A report submitted to the Department of Computer Science in partial

fulfillment of the requirements for the degree

BSc (Honours) in Computer Science by

Junaid Ali

M. Hissan Zafar

Nabeel Akhtar

Lahore University of Management Sciences

May, 2010

Acknowledgements

We would like to thank our senior year project supervisor Dr Fareed Zaffar for his guidance, support and assistance throughout the duration of the project.

Junaid Ali 2011-02-0411

M. Hissan Zafar 2011-02-0493

Nabeel Akhtar 2011-02-0228

Date:

23rd May, 2011

1 .1 Introduction

Vehicles connected to each other through an ad hoc formation form a wireless network called "Vehicular Ad Hoc Network" (VANET). Vehicles parts of this network are known as smart vehicles.

Smart vehicles are aware of its neighborhood including the presence and location of other vehicles, these cars now possess a network of processors connected to a central computing platform that provides Ethernet, Bluetooth, and IEEE 802.11 interfaces. These cars also have features like EDR, GPS Receiver, Front and Rear radar for detecting obstacle.

What is important is to make communication between these smart vehicles and RSUs secure to increase the driving safety. Much work has been done on making current mobile ad hoc networks secure but much is needed to be done to make VANET secure. The main difference between VANET and current mobile ad hoc network is the high mobility of the nodes (smart vehicles) and the large scale of the network. Security and privacy must be two primary concerns in the design of VANET because for one lack of security has very high price and secondly VANET is not fully developed yet so it is easier to implement security aspects within network now. Poorly designed VANETs that permit serious attacks on the network can jeopardize the goal of increased driving safety. Also, a VANET design that enables third parties to collect private information about drivers, for example by making tracking vehicles a possibility, will certainly be avoided by drivers. Thus the specific characteristics of VANETs result in hard to address security issues, which make the field of secure inter-vehicular communications an interesting research topic.

There have been many solutions proposed for the security of VANET and are described individually but there is no systematic way to compare and contrast them. We have provided the solution of this situation by presenting a framework to describe the features of these systems and the level of security they offer. Any secure solution must take into account a special set of functions which are core, although they may vary in the detailed design choices. These choices affect both the level of security that the solution provides and the performance the system achieves.

Any secure solution should take into account, in addition to security and performance, is the level of inconvenience users are willing to tolerate. If users have to check many things themselves, they will soon begin to avoid the best intentions of the system designers.

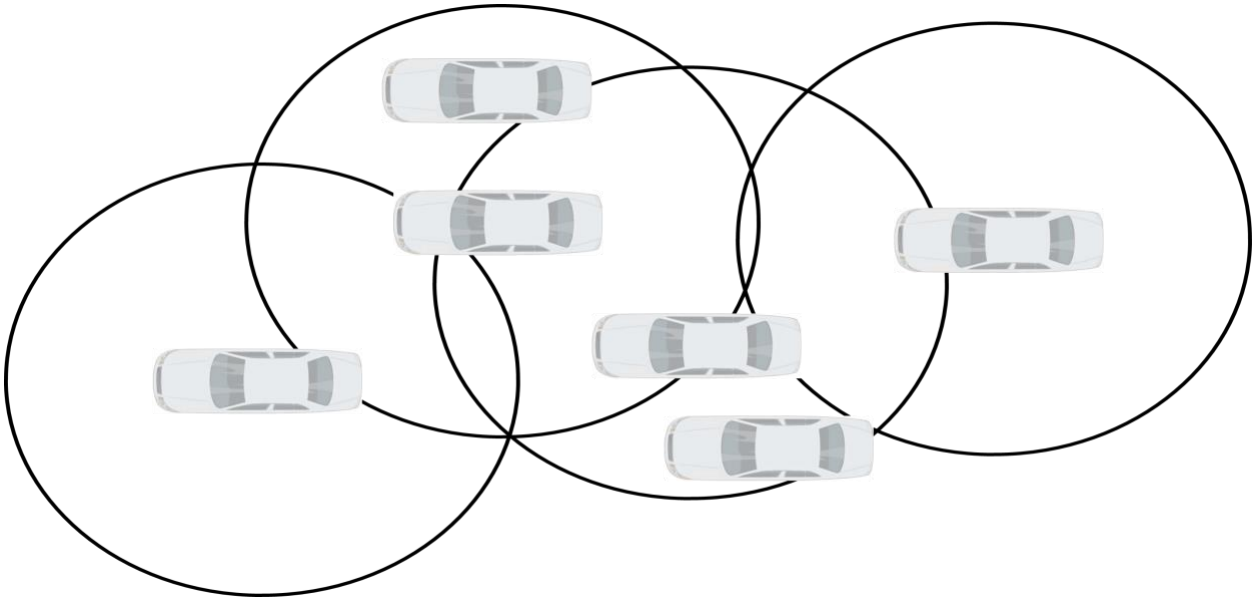


Figure 1.1.1 an overview of Vehicular Network

The second problem this document deals with is the Best path algorithm, provided we have a secure VANET. In this part, we will be discussing how to use the Vehicular Network to find the best available path. It's become almost necessary for user to have the Best possible path while travelling. This not only saves time but also avoid bottle-neck scenarios on some busy streets. Our approach, to solve this critical problem, just not only take into account the static factors like Distance, Speed limit, Traffic lights etc., but also the dynamic factors like Congestion, Road Conditions etc.

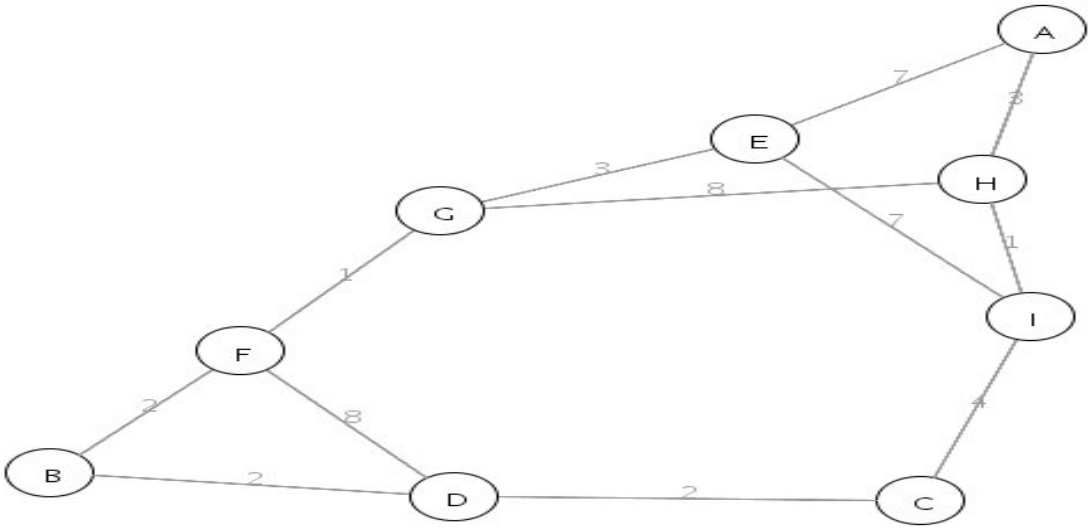


Figure 1.1.2 Find a Best path from A to B

1.2 Definitions, Acronyms and Abbreviations:

VANET	-	Vehicular Ad Hoc Network
RSUs	-	Road Side Units
EDR	-	Event Data Recorder
GPS	-	Global Positioning System
OBU	-	On Board Unit
TPD	-	Tamper Prove Device
TPM	-	Trusted Platform Module
HSM	-	Hardware Secure Module
CA	-	Central Authority
RA	-	Regional Authority
PKI	-	Public Key Infrastructure
VC	-	Vehicular Communication
SeVeCom	-	Secure Vehicular Network Communication
V2V	-	Vehicle to Vehicle
V2I	-	Vehicle to Infrastructure
CRL	-	Certificate Revocation List
VSM	-	Vector Space Model
IR	-	Information Retrieval
NS-2	-	Network Simulator
NCTUns	-	National Chiao Tung University-network simulator

2 Architecture

In this chapter we have provided an overview of VANET architecture in general.

2.1 System Architecture

As discussed earlier VANETs consist of smart vehicles and RSUs so each vehicle must have some interface that enables wireless communication between V2V and V2I.
Also due to high mobility and dynamic topology of VANET, IEEE developed special protocol 802.11p for this. Each vehicle must also have TPD or HSM and also some device that will give us the current location of vehicle. The standard choice for such hardware is a GPS or DGPS receiver (which has the added benefit of clock synchronization). RSUs and CA are also part of VANETs architecture and the number of RSUs varies in different approaches.

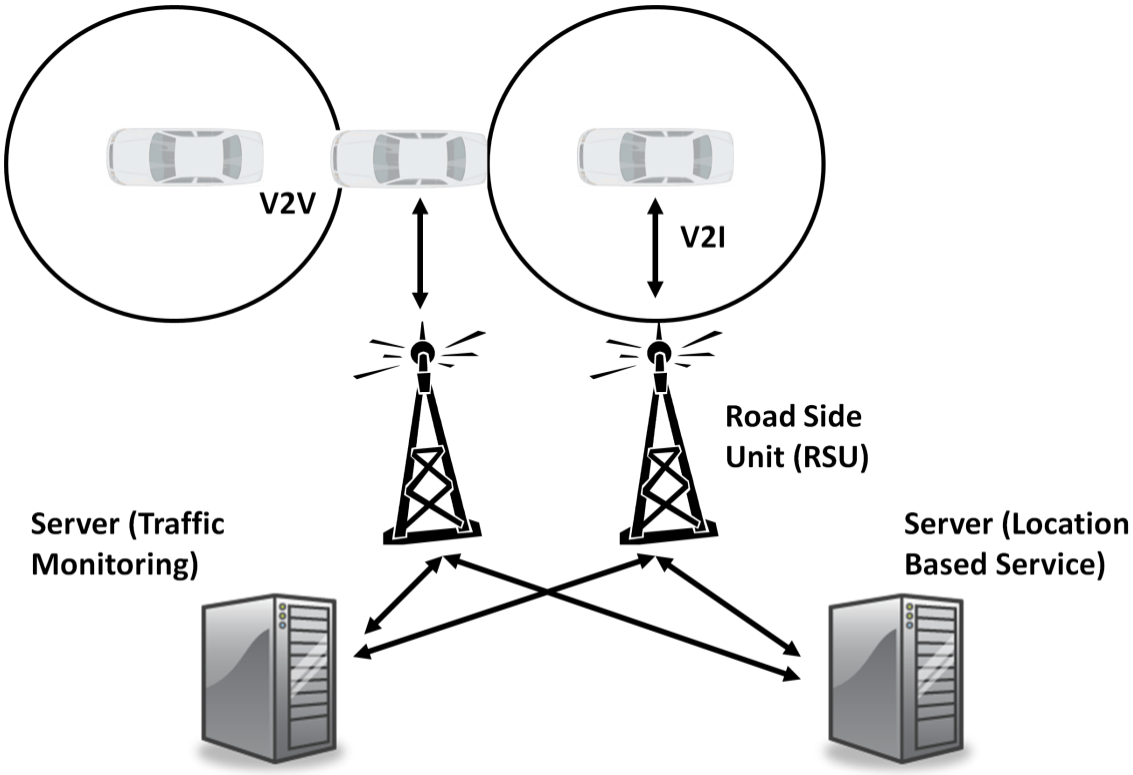


Figure 2.1.1 overview of VANET architecture

3 Characteristics of VANET Related to Security

In this chapter we have provided the requirements that vehicular networks must address in order to be considered suitable for widespread deployment, also we have discussed some of the characteristics of VANETs that will help in effectively addressing security issues.

3.1 Security Requirements

3.1.1 Authentication

Authentication of a message is one critical issue while addressing security requirement of VANETs. It is necessary to know that message originates from real vehicle rather than from fake ones. Otherwise, fake nodes can transmit false data and can nullify the use of system. This brings the need of some mechanism that can ensure not only the authenticity of message but can also prevent reply attacks by adding time stamps.

3.1.2 Privacy

While addressing the authentication issue, it is necessary to keep privacy aspect in that mechanism. We don't want any adversary to trace down the vehicle in the long run, so certain degree of privacy is necessary for the users of this network

3.1.3 Non-Repudiation

In case of emergencies and other related stuff, system needs to identify which vehicle sent that message and that vehicle cannot deny that the message originates from it. Here we want that only appropriate authorities should identify the vehicle. Then the issue of trust of these authorities is also raised and it has to be addressed

3.1.4 Availability

Most VANET applications require real time response, which means there is high probability that adversary use DoS. This problem is very critical in this real time system and need to be addressed in an efficient solution

3.1.5 Mobility

Vehicles are moving at very high speed and the network is highly dynamic so no solution is possible which include already stored public private keys.

3.2 Security Problems

Here in this section we have discussed some possible attacks on our Vehicular Network and also highlighted the impact of that attack on our system

3.2.1 Adversaries

Before discussing about the attacks its better if we know about the adversaries.

a) Malicious Attackers

This is most dangerous kind of attackers. These types of attackers include those who deliberately want to attack the system and have specific goals and are much more professional.

b) Insiders

Attacks from inside are always more harmful and this group of adversaries include those who have access to the vehicle and can change/update some part of it. Once any part of system compromised then the chain is as strong as its weak link.

c) Greedy Drivers

This category of adversaries includes those drivers who do not follow the protocols to maximize their gains rather than that of system. It's a safe assumption that, this kind of drivers will be less in number and can easily be identified.

3.2.2 Attacks

a) Denial of Service (DoS)

This is one famous attack that happens in almost every network (wired and wire-less). Here the adversary flooded the network and can jam the whole channel of communication so that all important data is dropped or cannot be delivered. In real time systems like VANET, the unavailability of information even for short period can cause serious problems.

b) Sybil Attack

As discussed earlier in last section, if there is no authentication protocol, non-existence nodes (fake vehicles) can spread false information over the network. This can lead into serious problems and can nullify the use of this network

c) Replay Attacks

If there is no authenticated timestamps in messages, replay attack is quite likely a possibility. Adversaries can send the right message at the wrong time causing sever confusion.

a) Message suppression Attacks

This type of attacks includes those where adversary can drop selected messages which are important, like dropping an important accident/congestion alert. This type of attacks is not a severe blow for the system but cannot be overlooked.

3.3 Challenges

3.3.1 Tradeoff between Core components

To develop a new approach for security of VANET requires lots of things to look at. As we describe in section 3.1 that authentication, non-repudiation and privacy are core components of well secure VANET system and addressing the trade-off between authentication and non-repudiation versus privacy is an important challenge. Approaches used in other types of Networks are not always applicable here due to Time sensitivity, which is an added challenge, because it prohibits the use of security protocols that have high overhead or rely on multiple stages of full-duplex communication between nodes (like hand shaking etc).

3.3.2 Sheer Scale of Network

Another challenge is the sheer scale of Network. Once this system adopted, billions of cars will rule out protocols that require pre-stored information about participating nodes or massive distribution of aggregated data to all mobile nodes (for example, distribution of certificate revocation lists is impossible).

3.3.3 Low Tolerance

Low tolerance for errors can also be considered as a problem. Most applications of VANET are real time and have life and death applications at times.

3.3.4 High Mobility

High mobility of cars makes this system highly dynamic where cars can enter and leave the network very often. Nodes can be in one part of network at time t and will be in other at time $t+1$.

3.3.5 Key Distribution

Key distribution is one of the challenges that we not only face in VANET but in other networks as well. But here the challenge is bit more due to privacy of a node which requires

changing keys of a node often. If not done then vehicle can be traced and privacy is compromised.

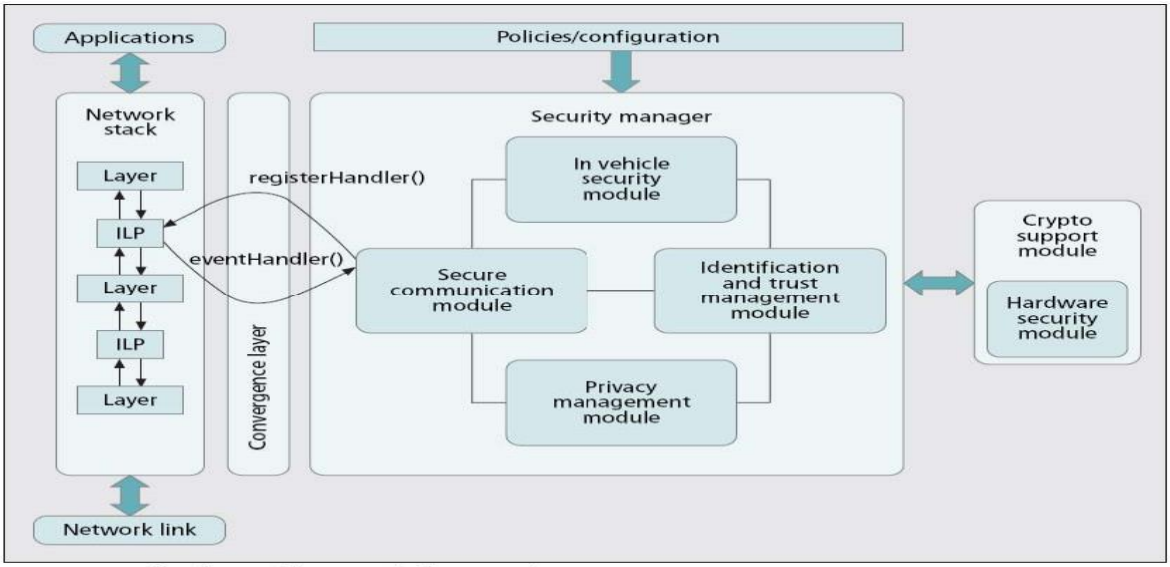
4 Solutions proposed in the literature

Different approaches have been discussed in literature but are not yet implemented in practical situations. Here in this section we have given some overview of the solutions with the papers name as heading

4.1 Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges

This paper addressed the Security and privacy protection of vehicular networks. In order to show the feasibility of secure VC, certain implementations are required. Paper discusses the design of a VC security system that has emerged as a result of the European SeVeCom project. First, paper explains why the deployment of a security system for a vehicular environment is different compared to other common information technology systems. Then paper present the SeVeCom baseline architecture, and highlight various implementation- and deployment-specific aspects such as flexible integration in existing communication stacks, use of a hardware security module, and secure connections of VC onboard units to in-vehicle bus systems. Furthermore, paper analyze the performance and communication overhead of the suggested security mechanisms and propose optimizations for efficient secure communication.
Finally, paper presents selected topics for future research on VC system security. One aspect is the use of complex forms of data dissemination, such as aggregation schemes, which require different security approaches than those used for broadcast and unicast communications. Another aspect is integrating VC systems with other networks or connecting them with mobile commodity devices, which raise additional security problems. Other future research aspects include secure localization and discovering whether existing VC privacy solutions are sufficient.
Baseline architecture is given on next page:

The SeVeCom baseline architecture consists of modules that are responsible for a certain system aspect, such as identity management. The modules, in turn, are composed of multiple components, each handling a specific task. For instance, the secure communication module is responsible for implementing protocols for secure communication and consists of several components, each of them implementing a single protocol. Components are instantiated only when their use is required by certain applications, and they use well defined interfaces to communicate with other components. Thus, they can be exchanged by more recent versions, without other modules being affected.



Baseline architecture: deployment view.

Figure baseline architecture : deployment view

The problem with this approach is that they are assuming that we have Hardware Security Module (HSM) integrated in every vehicle. They are using these temper proof hardware to provide the security. This is not a practical assumption as temper proof hardware is expensive and cannot be deployed in each car.

4.2 Secure Vehicular Communication Systems: Design and Architecture

This is one of the papers of SeVeCom project on Design and Architecture in which security aspects of the VANETs are addressed. One approach that they propose is all the nodes have HSM which contains all the keys and which could not be breached. All nodes are registered to one CA. They use pseudonym approach in which vehicle is given a lot of certified keys and it uses each of them for short period of time the message in this way can be signed and cannot be linked with one user only CA has the authority make that connection. There are two private keys (K1 and K2) of CA, and every HSM has those keys. In case one of the CA‟s private keys is compromised, the corresponding public key, say *K*1, can be revoked, as discussed in the next paragraph. The revocation command must be signed with the private key corresponding to *K*1 itself. Once *K*1 is revoked, a new key *K*`1 can be loaded into the HSM by a command signed with the private key corresponding to *K*2.

4.3 Efficient Secure Aggregation in VANETs

They propose that vehicle form dynamic group and instead of everyone in a same group sending same information data should somehow be integrated and only a summary should be sent. One of the solutions that they proposed was that only one copy should be sent with all the signatures from intermediate nodes appended with the message. This reduces channel usage but increase space overhead and author gives another approach in which they suggest using onion signatures i.e. instead of appending signatures with the message all the intermediate nodes can sign the current signature, if the outer signature is trustworthy, sent to

them and while a receiver is checking the message if the anyone of the signature raises any flags the message can be discarded. Hence the authentication of the data can be done by only two signatures.

4.4 Probabilistic Validation of Aggregated Data in Vehicular Ad-hoc Networks

This proposal can also handle messages that are similar but not identical, and expects nodes receiving multiple messages with similar information to summarize the information in them using only syntactic aggregation. This means that the information of all the messages is retained in separate entries, but can be compressed or reduced in precision. The main idea that the authors propose is to challenge the forwarding vehicle to provide probabilistic proof that the aggregated message is authentic and not constructed. We assume that the TPD provides a transmit buffer service where applications place messages to be transmitted. The TPD signs and sends these
messages after a small delay, during which the applications can append data to them. Also, it provides a trusted random number generator service. The proposed protocol works as follows. The application that aggregates the data puts the summarized message in the transmit buffer. This includes N entries, one for each incoming message that is summarized. The TPD includes a random number in the message, signs it, and is ready to transmit it. In the meantime, the application must read the random number, and include the original message of index i along with its signature, where i is determined by applying some function to the random number (scaling it to range 1 to N). In case this is successful, the message sent will include both the aggregated data and one original message, which serves as probabilistic proof of the authenticity of the data: it can be verified by other nodes that this message is authentic and the information contained in it agrees with the aggregation. In case it isn't, it means that the sender of the aggregated message was malicious, since that's the only case where the original message and its signature could not be produced. Since the transmit buffer will transmit the message anyway, the transmitted message serves as proof of malicious behavior. This solution is very interesting, in the sense that it only requires minimal overhead and is quite effective in ruling out malicious behavior, as preliminary analysis in the paper shows. Extensions to handle semantic aggregation are still to be investigated.

TACKing: Together Efficient Authentication, Revocation, and Privacy in VANETs

This paper deals with group based approach for the security of vehicular networks. A public key infrastructure has been used to provide security using certificates and fixed public keys. However, fixed keys allow an eavesdropper to associate a key with a vehicle and a location, violating drivers' privacy. In this work they have examine a VANET key management scheme based on Temporary Anonymous Certified Keys (TACKs).

Group signatures were first introduced by Chaum and van Heyst. In contrast to normal signatures, group signatures protect the signer's anonymity. A trusted entity (usually referred to as the group manager) assigns to each valid member of the group a group user key. This group user key allows a member of the group to sign a message and produce a group

signature. Group signatures can be verified by anyone using the group's public key. A group signature reveals no information about the signer's identity; and only the group manager can trace the identity of the signer from a group signature.

This paper proposes a group signature scheme that provides tracing and revocation. When a group member misbehaves, the group manager can trace the identity of the signer from the group signature, and henceforth revoke that user from the group. In TACKs, a revocation method called Verifier-Local Revocation (VLR) has been used. In VLR, the group manager computes and publishes a revocation list RL consisting of a revocation token for each revoked member. When verifying a group signature, the verifier tests the group signature against all revocation tokens in RL, to make sure that the signer has not been revoked. The verifier only accepts the signature if it comes from a valid signer that has not been revoked.

The TACKs system utilizes a group signature scheme in the following way. The group manager is a trusted entity such as the Department of Motor Vehicles. Each OBU is a group member and obtains a group user key (a.k.a. a long-term private key) from the group manager. To obtain a certificate for a short-lived Temporary Anonymous certified Key (TACK), an OBU needs to present a group signature to the appropriate RA. The RA is then able to verify that the requesting OBU is a valid member of the set V, without learning any identifying information about the OBU.

Notions used in TACKing has been given below

gSign	group members' algorithm to generate a group signature
gVerify	algorithm for verifying a group signature
$\mathsf{sign}_{K^{-1}}(M)$	a traditional signature for a message M signed with private key K^{-1}
guk	an OBU's group user key
gpk	group public key
gmk	group master key, owned by group manager
RL	revocation list
(K_S^{-1}, K_S^+)	an OBU's TACK pair: K_S^{-1} is the private key, K_S^+ is the public key

Updating an (K_S^+, K_S^{-1}) pair :

OBU : $(K_S^+, K_S^{-1}) \xleftarrow{R}$ key space

OBU : $\sigma \leftarrow \mathsf{gSign}(\mathsf{guk}_i, \mathsf{gpk}, K_S^+)$

OBU $\rightarrow$ RA : K_S^+, σ

RA : $b \leftarrow \mathsf{gVerify}(\mathsf{gpk}, \mathsf{RL}, \sigma, K_S^+)$

RA : if $b = 0$ then exit

RA : $\mathsf{cert} \leftarrow \mathsf{sign}_{K_{RA}^{-1}}(K_S^+ || \text{expiration})$

RA : Add (σ, K_S^+) to history table (less than δ seconds later)

RA $\rightarrow$ OBU : cert

Algorithm used for TACKing is given below:

This approach is one of the best that is out there is the research community. The problem with this approach is that they have made it less dynamic by fixing the group leaders (RA) to geographical boundaries. This approach makes it less dynamic and also requires lot of infrastructure.

Now after presenting all the related research next section contains the framework we developed

5 Framework

We have first identified the commonalities among the security solutions that have been proposed in the literature. We have formed a general framework after looking into different solutions proposed in literature.

It is important to note that the framework provided here is not used for evaluating end-to-end security of a particular solution. This requires careful analysis of each system component and combination of system components. Any secure system is as secure as its weakest link. The framework that we have provided here does not identify the weakest link. It gives a high level comparison and analysis of different schemes.

The framework consists for six main components Players, Type of Attacks, Trust Assumptions, Core Security Primitives, Granularity of Protection and User Connivance. We will elaborate each of these next.

5.1 Players:

In this section, we are defining all the possible players in Vehicular network. Each player has some set of functionalities that it has to perform and has to consider the security of data that it is using. Each player can only perform the set of legitimate actions. Any other action performed by the player is considered as attack.

Following are the possible players in Vehicular Network. We are defining the set of legitimate operations that each player can perform. The set of operations defined here are just the necessary operations that each player should have.

5.1.1 On Board Unit (OBU)

OBU is responsible for all processing data inside vehicle. It is like a small computer which is responsible for not only process data for the vehicle, but is also responsible for communicating with other vehicles or infrastructure. OBU is the brain of Vehicle. It is also responsible for the encryption of data.

5.1.2 Manager or Central Authority

Central authority is the core of the whole network. It has the data if all the legitimate vehicles in the network. It is responsible for the authentication of vehicles. It also has the revocation list which contains all the vehicles which have been compromised. Central Authority communicates with Road Side Units or Vehicles. It helps Vehicles identify illegitimate vehicles on the network. If Public Key Infrastructure (PKI) is used, then the Central Authority is also responsible for the distribution of Keys.

5.1.3 Road Side Unit (RSU)

RSU is responsible for communication with vehicles and the central authority. RSU can also have processing unit for encryption and decryption of data. Usually RSU is a bridge between the Central Authority and Vehicles.

5.1.4 Group Leaders: (if applicable)

Many of the security solutions proposed in literature make use of Group based approach to provide security in Vehicular Networks. Group leader is responsible for the formation of groups and distribution of Keys used for implementing security. Group leader also works as bridge between the vehicles and the central authority.

5.1.5 Transport Protocol:

Different transport protocols can be used for communication in vehicular network. Protocol used should be fast as vehicles are moving at high speeds. It should also be secure and should be able to handle encrypted traffic.

The above mentioned players are few of the players that are usually present in most of the solutions. There may be more players that have not been mentioned above. The functionality of players is different in each implementation of solution but the basic functionalities remain same.

5.2 Adversaries

We define adversaries to be entity who attempts to perform functions other than those it is authorized to do. Even if the legitimate users try to access/change data that they are not authorized to access, it is considered as attack and the user is marked as adversary.

5.3 Attacks

Attacks can be broadly classified into two types of attacks

1. Attacks on short lived data.
2. Attacks on long lived data or persistent storage.

Existing security solutions have mostly dealt with the attacks on the short lived data. We need to secure data not only on the wireless medium but we also need to secure data stored in the car's OBU and Road Side Unit (RSU).

Following are the set of attacks that are possible by the players

a. By the adversary on the wireless medium
   e.g. Filling the wireless medium with garbage data that can chock the network
b. By the adversary on the Central Authority
   e.g. Denial of service attack on the central server
c. By the revoked vehicles
   e.g. Replay attack
d. By the adversary on the group server (if group based approach is used)
   e.g. message suppression attack

The attacks mentioned above can also be further divided into three categories.

a. Leak attacks- all those attacks where the adversary gets hold of confidential information
b. Change attacks- all those attacks where the adversary changes the data in the secure data on the network
c. Destroy attacks- all those attacks where the adversary changes the data but the changes are invalid and they are detected by the system.

Few of the well-known attacks have been discussed earlier in the report.

5.4 Trust Assumptions:

Different trust assumptions have been taken by different solutions proposed in the literature. These trust assumptions varies across all the proposed solutions. Some of the solutions in literature have taken trust assumptions that cannot be taken in practical situations. Such solutions cannot be implemented in real life scenarios.

5.5 Core Security Primitives:

This includes all the important security primitives. Without these primitives, it is impossible to implement security of vehicular systems. These security primitives are very similar to those used for Mobile Ad Hoc Networks (MANETs).

5.5.1 Authentication:

The purpose of authentication is to establish the identity of a particular player in order to authorize their actions. For example, vehicles identified as ambulance will be given preference over the network as compared to normal vehicles.

In general, there are three ways to achieve authentication.

a. Public Key Infrastructure (PKI):

Each user is assigned a pairs of public and private keys and they can be used for authentication.

b. Central authority:

Central authority is used to authenticate each vehicle of the network.

c. Password based scheme:

Each user is given a user name and password and that can be used for authentication.

Most of the solutions proposed in the literature used PKI for authentication. Although PKI is the most secure among the approaches, it is also computationally most expense process.

5.5.2 Authorization:

The purpose of authorization is to allow the vehicle to access the data that it is authorized to access e.g. police vehicles can access data about other vehicles on the road.

5.5.3 Securing data on wireless medium:

We identify that protocol that is used for communication in wireless medium. It is important to secure data on the wireless medium. Strong encryption need to be used to make sure that data cannot be changed by adversaries while it is on wireless medium but there is always a tradeoff between the efficiency and secure encryption. Highly encrypted data makes the whole process computationally very expensive and thus less efficient.
There are also hardware available that support heavy weight cryptographic operations but they are expensive and sometimes their cost increase so much that they cannot be used in practical situations.

5.5.4 Key Distribution:

Most of the solutions implemented in the literature use Public Key Infrastructure (PKI). It is important to know how the keys are distributed among the players.

5.5.5 Revocation List:

It is important to keep a revocation list of all the vehicles that have been compromised. Revocation list is usually not stored in every vehicle because there are thousands of revoked vehicles and it is computationally expensive for vehicles to check each vehicle if it is revoked or not.

5.6 Granularity of Protection:

A system with security overhead has to deal with lots of cryptographic operations. To limit the overhead of these cryptographic operations, various systems implements different optimization techniques including aggregation of players into groups to simplify

authorization, and trading off the security of short-lived keys against the ease of management of long-term keys.

5.6.1 Group Membership:

The purpose of group based approach is to compactly represent the permission on a particular set of data by simply verifying the membership of a player into a group. Group leader is responsible for distributing group membership key. Communication is done between the vehicles and the group leader or between group leaders. Group leaders share the load of encrypting the data over the network.

5.6.1.1 Granularity of keys:

There are two types of keys that are can used in PKI

a. Short- lived keys:
These keys typically last for a short duration of time. Although it is more secure, it has larger overhead.

b. Long lived keys:
These keys typically last across sessions. Although it has lower overhead, it is less secure as compared to solutions with short lived keys.

There are few keys which are very long lived keys. These keys can create additional security concerns.

User Convenience:

It is very important that the proposed solution is user friendly and do not create problems for the users. E.g. if the user of vehicular network has to input username and password each time he/she is going to drive car will create inconvenience for the user. Solution should be such that it can be used in real life scenarios. Feasibility of the solution is also very important.

6 Evaluation of Proposed Security Solutions

In this section we will evaluate two state of the art security solutions proposed in literature, with the framework we have devised which is mentioned in the previous section. We will evaluate the solution proposed in SeVeCom project and a technique proposed by CMU lab which called “TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs”.

6.1 Secure Vehicular Communication Systems: (SeVeCom)

	Details
Players	OBU, RSU, Central Authority
Trust assumptions	Trusted Authority Greater computation power at RAs Adversaries will be less than legitimate vehicles Hardware Security Model
Attacks	Public Key Infrastructure (PKI) has been used Denial of Service attack possible Sybil Attack possible
Core Security Primitives	Authentication using PKI Authorization using PKI Central authority has the list of revoked users Central authority responsible for revocation of vehicles
Granularity of Protection	Holistic approach used Central authority responsible for computations Keys generated by the OBU
User Convenience/Feasibility	Expensive hardware used for OBU. Not feasible Large infrastructure needed for implementation

This table show the evaluation of the technique proposed in SeVeCom. Some of the factors, as shown in the table make this scheme unfit to be deployed in actual environment. For example

- This techniques is proposing to use HSM (hardware secure module), which is practically not possible. Even if there is a hardware in existence which is tamper proof, they deployment of these hardware to every car would be very expensive.
- For revocation it is proposing use of Certificate Revocation Lists (CRLs), but there are a lot of problems in using CRLs.
    a. First thing they propose is that we let the RSUs (Road side units) distribute the lists. But if we consider the size of the list could get very big if we were to become very big, and the speed of the transfer will not be sufficient to the transfer that amount of data in the short time.

b. Second way to revoke a vehicle, involves using HSM: It says that CA will send a kill signal to HSM and it will delete every this to prevent it from making new keys. The obvious problem in this approach is that using HSM is not feasible, as I mentioned in the first point. Secondly even if we do use HSM and an adversary can cut off the communication between the HSM and CA by dropping every message from CA to HSM, and if CA tries to send kill message through radio signal, an adversary can jam the band of frequencies the CA is transmitting on so no discernable message can reach to HSM. So even if we use the expensive and "supposedly" secure solution i.e. HSM the system is still not completely secure.
c. If we let the users download the CRLs from CA once a day it will give adversary much time to do the damage they want to do.
d. Another approach which is provided in this paper is to let the other vehicles decide which vehicle should be black listed. This technique is good but a possible attack could be that adversary vehicles surround a friendly vehicle and decide that it should be revoked.

- This technique used PKI (public key infrastructure), which is very good for cryptography but computationally it is very expensive, since VANET is very dynamic and the contact between vehicles is for very short time, it seems very unpractical to use PKI.
- As this techniques also proposes to use short term keys, which are provided to a used by CA, so that a user cannot be tracked by someone. But the problem here is that if an adversary gets a bunch of these short term keys from CA and distributes them to all his other adversary friend, this techniques doesn't propose any precautions for that case. This scenario would also be called Sybil attack.

6.2 TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs

In the table below, I have evaluated the TACking approach given by CMU-lab. In most of the scenarios this technique provides very good answers. But some of the short comings are discussed below.

- This technique tries to avoid Sybil attack by this

"P1. If an OBU sends two requests for TACK certificates to the same RA within a single time epoch, the RA is able to link these two requests to the same OBU.
P2. If an OBU sends two requests for TACK certificates in different time epochs or at different RAs, these requests are completely unlinkable. Property P1 prevents a malicious OBU from requesting multiple TACK certificates at the same RA within the same time epoch. On the other hand, property P2 guarantees legitimate senders' anonymity in the long run."

But what if an adversary gets the multiple keys and gives them to bunch of his friends and they use them in different RAs area. Then the Sybil attack is possible.

- There is always the problem of distribution of revocation lists, as mentioned for the previous approach.
- This technique also uses PKI which is computationally very expensive.

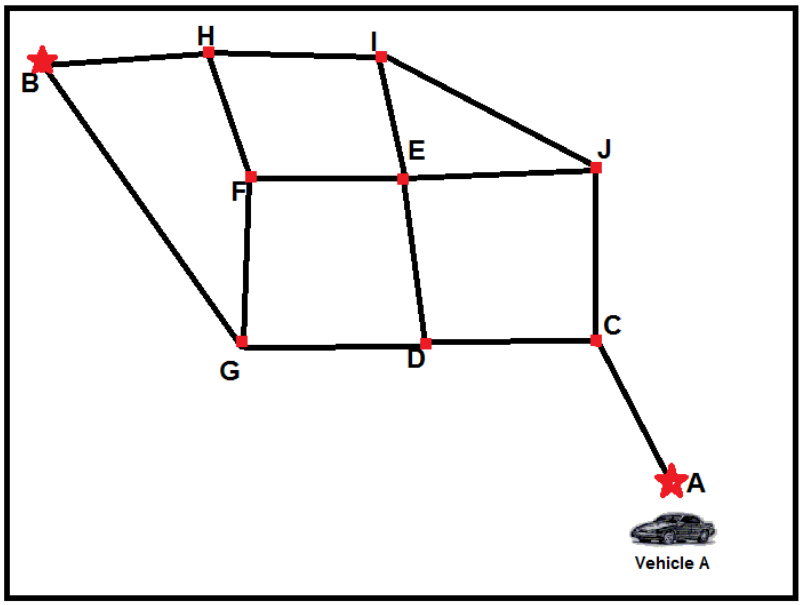
	Details
Players	OBU, Regional Administrators, Manager or central authority, Road side units
Trust assumptions	Trusted Authority Greater computation power at RAs Complete communication coverage
Attacks	Public Key Infrastructure (PKI) has been used Denial of Service attack possible Special defense against Sybil Attack Minimized the dynamic behavior of the network
Core Security Primitives	Authentication using PKI Authorization using PKI Manager has the list of revoked users Key distribution using long term key Revocation list is updated by the central authority
Granularity of Protection	Group membership is used Regions divided into Geographical locations. RA for each region Manager communicates with RAs Short term keys used for authentication and short term linkage
User Convenience/Feasibility	Computationally expensive solution Expensive Infrastructure needed for the implementation

7 Optimal Path Problem

The problem that we were dealing with was to finding an optimum path between the two points i.e. if vehicle wants to move from point A to point B, our algorithm should provide it with the best path between the two points. This algorithm will be 'smart' as it will keep traffic conditions into account when calculating the best path. The normal GPS navigators do not take this thing into account when calculating the path.

Our algorithm will integrate data collected from vehicular networks and GPS navigator systems to find the best path. The problem with the current navigators is that they use saved maps and GPS location to calculate the path for the driver. If we use data about traffic conditions from vehicular networks, it will calculate better result which will also decrease congestion on the roads.

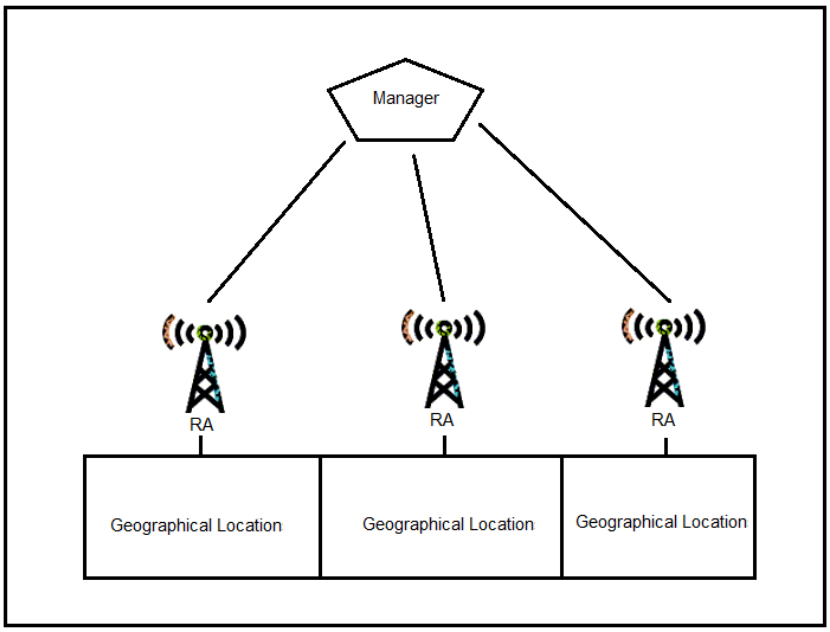
For example, Vehicle A wants to move from point A to point B on the road as shown in the figure below.



To move from point A to point B, the GPS system will just calculate the shortest path between the two points and give that path to the user. By using our algorithm, traffic conditions will be taken into account while calculating the path. The RA will do this for the cars. Each region will have an RA and it will calculate the time that each vehicle take while moving from one point to the other. It vehicles are taking too much time while moving between two points, it will find a different path for other vehicles so that other vehicles take alternative path and traffic

congestion is as minimum as possible. E.g. if path CDE is taking too long for the vehicles, it will find a different path and divert traffic to path CJE. This will 'intelligently' reduce the traffic congestion.

The basic architecture of vehicular network will be same as used in TACKing [10] that has been discussed earlier in the report. There will be one RA for each geographical region and there will be Manager that will be connecting RA's with each other. Path between two points will be calculated using data collected from each RA that lies on all possible paths between two points. Overall architecture for the vehicular network is given in the figure below.



We are still in the process of developing the algorithm. Once developed

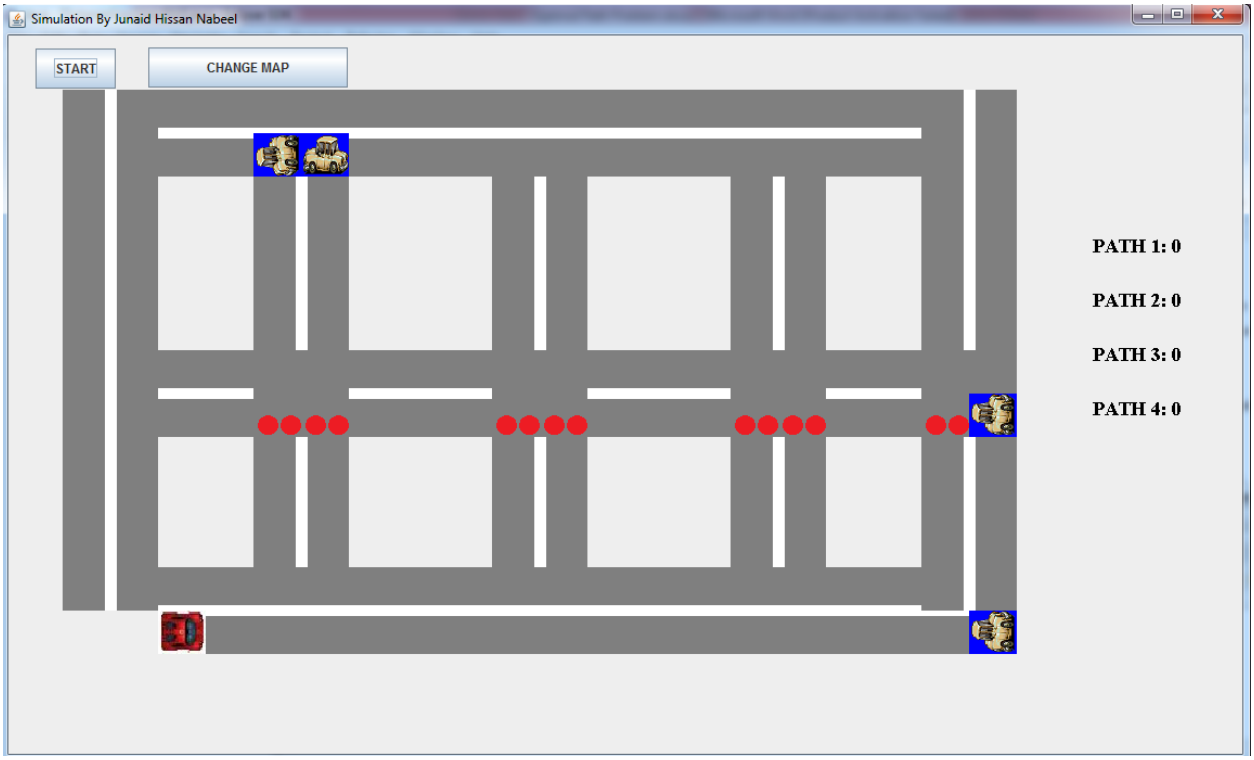
7.1 Algorithm

- A Vehicle at location A wants to go to point B.
- Contact local RA and ask for shortest path.
- If RA has a cached path or point B lies within the signal limit of RA it will return the shortest path.
- If not then the RA will contact CA, assuming it has all the paths from point A to B, will contact all the RAs responsible for the nodes present in all the path and calculate the shortest path and return it to A's RA with the result.
- Query CA every time we reach to next RA to get the updated path

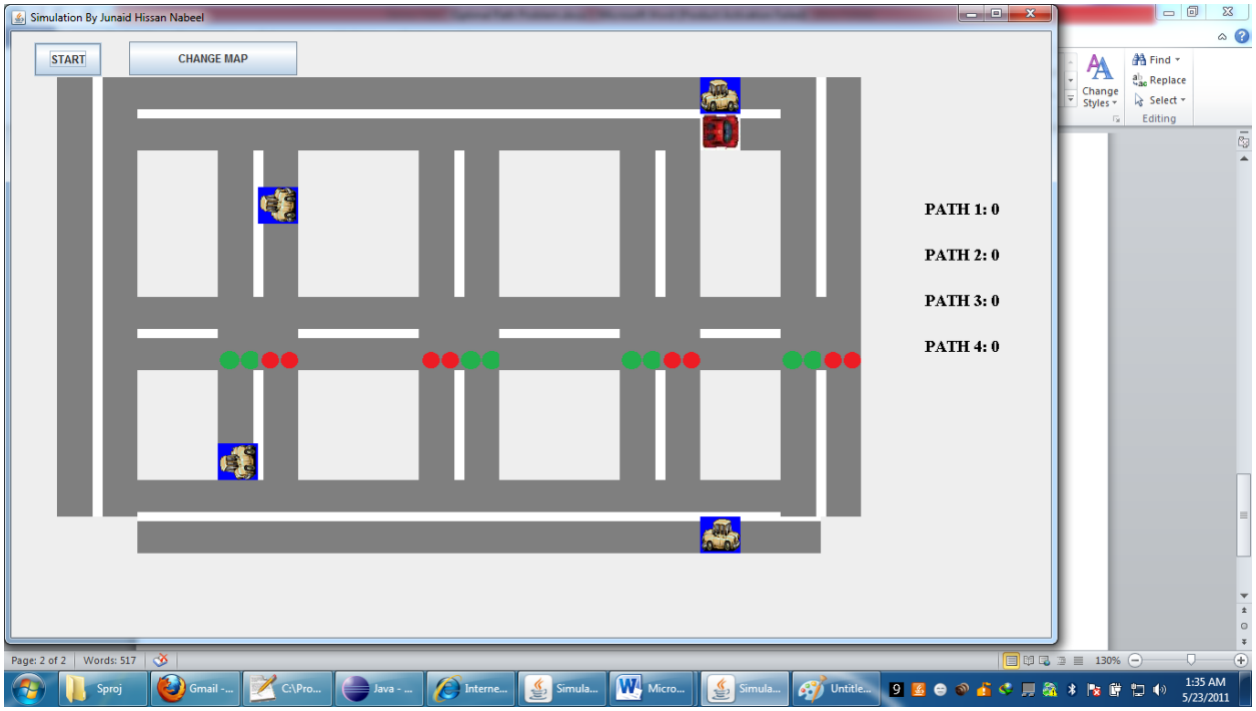
Updation of a path will take place base on the weighted average i.e. the most recent vehicles' input will be given most weightage.

7.2 Simulation

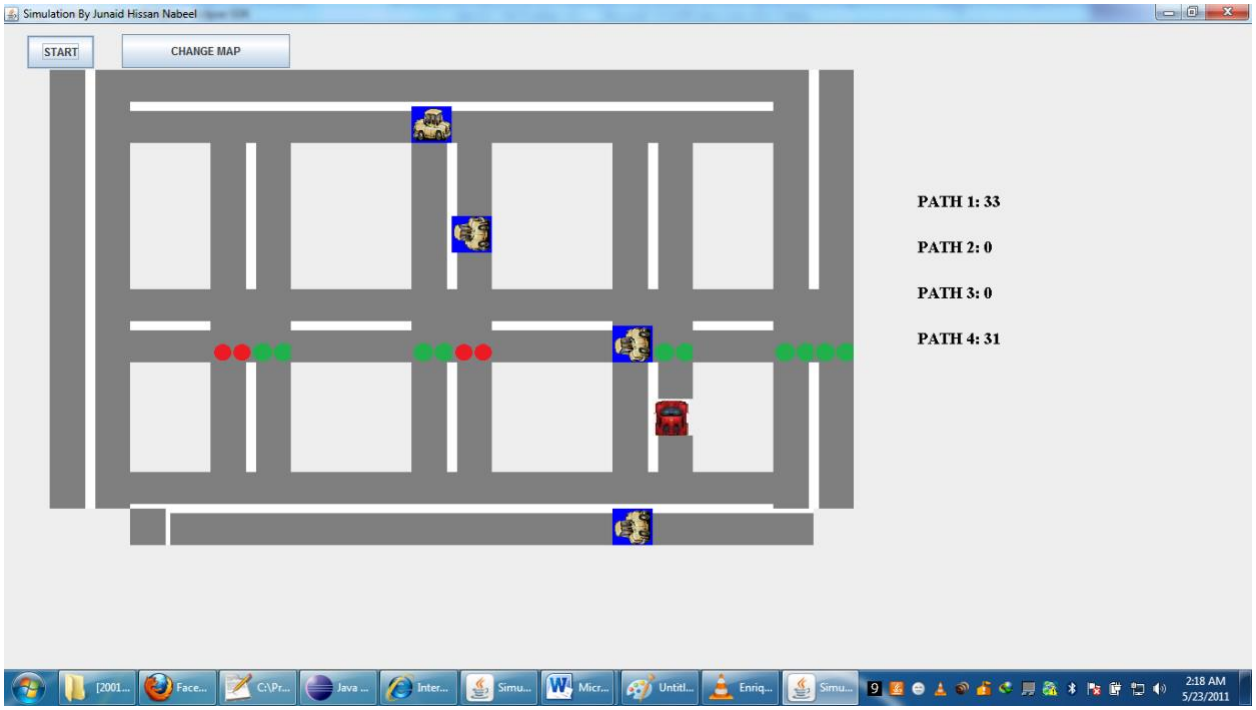
We have simulated this algorithm using Java (swing). The GUI shows a layout of roads which have varying length.

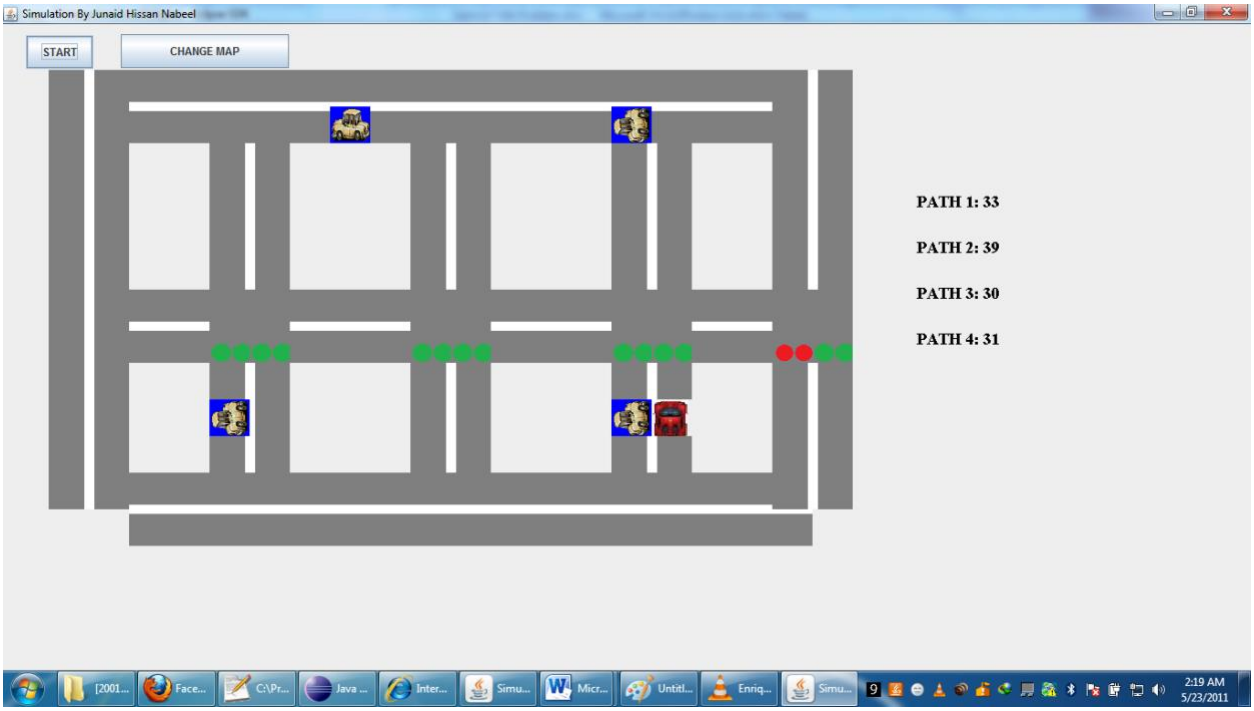


With a number of preprogrammed cars which move randomly in this layout and they follow all the rules of the traffic i.e. they only travel on the road, they only cross at the intersections, they only travel the right direction in the two way roads, they obey the rules of traffic lights etc. There is also a red colored car which has to move to point B (which is shown in the next figure). To get to the point B this car can take a lot of paths but we are only taking into consideration four paths whose travel times are shown at the right side in the figure. Initially these distances are set to zero. We have to choose an optimal path from these four paths. As currently in the database time taken for every path is zero so in first try it will take any path from these four paths, then the car will take the shortest path out of



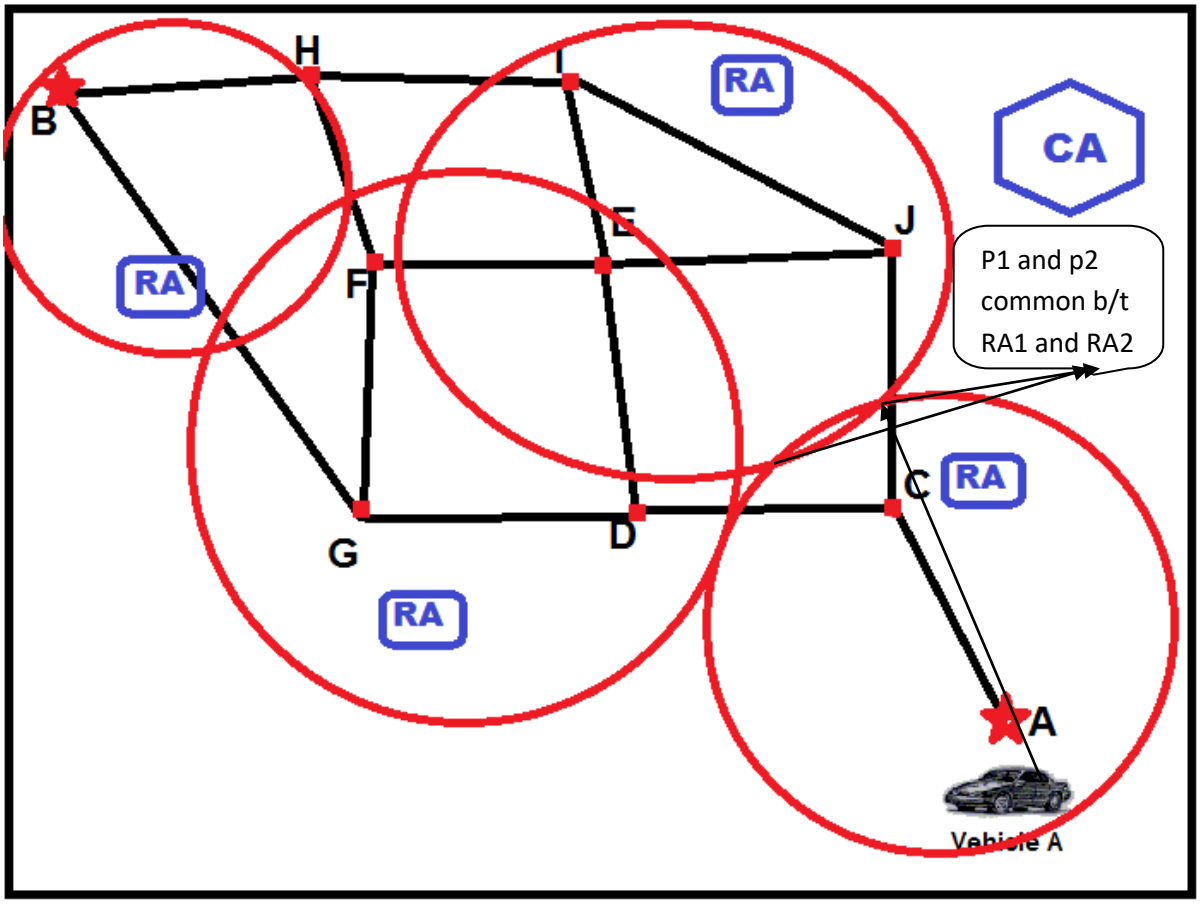
four paths we are considering. After a car goes through first path it will have a non-zero time of travel hence first four times the cars traveling from point A to B will go from all four paths and when we get the travel time of all the paths, next car will choose the shortest distance.





We have simulated this environment for one RA (regional authority). As a car wants to go to its destination which is outside the field of its RA it will contact CA (central authority). CA will tell it the overall shortest path considering the current constraints of the road. Then the current RA will find the shortest path which lies at some common point between itself and next RA which is in the shortest point mentioned in the path given by CA e.g.

As shown in the figure below there are multiple points common in RA1 and RA2 but CA will tell this RA to which path to choose to traverse the current optimal path. Then RA1 will find the least time consuming path till that point (p1), even if another shortest path between two RAs exists but between different points of RA1 and RA2 (say p2).



We are assuming here that when a vehicle sets out to take a path within one RA the region is small enough so that the roadside conditions don't change considerably to change the shortest path outcome. Anyway our results of the most optimal path are based on heuristics so given small scale of RA's region; the amount of time a car will take to traverse across the RA's reign won't be enough that most optimal path could drastically change in that time period. But for being on the safe side we will keep congestion control on each RA's end too so it doesn't send all the traffic to the most optimal path rendering it congested.

As we simulated our results for one RA, and we can replicate the same simulation for every RA which lies in the path provided by CA. We can query CA every time we reach to next RA to get the updated path.

8. References

1. Y. Zhang, J. Zhao and G. Cao, "Roadcast: A Popularity Aware Content Sharing Scheme in VANETs", Mobile Computing and Communications Review, Volume 13, Number 4, 2010

2. A Fundamental Scalability Criterion for Data Aggregation in VANETs Published: MobiCom 2009: Proceedings of the Fifteenth ACM SIGMOBILE International Conference on Mobile Computing and Networking, Beijing, China, September 2009

3. ” Secure Vehicular Communication Systems:Design and Architecture” P. Papadimitratos, L. Buttyan*y, T. Holczery, E. Schoch, J. Freudiger, M. Raya, Z. Mao, F. Kargl, A. Kung J.-P. Hubaux IEEE Communications Magazine, vol. 46, num. 11, 2008, p. 100-109*

4. Efficient Secure Aggregation in VANETs, *Maxim Raya, Adel Aziz and Jean-Pierre Hubaux*

5. Probabilistic Validation of Aggregated Data in Vehicular Ad-hoc Networks, *Fabio Picconi, Nishkam Ravi, Marco Gruteser and Liviu Iftode*

6. *Improved Security in Geographic Ad-hoc Routing through Autonomous Position Verification, Tim Leinmueller,Christian Maihoefer, Elmar Schoch and Frank Kargl*

7. Maxim Raya, Panagiotis Papadimitratos, Virgil D. Gligor, Jean-Pierre HubauxSchool of Computer and Communication Sciences EPFL, Switzerland

8. “Service Scheduling of Vehicle-Roadside Data Access” Yang Zhang · Jing Zhao · Guohong Cao

9. F. Kargl et al., “Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges,” IEEE Commun. Mag., vol. 46, no. 11, 2008, pp. 110–18.

10. A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing Together Efficient Authentication Revocation, and Privacy in VANETs," *IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2009*

11. Detecting and CorrectingMaliciousData in VANETs, *PhilippeGolle, Dan Greene and Jessica Staddon*

16

12. Securing Vehicular Ad Hoc Networks, *Maxim Raya and Jean-Pierre Hubaux*

13. Attacks on Inter Vehicle Communication Systems - an Analysis, *Amer Aijaz, Bernd Bochow, Florian Doetzer, Andreas Festag, Matthias Gerlach, Rainer Kroh and Tim Leimueller*

14. Securing Vehicular Communications, *Maxim Raya, Panos Papadimitratos and Jean-Pierre Hubaux*

15. Rate Adaptation in Vehicular Networks

16. Challenges in Securing Vehicular Networks, *Bryan Parno and Adrian Perrig*

17. Security Issues in a Future Vehicular Network, *Magda El Zarki, Sharad Mehrotra, Gene Tsudik and Nalini Venkatasubramanian*

18. AMOEBA: Robust Location Privacy Scheme for VANET Krishna Sampigethaya, Mingyan Li, Leping Huang, and Radha Poovendran

19. Survey of Inter-Vehicle Communication, *Jun Luo and Jean-Pierre Hubaux*

20. T-Drive: Driving Directions Based on Taxi Trajectories

21. Intelligent Transportation with Networked Cars

22. Probabilistic Path Queries in Road Networks: Traffic Uncertainty Aware Path Selection¤

23. A Frame Work For Evaluating Storage System Security.

24. Heuristic shortest path algorithms for transportation applications: State of the art L. Fua, *⁎, D. Sunb, L.R. Rilettc*