The Security Problems of Vehicular Ad Hoc Networks (VANETs) and Proposed Solutions in Securing their Operations

L. Ertaul[1], **S. Mullapudi**[2]
[1]Department of Mathematics and Computer Science, California State University, East Bay, Hayward, CA, USA,
Levent.Ertaul@csueastbay.edu
[2]Department of Mathematics and Computer Science, California State University, East Bay, Hayward, CA, USA,
smullapadi@horizon.csueastbay.edu

Abstract - *The successful deployment of vehicular ad hoc networks (VANETs) has to overcome the serious security threats which impair the operation of different vehicular applications. This paper presents the vulnerabilities of vehicular ad hoc networks and analyzes some of the security problems inherent in VANETs and also presents proposed solutions to overcome some of the vulnerabilities and security problems.*

Keywords: CA, ICV, Security of VANETs, VANETs.

1 Introduction

Inter-Vehicular Communications (IVC) also known as vehicular ad hoc networks (VANETS) have become very popular in recent years. A Vehicular Ad hoc Networks is a special type of Mobile Ad hoc Networks (MANETs is a kind of wireless ad hoc networks and is self configuring network of mobile routers connected by wireless links) which use vehicles as nodes [1], [2], [3], [4], [5], [6]. The main difference is that mobile routers building the network are vehicles like cars or trucks [3], [4], [7], [8]. Several different applications are emerging with regard to vehicular communications. For example, safety applications for safer driving, information services to inform drivers about the driving hazards and other business services in the vicinity of the vehicle. Governments, corporations, and the academic communities are working on enabling new applications for VANETs. A main goal of VANETs is to increase road safety by the use of wireless communications. To achieve these goals vehicles acts as sensors and inform each other about abnormal and potentially hazardous conditions like accident, traffic jams and glaze [2], [4], [7], [9], [10], [11]. Vehicular networks closely resemble ad hoc networks because of their rapidly changing topology; [2], [3], [11], [12], [13] therefore; VANETs require secure routing protocols. “Numerous Applications are unique to the vehicular setting. These applications include safety applications that will make driver safer, mobile commerce, roadside services that can intelligently inform drivers about congestion, businesses, and services in the vicinity of the vehicle” [2]. “VANETs, especially compared to MANETs are characterized by several unique aspects. Nodes move with high velocity, resulting in high rates of topology changes” [3]. “Because of rapidly changing topology due to vehicle motion, the vehicular network closely resembles an ad hoc network. The constraints and optimizations are remarkably different. From the network perspective, security and scalability are two significant challenges” [2]. “A formidable set of abuses and attacks become possible. Hence, the security of vehicular networks is indispensable” [4]. “The growing importance of inter-vehicular communications (IVC) has been recognized by the government, corporations, and the academic community. Government and industry cooperation has funded large IVC partnerships or projects such as Advanced Driver Assistance Systems and CarTALK 2000 in Europe, and FleetNet in Germany. VANETs pose many challenges on technology, protocols, and security which increase the need for research in this field” [2].

This paper is organized in the following way. Section 2, gives general introduction to Vehicular Ad hoc Networks (VANETs). Section 3 presents the security issues inherent in VANETs which gives an insight into the vulnerabilities of vehicular ad hoc networks. Section 4 describes the false position information problem and also presents the effects of falsified position information. Section 5 gives an overview of the Sybil attacks in VANETs. Section 6 discusses the proposed solutions to security problems in VANETs thereby providing the security architecture needed to overcome the security threats. Section 7 introduces the proposed solutions to false position information in which each node uses multiple sensors like Acceptance Range Threshold (ART), Mobility Grade Threshold (MGT), and Maximum Density Threshold (MDT) to detect malicious and selfish behavior of nodes. Section 8 addresses the Sybil attack problem presented in Section 5 by presenting a proposed solution called Basic Signal Strength Based Position Verification. Section 9 concludes the paper.

2 Vehicular Ad Hoc Networks (VANETs)

The networks that interconnect vehicles on road are called Vehicular Ad hoc Networks (VANETs) [2], [3], [4], [14]. “A mobile ad hoc network (MANET) consists of mobile nodes that connect themselves in a decentralized, self-organizing manner and may also establish multi-hop routes. If mobile nodes are cars this is called vehicular ad hoc network” [15]. “The main target of research in VANETs is the improvements of vehicle safety by means of inter vehicular communication (IVC)" [3]. Several different applications are emerging in VANETs. These applications include safety applications to make driving much safer, mobile commerce, and other information services that will inform drivers about any type of congestion, driving hazards, accidents, traffic jams [2], [4], [9], [10], [16]. VANETs have several different aspects compared to MANETs, in that the nodes move with high velocity because of which the topology changes rapidly [2], [3], [9], [11], [12], [13]. VANETs are also prone to several different attacks. Therefore, the security is of VANETs is indispensable. VANETs pose many challenges on technology, protocols, security which increase the need for research in this field [17].

3 Security Vulnerabilities of VANETs

Vehicular ad hoc networks are also prone to several vulnerabilities and attacks. These vulnerabilities can cause small to severe problems in the network and also poses some potential security threats which can deteriorate their functioning. The following section gives a general overview of Vehicular Communications vulnerabilities which are discussed in [4].

A. Jamming: The jammer deliberately generates interfering transmissions that prevent communication within their reception range. Fig. 1 illustrates that an attacker can relatively easily partition the vehicular network. As the network coverage area (e.g., along a highway) can be well-defined, at least locally, jamming is a low effort exploit opportunity.

B. Forgery: The correctness and timely receipt of application data is major vulnerability. The attacker forges and transmits false hazard warnings which are taken up by all vehicles.

C. Impersonation: Message fabrication, alteration, and replay can also be used towards impersonation. For example, an attacker can masquerade as an emergency vehicle to mislead other vehicles to slow down and yield. A vehicle owner deliberately stealing another vehicle's identity [5] and attributing it to his or her own car or vice versa.

D. Privacy: The inferences on driver's personal data could be made, and thus violating his or her privacy. The vulnerability lies in the periodic and frequent vehicular network traffic: Safety and traffic management messages, transaction based communications (e.g., automated payments).

E. Authentication: Authentication and the inherent integrity property counter the in-transit traffic tampering and impersonation vulnerabilities.

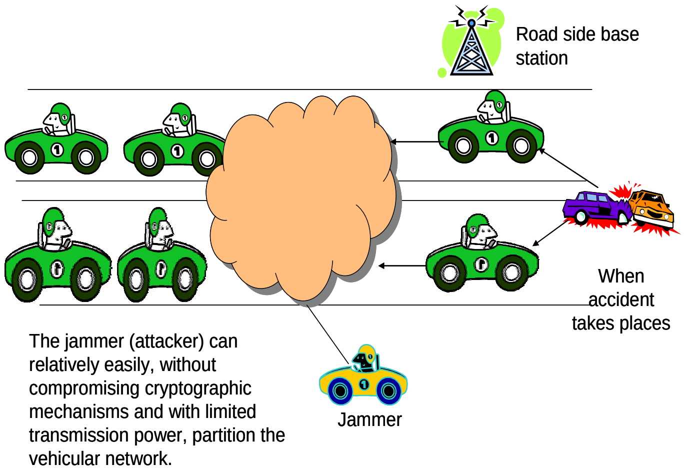

Road side base station
When accident takes places
The jammer (attacker) can relatively easily, without compromising cryptographic mechanisms and with limited transmission power, partition the vehicular network.
Jammer

Figure. 1. Jamming

4 False Position Information

In VANETs, one critical issue is that when nodes send false position information in their beacon messages, which can severely impact the performance of the network. A potential source for such false position data is malicious nodes. Hence Security in VANETs relies upon the potentially more challenging problem of detecting and correcting malicious data.

VANETs have special requirements in terms [3] of node mobility and position-dependent applications, which are well met by geographic routing protocols. One critical issue is that when nodes send false position information in their beacon messages, this can severely impact the performance of the network. A potential source for such false position data is malicious nodes. The intents of an adversary may range from simply disturbing the proper operation of the system to intercepting traffic exchanged by ordinary users, followed by a potential modification and retransmission.

This section outlines the effects presented in [3] which are caused by falsified position information. Fig. 2 shows an example scenario where node A claims to be at two additional (faked) positions A_{vi} and A_{vr}. Based on a greedy forwarding strategy nodes always select the node nearest to the destination as the next forwarding node. Assuming that F wants to send a packet to node K, it will first send the packet to its only direct neighbor G. G will then forward the packet to the node nearest to the destination from which it received beacons. This seems to be A_{vr}, so the packet ends up at node A, which can now forward, modify, or discard it at will. In the opposite direction, the packet from K will go to I, which will again send it to the assumed best node A_{vi}. So faking only two positions, A is able to intercept all traffic along the road.

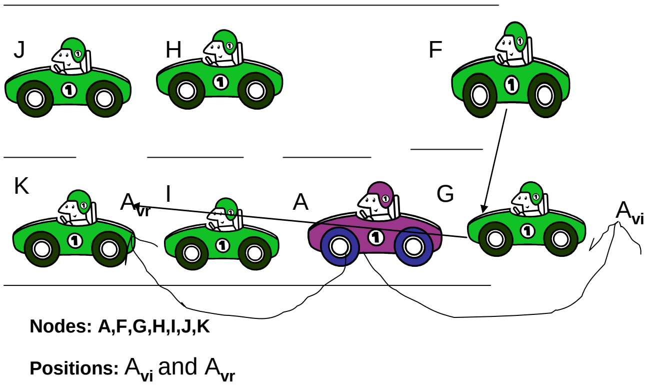


Figure. 2. Falsified Position Information

5 Sybil Attacks in VANETs

Sybil attacks have been regarded [9] as serious security threat to ad hoc and sensor networks. They impair the potential applications of VANETs by creating an illusion of traffic congestion. In the opinion of researchers [12] [16] VANETs are facing a number of security threats, which impairs the efficiency of many VANETs potential applications and poses threat to even life safety. In Sybil attack a malicious vehicle claims to be at multiple locations with multiple identities thereby creating an illusion of traffic congestion. The malicious node can even spoil the proper functioning of the network by injecting false information.

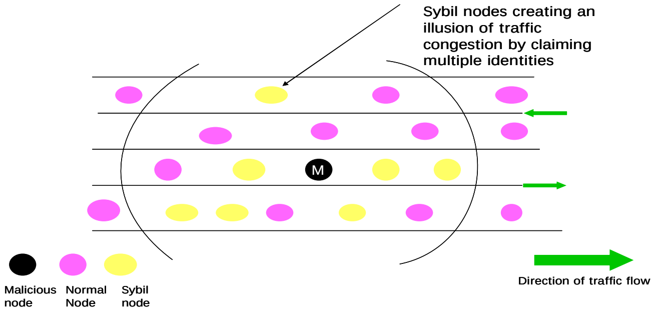

Sybil nodes creating an illusion of traffic congestion by claiming multiple identities
M
Malicious node
Normal Node
Sybil node
Direction of traffic flow

Figure. 3. Sybil Attack

Basically, in Sybil attack a malicious node illegitimately takes on multiple identities [18]. In mobile networking, each node gets the information of the neighboring node by receiving periodic beacons from neighbors in which they claim their identity. A malicious vehicle can manage to get identities of other vehicle by non-technical means such as stealing or it can also borrow from its friends. In the above Fig. 3 the malicious node M creates an illusion of traffic congestion by claiming multiple identities thereby convincing other vehicles that there is a traffic jam and makes them to choose alternate route so that he makes his path clear [12].

6 Proposed Solutions to Security Problems in VANETs

The successful deployment of inter vehicular communications require a robust and secured architecture [4]. Like in many areas of networking, IVC is also prone to a set of abuses and security related attacks. The security of vehicular networks is indispensable, because otherwise these systems could make antisocial and criminal behavior easier, in ways that would actually jeopardize the benefits of their deployment. Therefore, taking the security issues into consideration a secured VC architecture followed by different solutions have been proposed in [4] to over come some of these security risks mentioned earlier. This section presents the proposed vehicular communication architecture and some of the proposed solutions to security issues discussed at the beginning of the paper.

A. Security Architecture: The following are components needed protect vehicular communications against security threats. Among the vehicle onboard equipment, there are two hardware modules needed for security, namely. The event data recorder (EDR) records the vehicles critical data such as position, speed, time and so forth during an emergency events and provides only tamper-proof storage. Tamper-proof device (TPD) will take care of storing all the cryptographic material and performing cryptographic operations, especially signing and verifying safety messages. Fig 4. gives the overview of how vehicular communication architecture would look like and how vehicular communications takes place between vehicles and roadside infrastructure and also with the certificate authorities in case of an emergency event.

1) Vehicular Public key infrastructure: The huge number of vehicles registered in different countries are traveling long distances, well beyond their registration regions, requires a robust and scalable key management scheme. In addition Symmetric Cryptography does not provide the nonrepudiation property that allows the accountability of drivers' actions. The use of public key cryptography is a more suitable option for deploying VC security. Communication via base stations is considered insufficient in VC because vehicles are required not only to authenticate themselves to the base stations but also to each other.

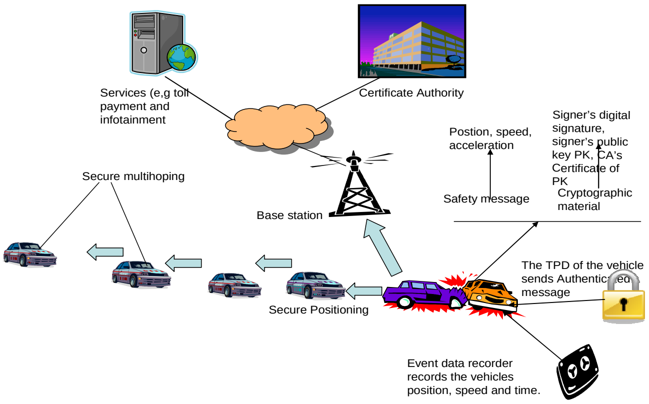
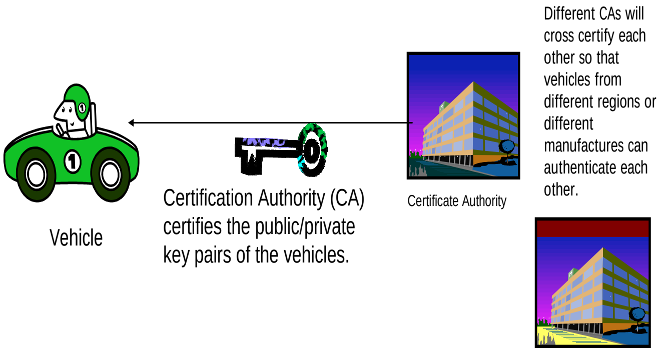

Services (e,g toll payment and infotainment
Certificate Authority
Postion, speed, acceleration
Signer's digital signature, signer's public key PK, CA's Certificate of PK
Safety message
Cryptographic material
Secure multihoping
Base station
The TPD of the vehicle sends Authenticated message
Secure Positioning
Event data recorder records the vehicles position, speed and time.

Figure. 4. Overview of Security Architecture

In vehicular public key infrastructure (VPKI) where Certificate Authorities (CAs) will issue certified public/private key pairs to vehicles, vehicle registration authorities presented in Fig 5. Different CAs will have to be cross-certified so that vehicles from different regions or different manufacturers can authenticate each other. This will require each vehicle to store the public keys of all the CAs whose certificates it may need to verify.


Different CAs will cross certify each other so that vehicles from different regions or different manufactures can authenticate each other.
Vehicle
Certification Authority (CA) certifies the public/private key pairs of the vehicles.
Certificate Authority

In Vehicular public key infrastructure (VPKI) where the CA will certify Public/private key pairs of the vehicles (with many pairs per vehicle for privacy reasons).

Figure. 5. In Vehicular Public Key Infrastructure the Certificate Authority certifies the public/private key pair of the vehicle.

*2) **Authentication:*** The fundamental security functions in VC will consist of authenticating the origin of a data packet. Authentication and the inherent integrity property counter the in-transit traffic tampering and impersonation vulnerabilities. As per the information presented in [19] digital signatures are considered a better choice than symmetric authentication mechanisms in VANET setting. In addition, given the huge amount of network members and the sporadic connectivity to authentication servers a PKI (Public Key Infrastructure) is the most suitable way for implementing authentication. For the purpose of privacy a set of anonymous key pairs are used. The use of secret information such as the private keys is stored in the tamper proof device. Anonymous keys are preloaded by the transportation authority or manufacturer and renewed periodically. An anonymous key pair is a public/private key pair that is authenticated by the Certificate Authorities (CA's) but contains neither information about nor public relationship with the actual identity of the vehicle. As safety messages will not contain any secret data about their senders, vehicle owners will be concerned only about the identity and location privacy. Normally a vehicle contains large set of anonymous key to prevent tracking. And also anonymous keys do not contain any publicly known relationship to the true identity of the key holders. CA's will be responsible for issuing key certificates to vehicles. Vehicles are registered with different transportation authorities corresponding to their region. The advantage of this is that Certification procedure will be directly under the control of the regional authority concerned. Certificates can also be issued by vehicle manufacturers depending on their limited number and the trust already endowed in them. The advantage of this approach is reduced overhead Each vehicle need to store a small number of manufacturer public keys in order to be able to verify any other vehicle it encounters., which is not the case if the CA is a local authority. Under the public key infrastructure (PKI) each vehicle will be assigned a certified public/private key pair (with many pairs per vehicle for privacy reasons) by a certification authority (CA) as shown in Fig. 5 and to authenticate each other, as shown in Fig. 6 before sending a safety message each vehicle will sign each message with their private key and attach the corresponding certificate as follows (T is time stamp). Where V represents the sending vehicle, * represents all message receivers, M is the message | is the concatenation operator, and T is the timestamp to ensure the message freshness, $SigprK_v$ [M] is the signature of M by the sending vehicle V and also includes the CA's Certificate $Cert_{v.}$

$$V \rightarrow * M, SigprK_v [M|T], Cert_v$$

When another vehicle receives this message, it has to extract and verify the public key of the vehicle V using the certificate and then verify V's signature using its certified public key. In order to do this the receiver should have the public key of CA.

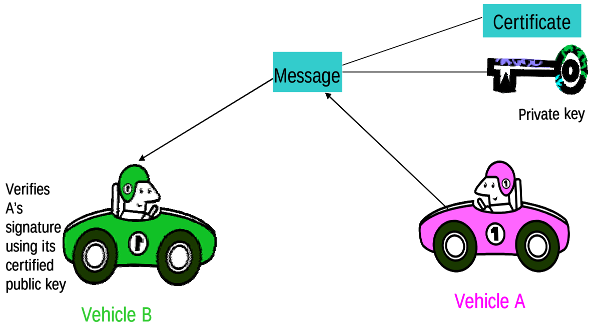


Figure 6. Authentication

*3) **Certificate Revocation:*** According to solution discussed in [4] the certificates of a detected attacker or malfunctioning device have to be revoked. The most common way to revoke certificates is the distribution of certificate revocation lists (CRLs) that contain the most recently revoked certificates. CRLs are provided when infrastructure is available. In addition, using short lived certificates automatically revokes keys. There are several drawbacks to this approach. First, CRLs can be very long due to the enormous number of vehicles and their high mobility. Second, the short lifetime of certificates still creates a vulnerability window.

To avoid the above shortcomings, a set of revocation protocols called Revocation protocol of the tamper proof device explained in Fig. 7 in which once the CA has decided to revoke all keys of a given vehicle M,(detected attacker or malfunctioning device) it sends to it a revocation message encrypted with the vehicle's public key. After the message is received and decrypted by the TPD of the vehicle, the TPD erases all the keys and stops signing safety messages. The TPD sends ACK to the CA. All the communications between the CA and the vehicle take place via base stations. Other vehicles (neighbors) verifying vehicle M's keys should be made aware of vehicle M's keys invalidity. Another protocol called Revocation protocol using Compressed Certificate Revocation Lists (RCCRL) is used when the CA wants to revoke only a subset of a vehicle's keys or when the TPD of the target vehicle is unreachable. Compared to RTPD, RCCRL has the special feature of warning the neighbors of a revoked vehicle as they also receive the CCRLs. Finally, the Distributed Revocation protocol in which vehicles accumulate accusations against misbehaving vehicles, evaluate them using a reputation system, and, in case misbehavior is detected, report them to CA once the connection is available.

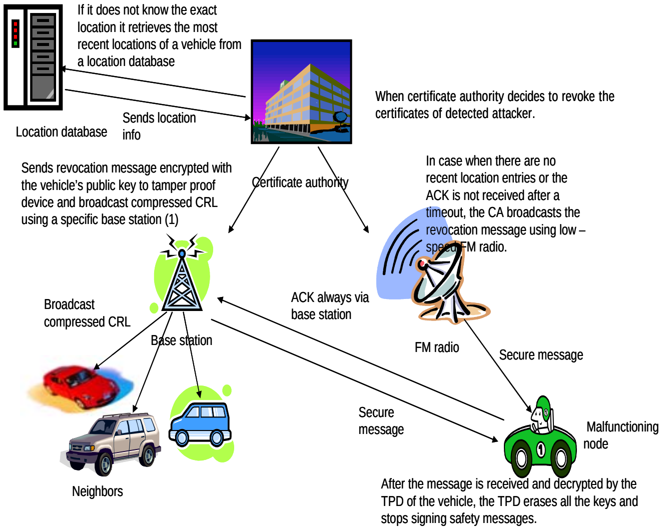

If it does not know the exact location it retrieves the most recent locations of a vehicle from a location database
Location database
Sends location info
When certificate authority decides to revoke the certificates of detected attacker.
Sends revocation message encrypted with the vehicle's public key to tamper proof device and broadcast compressed CRL using a specific base station (1)
Certificate authority
In case when there are no recent location entries or the ACK is not received after a timeout, the CA broadcasts the revocation message using low – speed FM radio.
Broadcast compressed CRL
Base station
ACK always via base station
FM radio
Secure message
Secure message
Malfunctioning node
Neighbors
After the message is received and decrypted by the TPD of the vehicle, the TPD erases all the keys and stops signing safety messages.

Figure. 7. Revocation protocol of the tamper-proof device (RTPD)

4) Privacy: Privacy vulnerability was addressed in [4], which proposes using a set of anonymous keys that change frequently (every couple of minutes) according to the driving speed. These keys are preloaded in the vehicle's TPD for a long duration. Each key is certified by the issuing CA and has a short lifetime. In addition it can be tracked back to the real identity of the vehicle (only in case law enforcement necessitates this only after obtaining permission from the judge). The downside of this approach is the necessity for storage space for all the keys for one year.

7 Solution to Position Falsification Attack

The only solution to position falsification attack is to introduce position verification [3]. One approach called 'Verifiable Multilateration' was proposed in [5] in which four base stations measure the time between sending a challenge to the corresponding node and the arrival of answer. In case a node delays the answer and thus enlarges the distance to one base station, it is discovered by looking at all four distance measurements. A concept called "Position Cheating Detection System" proposed in [3] in which each node uses multiple sensors to detect malicious or selfish behavior of nodes in the network. Based on sensors' observations each node calculates a trust value that determines whether nodes are trustworthy or should be excluded from further routing decisions. Two classes of position verification sensors have been defined. Sensors which work autonomously on each node and contribute their results to determine the trust ratings for neighbors. Another type of sensors work in cooperation with other nodes surrounding the neighbor node in question.

A. Combination of Verification Sensors: The mathematical calculation of trust value was derived from the one presented in [20] in which all nodes stores trust values r Є [-1; 1] for all direct neighbors.

r = 0 is equivalent to neutral trust, r Є [0;1] means a node is trustworthy and r Є [-1; 0] means no trust.

nth observation of a sensor s is denoted by σsn.

Every observation σsn is stored with timestamp tsn.

The timestamp tsn.of an observation σsn is used to calculate the observation's time factor wt (t, tsn.)

$$wt\ (t, tsn.) = 1-\frac{[t-tsn.]x}{T}$$

Finally, the trust value rt of a neighbor node at a time t is calculated by multiplying the available observations by their weight factor and their time factor, then summarizing the results and at the end normalizing to [-1; 1].

***B. Autonomous Sensors* - Acceptance Range Threshold:** The ART sensor as in [3] called Acceptance Range Threshold (ART) are based on the radio networks used in VANETs. A maximum acceptance range threshold Δmax has been defined for this sensor. The beacons from nodes which claim be at distance greater than the one defined by Δmax are discarded. This in turn helps to avoid some types of attacks.

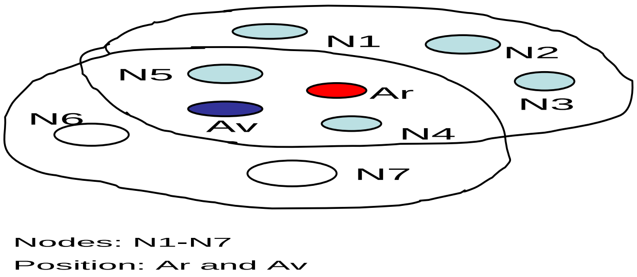


Figure. 8. Acceptance Range Threshold

Fig. 8 explains that position beacons from node A, being at real position Ar but claiming to be at position Av will be rejected by nodes N1 through N3 as the ART is exceeded. On the other hand nodes N6 and N7 do not receive the beacons from node A any way. This mechanism is also capable of preventing routing loops caused by position information in many greedy routing strategies.

C. Mobility Grade Threshold: The MGT sensor also discussed in [3] is based on the assumption that nodes can move only at a well-defined maximum speed. Timestamps are recorded by nodes on receiving beacons. When subsequent beacon is received from the same node the average speed of the node for two positions is checked to see if it exceeded MGT. Once the MGT is exceeded, beacons from those nodes are discarded. As shown in Fig. 9 it is assumed that a rational attacker *A* (again located at position *Ar*) promiscuously listens the communication channel for packets he would like to intercept. If node *M* forwards packet *P*1 to Node *N*, *A* receives it as well, but cannot prevent further forwarding, because *A* is not in the route However, *A* may instantly send a beacon with a virtual position *Av*1 that *N* will likely select as next forwarder for *P*1. The only constraint is to be faster than the forwarding processes at *N*. Using this method, *A* is able to intercept all nearby packets assuming it is capable of taking in new positions as often as required. For example, shortly after setting its position to Av1, *A* may set it to *Av*2 in order to intercept another packet *P*2. This uncontrolled Position hopping is detected by the MGT sensor.

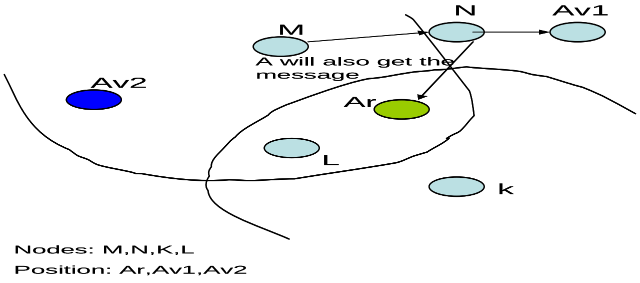


Figure 9. Mobility Grade Threshold

D. Maximum Density Threshold: This is based on the assumption that only a restricted number of physical entities (e.g. cars) can reside in a certain area as discussed in [3]. For instance, cars have certain physical dimensions preventing too many cars to be on the same road segment. This sensor defines a MDT which, when exceeded, rejects further position beacons for this area.

E. Overhearing: Another approach to verify nodes position presented by Marti et al. [21] in which nodes use the indiscriminate mode in order to capture packets addressed to different nodes from nodes with in the reception range.

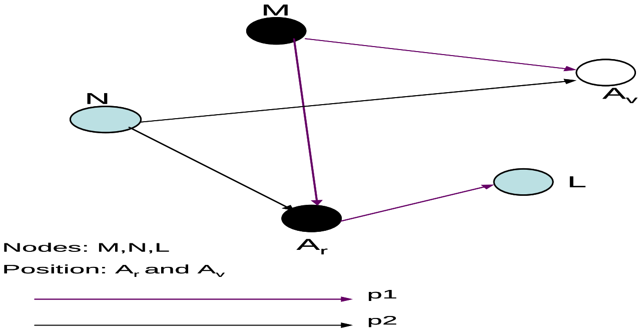


Figure. 10. Overhearing

This concept was further illustrated in Fig.10 in which A_r represents the real position of node A where A_v denotes the position A pretends to be by sending it to neighboring nodes in its beacon messages. In the first case node M forwards packet P1 to node A. Later, M overhears P1 being sent to node L, which is at an inferior position compared to A. This indicates that A may have forged his position A_v. In the second case, node M overhears the transmission of packet P2 from N to A, although given the last position of A known to M and the MGT (Mobility Grade Threshold), A should not be in reach of N. Again this indicates that A may have forged his position A_v.

F. Cooperative Sensors :As per the solution presented in [3] this type of sensors also facilitate in providing information on nodes to detect whether nodes are malicious or genuine. The sensors are required to exchange information to prove that nodes are at fake positions.

1) Proactive Exchange of Neighbor Tables: In this method nodes exchange their neighbor's table to check whether the position mentioned in the table corresponds to their own position. For example node A receives a beacon from B claiming to be at position Pb. Node A also receives another beacon from Node C saying that B is at position Pb1. Since the two positions differ significantly A cannot decide which position claim of B is fake. Therefore A considers beacons from many other nodes and based on the majority decides which node claim of B is false.

2) Reactive Position Requests*:* Here nodes agree to exchange information for position verification only upon request. This situation can arise when node A meets an unusual node B which it has never met before. In this method node A designates some nodes as acceptors and some nodes rejecters by sending them position requests (PREQ). The PREQ consists of request for the position of node B. After receiving responses from acceptors and rejecters A is able to determine the position claim of B

8 Basic Signal Strength Based Position Verification

The following approach of verifying nodes position is taken from [9] in which Sybil attacks are considered to be one of the biggest threats to VANETs security. These attacks are believed to impair VANET safety applications thereby creating an illusion of traffic congestion. To overcome the above security threat a scheme called basic signal strength based position verification has been proposed to verify position claims based on signal strength of beacons. This technique takes full advantage of inherent properties of VANETS such as mobility, traffic pattern and also road side base stations. The detection of Sybil attacks relies on three categories of approaches namely, radio resource testing, identity registration, and position verification. As explained in [10], [18] position verification seems to be a promising approach for VANETs whereas radio resource testing requires special radio modules such as multi- channel radio, and identity registration doesn't work well in VANETs. The following approach of position verification relies on monitoring the signal strength of periodical beacons. The following categories of roles are played by each node.

A. Claimer: Each node periodically broadcasts a beacon message at beacon intervals, tb, for the purpose of neighbor discovery. In the beacon message it claims it identity and position. The beacon message can be in the following format.

{ NodeID, Beacon#, Position, NebList, Signature }

Where NodeID is the claimer's identity, Beacon# is a beacon sequence number, Position is the sender claimed position, and the neighbor list contains the following information.

NebList: {NodeIDi, Beacon#i, RSSi}

NebList is the sender's most recent neighbor list containing signal strength measurements. Signature is the digital signature for the whole packet. In each item of NebList, RSSi is the Received Signal Strength of beacon Beaconi, recently received from neighboring node NodeIDi.

B. Witness: The neighboring nodes residing within the signal range of the claimer, receives the previous beacon. They measure the signal strength and measure the corresponding neighbor information in their memory. They include this neighbor information along with the signal strength when broadcasting a beacon message next time.

C. Verifier :The node waits for a specific time interval tv after receiving a beacon message during which it collects signal strength measurements for the previous beacon from neighboring witnesses. Based on the collected measurements it can compute the position of the claimer. For example by performing MMSE (Minimum Mean Square Error)

To obtain the estimated position we first calculate the mean square error.

$$MSE\ (p) = \frac{\Sigma\ ki=1(Sr(wi) - Sm\ (wi,p))2}{K}$$

Where p is the potential position of the claimer. K is the number of witnesses. Sr is the received signal strength at witness wi. Sm is the calculated signal strength at wi obtained from radio propagation model. By varying p we can minimize MSE and finally get the optimized estimated position p. If the estimated position of claimer is far away from its claimed position, we regard this node as suspect node.

9 Conclusions

This article presented some of the security threats of vehicular ad hoc networks focusing on the vulnerabilities; false position information and Sybil attack problems and also presented some of the proposed solutions to overcome these security threats. The proposed security architecture and the authentication mechanism counter the in-transit traffic tampering and impersonation vulnerabilities. A set of revocation protocols are used to revoke the certificates of a detected attacker or malicious node. In Position cheating detection system each node is able to use multiple sensors to detect malicious and selfish behaviour of nodes in the network. Finally the Basic Signal Strength Based Position Verification approach significantly detects the Sybil nodes in the network. Based on the security issues discussed in this paper it is clear that the field of inter vehicular communications requires the design of robust and secured architecture in order to prevent the security problems. This emerging field requires a coordinated effort and extensive research to identify and eliminate the security issues.

10 References

[1] Weihua Sun, Hirozumi Yamaguchi, Koji Yukimasa, Shinji Kusumoto, “GVGrid: A Qos Routing Protocol for Vehicular Ad hoc Networks,” Web, Osaka University Japan, June 20 2006.

[2] K. Daniel Wong, K.E Tepe, Wai Chen, Mario Gerla, “Inter Vehicular Communications,” IEEE Wireless Communications, Vol 13, no 5, October 2006, pp.6.

[3] Tim Leinmuller, DaimlerChrysler AG, Elmar Schoch and Frank Kargl, ULM University “Position Verfication Approaches for vehicular Ad hoc Networks,” IEEE Wireless Communications, Vol 13, no 5, October 2006, pp.16-20.

[4] Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux EPFI, “Seuring Vehicular Communications,” IEEE Wireless Communications, Vol 13, no5, October 2006, pp.8-13

[5] J.P Hubaux, Srdjan, Capkun, and Jun Luo. “The security and privacy of smart vehicles,” IEEE Security and Privacy, Vol 4, no.3, 2004, pp. 49-55.

[6] S. Corson, J. Macker. “Mobile Ad hoc Networking (MANET): Routing protocol performance issues and evaluation considerations,”. 1999. RFC 2501.

[7] Klaus Plobl, Thomas Nowey, Christian Mletzko, “Towards a Security Architecture for Vehicular Ad hoc Networks,” First International Conference on Availability, Relaiability and Security (ARES’06). pp. 374-381.

[8] Valrey Naumov, Rainer Baumann, Thomas Gross. “ An evaluation of inter-vehicle ad hoc networks based on realistic vehicular traces,”. In Proc. of the 7th ACM international symposium on mobile ad hoc networking and computing, 2006, pp. 108-119.

[9] Bin Xio, Bo Yu, Chuanshan Gao., “Detection and Localization of sybil nodes in VANETs,” Proc. Wksp. Dependability issues in wireless Ad hoc Networks and Sensor Networks, 2006, pp. 1-8.

[10] P. Golle, D. Greene, and J. Staddon. “Detecting and Correcting Malicious data in Vanets,”. In Proc. of the 1st ACM international workshop on vehicular ad hoc networks (VANET 2004), pp. 29-37, 2004.

[11] Jeppe Bronstead, Lars Michael Kristensen. “Specification and performance evaluation of two zone dissemination protocols for vehicular ad hoc networks,”. In Proc. of the 39th annual symposium on simulation, 2006, pp. 68-79.

[12] M. Raya and J.P Hubaux. “The Security of Vehicular Networks. In Proc. of the 3rd ACM wksp. on Security of ad hoc and sensor networks (SASN 2005), pp. 11-21, 2005.

[13] Shabbir Ahmed, Salil S. Kanhere. “VANETCODE: Network Coding to enhance cooperative downloading in vehicular ad hoc networks,” In Proc of the 2006 international conference on communications and mobile computing, 2006, pp. 527-532.

[14] Timo Kosch, Christian j. Adler, Stephan Eichler, Christoph Schroth, and Markus Strassberger. “The scalability problem of vehicular ad hoc networks and how to solve it,” IEEE Wireless Communications, Vol 13, no 5, October 2006, pp.22-28.

[15] Florian Dotzer. “Privacy issues in Vehicular Ad hoc Networks,” BMW group research and technology.

[16] B. Parno and A. Perrig. “Challenges in Securing Vehicular Networks,”. In Proc. of the Fourth wksp. on Hot topics in Networks (HotNets-IV), 2005.

[17] Stephen Eichler, Christoph Schroth, Jorg Eberspacher. “Car-to-Car Communication,” Institute of Media and Communication Management, SAP Research CEC, University of St. Gallen , Switzerland.

[18] J. Newsome, E. Shi, D. Song, and A. Perrig. “The Sybil Attack in Sensor Networks,” Analysis and Defenses. In Proc. of the Third International Symposium on Information Processing in Sensor Networks (IPSN 2004), pp.259-268,2004.

[19] M. Raya and J.P Hubaux, “The Security of vehicular networks,” EPFL Technical report, 2005.

[20] P. Michiardi and R. Molya, “CORE: a collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad hoc Networks,” Proc. IFIP TC6/TC11 6th Joint Working Conf. Commun. And Multimedia Security, Deventer, The Netherlands, 2002, pp. 107-21.

[21] S. Marti et al., “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” Proc. 6th Annual Int’l. Conf. Mobile Computing and Net. 2000, pp. 255-65.