**Efficient Conditional Anonymity With Message Integrity and Authentication in a Vehicular Ad-Hoc Network**

**Abstract:**

 Vehicles in a vehicular ad-hoc network (VANET) broadcast beacons giving safety-related and traffic information. In an open-access environment, this means that the VANET is susceptible to security and privacy issues. In this paper, we propose a new pseudo-identity-based scheme for conditional anonymity with integrity and authentication in a VANET. The proposed scheme uses a pseudonym in the joining process with the road-side unit (RSU) to protect the real identity even from the RSU, in case it is compromised. All previous identity-based schemes have been prone to insider attackers, and have not met the revocation process. Our scheme resolves these drawbacks as the vehicle signs the beacon with a signature obtained from the RSU. Our scheme satisfies the requirements for security and privacy, and especially the requirements for message integrity and authentication, privacy preservation, non-repudiation, traceability, and revocation. In addition, it provides conditional anonymity to guarantee the protection of an honest vehicle's real identity, unless malicious activities are detected. It is also resistant to common attacks such as modification, replay, impersonation, and man-in-the-middle (MITM) attacks. Although the numerous existing schemes have used a bilinear pairing operation, our scheme does not depend on this due to the complex operations involved, which cause significant computation overhead. Furthermore, it does not have a certification revocation list, giving rise to significant costs due to storage and inefficient communication. Our analysis demonstrates that our scheme can satisfy the security and privacy requirements of a VANET more effectively than previous schemes. We also compare our scheme with the recently proposed schemes in terms of communication and computation and demonstrate its cost-efficiency and appropriateness in working with the VANET. Meanwhile, the computation costs of the beacon signing and verification in our scheme are reduced by 49.9%

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium Dual Core.
* Hard Disk : 120 GB.
* Monitor : 15’’ LED
* Input Devices : Keyboard, Mouse
* Ram : 1 GB

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows XP/UBUNTU.
* Implementation : NS2
* NS2 Version : 2.28
* Front End : OTCL (Object Oriented Tool Command  Language)
* Tool : Cygwin (To simulate in Windows OS)