Asymmetric Encryption For The Autonomous Vehicle

Ron Davidescu and Eugen Negrus

University POLITEHNICA of Bucharest, Romania

Abstract. The future of the vehicle is of cars, roads and infrastructures connected in a two way automated communication in an holistic system. It is a mandatory to use Encryption to maintain Confidentiality, Integrity and Availability in an ad hoc vehicle network. Topology of the network produces its structure and key distribution. Both Star and ad hoc (Manet) topologies were investigated as a solution for autonomous / smart vehicle system. As a conclusion a combined topology was developed, as the nature of the vehicle and infrastructure allows combined solution, that benefits from both topologies advantages, with low number of Keys, real time performance of the Vehicle to Vehicle (V2V) and strong reliable encryption on the Infrastructure to Vehicle (I2V) as well as easy integration of old (dumb) vehicles.

Keywords: connected car, asymmetric encryption, key exchange, real time communication.

1 Introduction

Not too long ago, security of automotive was equal with theft prevention. However as computerization in the modern vehicle is growing quickly to enable the implementation of autonomous driving and the connected car, safety has become synonymous with security.

It is clear that the autonomous car is unique in the requirement for operation with zero tolerance for failure in availability, continuity and security. Farther more current demonstrations by research groups have proven that vehicles can be penetrated remotely through their communication units and ordered to run malicious code that permits the intruder to control remotely the vehicle. Therefore, it has been confirmed that automobiles breaches in security already have severe safety effects. As safety is always the primary concern of every car manufacturer, automobile manufacturers must make security the same priority as safety.

As automobiles open to peripheral networks, they become potential targets of malicious hackers. New embedded computers and external communication interfaces create even more treats and bring new attack surfaces. Communication interfaces not only suffer from classical IT weaknesses but from the fact that vehicles by nature have to rely on wireless communication with no wired back up.

International Congress of Automotive and Transport Engineering, CONAT 2016
Transilvania University of Brasov, 2016
ISSN 2069-0401

One of the clear difficulties in massive implementation of the connected car are the opposite demands of strong, reliable, encryption and description while keeping real time operation in a moving vehicle with low computer resource environment.

It is known that a key advantage of Asymmetric Encryption over Symmetric Encryption is that no secret channel is required for the transfer of the public key. Furthermore the benefit of simple key management in asymmetric encryption in V2I (Vehicle to Infrastructure) and even more in V2V(Vehicle to Vehicle) communication allowed us to develop and demonstrate through software simulation, an holistic model of multilevel authorization in communication, even in the case of ad hock V2V network. Multilevel authorization network is guaranteed in the V2I communication, expanding it to the V2V case allows stronger read and write permits for a part of the fleet, for example emergency and security vehicles.

2 Vehicular Communication Infrastructure Topology

In the near future the majority of new automobiles will be equipped with two way radio systems for car to car and car to Infrastructure communication.

A comparison between the Vehicle and Infrastructure of computer and connectivity foundations (table 1), shows a contradiction between the demands to capability of the vehicles and infrastructure. Vehicles by nature are mobile, require real time multi party wireless communication with limited computer communication and bandwidth access on the other hand infrastructure is on a fixed location, backed up by wired communication with almost unlimited computer, memory and back up availability. Furthermore wireless towers are by design redundancy.

Table 1. Vehicle Vs. Infrastructure : computer and connectivity foundations.

Heading level	Vehicle	Infrastructure
Location	Mobile	Fixed
Computer power	Low	High
Communication	Wireless	Wired/Fast - I2I Wireless I2V, V2I
Memory	Low/Limited	Large/expandable
Band width	Low	High
Back up	Local/limited	Large/Cloud
Availability	Part time	Always On

The wireless network topology structure is defined from the functionality required by the different parties. By nature I2V and V2I is of a central address (Infrastructure) that communicates with multi parties (Vehicles), in other words star network topology.
In this topology all components connect to a central Infrastructure. The vehicles are not linked to each other and it does not allow direct traffic between devices. The ac-

tive star network has an active Infrastructure central node that usually has the means to prevent security problems.

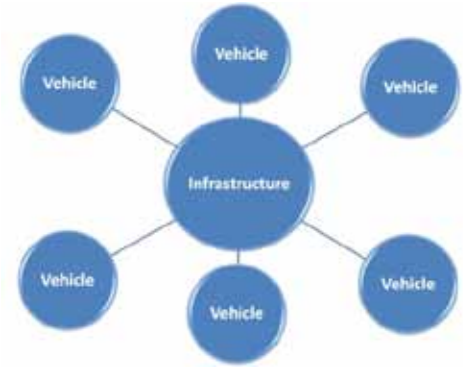

Fig. 1. Star topology (Source: Nivedita Bisht , p. 1)

Star topology advantages Easy to diagnose network fault, Good performance, Scalable, easy to set up and to extend on the other hand, Star topology main disadvantage is that it totally depend on a single hub.

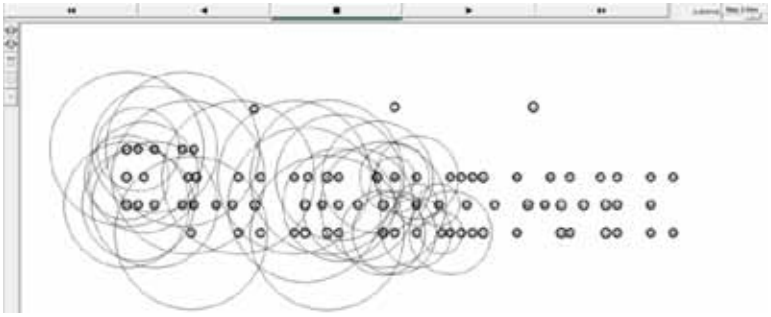

Fig. 2. AD hoc network (Source: Simulation results [2])

On the other hand V2V, requires multi channel interaction between mobile, moving and changing parties to insure the full benefit from data sharing and real time decision making, a network of such users referred as mobile ad hoc network (MANET) [A survey of secure Mobile AD HOC. A Mobile Ad-hoc Wireless Network (MANET) is a collection of autonomous nodes that communicate with each other by forming a multi-hop network, maintaining connectivity in a decentralized manner. It consists of a set of mobile hosts communicating amongst themselves using wireless links, without the use of any other communication support facilities, such as base-stations. The nodes in a MANET can be any device that is capable of transmitting and receiving information. Each node in such a network acts as a host or end system (transmitting and receiving data) and simultaneously as a router. The nodes in a MANET are generally mobile and may go out of range of other nodes in the network [2].

3 Ad Hoc Network Performance Simulation

In order to evaluate the performance of Ad Hoc networks in a changing conditions a simulation of different Ad Hoc protocols was performed on multiple number of mobile nodes. We have examined three common routing protocols for MANET.

DSDV is a proactive protocol, every mobile station maintains a routing table with all available destinations along with information like next hop, the number of hops to reach to the destination, sequence number of the destination originated by the destination node, etc. DSDV uses both periodic and triggered routing updates to maintain table consistency. Triggered routing updates are used when network topology changes are detected, so that routing information is propagated as quickly as possible [3].

DSR is a reactive routing protocol which allows nodes in the MANET to dynamically discover a source route across multiple network hops to any destination. In this protocol, the mobile nodes are required to maintain route caches or the known routes. The route cache is updated when any new route is known for a particular entry in the route cache.

AODV is a reactive routing protocol instead of being proactive. It minimizes the number of broadcasts by creating routes based on demand, which is not the case for DSDV. When any source node wants to send a packet to a destination, it broadcasts a route request (RREQ) packet. The neighboring nodes in turn broadcast the packet to their neighbors and the process continues until the packet reaches the destination [2]. For the simulation of the developed system ViSim 1.0 has been used, ViSim calls ns-2 simulations in a Windows environment, to allow rapid configuration for any MANET routing scenario [2].

Table 2. Simulation Parameters.

```
# Define options
set val(chan)         Channel/WirelessChannel        ;# channel type
set val(prop)         Propagation/TwoRayGround   ;# radio-propagation model
set val(netif)        Phy/WirelessPhy                ;# network interface type
set val(mac)          Mac/802_11                     ;# MAC type
set val(ifq)          Queue/DropTail/PriQueue        ;# interface queue type
set val(ll)           LL                  ;          # link layer type
set val(ant)          Antenna/OmniAntenna           ;# antenna model
set val(ifqlen)       50                             ;# max packet in ifq
set val(nn)           20/40/60/80/100                ;# number of mobilenodes
set val(rp)           DSR/AODV/DSDV                 ;# routing protocol
set val(x)            2000                                  ;# X dimension of topo-
graphy
set val(y)            1000                                  ;# Y dimension of topo-
graphy
set val(stop)           150                                 ;# time of simulation end
```

All three protocols were compared in a 20,40,60,80 and 100 mobile nodes in random four traffic lanes as can be seen in figure 2.

The following performance metrics were evaluated to understand the behavior of DSDV,DSR and AODV, Max throughput, Goodput (In terms of Packet Size in Bytes), Routing Load (In terms of Bytes).

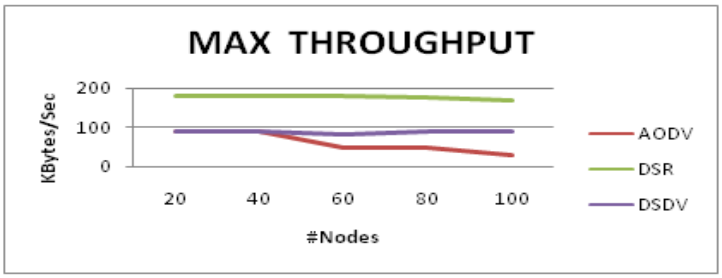

Fig. 3. MAX Throughput results (Simulation results)

Max Throughput is the max bytes received by the destination node per second (Data packets and Overhead).

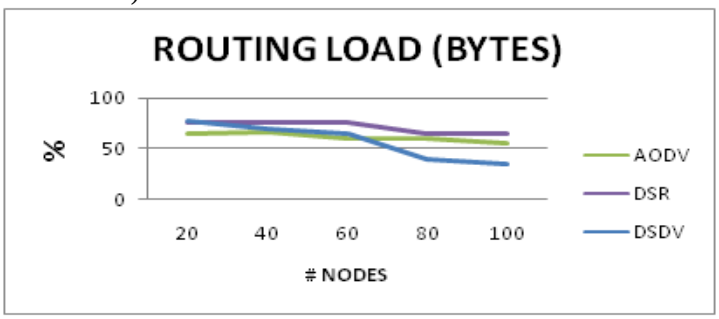

Fig. 4. Routing Load results -Bytes (Simulation results)

Routing Load (in terms of Packet Size in Bytes) is the ratio of the total bytes of routing packets that are sent within the network to the total number of bytes that are transmitted within the network to reach the destination.

Goodput (In terms of Packet Size in Bytes) is the ratio of the total bytes of data that are sent from the source to the total bytes that are transmitted within the network to reach the destination.

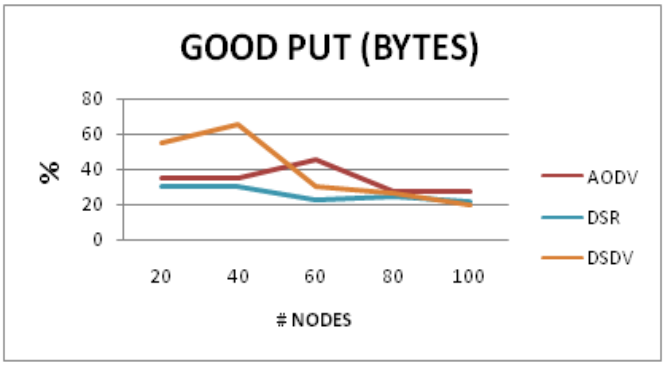

Fig. 5. Goodput results -Bytes (Simulation results)

It is clear that in terms of performance of throughput and routing load DSR protocol has a clear advantage, and even in the Goodput parameter is similar to the AODV and DSDV protocols in the high node number mode.

4 Hybrid Network Asymmetric Encryption

The most important challenge that MANET is facing is the security issue Some of the issues that cause that is that there is no centralized administration control, that the wireless channel is unprotected [4].

However in the case of connected /autonomous vehicles most of the weakness of a classic ad hoc network can be migrated due to the hybrid nature of the network, that allows V2I and I2V is a trusted secure star topology and V2V in an ad hoc model.

ARAN [5] or Authenticated Routing for Ad hoc Networks detects and protects against malicious actions by third parties and peers in an ad hoc environment. ARAN introduces authentication, message integrity, and non-repudiation.

It is composed of two distinct stages. ARAN makes use of cryptographic certificates for the purposes of authentication and non-repudiation. Stage 1 contains a preliminary certification stage and a mandatory end to end authentication stage. ARAN requires the use of a trusted certificate server T. Before entering the ad hoc network, each node requests a certificate from the trusted server.

The certificate contains the IP address IPA of the node, the public key of the node, a timestamp, of when the certificate was created, and a time at which the certificate expires. These variables are concatenated and signed by the trusted server. All nodes must maintain fresh certificates with the trusted server and must know the trusted server public key. The goal of Stage 1 is for the source to verify that the intended destination was reached. In this stage, the source trusts the destination to choose the return path. Stage 2 is performed only after Stage 1 has been successfully executed. This is because the destination certificate is required in Stage 2. This stage is primarily used for discovery of shortest path in a secure fashion. Since a path is already dis-

covered in Stage 1, data transfer can be pipelined with Stage 2)'s shortest path discovery operation.

$$
\begin{array}{lcll}
A & \rightarrow & * & : \{\mathtt{RDP}, X, N_A\}_{K_{A-}}, [cert_A] \\
B & \rightarrow & * & : \{\{\mathtt{RDP}, X, N_A\}_{K_{A-}}\}_{K_{B-}}, [cert_A, cert_B] \\
C & \rightarrow & * & : \{\{\mathtt{RDP}, X, N_A\}_{K_{A-}}\}_{K_{C-}}, [cert_A, cert_C] \\
X & \rightarrow & C & : \{\mathtt{REP}, A, N_A\}_{K_{X-}}, [cert_X] \\
C & \rightarrow & B & : \{\{\mathtt{REP}, A, N_A\}_{K_{X-}}\}_{K_{C-}}, [cert_X, cert_C] \\
B & \rightarrow & A & : \{\{\mathtt{REP}, A, N_A\}_{K_{X-}}\}_{K_{B-}}, [cert_X, cert_B]
\end{array}
$$

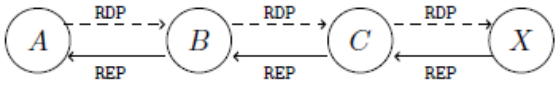

Fig. 6. The ARAN protocol (an example with four nodes) (Simulation results) (Source Benetti p2 [6])

5 Summary

It is known that a key advantage of Asymmetric Encryption over Symmetric Encryption is that no secret channel is required for the transfer of the public key. Furthermore the benefit of simple key management in asymmetric encryption in V2I and even more in V2V communication allowed us to develop and demonstrate, an holistic model of Combined network topology, consist of Star topology for I2V communication, with strong encryption and ad hoc topology for V2V and V2I communication with ARAN topology encryption, therefore implementing multilevel encryption in an holistic system.

The combined topology model allows real time performance in V2V network due to with asymmetric encryption.

Furthermore as Asymmetric encryption allows easy public key delivery to allow read permission for a 3rd party communication without compromising the network, the combined topology permits easy integration of older system including regular (dumb) vehicles that can benefit from the network knowledge through one way communication.

References

1. Nivedita Bisht, Sapna Singh : ANALYTICAL STUDY OF DIFFERENT NETWORK TOPOLOGIES : International Research Journal of Engineering and Technology : Volume: 02 Issue: 01 :Mar 2015.
2. Nazmus Saquib, Md. Sabbir Rahman Sakib : ViSim: A user-friendly graphical simulation tool for performance analysis of MANET routing protocols : Mathematical and Computer Modelling 53 (2011) 2204–2218.

3. Sachin Kumar Gupta, R. K. Saket : PERFORMANCE METRIC COMPARISON OF AODV AND DSDV ROUTING PROTOCOLS IN MANETs USING NS-2: International Journal of Research and Reviews in Applied Sciences : June 2011 : Volume 7
4. Spinder Kaur, Harpreet Kaur : Implementing RSA Algorithm in MANET and Comparison with RSA Digital Signature : INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY : Volume 3, Issue V, May 2015
5. C. Sreedhar, Dr. S. Madhusudhana Verma, Prof. N. Kasiviswanath : A Survey on Security Issues in Wireless Ad hoc Network Routing Protocols : International Journal on Computer Science and Engineering: Vol. 02, No. 02, 2010,
6. Davide Benetti, Massimo Merro, Luca Vigan : Model Checking Ad Hoc Network Routing Protocols: ARAN vs. endair A: Software Engineering and Formal Methods (SEFM), 2010 8th IEEE International Conference.
7. Intelligent Transportation Systems, Joint Program Office, *INTELLIGENT TRANSPORTATION SYSTEMS (ITS) Information Security Analysis*, U.S. Highway Administration, Department of Transportation, Federal Highway Administration, 1997.
8. Bryan Parno, Adrian Perrig,: Challenges in Securing Vehicular Networks: http://www.sparrow.ece.cmu.edu.
9. Maxim Raya, Panos Papadimitratos, : Securing Vehicular Communications: http://www.ece.cmu.edu.