Sindh Univ. Res. Jour. (Sci. Ser.) Vol.43 (1-A) 35- 42 (2011)

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

Privacy issues in VANETs Intelligent Applications

A. Sajid[1], A.H.S Bukhari[2] and A.W. Shaikh[3]

[1]Department of Computer Science, "Balochistan University of Information Technology, Engineering and Management Sciences, Quetta"

[2]Dean Faculty of Information and Communication Technology, "Balochistan University of Information Technology, Engineering and Management Sciences, Quetta"

[3]Department of Computer Science, Shah Abdul Latif University, Khairpur, Pakistan
Bukhari@buitms.edu.pk, Awahid.shaikh@salu.edu.pk

Cor A. Sajid: ahthasham.sajid@buitms.edu.pk
rev

Abstract: The communicating nodes in Ad-hoc networks are dynamic in nature if we compare them by the traditional network nodes which appears in any fixed network infrastructure and usually Adhoc networks are deployed in specific environment to achieve certain goals so therefore due to these features security challenges also increases in comparison with other traditional networks or we can say the method used in fixed infrastructure networks is not directly be applied in the case of Adhoc networks. So a short-range wireless channel has security problems that differ from those of more conventional networks.

This paper focuses on the security issues concerned with Vehicular networks which are the most emerging forms of Adhoc network now days. Basically privacy is the main concerned under the security umbrella in the case of Adhoc networks because user private data need to be protected by the authorities such that from location profiling and from other attacks on their privacy.

Goals like system availability and security can be achieved only with the coordination among system operators and car manufacturers so that the faulty units can be identified easily.

Keywords: MANETs, VANETs, GPS, EDR

INTRODUCTION

Ad-hoc Networks:

There is no predefined infrastructure in case of Adhoc networks because network can changed dynamically so to manage operations under this type of network; it can be partitioned in different sub networks as well It is a collection of nodes which do not depend on a predefined infrastructure to keep the network connected. If Adhoc network consists of mobile node which can be static and wired nodes it will be called (MANET) and can obtain services offered by the fixed infrastructure. (b)

Adhoc networks allow users to access any information and resources similarly as it can be done in wired networks. (a)

SECURITY THREADS IN ADHOC NETWORKS:

Attacks Categories:

- Passive Attacks (b)
- Active Attacks (b)

Passive Attacks:

These are the types of attacks by which any attacker can Only monitor the transmission by obtaining messages contents or monitor traffic flows by eavesdropping. (b)

Active Attacks:

By active attacks an attacker can cause any serious damage to the data or information like data can be modified, replay previous messages to cause denial of service attack or successfully masquerade of one entity as some other. (b)

External Attacks:

These are targeted Active Attacks which actually damage the routing information or can cause any service so that it can't work properly or even at maximum the specific service can be shut down by these attacks and the most dangerous is that these external active attacks can cause network congestion. The best way to prevent these types of attack is by applying security mechanism standards like firewalls, encryption. (b)

Insider Attacks:

They are the more harsh attacks, it is done by the node which already is a trusty node within the network and protected by the security mechanism of that network. (b)

Denial of Service:

This attack is usually thrown to cause damage to a centralized service provided by any machine but in the case of Adhoc it is difficult to cause DOS attack due to the distribution of responsibility. Due to the bandwidth to operate with in smaller Adhoc networks they can be crashed by Distributed denial of service attack. (b)

Impersonation:

The major security risk occurs in Adhoc networks if there is not any proper authentication of communication parties involved within the network so by that any node will become the compromising node and by accessing that node any other unauthorized party can become a part of network as well by masquerading and send even false routing information. (b)

BACKGROUND OF VANETs

Any Adhoc network refers to the network in which the devices connect themselves not in a centralized manner therefore the network will be organized in self manner as well as hoping will be multi-hop routes for the network.

VANETs differ from MANETs due to the movement of node is high and also they are large in number the communicating nodes even though VANETs is operated and rolled out by multiple companies and similarly the participating nodes belong to people within different organizational structures. (c)

Both MANETs and VANETs has property that characterizes them is that they are self-organizing and decentralized systems. Due to this dynamic characteristics of Adhoc networks approaches for security and privacy therefore must not rely on central services or mandatory connections to some fixed infrastructure. In the case of VANETs at the time of car production or at the time of regular maintenance only the access should be given to central services. (c)

MATERIAL AND METHODS

INTRODUCTION OF VANETS:

In recent few years to recognize the events to widen the driver's horizon which local sensors cannot detect or even by the drivers alone so car manufactures realizes to interconnect their vehicles. So that the events like critical driving conditions can be detected and related information can be passed on to vehicles in the vicinity with on-board sensors. For exchanging that information about the current driving situation, vehicles form a natural network, known as a vehicular ad-hoc network (VANET) using direct inter-vehicle communications (IVC).The basic concept of such so called local danger warnings (LDW). (e)

(Fig. 1) llustrates the concept of LDW (Local Dangerous Warnings). Information about the observation of locally reduced resistance caused by an oil slick is communicated among the vehicles. In particular, the following problem domains have to be addressed: (e)

1. **Data collection**: Collection of data on the current road situation.
2. **Individual situation analysis**: Analyze locally collected data to detect special situations.
3. **Information dissemination**: Dissemination of information within the VANET.
4. **Cooperative situation analysis**: Analyze distributed data to detect special situations.
5. **Relevance evaluation**: Evaluate significance for individual driving task.
6. **Situation prediction**: Predict future individual driving situation.
7. **Situation indication**: Indication of special situations to the driver.

Fig. 1: Exemplary LDW Scenario. (a)

Vehicle information system architecture can be capable of managing the huge amount of data. The LDW application must have the followings.

- **Reliable**
- **Secure**
- **Protect the customers' privacy rights in all circumstances.**

NETWORK MODEL*:*

Communication among the VANETs networks will be done by two nodes or entity one will be obviously vehicles while the second entity can be base station. In the case of vehicles the communicating node either base station or vehicle could belongs to private individual as well as government organization as illustrates in **(Fig. 2)**.

Because in VANETs the network totally dependent on the basic communicating node that is vehicles so therefore the two main factors will be involved due to the high speeds movement of vehicles will be mobility and short connection times between neighbors at the time of takeover. (g)

The features of power generation and computation as well as power consumption are the advantages which differentiate Adhoc network with the traditional networks. VANETS can support huge number of microprocessor Devices like EDR (Event data recorder) and GPS (Global Positioning System). So by the use of GPS devices is not only the solution for security support in VANETS; we have also describe alternative options. (g)

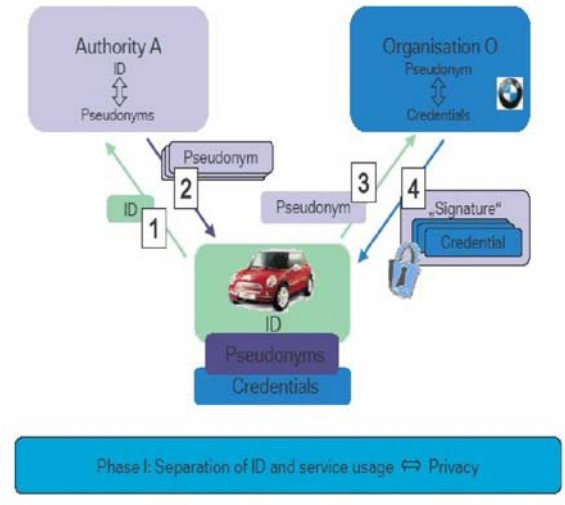

Fig. 2: A VANET Setup describing primarily safety messages exchanges to the drivers. (g)

THREE PHASES OF OPERATION:

A single vehicle lifecycle can be distinguished from three phases. [c]

1. The initialization phase illustrates in **(Fig. 3)** (where the systems of a vehicle are set up). (c)

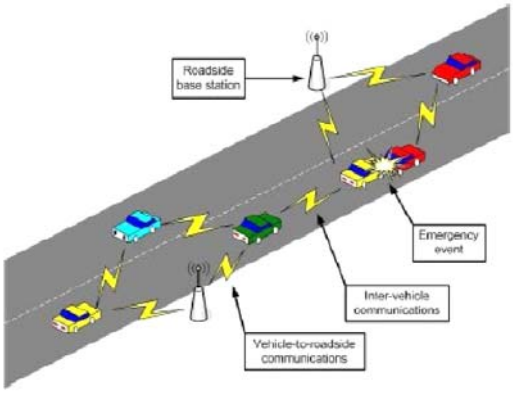

Fig. 3. Phase I (initialization phase) (c)

2. The operational phase illustrated in **(Fig. 4)** (where the major mode of operation, where vehicles can send messages signed according to a chosen pseudonym). (c)

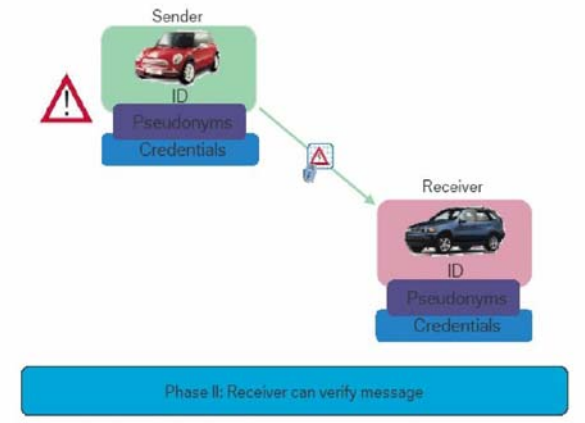

Fig 4. Phase II (operational Phase) (c)

TYPES OF COMMUNICATION:

Type of communication addressing in VANETs focused on geographical areas due to the mobility factors of vehicles so therefore the communication requirement among VANETs is different from other network application which uses uni-cast or multi-cast communication. (f)

Self-organization and -management:

In VANETS the control should be decentralized always. Even more, VANETs hold an additional complexity due to special conditions (i.e.,

the above-mentioned timing and reliability requirements together with probable saturation conditions when a VANET is fully deployed). (f)

Interaction with on-board sensors:

Position based routing is used in VANETs so for that on-board sensors like GPS should be used by network protocols other then applications themselves. There can be many factors which can be cited and play a part in explaining the nature of VANETs specifically in comparison with other Adhoc networks the list appears in this article is sufficient to motivate the need for a specific VANET protocol architecture. (f)

Packets vs. information:

VAN ETs application is mostly used for security measures during driving to protect different kinds of attack and accidents so therefore the VANETS data payload is not just the actual packet payload as used in other classical networks However, information dissemination in VANETs is done basically on the basis of evaluating actual packet contents with comparison with the state of specific node to decide the updated information to be disseminated always

3. And the credential revocation phase illustrated in his operation is known as 'in-network' processing. (f)

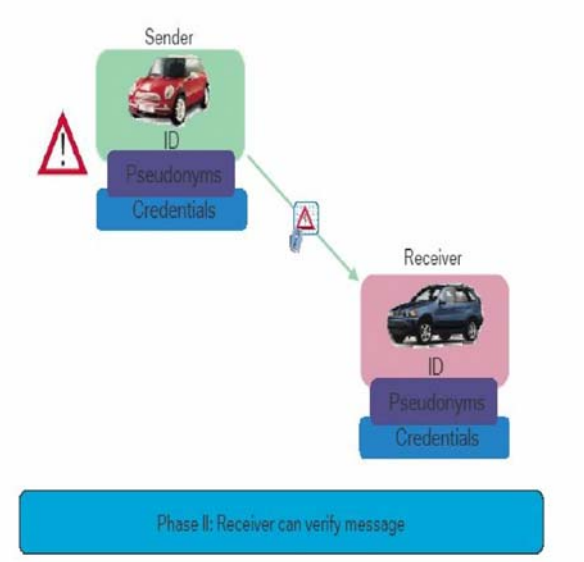

Fig 5. Phase III (Credential Revocation Phase) (c)

(Fig. 5) (where predefined situations can lead to the disclosure of a vehicle's real ID and the shutdown of its system). (c).

End-to-end notion revisited:

Communication endpoints' are well defined by an ID or by a multicast group in traditional network by the use of peer application and protocols entities. However, the VANET communication entities works on the basis of geographic and topology basic which may change due to its dynamic nature in case of VANETs so similarly if two entities are communicating like a peer so only uni-cast communication is possible between them.(f)

ARCHITECTURE:

The goal of designing any protocol architecture is to achieve Interoperability for communication among network nodes. If we talk about just communication suit for VANETs two approaches can be taken: (f])

In first approach overall functionality could be arranged in layered approach like TCP/IP and ISO/OSI by decomposing different functionalities at each. Second approach is a customized approach which will meets the requirements of VANETs. (f)

Non-layered approach: figure 6 describing the fact that by the use of modular approach the constraints like assigning a function to a specific layer and interaction between the layers can be removed. In the following, we will describe both fundamentally feasible but extremely opposite approaches and briefly outline the advantages and disadvantages. Afterward, having learned the benefits of both systems, we will describe a third approach and argue why we think this protocol Architecture would be better-suited for a VANET system. (f).

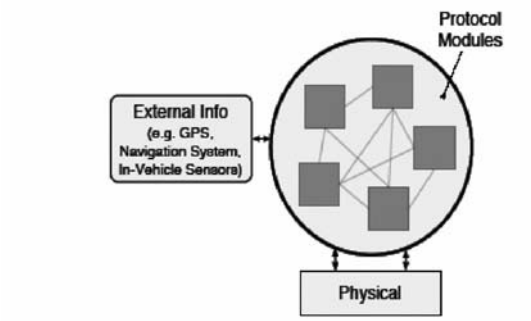

Fig. 6. Un-layered Approach (f)

Safety application is the primary concerned of *un-layered approach* as per the needs of VANETs.The idea in this approach is that put all protocols and application involved in communication

is a single logical block over the physical interface by which sensors are connected to the external sources (like sensors) as illustrated in **(Fig. 7)**.

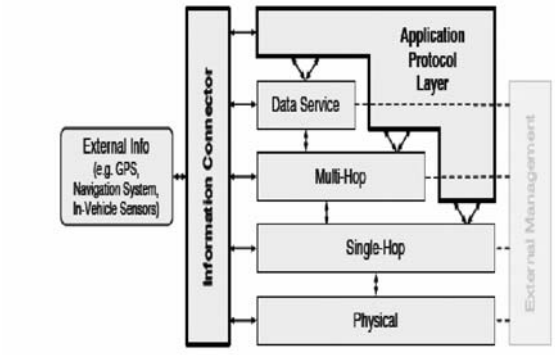

Fig. 7. Sketch of VANET architecture (f)

Presents a concept in between the two 'extreme' options commented above. With this proposal we intend to use the most adequate features of both options, i.e., *i)* having a layered approach that gives us a clear and modular structure where to build our applications and protocols, but also offering *ii)* a clean way of sharing information and to cooperate between any protocol module on any layer as needed. Describing our proposal, we identify the following key features: (f)

RESULTS AND DISCUSSION

SITUATION ANALYSIS:

In order to develop a picture of the vehicle's current and future ambient road conditions a situation analysis is used, its goal is to gain knowledge from collected & received date, which can be improved by exchanging the information. In general, situation analysis can be classified into two types that are further described in the following: (e)

- **Individual situation analysis**: analysis of collected data by an individual vehicle (e)

- **Cooperative situation analysis**: distributed situation analysis using shared information. (e)

APPLICATION CATEGORIES:

Most of the vehicle applications are proposed by car manufactures. The range of application can be very wide but we can divided them into two major categories: (d)

Safety-related applications: The main concerned while driving is the life of a human being so every situation in which any incident or action can damage a human life (such as collision avoidance, cooperative driving, and traffic optimization) may need to be communicated on time by these applications.

Non Safety-related applications: These application targeted all other activities in which the primary focused is not to safe a human life including payment services (e.g., toll collection), location-based services (e.g., finding the

Closest fuel station), infotainment (e.g., Internet access). Security is also required in the discussed application but just only where the E-payment involves by any mean. (d)

The most intelligent application among different car manufacturers is local danger warning message as illustrated in Fig 9 during driving, such as accidents, road conditions, their own behavior (e.g. emergency braking) and so on. So the feature of these applications is to distribute those messages to the neighboring nodes (cars) by using wireless communication or it can also store those safety related messages by moving along the road if at that time no neighboring node found when the specific event occur and recorded by the application. (c)

Methods to detect any safety measure are different. (c)

- Like any safety event detected by a single car by its sensor is basically aggregated as local information only if the event got matched in that case message will be communicated outside the local domain. (c)

- To detect event regarding the traffic whether it is jam or open so that have to be detected by using the information collected by multiple cars position and later it will be aggregated, in this case individual car may wrap up it its status is anywhere in between the traffic jam (like before or after). Duplicate or matching information can affect reliability as well as privacy. (c)

INFORMATION MANAGEMENT:

To describe the current driving context the vehicles had to gather a huge amount of different information, and then share this information with all other vehicles, the amount of data that has to be managed by the in-vehicle information system increases tremendously. (e)

So in this contest, the in-vehicle information system has to offer efficient means of storing and

accessing geographical related information, comprising both own observations and remote observations from distant vehicles. (e)

In general, it can be assumed that information is valuable if it contains new knowledge about a particular road situation. This knowledge can be of three types. (e)

- **Presence of a special** situation that was previously unknown. (e)
- **Deviation of a special situation** from what was expected. (e)
- Absence of a special situation that was expected. (e)

INFORMATION DISSEMINATION:

Information dissemination is the most challenging part of the LDW (Local Danger Warning), due to the reason being that it is influenced by almost all of the problem domains. The items that the vehicles exchange are referred to as messages, which are used in VANET to distribute information about the current road situation and inform other vehicles of unexpected situation. Receiving vehicles evaluate the message content. Obviously, there are many possible designs for the message format, content and communication protocols. (e)

PRIVACY ISSUES IN VANETs:

Why is Privacy Important for VANETs?

In 21st century most of the human beings identified by the cars they are holding which indeed highlights their image and status among the society. Car may be used by a person to store any personal information as the technology becomes superior. Like many of the car manufacturers and various vendors introduced navigation (direction findings) systems by which the movement of the car can be traced out by a car owner itself at any time. (c)

Privacy Threats:

The degree of privacy may differ under prescribed circumstances accordingly so therefore it is not desirable to achieve perfect privacy in every situation. The degree of privacy determines the goals of the system for which the privacy has to be designed ultimately. (c)

In the following we will give some examples for the problems we have to tackle in a widespread VANET. (c)

To calculate behavior of a driver during its drive hello beacons is used for that by police so that if he or she is over speeding so tickets may be issued to the concerned user. (c)

Similarly if any communication is taking place in the parking area of a organization so by using the car identifier it can be identify easily which car belongs to which personnel therefore arrival and departure status can be maintained accordingly in effective manner. (c)

By detecting the movement of a car by its patterns any penalty can be charged for any misuse or harmful act this is usually done by insurance companies. (c)

Similarly as above law enforcement vehicles can also be monitored by the criminal organization with the use of stationary information and VIPs can be tracked too. (c)

Privacy Related Requirements:

The followings are a number of requirements to achieve adequate privacy. (c)

Better not to use any real-world identity which may behave as an identifier for that particular user or node solution is that only pseudonyms. (c)

Even pseudonyms can be changed with respect to the application and threat model if defined any. (c)

Only in special situation pseudonyms should be mapped to real-world identities (c)

By the use of cryptography we can bound pseudonyms by combining properties or privileges group wise. (c)

SAFETY MESSAGES:

Traffic information messages: Any information regarding traffic may be distributed by these messages for any specific area which definitely affect public safety but these messages are not time-critical. (d)

General safety-related messages: Information regarding collision during driving may be covered by these types of messages for every application which is designed for public safety so there should not be any type of delay while communicating these messages. so keeping that in mind it should contain information like Position, Speed, Direction Acceleration of the vehicle (d)

Liability-related messages: theses messaged are exchanged just in the case of accidents mean in liability situation. (d)

BASIC SAFETY MESSAGING PROTOCOL:

Protocol to efficiently disseminate safety messaging in VANETs communication. (d)

In compliance with the DSRC specifications, we assume that each vehicle V periodically sends messages over a single hop every 300 ms within a range of 10 s travel time (the minimum range is 110 m and the maximum is 300 m). (d)

- The inter-message interval drops to 100 ms and the range to 15 m if the vehicles are very slow or stopped (i.e., their speed is less than 10 miles/h or ≈ 16 km/h). (d)

- Vehicles transmit new messages but take decisions based on the received messages. For example, if vehicles V receives any emergency warning by its neighboring vehicles W at certain time the both vehicles will mutually decide either which one is in danger keeping in mind their mutual position it sends out its own warning messages. (d)

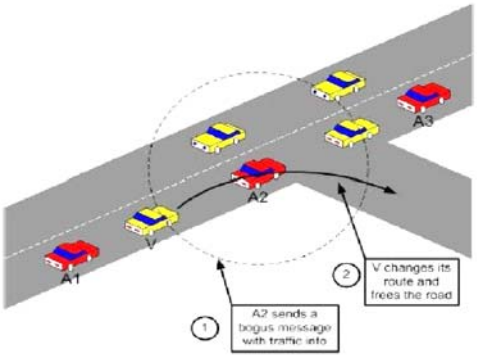

Fig. 9: Bogus Information Attack

ATTACKS ON VEHICULARNETWORKS:

Attacker's model

There are three dimensions to classify the capacities of an attacker. (d)

1. Insider vs. Outsider.

- Insider is actually any node within the network which will have public key by that it will be identified as authenticated. (d)

- The outsider node may be any node which will become as an intruder similarly the types of attack which may be attacked by internal node will differ from this malicious node. (d)

2. Malicious vs. Rational.

- A malicious attacker seeks no personal benefits from the attacks and aims to harm the members or the functionality of the network. Hence, he may employ any means disregarding corresponding costs and consequences. A rational attacker seeks personal profit and hence is more predictable in terms of the attack means and the attack target. (d)

3. Active vs. Passive.

- Attacker who can initiate any operation within the network like he can generate packets or signals.

Where on the other hand any attacker who cannot took such action is considered to be passive such that he or she can just monitor the traffic of wireless channel.(d)

SPECIFIC ATTACKS:

1. Bogus information: As name suggests an attacker may launch a attack by using the bogus (mock) information by that false information it may disturb the behavior of the network as well as nodes behavior too. (d)

2. Cheating with positioning information: As name suggest cheating can be done regarding the position of a car it direction and as well as speed the attacker Im.R.A may do that to get rid of any type of liability regarding him or her if an accident happen.

3. ID disclosure of other vehicles in order to track their location. Targeted vehicles can be observed or monitor by using trajectories from global node and that information such that IDs can be used for many purposes this is usually done by the vehicle car tracking companies to track their vehicles. (d)

Denial of Service: The attacker is *.M.A and may want to bring down the VANET or even cause an accident. Example attacks include channel jamming and aggressive injection of dummy messages. (d)

Masquerade: If an attacker can successfully claim the identity of another vehicle on the basis of its identity so attacker may achieved malicious or rational objectives. (d)

HOW TO SECURE VANETS?

Requirements:

A security system for safety messaging in a VANET should satisfy the following requirements: [d]

• **Authentication:** Vehicle reactions to events should be based on legitimate messages (i.e., generated by legitimate senders). Therefore we need to authenticate the senders of these messages. (d)

Verification of data consistency: The legitimacy of messages also encompasses their consistency with similar ones (those generated in close space and time), because the sender can be legitimate while the message contains false data. (d)

• **Availability:** Even assuming a robust communication channel, some attacks (e.g., DoS by jamming) can bring down the network. Therefore, availability should be also supported by alternative means. (d)

Non-repudiation: Drivers causing accidents should be reliably identified; a sender should not be able to deny the transmission of a message (it may be crucial for investigation to determine the correct sequence and content of messages exchanged before the accident). (d)

Privacy: People are increasingly wary of Big Brother enabling technologies. Hence, the privacy of drivers against unauthorized observers should be guaranteed. (d)

Real-time constraints: At the very high speeds typical in VANETs, strict time constraints should be respected. (d)

CONCLUSION

In this paper we have explained security needed in Mobile-Adhoc networks, security threats related to Ad-hoc network the types of attacks which can occur and their solutions. We have also explained in the second part of this report! Why vehicular networks need to be secured, and why this problem requires a specific approach we discussed why privacy is important in VANETs and threats related to its privacy. Whereas privacy among VANETs may vary due to change in environment and it can also dependant on requirements needed by certain applications which could be adjustable.

Two approaches are discussed to cover the privacy concerned in VANETs and also a security architecture is proposed which best cover the privacy concerned related with VANETS along with the related protocols during the proposed architecture it being identify that public key cryptography is the best technique in case of VANETs.

In terms of future work, how manufacturers and governmental bodies can cover the issue of how to successfully and effectively key may be distributed by using a secure channel.

ACKNOWLEDGMENT

This is the extended version of our own paper presented and published as Conference proceedings in "International Conference on Computers & Emerging Technologies" (ICCET 2011) held on 22-23 April 2011 at Shah Abdul Latif University, Khairpur, Sindh, Pakistan.

References:

http://www.webopedia.com/TERM/S/secu rity.html

users.tkk.fi/~vkarpijo/netsec00/netsec00_manet_sec.pdf

www13.in.tum.de/personen/doetzer/publications/Doetzer-05-PrivacyIssuesVANETs.pdf

cawww.epfl.ch/Publications/raya/RayaH0 5C.pdf

www.mobile.ifi.lmu.de/common/Literatur/MNMPub/Publikationen/adst06/PDF-Version/adst06.pdf

dsn.tm.unikarlsruhe.de/medien/publicationconfs/fuesler-wit05-thoughts-protocol.pdf

ducati.doc.ntu.ac.uk/uksim/journal/Vol-5/No-3&4/THOMAS**.pdf**