشد. از شبکه های پتری، در تحلیل امنیت طرح پیشنهادی استفاده کردیم.

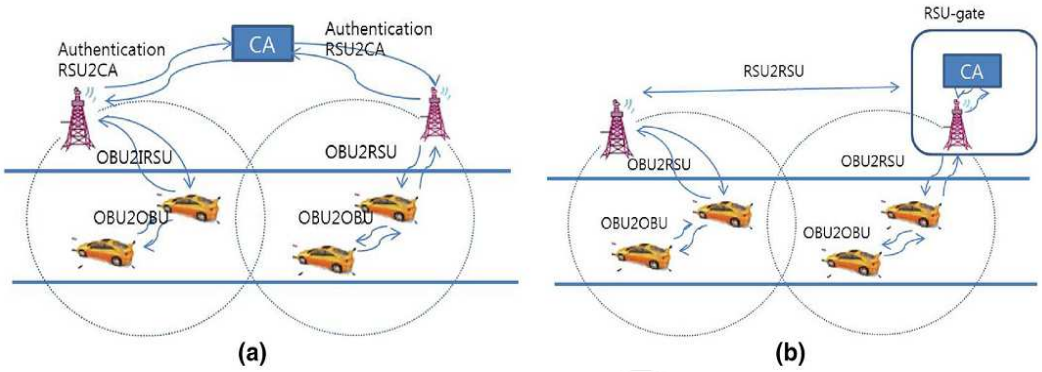
ادامه مقاله به شکل زیر است. بعد از مقدمه در بخش 1، بخش 2 به بررسی مقدمات و فرضیات اثار می پردازد. بخش 3 به تبیین طرح امنیت احراز هویت وسیله نقلیه VASS پیشنهادی در این تحقیق می پردازد. در بخش 4، مدلهای شبکه پتری و نحوه اعمال مکانیسمی ارائه می شود که براساس اهداف امنیتی متغیر هستند. بخش 5 به تبیین تحقیقات آینده و نتیجه گیری این تحقیق می پردازد.

2. مقدمات و فرضیات

ارتباط در VANET به سه نوع ارتباط OBU2RSU بین OBU و RSU –که در جاده قرار دارد–، ارتباط OBU2OBU بین OBU and RSU2RSU تقسیم می شود. معمولا ساختار این نوع پیامها، نیازمند فرایند احراز

هویت OBU and RSU در شبکه است. این گفته بدین معنی می باشد که OBU وRSU ها، توسط شخص ثالث و در مقداردهی اولیه VANET تایید می شوند (تصویر 1a). همچنین این ساختار ارتباطی، نیازمند چندین پیام ارتباطی جهت حفظ گواهی، بعد از تعیین احراز هویت است.

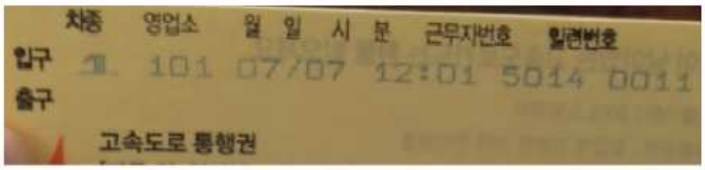
برای احراز هویت، داشتن چندین ارتباط با CA ضروری است. اگر طرح امنیتی، فعالیت های احراز هویت را به حداقل رساند، کاهش حجم ارتباطی میان RSU2RSU, RSU2OBU and OBU2OBU کافی است. برای کاهش پیام ارتباطی، و حفظ احراز هویت، دو ایده را در نظر می گیریم، همانند 1. RSU استفاده شده اولی به جای CA، همچون عوارضی در شاهراه و 2. فرایند احراز هویت دوره ای در RSU (تصویر 1b).



تصویر 1. VANET a. محیط کلی b. محیط پیشنهادی

زمانیکه به شاهراه می رسیم، هر کسی باید با استفاده از کارت hi-pass یا بلیط عبور (تصویر 2) از عوارضی رد شود. ما قادر به فهم زمان ورود، شماره ورودی و شماره نوبت هستیم. سیستم رمزگذاری مبتنی بر ID، توسط Adi Shamir و با استفاده از مشکل فاکتورگیری عدد صحیح پیشنهاد شد. سیستم احراز هویت مبتنی بر ID، طرح موثری برای VANET است که نیازمند ذخیره و تایید کلید عمومی با CA نیست. در این اثر، از شماره کارت hi-pass و شماره پلاک مجوز، به هنگام عبور از عوارضی شاهراه استفاده کردیم (تصویر 2a.b).

برای احراز هویت OBU در VANET، دو فرایند زیر را برای ارتباط RSU-OBU ارائه می دهیم: 1. احراز هویت OBU، بعنوان شماره معتبر RSU متناظر و 2. تحویل پیام به OBU امضا شده توسط RSU. این بدین معنی می باشد که مرحله اول، مرحله ثبت OBU به RSU و مرحله دوم، مرحله احراز هویت در دوره زمانی، جهت حفظ وضعیت احراز هویت می باشد. براساس این مفاهیم، رابطه بین RSU و OBU را در تصویر 3 نشان می دهیم.



(a)

(b)

تصویر2. نمونه بلیط و کارت شاهراه a. بلیط b. کارت hi-pass

3. احراز هویت VASS

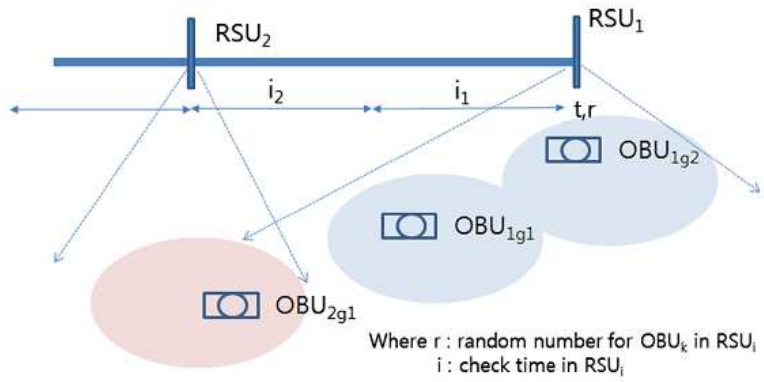
طرح امنیت احراز هویت وسیله نقلیه VASS در شاهراه که در این تحقیق پیشنهاد شد، شامل فرایند احراز هویتRSU توسط OBU ورودی به گروه و فرایند احراز هویت دوره ای OBU تاییدی در ارتباط OBU2RSU می باشد. بعد از احراز هویت اولیه، ضروری است که OBU، از طریق فرایندهای احراز هویت دوره ای و در دوره های زمانی معین، نسبت به تهدید امنیتی حاضر شود.

زمانیکه خودرو با استفاده از شماره کارت hi-pass و OBU-id از عوارضی رد شد، OBU در RSU ثبت می شود. اگر ID و شماره ثبت شده OBU به محض بررسی RSU یکسان بودند، پیام جهت احراز هویت به OBU ارسال می شود. با این حال، اگر متفاوت باشند، OBU را نمی توان احراز هویت کرد. همچنین، TPD، شماره کارت OBU-id, Hi-pass و پسورد را در OBU ذخیره می کند. جدول 1، مفاهیم استفاده شده در این مقاله را نشان می دهد.

در این بخش، به توصیف VASS برای محیط ارتباطی V2I در VANET می پردازیم. VASS دو رویکرد اصلی دارد که شامل فرایند احراز هویت اولیه و فرایند احراز هویت دوره ای است.

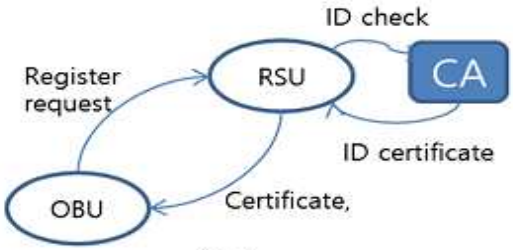
3.1 فرایند احراز هویت اولیه

برای مدیریت احراز هویت موثر اولیه OBU، RSU شماره OBU را به سطح معینی تنظیم می کند.

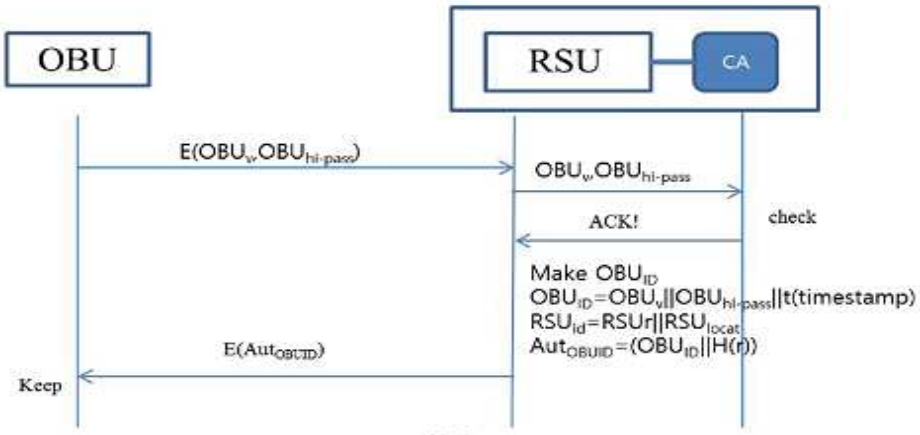


تصویر3. ارتباط بین RSU و OBU

OBU، ID خود را به محض رفتن به گروه RSU، RSU تحویل می دهد. OBU، ID، t و r را با استفاده از کلیدهای باز RSU رمزگشایی می کند که تنها برای OBUهایی با IDهای نرمال از هستند و بعد از رمزگذاری مقادیر و کلیدهای رمزی آنها در کلیدهای باز RSU، به RSU ارسال می کند. RSU اطلاعات حاصل از OBU را با کلید رمزی خود منتشر می کند و اگر ID, t and r دریافتی در ثبت اولیه، مشابه باشند، RSU کلید رمزی OBU را ذخیره کرده و آن را در مرحله احراز هویت دوره ای بعدی استفاده می کند (تصویر 4a,b).



(a)



(b)

تصویر4. فرایند احراز هویت اول a. اتومات احراز هویت اول b. پروتکل احراز هویت اول

فرایند احراز هویت اولیه بصورت زیر است:

1. RSU، OBUv and OBUhi−pass و پسورد را دریافت کرده و برای تایید به CA ارسال می کند

2. CA در RSU، OBUv and OBUhi−pass را بررسی می کند و اگر صحیح باشد، پیام ACK را به RSU ارسال می کند.

3. RSU ، OBUid را بصورت زیر ایجاد می کند:

$$OBUid = OBUv||H(OBUhi\text{-}pass)||t(TIMESTAMP)$$

4. RSU، RSUI مبتنی بر RSUR (شماره نوبت RSU) و RSUlocat (محل) را ایجاد می کند

$$RSUid = RSUR||RSUlocat$$

5. RSU، $AutOBUID = (OBUID||\ H(r))$ را ایجاد کرده و برای احراز هویت به OBU ارسال می کند

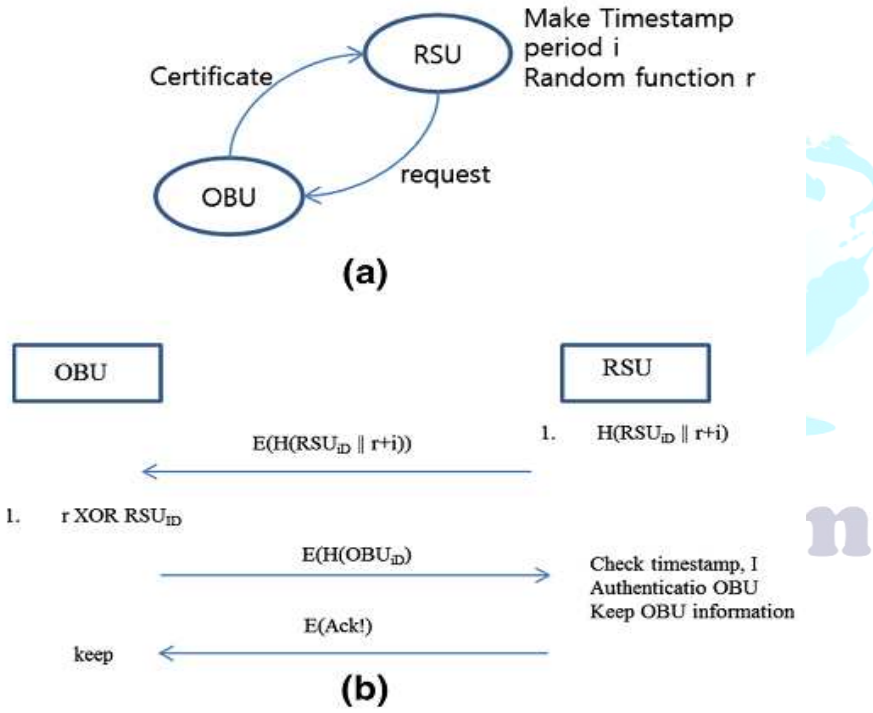
جدول 1 : نشانه‌ها در این مطالعه

نشانه ها	تعریف
E	رمزگذاری
D	رمزگشایی
OBU_V	تعداد وسایل نقلیه OBU
$OBU_{Hi\text{-}Pass}$	شماره پاسپورت OBU
H	تابع هش
t	تمبر زمان
r	عدد تصادفی
i	زمان دوره
RSU_r	شناسه‌ی RSU

3.2 فرایند احراز هویت دوره ای

جهت حفظ احراز هویت از RSU، OBU باید گواهی دوره ای را از RSU کسب کند. برای این مسئله، RSU باید احراز هویت OBU را در دوره زمانی i بعد از پذیرش احراز هویت اولیه، براساس مهر زمان اولیه و تابع هش r بررسی کند. درهر دوره زمانی، OBU باید اطلاعات TPD همچون شماره ID, hi-pass، و مهرزمان را به RSU ارسال کند. با این حال، اگر مقادیر متفاوت باشند، OBU باید از گروه RSU حذف شود چون OBU در معرض تهدید امنیتی قرار دارد (تصویر 5a,b).

فرایند دقیق احراز هویت اول، بصورت زیر است:



تصویر 5. رویکرد احراز هویت دوره ای a. اتوماتای احراز هویت دوره ای b. فرایند احراز هویت دوره ای

1. بعد از اینکه عدد تصادفی کوتاه تولیدی r از تابع هش H(RSUID||r + i) استفاده کرد، RSU پیامی به OBU می فرستد

2. OBU تابع هش r را دریافت کرده، r XOR RSUID را تولید کرده و H(OBUID) را به RSU ارسال می کند

3. RSU برای احراز هویت، OBUID را بررسی می کند. اگر OBU عضو قانونی باشد، به مرحله 4 بروید در غیراینصورت، OBUID را حذف کنید.

4. OBU، $H(r(RSUID||r + i)$ را دریافت می کند.

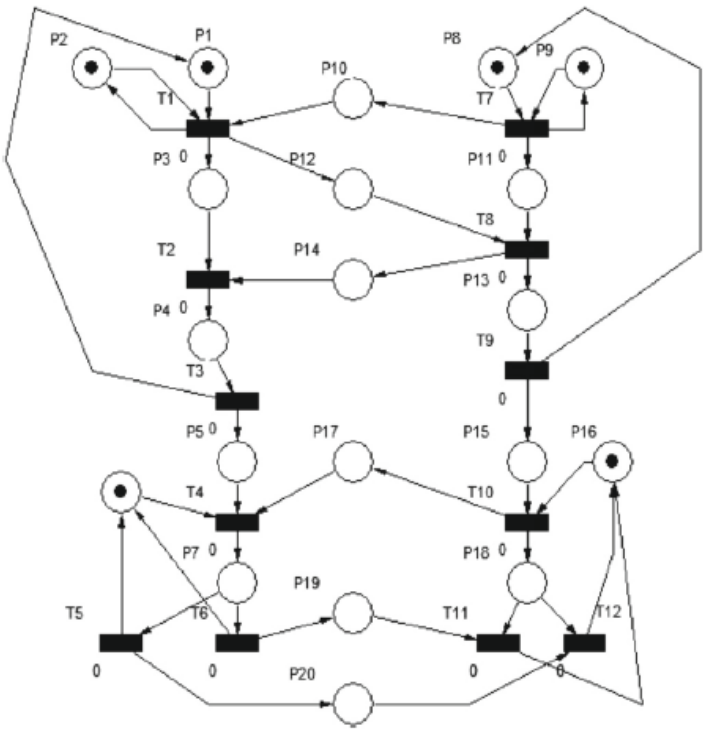
4. تایید مدل پیشنهادی با استفاده از شبکه های پتری

4.1 تایید

شبکه های پتری، کاربرد گسترده ای در زمینه های مختلف، به خاطر سادگی و قابلیت انعطاف آنها در نمایش رفتارهای سیستم پویا دارند. معنی شناسی همزمان آسنکرون آنها، با سیستم های فیزیکی مورد نظر، تطابق دارد. برای مثال، برای توصییف معماری، خدمات و پروتکل شبکه بسیار مناسب می باشند. شبکه های پتری دارای مزایایی در مدلسازی، تحلیل و تایید ناشی از نمایش گرافیکی بصری و نظریه ریاضی دقیق و تکنیک های تحلیلی و ابزار هستند.

در بخش قبل، VASS را برای OBU و RSU در VANET پیشنهاد دادیم. حالا می خواهیم مکانیسم خود را که از شبکه های پتری استفاده می کنند، تایید کنیم. براساس VASS بالا، مدل پتری متناظر در تصویر 6 تایید شد و مکان ها و انتقال ها در جدول 2 ارائه شده اند.

ما از VisObjNet برای تحلیل مدل VASS در IBM-PC با محیط ویندوز 8 استفاده کردیم. مدل پیشنهادی ما می تواند قابل دسترس بودن و زنده بوند را تامین کند. همانگونه که نتیجه شبیه سازی بالا نشان می دهد، می توان دریافت که فرایند احراز هویت OBU و فرایند احراز هویت دوره ای OBU در مدخل اولیه وسیله نقلیه OBU به گروه RSU اجرا می شوند. بعلاوه، موقعیت های مشکل زای متعدد در طول فرایند احراز هویت، همچون قدرت امنیت در احراز هویت خودرو، در شبکه ادهاک وسیله نقلیه را می توان از طریق بسامد وضعیت احتراق t4, t5, t7 and t10 مشخص کرد.



تصویر 6. مدل شبکه پتری VASS

جدول 2. لیستی از مکان های و انتقال ها در مدل پتری VASS

نشانه‌ها	مکان‌ها
RSU محل اولیه	P1
محل کار	P2
در حال انتظار	P3
را نگه دارید OBU اطلاعات	P4
در حال انتظار	P5
محل کار	P6
OBU تأیید	P7
OBU محل اولیه	P8
محل کار	P9
شماره واحد	P10
در حال انتظار	P11
ACK	P12
در حال انتظار	P13
RSU_pri (r، t شماره واحد،	P14
	P15
	P16

در حال انتظار محل کار برای احراز هویت OBU_pub (شماره واحد، t ،r + l) محل کار تأیید بله تأیید نکردن	P17 P18 P19 P20
نشانه‌ها	انتقال‌ها
دریافت شماره واحد OUU تایید شماره واحد OBU OBU اطلاعات اطلاعات مدت زمان دریافت شده اطلاعات را تأیید کنید نه اطلاعات را تأیید کنید بله ارسال شماره واحدOBU دریافت اطلاعاتRSU زمان انتظار ارسال احراز هویت مدت زمان درخواستi تأیید بله تأیید نکردن	t1 r2 t3 T4 T5 T6 T7 T8 T9 T10 T11 T12

4.2 تحلیل

در این بخش، درباره تحلیل امنیت و سربار محاسبه مکانیسم پیشنهادی بحث می کنیم.

4.2.1 تحلیل امنیت

این مکانیسم از رمزنگاری مبتنی بر ID و براساس شماره OBU ID و شماره کارت و پسورد Hi-pass استفاده کرد.

جدول 3. سربار محاسبه

	ثبت	احراز هویت
PPAS[8]	n(3Ch)	9Ch+2Cr+2CXOR
Ashritha [17]		3Ch+2Cr+2CXOR
VASS		2Ch+2Cr+CXOR

Ch هزینه تابع هش، Cxor هزینه اجرایی XOR، Cr هزینه تعداد تصادفی، n تعداد OBUها در VANET از آنجاییکه RSU با CA، شماره Hi-pass از قبل ثبت شده و پسورد را برای OBU-ID and TPD تایید می کند، مکانیسم دربرابر مسائل امنیتی و حریم خصوصی امن خواهد بود. بعد از احرازهویت و اعتبار OBU اول توسط RSU، OBU بصورت دوره ای تایید خواهد شد. این سیستم، امنیت احراز هویت OBU را تضمین می کند. ارتباط بین OBU and RSU نسبت به حمله کنندگان Sybil امن خواهد بود چون RSU ، مهر زمان جدیدی دارد.

4.2.2 سربار محاسباتی

سربار محاسباتی VASS و روشهای قیاسی [8،17] در جدول 3 نشان داده شده است.

VASS که مکانیسم پیشنهادی است، یکی از موثرترین مکانیسم ها در تلاش محاسباتی، به جای روشهای دیگر مسئله تابع هش می باشد.

5. نتیجه گیری

طرح امنیت احراز هویت وسیله نقلیه VASS در شاهراه، با استفاده از الگوریتم رمزگذاری شده و اعداد تصادفی زمان، برای احرازهویت دوجانبه، در این مقاله پیشنهاد شده و از شبکه پتری استفاده کرد. مدلسازی شبکه پتری، مقابله با تعریف و اجرای درخواست های امنیتی در VANET را ممکن می سازد. نتایج عملکرد نشان می دهند که تلاش محاسباتی، در تابع هش، بیش از روشهای دیگر است و VASS دارای اولویت های امنیتی همچون حریم خصوصی، احراز هویت و حمله Sybil است. در اثر آینده، طرح خود برای وسیله نقلیه، برای ارتباط زیرساختار مبتنی بر کاهش هزینه و حجم پیام ارتباطی را بسط خواهیم داد.

References

1. Zhang, C., Lin, X., Lu, R., Ho, P.H., Shen, X.: An efficient message authentication scheme for vehicular communications. IEEE Trans. Veh. Technol. **57**(6), 3357–3368 (2008)
2. Biswas, S., Tatchikou, R., Dion, F.: Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety. Proc. IEEE Commun. Mag. **44**(1), 74–82 (2006)

3. Sun, X., Lin, X., Ho, P.-H.: Secure Vehicular Communications Based on Group Signature and ID-based Signature Scheme. In: Proceedings of International Conference on Communications ICC 2007, pp. 1539–1545 (2007)
4. Li, C.-T., Hwang, M.-S., Chu, Y.-P.: A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. Comput. Commun. **31**, 2803–2814 (2008)
5. Eiza, M-H., Ni, Q.: A reachability-Based Routing Scheme for Vehicular Ad Hoc Networks, In: Proceedings of the 11th IEEE ICTSPCC, pp. 1578–1584 (2012)
6. Biswas, S., Misic, J.: Proxy Signature-based RSU Message Broadcasting in VANET. In: Proceedings of the 25th Biennial Symposium On Communication, pp. 5–9 (2010)
7. Hesham, A., A-Hanid, A., El-Nasr, M.A.: A Dynamic Key Distribution Protocol for PKI-based VANETs. In: Proceedings of the Wireless day, IFIP, pp. 1–3 (2011)
8. Chuang, M-C., Lee, J-F: PPAS: A Privacy Preservation Authentication Scheme for Vehicle-to-Infrastructure Communication Networks. In: Proceedings CECNet, pp. 1509–1512 (2011)
9. Raya, M., Hubaux, J.P.: Securing vehicular ad hoc networks. J. Comput. Secur. **15**(1), 39–68 (2007)
10. Lu, R., Lin, X., Zhu, H., Ho, P-H., Shen, X.: ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications. In: IEEE INFOCOM, pp. 1229–1237 (2008)
11. Zhang, C., Lin, X., Lu, R., Hp, P-H: RAISE: An Efficient RSU-Aided Message Authentication Scheme in Vehicular Communication Networks. In: IEEE ICC, pp. 1451–1457 (2008)
12. Peterson, J.L.: Petri Net Theory and the Modeling of Systems. Prentice-Hall, Englewood Cliffs (1981)
13. Shamir, A.: Identity Based Cryptosystems and Signature Schemes. In: CRYPTO 1984, pp. 47–53 (1984)
14. Biswas, S., Misic, J., Misic, V.: ID-Based Safety Message Authentication for Security and Trust in Vehicular Networks. In: 31th ICDCS 2011, pp. 323–331 (2011)
15. Murata, T.: Petri nets: properties, analysis and applications. Proc. IEEE **77**, 541–580 (1989)
16. Gniewek, L., Kluska, J.: Hardware implementation of fuzzy Petri net as a controller. J. IEEE Trans. Syst. Man. Cybern. Part B Cybern. **34**(3), 1315–1324 (2004)
17. Ashritha, M., Sridhar, C.S.: RSU Based Efficient Vehicle Authentication Mechanism for VANETs. In: IEEE ISCO 2015, pp. 1–5 (2015)