احراز اصالت در شبکه های اقتضایی خودرویی

(VANET)

میترا کاظمی دیزج

mkazemi994@yahoo.com

سرفصل ها

- مقدمه
- ارائه یک طرح متقارن
- ارائه طرح بر مبنای یک افزاره غیر قابل نفوذ
- نتیجه گیری
- مراجع

سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

علل پیدایش شبکه های اقتضایی بین خودرویی

مدیریت حمل و نقل ←
- کنترل ترافیک
- کاهش سوانح و تصادفات
- رفع آلودگی

جمع آوری اطلاعات
- عدم دریافت اطلاعات
- تاخیر در دریافت اطلاعات
- دریافت اطلاعات نامعتبر

سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

علل پیدایش شبکه های اقتضایی بین خودرویی

مدیریت حمل و نقل ←

- کنترل ترافیک
- کاهش سوانح و تصادفات
- رفع آلودگی

جمع آوری اطلاعات

- عدم دریافت اطلاعات
- تاخیر در دریافت اطلاعات
- دریافت اطلاعات نامعتبر

سرفصل ها

مقدمه

طرح متقارن

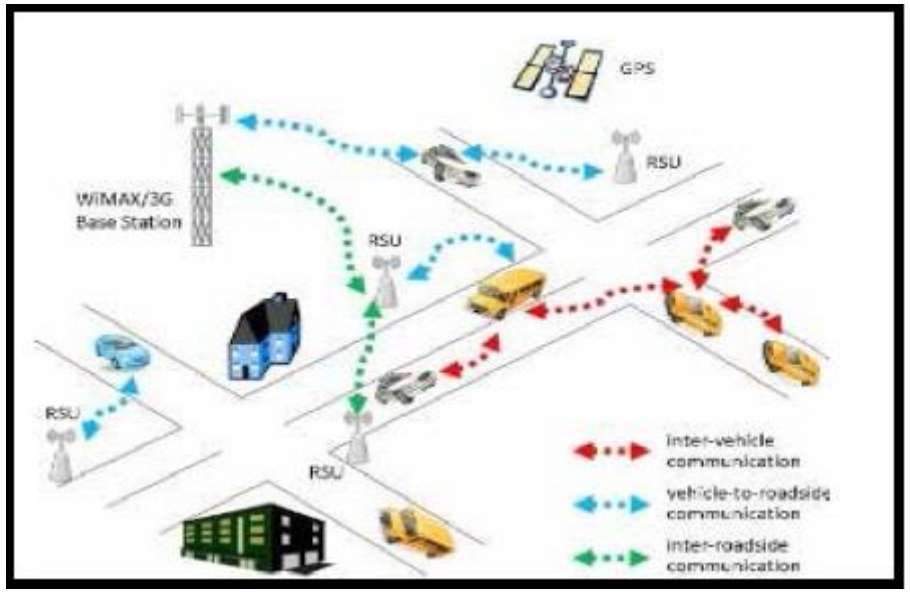
طرح بر مبنای TPD

نتیجه گیری

مراجع

معماری شبکه

- **TA(Trusted Authority): تولید پارامتر های سیستم، ثبت نام خودرو ها، شناسایی متخلفین در صورت لزوم**
- **OBU(On Board Unit): ارتباط با سایر OBU ها و RSU ها و ارسال پیام**
- **RSU(Road Side Unit): توسیع شبکه، ارسال اطلاعات، برقراری ارتباط اینترنتی**

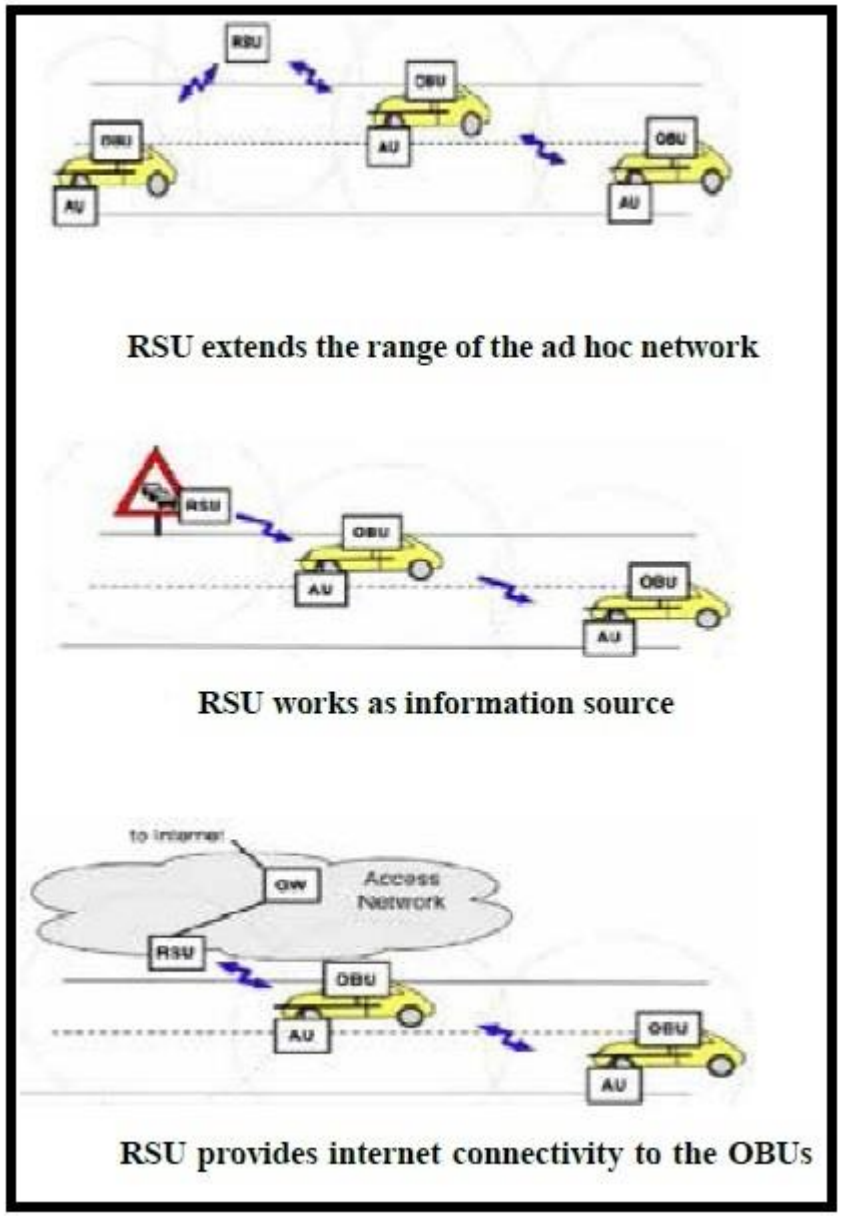


(2016). A threshold anonymous authentication protocol for VANETs. IEEE Transactions on vehicular technology

سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

معماری شبکه

- TA(Trusted Authority): تولید پارامتر های سیستم، ثبت نام خودرو ها، شناسایی متخلفین در صورت لزوم
- OBU(On Board Unit): ارتباط با سایر OBU ها و RSU ها و ارسال پیام
- RSU(Road Side Unit): توسیع شبکه، ارسال اطلاعات، برقراری ارتباط اینترنتی



سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

مقدمه

سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

ارتباطات شبکه

- V-2-V ← تبادل داده هایی به منظور مسیر یابی یا اعلام هشدار
- V-2-I ← داده هایی به منظور انتقال شرایط جاده، حجم خودرو ها، شرایط جوی،...

ویژگی های شبکه

- توپولوژی پویا
- ارتباطات Real-time
- محیط های ارتباطی متفاوت
- توان محاسباتی بالا
- شبکه مقیاس بزرگ

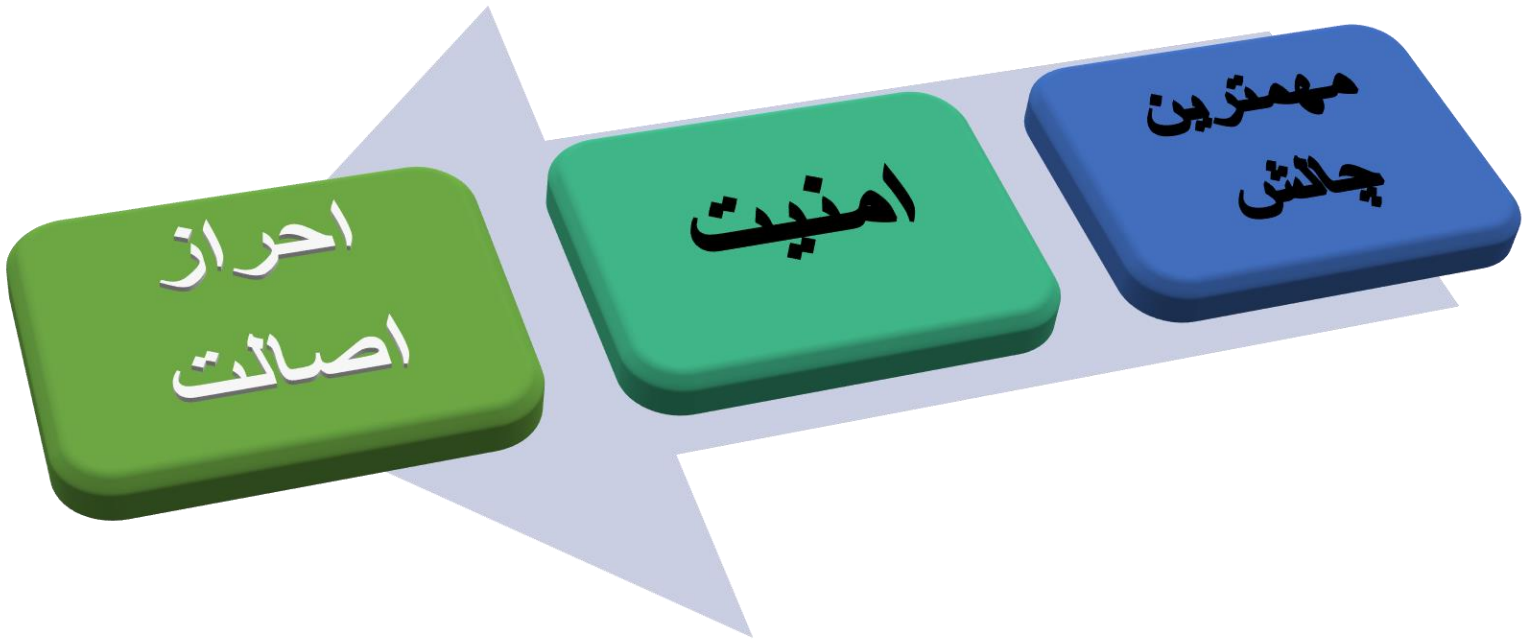
سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

چالش ها

- الگوریتم مسیر یابی مناسب
- ارتباطات
- مقیاس پذیری
- معماری
- امنیت
  - احراز اصالت
  - حفظ مشروط حریم خصوصی
  - محرمانگی
  - شناسایی متخلفین
  - مقاومت در برابر حملات

سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

پرداختن به مهم ترین چالش VANET



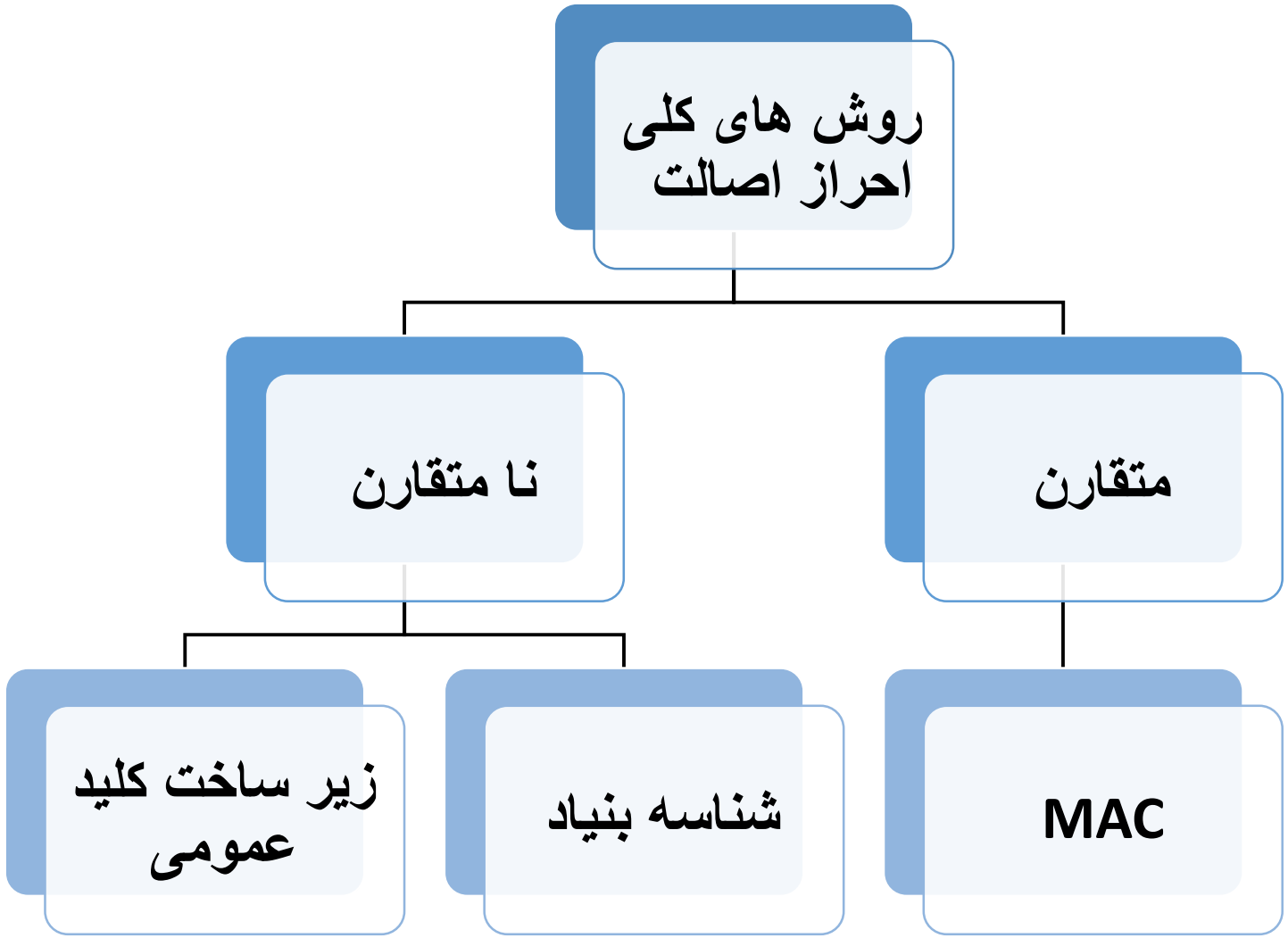
سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

حملات

- **DOS:** کنترل مهاجم بر منابع خودرو، مخدوش نمودن کانال ارتباطی، جلوگیری از عبور اطلاعات ضروری
- **جعل هویت:** ورود به شبکه با شناسه نادرست
- **حمله Sybil:** جعل هویت تعداد زیادی از خودرو ها
- **حمله تغییر:** تغییر پیام های منتشر شده
- **آشکار سازی شناسه:** دسترسی به اطلاعات هویتی فرستنده
- **پیگیری جغرافیایی:** دنبال کردن موقعیت مکانی فرستنده

سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

روش های کلی احراز اصالت



سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

طراحی پروتکل کارا

ارائه پروتکل کارا

- معماری مناسب
- در نظر گرفتن ویژگی های مطلوب
- رفع چالش های پیش رو
- در نظر گرفتن حمله های ممکن

سرفصل ها

مقدمه

طرح متقارن

طرح بر مبنای TPD

نتیجه گیری

مراجع

سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

- روش کلید عمومی ⟵ بار محاسباتی زیاد

اهداف طرح RAISE

- یکپارچگی پیام
- احراز اصالت فرستنده
- سربار محاسباتی کم
- وارسی سریع
- گمنامی جزئی

سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

مراحل پروتکل ←

- تولید کلید
- تولید MAC
- وارسی پیام های دریافتی

سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

احراز اصالت دو سویه میان خودرو و RSU و تولید کلید

$V_i \rightarrow RUS: \quad \{g^a | C_{vi}\}_{PK_R}$

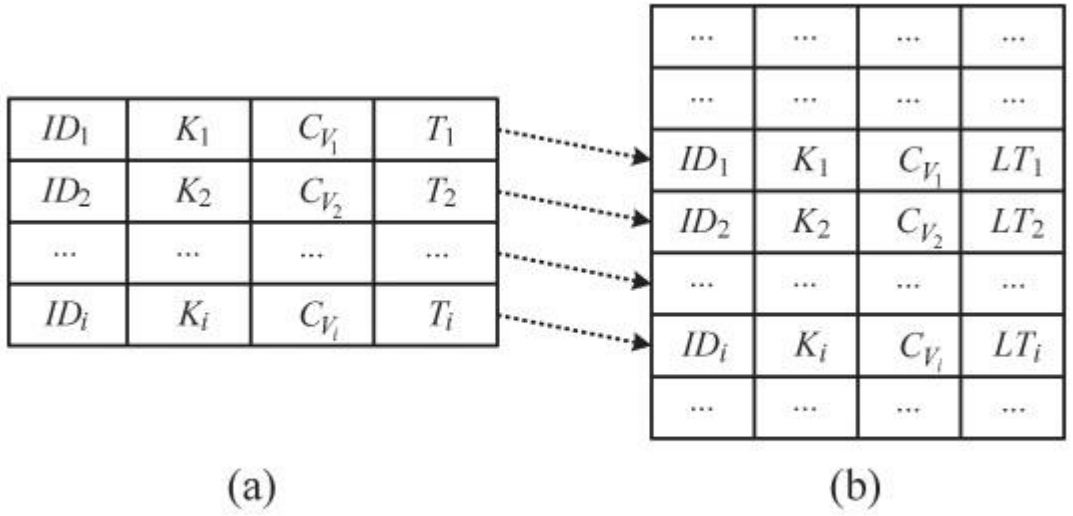
$RUS \rightarrow V_i: \quad ID_i \mid g^b \mid \{ID_i \mid g^a | g^b\}_{SK_R}$

$V_i \rightarrow RUS: \{ID_R \mid g^a | g^b\}_{K_i}$

$$K_i = g^{ab}$$

سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

تولید کلید



(a) ID-Key table. (b) Trace evidence table.

"An efficient message authentication scheme for vehicular communications." *IEEE Transactions on Vehicular Technology* 57.6 (2008): 3357-3368.

سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

تولید MAC

خودرو :

- تولید برچسب پیام توسط کلید
- الحاق به پیام
- ارسال پیام به RSU

$$< ID_i \parallel M_i \parallel TS_i \parallel MAC_{ki}(ID_i \parallel M_i \parallel TS_i) >$$

سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

RSU :

- استخراج کلید فرستنده از جدول
- بررسی صحت MAC موجود در پیام
- جمع آوری تمام پیام های دریافتی
- امضای پیام های دریافتی
- ارسال به خودرو

$$< \mathbf{H} \parallel \{H\}_{SK_R} >$$

$$H =< \mathbf{MAC_{k1}(ID_1 \parallel M_1 \parallel TS_1) \parallel MAC_{k2}(ID_2 \parallel M_2 \parallel TS_2)} \parallel \cdots \parallel \mathbf{MAC_{kn}(ID_n \parallel M_n \parallel TS_n)} >$$

سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

خودرو :

- ذخیره پیام های دریافتی از سایر خودروها بدون وارسی
- بررسی صحت H دریافتی از RSU
- وارسی پیام M_i ⟵ بررسی وجود M_i در H دریافتی

سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

نتیجه گیری طرح متقارن

- بهبود روند احراز اصالت
- کاهش سربار محاسباتی
- گمنامی جزئی هر خودرو

سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

- راه اندازی اولیه سیستم
- ارسال پیام
- وارسی پیام
- شناسایی متخلفین

سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

- مرجع مورد اعتماد، تولید گروه دوری G با مرتبه عدد بزرگ اول q
- تولید کلید خصوصی سیستم به صورت $x \in_r Z_q^*$

TPD

X ID_0	$H(.)$ $MAC(.)$

سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

ارسال پیام

- تولید ID_i و t توسط افزاره غیر قابل نفوذ و ارسال برای خودرو
- ارسال message توسط خودرو

$$ID_i=H^i(ID_0 \| T \| x)$$

$$t=MAC_x(M \| ID_i \| i)$$

$$message=\{t \| M \| ID_i \| T \| i\}$$

سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

وارسی پیام

- تولید $t'=MAC_X(M \| ID_i \| i)$ و مقایسه آن با t دریافتی از پیام

شناسایی متخلفین

- جستجو روی ID_0 در پایگاه اطلاعاتی خود طبق رابطه ی زیر

$$ID_i=H^i(ID_0 \| T \| x)$$

پیشنهادهایی برای پژوهش های آتی

- بررسی چگونگی استفاده از طرح‌های پساکوانتومی با کارایی قابل قبول
- افزودن قابلیت وارسی دسته‌ای پیام‌ها به طرح جدید ارائه شده
- استفاده از بلاکچین در VANET

سرفصل ها
مقدمه
طرح متقارن
طرح بر مبنای TPD
نتیجه گیری
مراجع

منابع

- Oulhaci, T., Omar, M., Harzine, F., & Harfi, I. (2016). Secure and distributed certification system architecture for safety message authentication in VANET. *Telecommunication Systems*, 1-16.
- Dixit, M., Kumar, R., & Sagar, A. K. (2016, April). VANET: Architectures, research issues, routing protocols, and its applications. In *Computing, Communication and Automation (ICCCA), 2016 International Conference on*(pp. 555-561). IEEE.
- Pourkiani, M., Jabbehdari, S., & Khademzadeh, A. (2016). Vehicular Networks: A Survey on Architecture, Communication Technologies and Applications. *Journal of Advances in Computer Engineering and Technology*, *2*(3), 43-53.
- Ayyappan, B., & Kumar, P. M. (2016, March). Vehicular Ad Hoc Networks (VANET): Architectures, methodologies and design issues. In *Science Technology Engineering and Management (ICONSTEM), Second International Conference on* (pp. 177-180). IEEE.
- Azees, M., Vijayakumar, P., & Deboarh, L. J. (2017). EAAP: Efficient Anonymous Authentication With Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks. IEEE Transactions on Intelligent Transportation Systems.
- He, D., Zeadally, S., Xu, B., & Huang, X. (2015). An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Transactions on Information Forensics and Security, 10(12), 2681-2691.
- Kazemi, mitra, Mahshid Delavar, Javad Mohajeri, Mahmoud Salmasizadeh. 2018. “On the security of an Efficient Anonymous Authentication With Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks”, 26th Iranian Conference on Electrical Engineering (ICEE2018)

سرفصل ها

مقدمه

طرح متقارن

طرح بر مبنای TPD

نتیجه گیری

مراجع


سپاس از حسن توجه شما