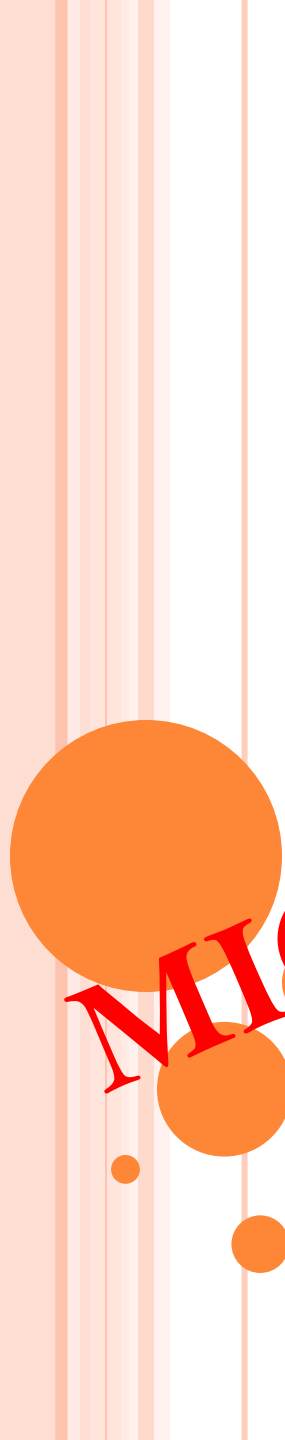


**EAAP: EFFICIENT ANONYMOUS  
AUTHENTICATION WITH  
CONDITIONAL PRIVACY-  
PRESERVING SCHEME FOR  
VEHICULAR AD HOC NETWORKS**

**MICANS INFOTECH**



# ABSTRACT

- Providing an efficient anonymous authentication scheme in vehicular ad hoc networks (VANETs) with low computational cost is a challenging issue.
- Even though, there are some existing schemes to provide anonymous authentication, the existing schemes suffer from high computational cost in the certificate and the signature verification process, which leads to high message loss.



- Therefore, they fail to meet the necessity of verifying hundreds of messages per second in VANETs. In our scheme, we propose an efficient anonymous authentication scheme to avoid malicious vehicles entering into the VANET. In addition, the proposed scheme offers a conditional tracking mechanism to trace the vehicles or roadside units that abuse the VANET. As a result, our scheme revokes the privacy of misbehaving vehicles to provide conditional privacy in a computationally efficient way through which the VANET entities will be anonymous to each other until they are revoked from the VANET system.



# EXISTING SYSTEM

- Usually, many existing schemes were designed to solve the security issues of VANETs based on a public key infrastructure (PKI).
- In the PKI based schemes, each vehicle user uses a pair of cryptographic keys, namely, a public key and a private key.
- The strength of the PKI schemes mainly depends on the computational impracticality of a properly generated private key from its corresponding public key.



- The vehicle user keeps the private key in the vehicle in a secret manner, whereas the public key is known to everyone, which is issued by a TA. The most commonly used two PKIs are Rivest, Shamir, and Adleman(RSA)-based PKI and the elliptic curve cryptosystem (ECC)-based PKI . Due to smaller key size and lower computational costs, the ECC-based PKI anonymity schemes are better than the RSA-based PKI schemes.



# PROPOSED SYSTEM

- 1) In order to minimize the computational cost, we have developed a computationally efficient anonymous authentication scheme for both vehicles and RSUs in our scheme.
- 2) To minimize the certificate and signature verification cost for providing efficient data integrity, which is suitably required for VANETs.
- 3) To minimize the message loss ratio during the message communication that takes place between the RSUs and vehicles.



- 4) To develop a computationally efficient conditional tracking mechanism to revoke the vehicles or RSUs that abuse the VANET.

**MICANS INFOTECH**



# HARDWARE REQUIREMENTS

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

**MICANS INFOTECH**





# SOFTWARE REQUIREMENTS

- Operating system : Windows XP/7.
- Coding Language : ASP.net, C#.net /java

**MICANS INFOTECH**



# CONCLUSION

- In this paper, we have proposed a new scheme called EAAP for secure vehicular communication in VANETs. In the proposed EAAP scheme, an RSU can effectively authenticate vehicles in an anonymous manner before providing LBSI messages to vehicles.
- Similarly, vehicles can also authenticate an RSU in an anonymous manner before receiving LBSI messages from RSUs. EAAP scheme not only provides the anonymous authentication with low certificate and signature verification costs which are essentially required in the VANET applications.



- But also able to provide an efficient conditional privacy tracking mechanism to reveal the real identity of the malicious vehicle for enhancing the efficiency of the VANET system. The proposed EAAP scheme also provides better efficiency in terms of fast verification on certificates and signatures than the previously reported schemes BLS, ECPP, CAS, GSB and KPSD.



# REFERENCE

- [1] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, “Anonymity analysis on social spot based pseudonym changing for location privacy in VANETs,” in Proc. IEEE ICC, Kyoto, Japan, Jun. 2011, pp. 1–5.
- [2] X. Lin, R. Lu, C. Zhang, H. Zhu, P. H. Ho, and X. Shen, “Security in vehicular ad hoc networks,” IEEE Commun. Mag., vol. 46, no. 4, pp. 88–95, Apr. 2008.
- [3] I. Blake, G. Seroussi, and N. Smart, Advances in Elliptic Curve Cryptography (London Mathematical Society Lecture Note Series), vol. 317. Cambridge, U.K.: Cambridge Univ. Press, 2005.

