A Surveying on Road Safety Using Vehicular Communication Networks

Padmavathi K
Asst. Professor,
Department of Computer Science,
PSG College of Arts and Science, Coimbatore.
E-mail:padhurajk@yahoo.com,

Maneendhar R
M.Phil., Research scholar,
Department of Computer Science,
PSG College of Arts and Science, Coimbatore.
E-mail:maneendhar@gmail.com

Abstract - Today's people are more and more concerned about their privacy and security. Vehicular communication (VC) systems have the potential to improve road safety and driving comfort. Vehicular communication based on wireless short-range technology enables spontaneous information exchange among vehicles and with road-side stations. A novel class of wireless networks that have emerged advances in wireless technologies and the automotive industry. This will enable the formation of vehicular networks, commonly referred to as VANETs, an instance of mobile ad hoc networks with cars as the mobile nodes. Security and privacy must be two primary concerns in the design of vehicular networks. Vehicular ad hoc networks (VANETs) are a specific type of self-organizing mobile ad hoc networks. So far, the security of Vehicular Communication applications has mostly drawn the attention of research efforts, accident prevention and post-accident investigation, while comprehensive solutions to protect the network operation have not been developed. In this paper, a brief analysis of vehicular communication using VANET's according to safety and security of drivers and travellers. In VANET's using Global Position based Routing.

Keywords: *vehicular communication, wireless sensor networks, accident prevention, post-accident investigation, Global Position based Routing (GPR), on board unit, road side unit, application units.*

I. INTRODUCTION

In order to make roads safer, cleaner and smarter, sensor and communication technologies are increasingly considered in research, standardization and development. Inter vehicle communication (IVC) is attracting considerable attention from the research community and the automotive industry, where it is beneficial in providing intelligent transportation system (ITS) as well as drivers and passengers' assistant services. The main goal of inter-vehicle communication technologies is to provide each vehicle with the required information about its surrounding in order to assist the driver avoiding potential dangers. The required information level, or awareness, can be achieved by the exchange of periodic status messages (beacons) among neigh boring vehicles together with the quick dissemination of information about potential hazards. Nowadays, road safety is one of the main concerns of the public opinion in developed countries. Several efforts have been started with the goal to improve road safety by means of intelligent systems.

In this context, vehicular ad hoc networks (VANETs) are emerging as a new class of wireless network, spontaneously formed between moving vehicles equipped with wireless interfaces that could have similar or different radio interface technologies, employing short-range to medium-range communication systems. A VANET is a form of mobile ad hoc network, providing communications among nearby vehicles and between vehicles and nearby fixed equipment on the roadside.

II. ARCHITECTURE

Recent advances in wireless technologies and the current and advancing trends in ad hoc network scenarios allow a number of deployment architectures for vehicular networks, in highway, rural, and city environments. Such architectures should allow communication among nearby vehicles and between vehicles and nearby fixed roadside equipment. Three alternatives include (i) a pure wireless vehicle-to-vehicle ad hoc network (V2V) allowing standalone vehicular communication with no infrastructure support, (ii) a wired backbone with wireless last hops that can be seen as a WLAN-like vehicular networks, (iii) and a hybrid vehicle to- road (V2R) architecture that does not rely on a fixed infrastructure in a constant manner, but can exploit it for improved performance and service access when it is available. In this latter case, vehicles can communicate with the infrastructure either in a single hop or multihop fashion according to the vehicles' positions with respect to the point of attachment with the infrastructure. Actually the V2R architecture implicitly includes V2Vcommunication. The in-vehicle domain refers to a local network inside each vehicle logically composed of two types of units: (i) an on-board unit (OBU) and (ii) one or more application unit(s) (AUs). An OBU is a device in the vehicle having communication capabilities (wireless and/or wired), while an AU is a device executing a single or a set of applications while making use of the OBU's communication capabilities. Indeed, an AU can be an integrated part of a vehicle and be permanently connected to an OBU.

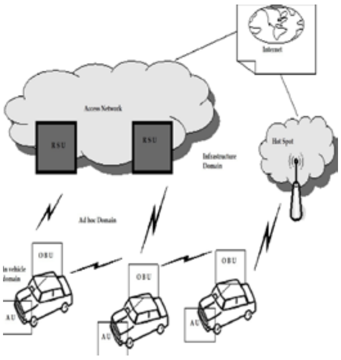


Figure 1.1: Vehicle to Vehicle Reference Architecture

It can also be a portable device such as a laptop or PDA that can dynamically attach to (and detach from) an OBU. The AU and OBU are usually connected with a wired connection, while wireless connection is also possible (using, e.g., Bluetooth, WUSB, or UWB). This distinction between AU and OBU is logical, and they can also reside in a single physical unit.

The ad hoc domain is a network composed of vehicles equipped with OBUs and road side units (RSUs) that are stationary along the road. OBUs of different vehicles form a mobile ad hoc network (MANET), where an OBU is equipped with communication devices, including at least a short-range wireless communication device dedicated for road safety. OBUs and RSUs can be seen as nodes of an ad hoc network, respectively, mobile and static nodes. An RSU can be attached to an infrastructure network, which in turn can be connected to the Internet. RSUs can also communicate to each other directly or via multihop, and their primary role is the improvement of road safety, by executing special applications and by sending, receiving, or forwarding data in the ad hoc domain.

Two types of infrastructure domain access exist: RSU and hot spot. RSUs may allow OBUs to access the infrastructure, and consequently to be connected to the Internet. OBUs may also communicate with Internet via public, commercial, or private hot spots (Wi-Fi hot spots). In the absence of RSUs and hot spots, OBUs can utilize communication capabilities of cellular radio networks (GSM, GPRS, UMTS, WiMax, and 4G) if they are integrated in the OBU.

III. IMPLEMENTATION OF VANET'S

Position-based routing provides multi-hop communication in a wireless ad hoc network. It assumes that every node knows its geographic position, e.g. by GPS, and maintains a location table with ID and geographic positions of other nodes as soft state. PBR supports geographic unicast (GeoUnicast), topologically-scoped broadcast (TSB, flooding from source to nodes in n-hop neighborhood), geographically-scoped broadcast (GeoBroadcast, packet transport from source to all nodes in a geographic area) and geographically-scoped anycast (same as GeoBroadcast, but to one of the nodes in the area). Basically, PBR comprises three core components: beaconing, a location service, and forwarding. Beaconing*:* Nodes periodically broadcast short packets with their ID and current geographic position. On reception of a beacon, a node stores the information in its location table.

Location Service: When a node needs to know the position of another node currently not available in its location table, it issues a location query message with the sought node ID, sequence number and hop limit. Neighboring nodes rebroadcast this message until it reaches the sought node (or the hop limit). If the request is not a duplicate, the sought node answers with a location reply message carrying its current position and timestamp. On reception of the location reply, the originating node updates its location table.

Geographic Unicast provides packet transport between two nodes via multiple wireless hops. When a node wishes to send a unicast packet, it first determines the destination position (by location table look-up or the location service). Then, it executes a greedy forwarding algorithm, sending the packet to its neighbor with the minimum remaining distance to the destination (most-forward-within-radius strategy [14]). The algorithm is executed at every node along the forwarding path until the packet reaches the destination.
Geographic Broadcast distributes data packets by flooding, where nodes re-broadcast the packets if they are located in the geographic area determined by the packet. Global position Routing updates on-the-fly the destination position and timestamp values in the packet header. Similarly, based on received packet headers with newer information, nodes update its location table.

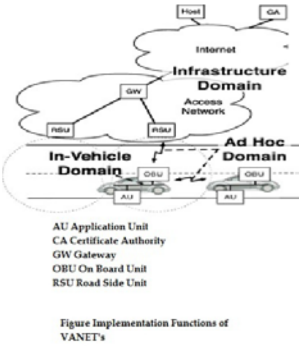
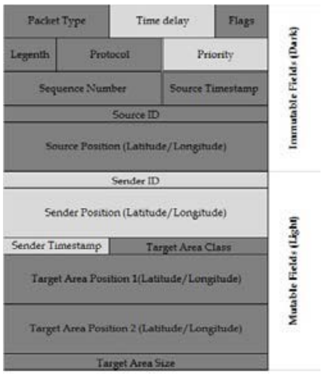


Figure 2: Implementation Functions of VANET's

GPR defines packet headers with fields for node ID, position and timestamp for a source, sender, and destination, and others. For GeoBroadcast, the header carries a destination area instead of a destination ID. For the header fields we distinguish between immutable and mutable fields. Immutable fields are not altered during forwarding, whereas mutable fields can be updated by forwarders (see the example GeoBroadcast header.



Packet Type | Time delay | Flags
Legenth | Protocol | Priority
Sequence Number | Source Timestamp
Source ID
Source Position (Latitude/Longitude)
Sender ID
Sender Position (Latitude/Longitude)
Sender Timestamp | Target Area Class
Target Area Position 1(Latitude/Longitude)
Target Area Position 2 (Latitude/Longitude)
Target Area Size

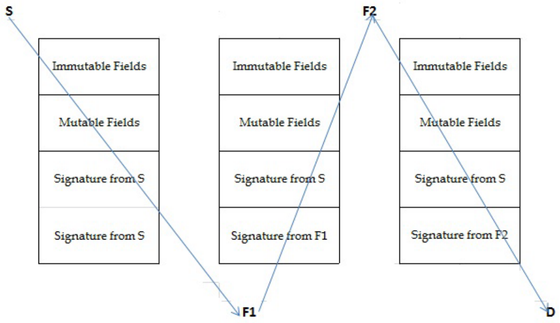
Figure 3: Mutable and Immutable Field's Types.

Data and control packet forwarding must be loop-free and towards the destination or target area location 4, having packets forwarded across the shortest path towards the destination is not a requirement due to the high network volatility.

The system should be robust against abuse of the position based communication services, in particular towards resource depletion. Abuses beyond the PBR functionality (e.g., data link or physical layer jamming) are out of scope. Gateway: Here, we describe attacks relevant to position based routing, to guide the design of security countermeasures. Attack trees provide a standardized method to classify attacks on a system: the root represents a general attack further refined in the tree structure using AND and OR logical connections. The complete attack tree analysis is out-of-scope.

IV. GLOBAL POSITION ROUTING SECURITY

We design mechanisms to safeguard the functionality of PBR, relying both on cryptographic primitives and plausibility checks, towards achieving the stated security objectives. We assume a public key infrastructure with a Certification Authority (CA) that issues public/private key pairs and certificates to vehicles. A certificate contains the node's public key, attributelist (e.g., to distinguish between RSUs, public emergency vehicles and regular vehicles), the CA identifier, the certificate lifetime, and the CA signature. We use asymmetric cryptography and digital signatures for all messages. In the case of beacons (one-hop communication) a single signature is applied, with the source signing the whole PBR packet. This is straightforward since there are no intermediate nodes which change PBR header fields. In contrast, for multi-hop communication, additional protection is necessary for the mutable fields in the GPR headers.



S-Source
F-Forwarder
D-Destination
Figure 4: Packet Holds a Sender Signature

V. CONCLUSION

In this paper, we proposed security architecture for VANETS.We have presented a solution to secure a global position-based routing protocol for wireless multi-hop communication in vehicular ad hoc networks.

After receiving one master key and a master certificate from the CA, the user can create his own certified pseudonyms without interaction with the CA.

The proposed secure geographical routing scheme provides protection of mutable and immutable fields in the data packet headers by combination of end-to-end and hop-by-hop signatures.

A main characteristic of the solution is its deployability due to usage of well-established security mechanisms. The integration in our experimental prototype for vehicular communication has shown a low implementation complexity. In a follow-up of this paper we will present a more detailed security analysis, additional plausibility checks, and protocol optimizations, as well as extensive experimental performance evaluation based on our test bed.

REFERENCES

1. B.N. Karp and H.T. Kung. GPSR: Greedy Perimeter Stateless Routing for Wireless Networks. In Proc. MobiCom, Boston, MA, USA, 2000.
2. H. F¨ußler, M. Mauve, H. Hartenstein, M. K¨asemann, and D. Vollmer. Location-Based Routing for Vehicular Ad-Hoc Networks. In MobiCom, 2002.
3. Festag, H. F¨ußler, H. Hartenstein, A. Sarma, and R. Schmitz. Fleet Net: Bringing Car-to-Car Communication into the Real World. In Proc. ITS World Congress, 2004. IEEE. Draft Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages. IEEE P1609.2/D3, 2005.
4. P. Papadimitratos, V. Gligor, and J.-P. Hubaux. Securing Vehicular Communications - Assumptions, Requirements and Principles. In Proc. ESCAR, 2006.
5. H. Fubler, M. Mauve, H. Hartenstein, C. Lochert, D. Vollmer, D. Herrmann, and W. Franz. Position-Based Routing in Ad-Hoc Wireless Networks. In Inter-Vehicle-Communications Based on Ad Hoc Networking Principles —The FleetNet Project, pages 117–143. Universit¨atsverlag, Karlsruhe, Germany, 2005.
6. M. Raya and J.-P. Hubaux. The Security of Vehicular Ad Hoc Networks. In Proc. of SASN 2005, pages 11–21, Alexandria, VA, USA, 2005.
7. J. P. Hubaux, S. Capkun, and J. Luo. The Security and Privacy of Smart Vehicles. IEEE Security and Privacy Magazin, 2(3):49–55, 2004.
8. K. Zeng. Pseudonymous PKI for Ubiquitous Computing. In Proc. of EuroPKI, pages 207–222, Turin, Italy, 2006.
9. J.-P. Hubaux. The Security of Vehicular Networks. In Proc. of WiSe 2005, pages 31–32, New York, NY, USA, 2005. ACM Press.