AD HOC NETWORKS FOR THE AUTONOMOUS CAR

Davidescu Ron, Eugen Negrus

Universitatea Politehnica din Bucureşti

rondavidescu@gmail.com

Abstract. The future of the vehicle is made of cars, roads and infrastructures connected in a two way automated communication in a holistic system. It is a mandatory to use Encryption to maintain Confidentiality , Integrity and Availability in an ad hoc vehicle network . Vehicle to Vehicle communication, requires multichannel 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) , however as ad hoc networks were not implemented in such a scale , it is not clear what is the best method and protocol to apply . Furthermore the visibility of secure preferred asymmetric encrypted ad hoc networks in a real time environment of dense moving autonomous vehicles has to be demonstrated, In order to evaluate the performance of Ad Hoc networks in changing conditions a simulation of multiple protocols was performed on large number of mobile nodes. The following common routing protocols were tested , DSDV is a proactive protocol ,every mobile station maintains a routing table with all available destinations , DSR is a reactive routing protocol which allows nodes in the MANET to dynamically discover a source route across multiple network hops , AODV is a reactive routing protocol Instead of being proactive. It minimizes the number of broadcasts by creating routes based on demand , SAODV is a secure version of AODV ,requires heavyweight asymmetric cryptographic , ARIANDE is a routing protocol that relies on highly efficient symmetric cryptography the concept is primarily based on DSR.

A methodical evolution was performed in a various density of transportation, based on known communication bench mark parameters including , Throughput Vs. time , Routing Load per packets and bytes. Out of the none encrypted protocols , It is clear that in terms of performance of throughput and routing load DSR protocol has a clear advantage the high node number mode . The encrypted protocols show lower performance with ARIANDE being superior to SAODV and SRP. Nevertheless all protocol simulation proved it to match required real time performance.

1. Introduction

Still today, security of automotive usually means accident or theft prevention. However as electronics and software in the modern vehicle is growing rapidly to enable the employment of autonomous vehicle and the connected car, safety has become equal with security.
It safe to say that the autonomous vehicle is distinctive in the need of procedure with no tolerance to failure in security, continuity and availability. On top of it, recent 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. Thus, was established that breaches in vehicle security already have dangerous safety effects. As security is always the main concern of all automobiles firms, vehicle manufacturers must make safety the same priority as security.

As vehicles open to external communication networks, they become probable targets of hacker's attacks. More computers and communication interfaces produce larger treats and bring new penetration surfaces .New communication interfaces suffer from classical IT weaknesses and from the fact that cars by nature have to rely on wireless communication with no wired back up.

One of the obvious difficulties in large implementation of the connected vehicle are the opposite demands of strong ,reliable , encryption and description while keeping real time operation in a moving vehicle with low computer resource environment and many times low communication infrastructure.

Vehicle to vehicle communication (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 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].

2. None secure Ad Hoc Network Performance Simulation

In order to examine the compatibility of different Ad Hoc protocols in changing conditions, a simulation was performed on large number of mobile nodes. We have examined three common none secure routing protocols for MANET.

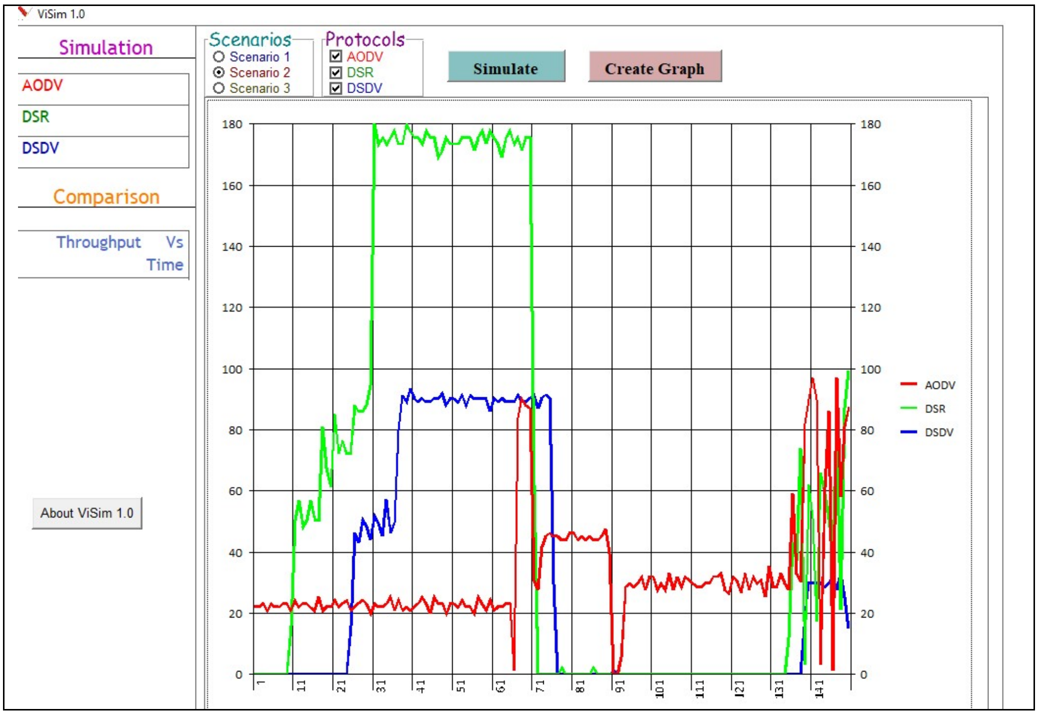
DSR is a reactive routing protocol which allows nodes in the MANET to dynamically discover a source route across multiple network hops to any destination. In this proto-col, the mobile nodes are required to maintain route caches or the known routes. The route cache is updated when any new route is known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

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 1 describes the simulation parameters for none secure as hoc protocols.

Table 1.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)     65                          ;# max packet in ifq
set val(nn)         100                         ;# number of mobilenodes
set val(rp)         DSR/AODV/DSDV               ;# routing protocol
set val(x)          1500                            ;# X dimension of topography
set val(y)          750                             ;# Y dimension of topography
set val(stop)         2500                          ;# time of simulation end
```

All three protocols were compared in a 100 mobile nodes in random traffic lanes , the following performance metrics were evaluated to understand the behavior of DSDV,DSR and AODV , Throughput Vs, Time , Routing Load (In terms of packets) & Routing Load (In terms of Bytes).

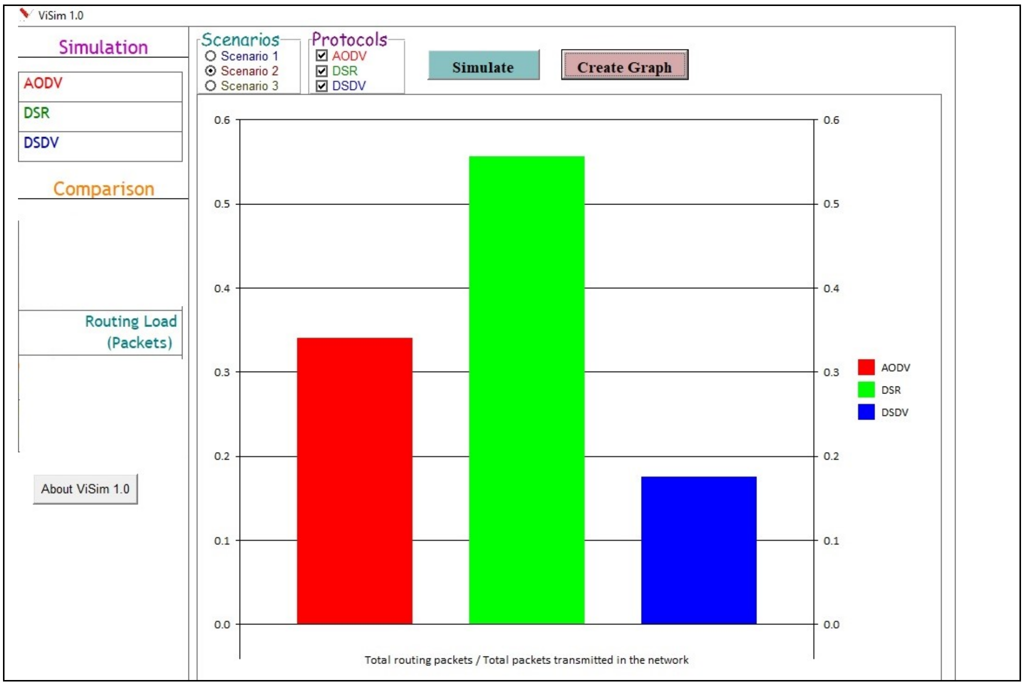


Scenarios
○ Scenario 1
● Scenario 2
○ Scenario 3

Protocols
☑ AODV
☑ DSR
☑ DSDV

Fig. 1. Throughput Vs, Time results (Simulation results)

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

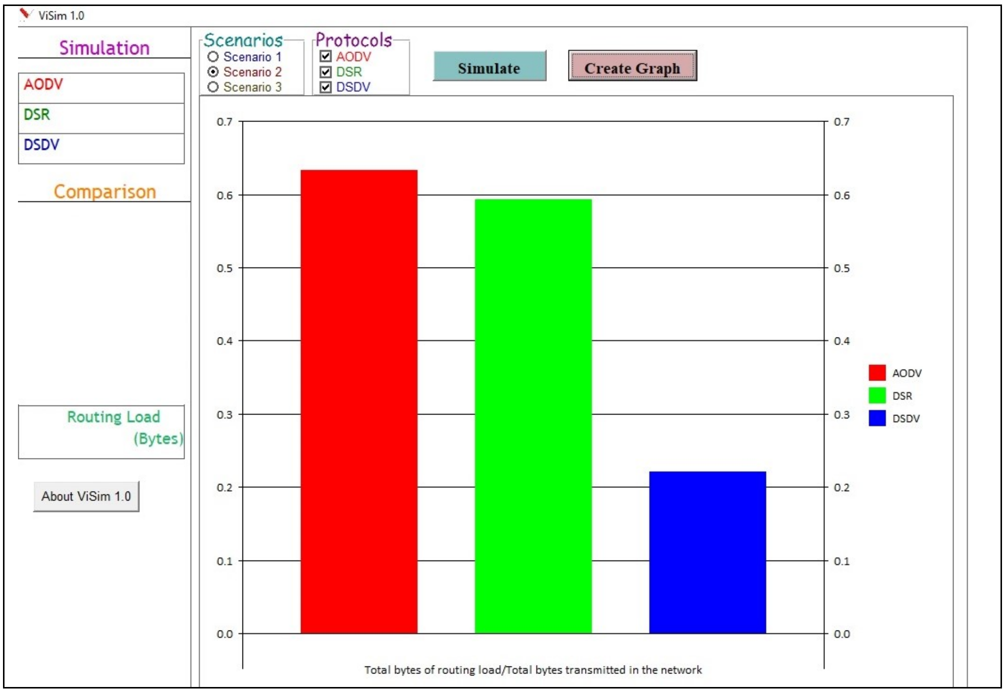


Scenarios: ○ Scenario 1 ● Scenario 2 ○ Scenario 3

Protocols: ☑ AODV ☑ DSR ☑ DSDV

Fig. 2. Routing Load - In terms of packets (Simulation results)

Routing Load (In terms of Packets) is the ratio of the total routing packets that are sent within the network to the total number of packets that are transmitted within the network to reach the destination.



Scenarios: ○ Scenario 1 ● Scenario 2 ○ Scenario 3

Protocols: ☑ AODV ☑ DSR ☑ DSDV

Fig.3. Routing Load - In terms of Bytes (Simulation results)

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

It is clear that the DSR protocol has an advantage in Throughput and Routing Load - In terms of packets.
In the third parameter Routing Load - In terms of Bytes it has similar performance to the AODV protocol and superior performance to the DSDV protocol.

3. Secure Ad Hoc Network Performance Simulation

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

Ariadne : is a routing protocol that relies on highly efficient symmetric cryptography the concept is primarily based on DSR

SAODV is a secure version of AODV, requires heavyweight asymmetric cryptographic.

SRP - The basic idea of SRP is to set up a security association (SA) between a source and a destination node without the need of cryptographic validation . [3]

Table 1.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)      65                          ;# max packet in ifq
set val(nn)          20/40/60/80/100             ;# number of mobilenodes
set val(rp)         Ariadne / SAODV / SRP              ;# routing protocol
set val(x)          1500                              ;# X dimension of topography
set val(y)           750                              ;# Y dimension of topography
set val(stop)          2500                           ;# time of simulation end
```

All three protocols were compared in a 20,40,60,80 AND 100 mobile nodes in random traffic lanes , the following performance metrics were evaluated to understand the behavior of Ariadne, SAODV and SRP , Max Throughput , Routing Load (In terms of packets) & Routing Load (In terms of Bytes).

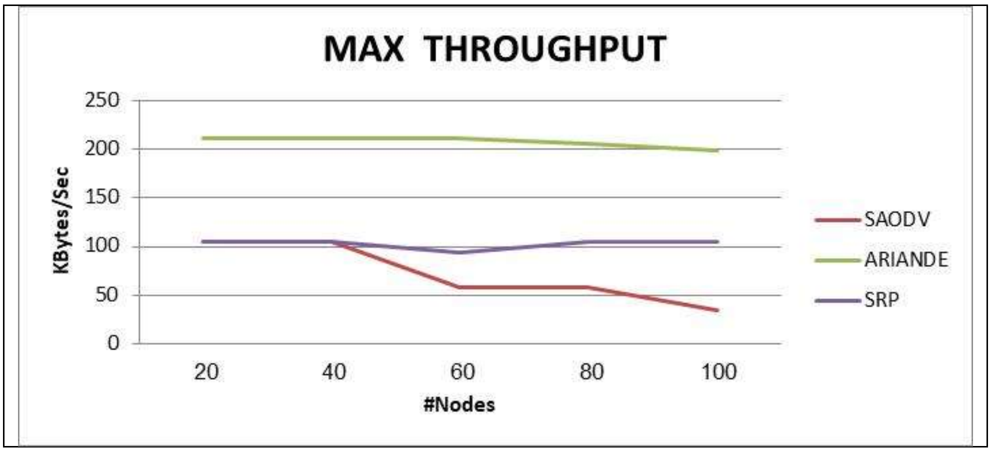


Fig. 4. Max throughput results (Simulation results)

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

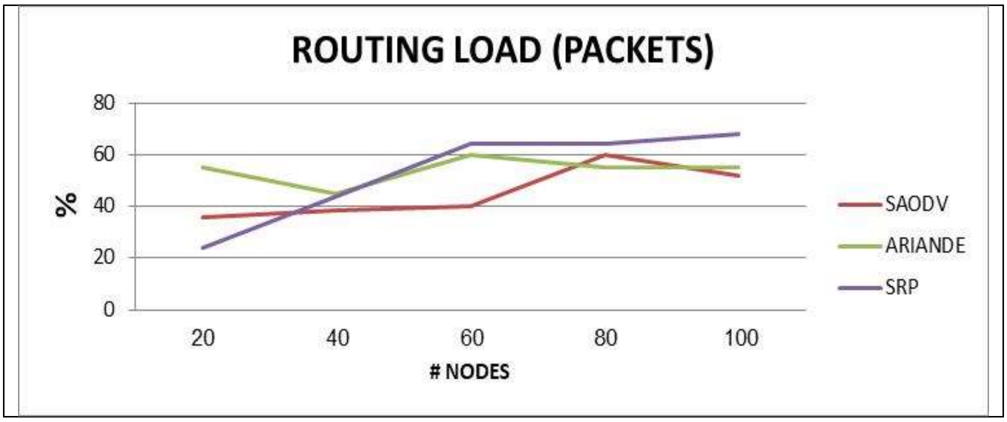


Fig. 5. Routing Load - In terms of packets (Simulation results)

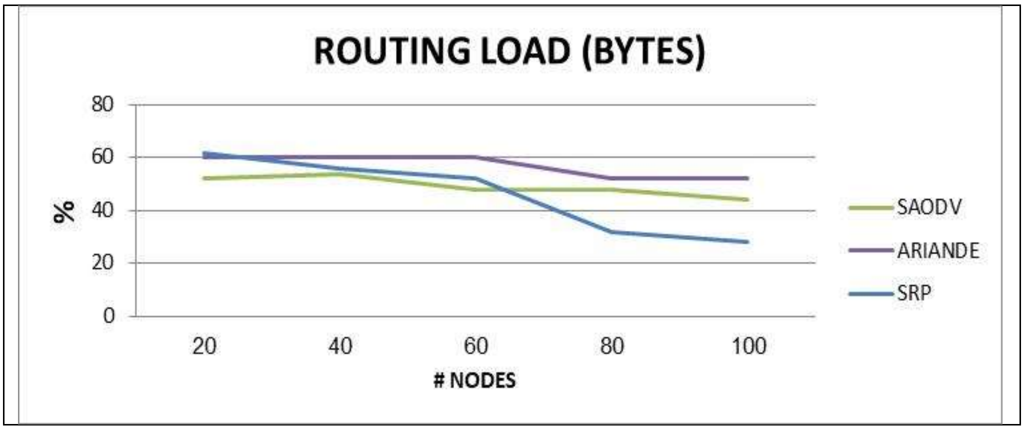


Fig.6. Routing Load - In terms of Bytes (Simulation results)

The ARIANDE protocol shows superior throughput and bytes routing load and similar performance to SRP on the packet routing. Very similar to the none secure DSR protocol behaviour it was developed from.

4. Summary

A full solution of autonomous cars will require Vehicle to Vehicle communication to enhance the local car sensors performance and enable the security and safety required for large connected car implementation and benefits. On top of that it will need integration of older none autonomous cars to share the road.

Never the less any none direct mean of communication will reduce the time to reaction in case of emergency and jeopardize the wellbeing of the passenger. Ad hoc networks allow such communication and create a network of communication that is independent from the vehicle to infrastructure network and that can act as a backup, by its nature the data goes first to the close vehicles. In this paper we evaluated common none secure ad hoc protocols, DSDV, DSR and AODV in terms of throughput and routing Load through computer simulation and concluded that the DSR protocol is superior. Furthermore three secure ad hoc protocols were evaluated in multi node conditions, Ariadne, SAODV and SRP. In that case Ariadne that was developed from the none secure DSR proved better. It is a common believe that autonomous cars will change the world we know for better, however without a standards for V2I and V2V communication that will probably never work. Secure ad hoc networks that will follow an international standard to be implemented on all autonomous and connected cars will resolve the issue.

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.