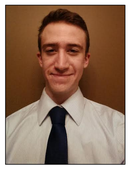
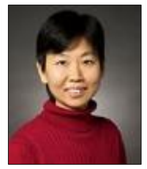
Securing Safety Messages in VANETs




Kevin Miller and Yakeen Alwishah

Advisors: Ahmad Mansour, Richard Bassous, and Dr. Huirong Fu





National Science Foundation

Research Experience for Undergraduates

Objectives

- Propose four models to secure messages in Vehicular Ad-hoc Networks using Ambiguous multi-symmetric cryptographic (AMSC) primitive.
- Compare performance of AMSC to other symmetric cryptographic algorithms in a mobile wireless environment using Android.

Introduction

Vehicular Ad-hoc Networks are an anticipated mobile ad-hoc system for communication between vehicles and roadside infrastructure to increase safety on the road. It is essential that this system is able to send fast and secure messages to prevent accidents. We apply the Ambiguous Multi-Symmetric Cryptographic primitive to vehicular ad-hoc networks for encryption and decryption of safety messages.

We present a protocol that contains four models to secure and disseminate safety messages. Each model also utilizes at least one of the following three modes of communication:

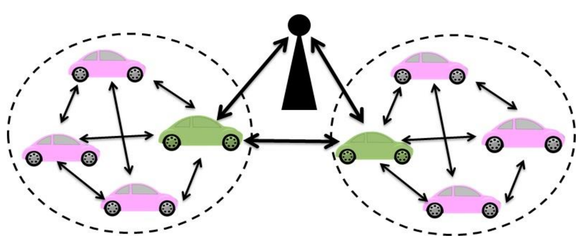
- Multicast (one-to-many broadcast).
- Multicast with 1 real and z fake messages.
- One-to-one communication using AMSC in parallel.

Furthermore, there are three communication paths:

- Vehicle to Infrastructure – V2I.
- Infrastructure to Vehicle – I2V.
- Vehicle to Vehicle – V2V.

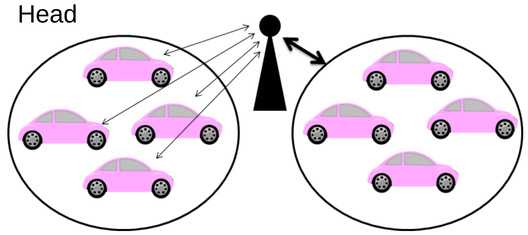
System Models

Model 1: Vehicle Clusters with Cluster Heads

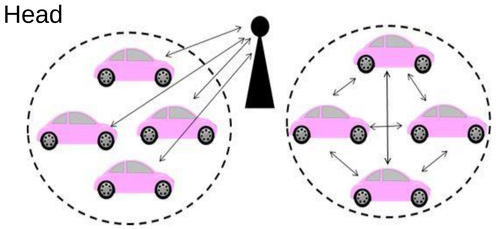


System Models (cont.)

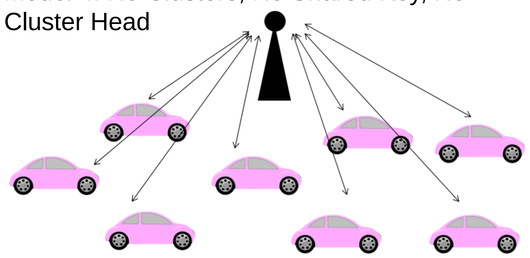
Model 2: Clusters, Shared Key, No Cluster Head



Model 3: Clusters, No Shared Key, No Cluster Head



Model 4: No Clusters, No Shared Key, No Cluster Head



Analysis

Table 1: Model 1

Advantages	Disadvantages
Location privacy for cluster members.	Relies on a trusted cluster head
Safety messages sent immediately to nearby vehicles in danger.	Clustering increases complexity of VANET architecture.
Does not rely on roadside infrastructure.	Scalability for individual vehicles can be worse than other models.
Decreases unnecessary bandwidth usage by deleting duplicate messages.	
Better scalability for entire system.	
All modes of communication can be used.	

Analysis (cont.)

Table 2: Model 2

Advantages	Disadvantages
Safety messages sent immediately to nearby vehicles in danger.	Relies on roadside infrastructure to send trusted messages.
Does not rely on trusted cluster head.	Clustering increases complexity of VANET architecture.
All modes of communication can be used.	Unnecessary consumption of bandwidth for duplicate messages.
	Untrusted cluster member can speak to other clusters on behalf of the group.
	Poor scalability for roadside infrastructure.

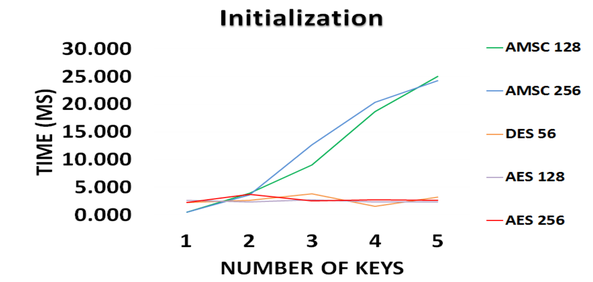
Table 3: Model 3

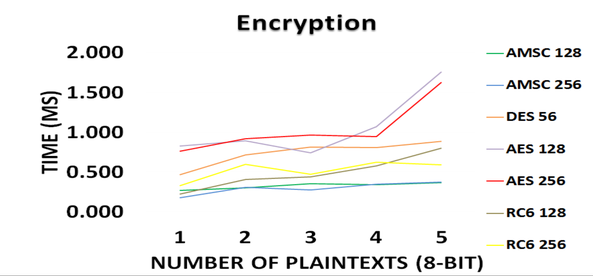
Advantages	Disadvantages
Safety messages sent immediately to nearby vehicles in danger.	Relies on roadside infrastructure.
Does not rely on trusted cluster head.	Clustering increases complexity of VANET architecture.
All modes of communication can be used.	Unnecessary consumption of bandwidth for duplicate messages.
	Poor scalability for roadside infrastructure.

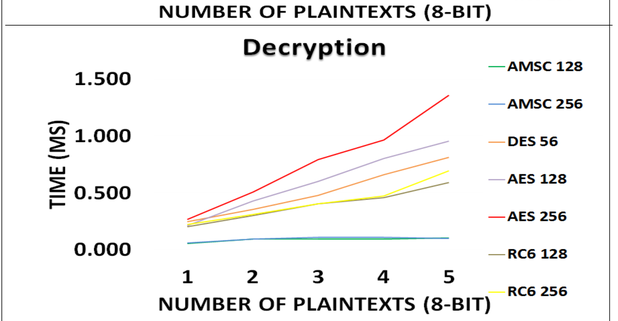
Table 4: Model 4

Advantages	Disadvantages
Simple to implement.	Relies on roadside infrastructure.
Does not rely on trusted cluster head	Unnecessary consumption of bandwidth for duplicate messages.
Best scalability for individual vehicles out of the four models	A vehicle cannot privately send a message to another vehicle.
	Safety messages cannot be sent quickly.
	Poor scalability for roadside infrastructure.
	Can only use one-to-one communication.

Results







Conclusion

- We proposed a comprehensive protocol that can be used for the efficient distribution of safety messages in Vehicular Ad-hoc Networks.
- The results obtained from our experiment have established that AMSC can encrypt and decrypt messages faster than other symmetric algorithms in a mobile wireless environment.

Acknowledgement

This research work was conducted at Oakland University in the UnCoRe program - REU site supported by the National Science Foundation under Grant No. CNS-1460897. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.