„A Privacy Protocol for Car-to-X Communication based on Diffie-Hellman Group Keying“

Sinn, Zweck und Ziel:

Ich habe ein „Privacy Protocol“ entwickelt (Diplomarbeit), in der Fahrzeuge ihre Privatsphäre wahren können, sodass eine digitale Verfolgung vereitelt wird.

Ausgangssituation:

Car-to-X Kommunikation ist eine vielversprechende Technologie, wobei auch es viele Verwundbarkeiten gibt. Beispielsweise werden Mobilitätsdaten und Identitäten unklug und in klartext verteilt werden. Fahrzeuge, welche entsprechend ausgestattet sind, senden periodisch Mobilitätsdaten, sogenannte CAMs (Cooperative Awareness Messages oder Beacons).

Problemstellung:

Diese Beacons können durch Angreifer gesammelt und ausgewertet werden, um beispielsweise Bewegungsprofile zu erstellen. Diese könnten dann an Ordnungsämter, Mautstellenbetreiber, etc. verkauft werden. Kein Kraftwagenfahrer möchte dies, wenn er sich über die Folgen im klaren wäre! Weiterhin würde dieses Negativimage (wenn die Privatsphäre weiterhin gefährdet ist) die Verbreitung dieser Technologie schaden hemmen und die Verbreitung der Car-to-Car Kommunikation würde sich sehr schleppend entwickeln.

Lösungsvorschlag:

Ich habe ein „Privacy Protocol“ entwickelt, wo Fahrzeuge ständig zwischen mehreren Pseudonymen wechseln und ggf. Gruppen bilden, in der sie mittels dem „Successive (N-Parties) Diffie-Hellman Key Exchange“ Mechanismus ein gemeinsames Gruppenzertifikat generieren und alle mit diesem Gruppen-Zertifikat ihre Mobilitätsdaten verteilen. Innerhalb der Gruppe wäre Authentifikation und Integrität weiterhin geschützt. Zudem würde die Privatsphäre gestärkt, da keine individuellen Daten mehr verteilt würden, da ja alle mit einer gemeinsamen Indentität senden.

Innovationsgrad

Es wurde schon vorgeschlagen anonyme Gruppen zu bilden. Jedoch ist es schwer Vertrauen zu noch nie vorher kontaktiereten Fahrzeugen aufzubauen. Mein Diffie-Hellman Schlüsselaustausch verfahren gewährleistet dies, solange das „diskrete Logarithmus“ Problem nicht gelöst wurde. Weiterhin könnte man bei N Fahrzeugen paarweise Verbindungen aufbauen, welches dann N(N-1)/2 Paarungen ergibt. Wobei für eine Paarung mehrere Nachrichten ausgetauscht werden müssten! Mein Verfahren benötigt bei N Teilnehmern weniger als 2*(N-1)+N Nachrichten (ohne Paketverlust).

Reifegrad

Mein Protokoll wurde zur Zeit für vSimRTI mit JiST/SWANS unter Java entwickelt und wird bis dato nur erfolgreich (s. Anhang) simuliert (SUMO und vSimRTI), da es noch keine speziellen C2X-Kommunikationsmodule (Hardware) gibt. Somit kann man es als „Konzept“ einstufen. Mann müsste erstmal auf Hardware-Ebene solch eine Hardwaremodul für Fahrzeuge entwickeln, welche die Kommunikation erst ermöglicht. Mein Protokoll müste dann nur noch auf dem „Session Layer“ (siehe ISO OSI -Schicht) angepasst werden. SUMO = Simulation of Urban Mobility. vSimRTI = Vehicle-2-X Simulation Runtime Infrastructure.

Wirtschaftliches Potenzial

Laut [0] sterben jährlich in Europa 40.000 Menschen und 1.700.000 Menschen werden durch Unfälle verletzt. Der dabei entstandene Sachschaden beträgt 160 Mrd. Euro (!), das sind 2% des innereuropäischen BSP! C2X kann entscheidend dazu beitragen, Menschenleben zu retten und den Sachschaden zu begrenzen. Jedoch würde die vernachlässigte Privatsphäre die Akzeptanz des C2X in der Bevölkerung hemmen. Die Anonymität muss gewährleistet sein! [0] European Commission: Saving 20.000 lives on our roads, 2003. http://ec.europa.eu/transport/roadsafety_library/rsap/rsap_en.pdf - ISBN 92-894-5893

Erfüllung neuer Kundenwünsche

Fahrzeugführer allgemein.
1. Sicherheit in Verkehr.
2. Effiziente Verkehrsführung (ökonomisch).
3. Mehrwertdienste.

Weiterentwicklung des Erlebnis beim Fahren oder während des Aufenthalts im Fahrzeug

Mein Verfahren sichert die Privatsphäre des Fahrzeugführers / -halters.

Figure 1: A global scenario - ©2008 ETSI

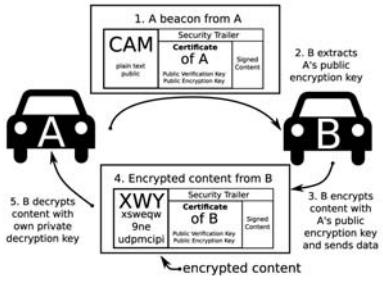

Figure 47: B sends enciphered data to A

Figure 70: Aimsun NG