Venkatamangarao Nampally *et al*, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 10, October- 2017, pg. 58-70 **ISSN: 2321-8363**
Impact Factor: 4.123

A Survey on Security Attacks for VANET

Venkatamangarao Nampally[1], Dr. M. Raghavender Sharma[2]

[1]*Department of Computer Science, University College of Science, Osmania University, Hyderabad, Telangana*
E-mail: n.venkat018@gmail.com

[2]*Department of Statistics, University College of Science, Saifabad, Osmania University, Hyderabad Telangana*
E-mail: drmrsstatou@gmail.com

Abstract

VANETs have become a fundamental component of many intelligent transportation systems. Security is an important aspiration for VANET in view of the facts that improved security which reduces accidents and consequently improves traffic conditions and yet save lives. Developing secure VANET infrastructures remains most significant challenge. As authentication allows trusting both user and data, it requires considerable attention in the security framework of VANETs. Most of the research concerted efforts in academics and industry are focused to provide efficient security architecture for VANET to protect the network from adversary nodes and attacks. The problem of VANET is transmitting information to correct destination without effect in that information. Pointing out security gaps regarding distinct threats, the classification will allow to designed new secure network control methods. This paper provides various attacks in VANET and possible solutions by using cryptographic operations.

Keywords: Ad-hoc Network, VANET, Attack, WAVE, Tunnelling, and ECDMA.

1. Introduction

Vehicular Ad hoc Network applications require security of applications in order to serve users and make their journey secure and comfortable. Transmission of data or information among vehicle-to-vehicle exists through wireless medium in VANET. So there are chances of various attacks in VANET. Security has always been an issue in vehicular networks which must be seriously considered and a security infrastructure has to be designed and implemented in such networks. Attackers try to make their impact on the network through various means and the dynamic behavior of these attackers is unpredictable. It is obligatory that all transmitted data can be injected or changed by users who have malevolent goals by attacker. On the other hand, by gaining unauthorized access to network, an attacker can gain the control of critical components of a vehicle and cause irreparable damage to the vehicle or its passengers. So, security is mandatory for successful transmission of such information. Besides safety, other services such as Internet access, weather forecast and geo-location information can enrich travel experience by providing travel comfort, convenience and infotainment. Committees are devoting efforts to finalize standards for VANET. These standards include IEEE 1609.x, 802.11p and Wireless Access in Vehicular Environment (WAVE). WAVE is a layered architecture for devices complying IEEE 802.11 to operate on Dedicated Short Range Communication (DSRC) band. The IEEE 1609 family defines the architecture and the corresponding protocol set, services and interfaces that allow all WAVE stations to interoperate within the VANET environment. Together the WAVE standard family forms the basis to implement a wide range of VANET applications across domains such as security, enhanced navigation, automatic tolls and traffic alerts, etc.

In order to achieve the best security features, VANET security issues are categorized as:
1.1) Security challenges in VANET
1.2) Security requirements in VANET
1.3) Attackers on VANET
1.4) Attacks on VANET

1.1 Security Challenges in VANET

We use two approaches in VANET in order to implement security challenges.

1) Technical Challenges
2) Social and Economic Challenges

In first approach we use low complexity security algorithms such as RSA, ECC. In second approach we use transport protocol choice. In order to achieve for better security in two approaches, for data encryption AES used.

1.2 Security Requirements in VANET

Security is a state of being or feeling protected from harm or attack. Security Requirements for VANETs are:

1.2.1 Authentication

An authentication framework is necessary to enable receivers of broadcast data to verify that the received data really originates from the claimed node without modification. Authentication methods categorized into two groups: message authentication and entity authentication.

1.2.2 Integrity

Integrity is required between two communicating nodes to protect data accuracy, which is main security issue desirable in VANETs.

1.2.3 Confidentiality

The challenge to protect data content from the adversaries is confidentiality.

1.2.4 Non-Repudiation

To repudiate means to deny. Nonrepudiation is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

1.2.5 Pseudonymity

Pseudonymity is the state of describing a disguised identity. A holder that is one or more human beings is identified but do not disclose their true names.

1.2.6 Privacy

The protection of personal information of drivers within the network from other nodes but extracted by authorities in case of accidents is a major privacy issue which is desirable for VANETs.

1.2.7 Scalability

The ability of a network to handle growing amount of work in a capable manner securely is Scalability, which is the main challenge in VANETs.

1.2.8 Mobility

The nodes communicating in VANETs constantly change their locations with different directions and speeds making the network dynamic in nature. Therefore, in order to make communication successful, it is challenging to establish security protocols.

1.2.9 Key-Management

The key is used to encrypt and decrypt information during communication process. When designing security protocols for networks like VANET, the issue of key management must be resolved.

1.2.10 Location-verification

This is necessary to prevent many attacks and is helpful in data validation process. Thus to improve the security of VANETs, a solid method is required to verify the nodes positions.

1.2.11 Data Encryption

Encryption is the act of encoding text so that others not privy to the decryption mechanism (the "key") cannot understand the content of the text.

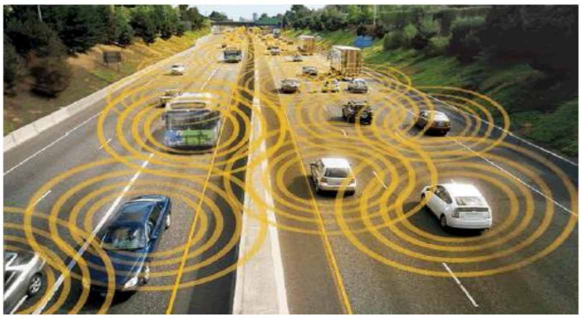


Figure 1: Communication criteria in VANET

1.3 Attackers on VANET

Attacker possesses various properties which are mentioned below:

1.3.1 Insider and outsider

This type of attacker is an authentic user of the network and has detail knowledge of the network. If the attacker is a member node who can communicate with other members of the network, it will be known as an Insider and able to attack in various ways. Insiders are authenticated members of network whereas outsiders are intruders

1.3.2 Malicious and Rational

Malicious attackers do not much harm to network but they do harm only to functionality of network. A wicked attacker uses different methods to ruin the representative nodes and the system without looking for its individual gain. On the adverse, a realistic attacker predicts personal assistance from the invasion. Thus, these attacks are more certain and follow some arrangements.

1.3.3 Active Vs passive

An active attacker can achieve new packets to corrupt the system whereas a passive attackers active only eavesdrop the wireless carrier but cannot make new packets (i.e., lesser harmful).

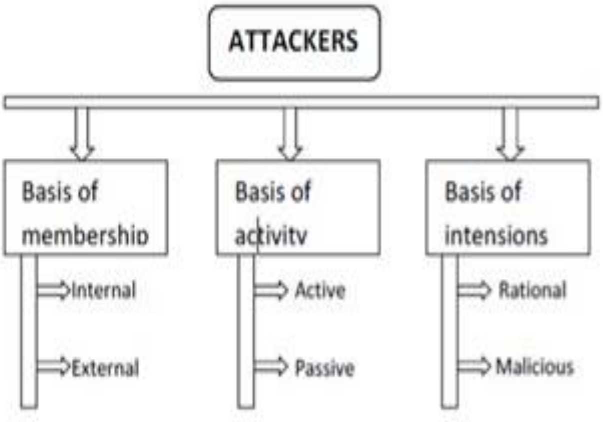


Figure 2: Classification of attackers

The three main characteristics on which attacker depends to achieve their goal are budget, manpower, and tools

1.4 Attacks on VANET

The security is most decisive issues because their information is broadcast through wireless medium. So, there are chances of a number of possible attacks in VANET due to open nature of wireless medium. *Attacker goal is t*he deliverance of information from source to destination with modified information in VANET system. The possible categorization of these attacks is depicted in following figure.

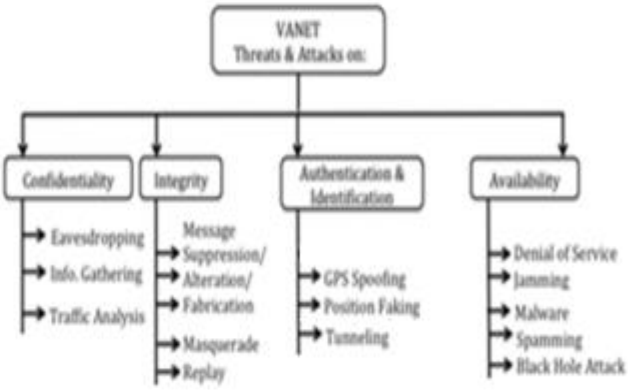


Figure 3: Classification of VANET threats

1.4.1 Confidentiality Attacks

1.4.1.1 Eavesdropping

Eavesdropping is the unauthorized real-time interception of a private communication, such as a phone call, instant message, video conference or fax transmission. The main goal o this attack is access of confidential data.

1.4.1.2 Information gathering attack

The attacker performing Bogus Information attack can be outsider (intruder) or insider (legitimate user). The idea is to transmit incorrect or bogus information in the network for personal advantage. For instance, an attacker may transmit a message announcing "Heavy traffic conditions" to the others in order to make its movement easier on the road. ECDSA (Elliptic Curve Digital Signature Algorithm) is one of the best solutions for this kind of attacks.

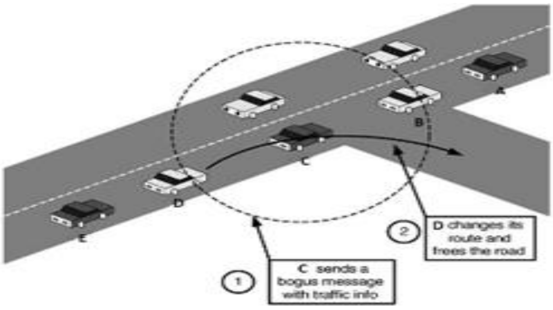

A
B
C
D
E
1
C sends a bogus message with traffic info
2
D changes its route and frees the road

Figure 4: Bogus information attack

1.4.1.3 Traffic analysis

Attackers can accept to the traffic on wireless links to determine the location of target nodes by evaluating the communication arrangement, the volume of data transmitted by nodes and the tendency of the transmission. For example, in a battlefield scenario, a substantial amount of network traffic commonly flows to and from the headquarters. Traffic pattern inquiry therefore allows an intruder to determine the commanding nodes in the network. Even if the data in a message is secured by encryption, traffic analysis can still be executed to extract some useful information. Although passive attacks do not straight affect the network' functionality, in some VANET utilization scenarios, such as military communication, important information disclosure through traffic analysis or simply eavesdropping could prove costly.

1.4.2 Integrity Attacks

1.4.2.1 Message suppression

The attacker performing Bogus Information attack can be outsider (intruder) or insider (legitimate user). The idea is to transmit incorrect or bogus information in the network for personal advantage. For instance, an attacker may transmit a message announcing "Heavy traffic conditions" to the others in order to make its movement easier on the road. ECDSA (Elliptic Curve Digital Signature Algorithm) is one of the best solutions for this kind of attacks. In this attack, an attacker selectively drops packets received from the neighbours, these packets may hold critical safety related information for the receiver, the attacker suppress or block these packets and can use them again at later time. Such type of attack can prevent warning messing to be forwarded. For instance, an attacker may block a congestion warning, so vehicles will not receive the warning and forced to wait in the traffic for the long time.

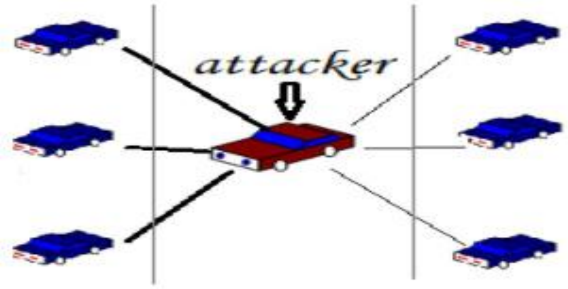


Figure 5: Suppression attack

1.4.2.2 Message alteration

Message alteration is the threat that an attacker intercepts messages in the middle of communication entities and alters certain information to reroute the call, change information, and interrupt the service, and so on.

1.4.2.3 Fabrication

In this type of attack a fake message is inserted into the network by an unauthorized user as if it is a valid user. This results in the loss of confidentiality, authenticity and integrity of the message.

1.4.2.4 Masquerade

The attacker uses MAC and IP spoofing in order to get identity of other nodes and hide into the network. If there is no authentication process in order to make the network secure from malicious nodes, a malicious vehicle can send message on behalf of other vehicles to gain its own benefits or create chaos, traffic jam or accidents and hide itself. It is achieved by using masquerade identity and messages fabrication, alteration and replay. For example, a malicious node may impersonate an ambulance to request others for priority lane or demand nearby RSUs to change traffic lights to green. Thus, the message from an OBU has to be integrity-checked and authenticated before it can be relied on.

1.4.2.5 Replay

An attacker can replay the received packets apart from acting as a normal node (forwards all the received packets). In this attack, packets are fraudulently repeated. This operation is carried out by a malicious node that intercepts the safety packet and retransmits it. This type of attack is usually performed to impersonate a legitimate vehicle or RSU. Since, Basic 802.11 security does not contain sequence numbers; therefore it provides no protection against replay. Because of keys can be reused, it is possible to replay stored messages with the same key without detection to insert bogus messages into the system.

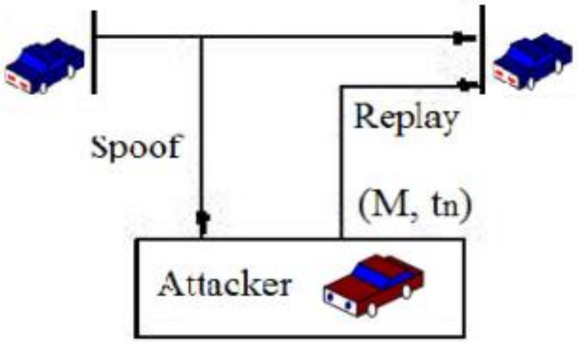


Figure 6: Replay Attack

1.4.3 Authentication and Identification Attacks

1.4.3.1 GPS spoofing

In VANETs, a location table with the geographic locations and vehicles identities is a critical element that is maintained due to GPS satellite. Using the GPS satellite simulator to generate signals, that are stronger than those generated by the actual satellite system are, an attacker can produce false readings in the GPS to deceive vehicles to think that they are in a different location. Hidden vehicle is another concrete example of cheating with positioning information. As Fig. illustrates, the vehicle B deceives the vehicle A to believe that it is better placed (at B') for forwarding the warning message, but then keep silence about the accident.

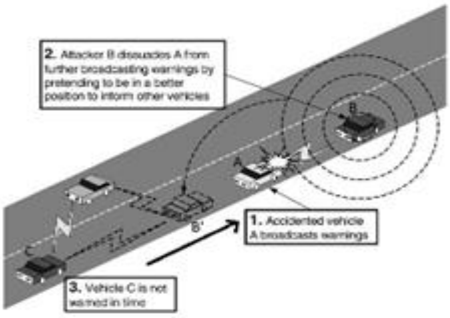

2. Attacker B dissuades A from further broadcasting warnings by pretending to be in a better position to inform other vehicles
B
A
B'
C
1. Accidented vehicle A broadcasts warnings
3. Vehicle C is not warned in time

Figure 7: Hidden vehicle threat

Because of the temporary disappearance of GPS signals in tunnels, an attacker is possible to inject false positioning information once the vehicle leaves the tunnel and before it receives an authentic position update, as Fig. 10 illustrates. This phenomenon happens with either a physical tunnel or an area jammed by the attacker, that leads to the same effects.

1.4.3.2 Position faking

Forging of message can be carried out by attacker directly or indirectly through another vehicle.

1.4.3.3 Tunnelling

This type of attack is also called hidden vehicle feasible in a very situation wherever vehicles neatly attempt to cut back the congestion on the wireless channel. As an example, a vehicle has sent a warning message to its neighbour and it's awaiting a response. Once receiving a response, the vehicle realizes that its neighbour is in a very higher position to forward the warning message and stops causing this message to different nodes.

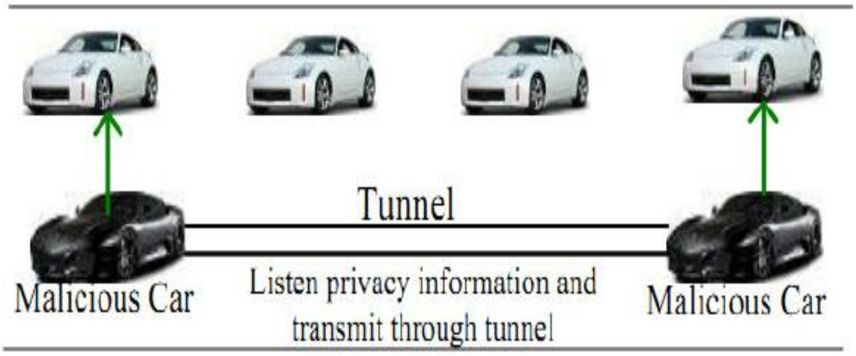


Figure 8: Tunnel attack

1.4.4 Availability Attacks

1.4.4.1 DOS attack

Denial of Service Attack: It is the most serious level attack in vehicular network. In this attack attacker jams the main communication medium and network is no more available to legitimate user.

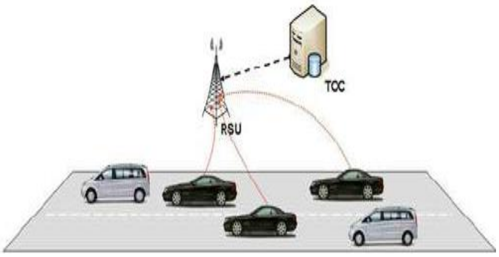


Figure 9: DOS attack

Above figure shows the whole scenario when the attacker A launches DOS attack in vehicular network as a result it jams the whole communication medium between V2V and V2I and the authentic users (B, C, and D) cannot communicate with each other. One form of DOS attack is Distributed Denial of Service Attack (DDOS Attack).DDOS attacks are those attacks in which attacker attacks in distributed manner from different locations. Attacker may use different timeslots for sending the messages. Nature and time slot of the message can be varied from vehicle to vehicle of the attackers. Here, the aim of attacker is same as DOS attack.

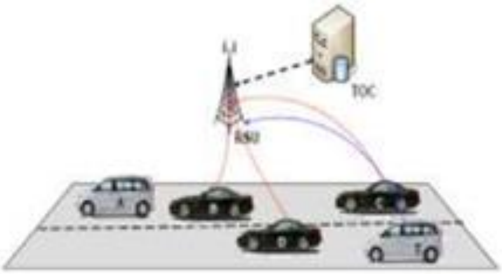


Figure 10: DDOS attack

1.4.4.2 Jamming attack

Transmitting of radio signals to disrupt the whole communications by decreasing the signal-to-noise ratio. The term jamming is used to differentiate it from unintentional jamming which called interference. In VANET Jamming is a serious threat to its security. Jammers constantly send repeated signals (in affected area) to interfere with the communication between nodes in the network. The victim feels that the state of the channel is still busy. Therefore, it cannot send or receive packets in the jammed area. When jamming is enabled, the sender may successfully send packets; the receiver cannot receive all the packets sent by the sender. Hence, its packet delivery ratio (PDR) is low. These packets can be carrying important information (life threatening) such as, road conditions, weather, accidents, etc. and failure to receive or disseminate these packets can lead to fatalities.

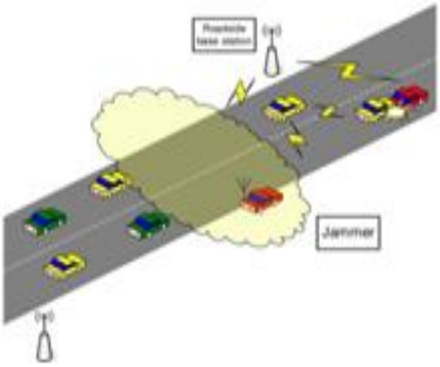


Figure 11: Jamming attack

1.4.4.3 Malware and Spamming

Malware and spam attacks, such as viruses and spam messages, can cause serious disruptions in the normal VANETs operations. This kind of attack is normally executed by malicious insiders rather than outsiders. For instance, an attacker sends a big amount of spam messages in the network to consume the bandwidth and to increase the transmission latency. It is not easy to control such kind of behaviour because of the lack of necessary infrastructure and centralized administration. Meanwhile, malwares are just like viruses that hamper the normal operation of the network. VANET get infected normally when On Board Units (OBU) of vehicles and Road Side Units (RSUs) perform software updates. Embedded anti-malware frameworks are still a problematic issue in VANETs research community.

1.4.4.4 Black hole

A black hole is an area where the network traffic is redirected. However, either there is no node in that area or the nodes reside in that area refuse to participate in the network. In a black hole attack, a malicious node introduces itself for having the shortest path to the destination node and thus, cheats the routing protocol. Instead of taking a look on routing table firstly, this hostile node advertises rapidly that it has a fresh route for the route request. In consequence, attacker node wins the right of replying to the route request and thus it is able to intercept the data packet or retain it. When the forged route is successfully established, it depends on the malicious node whether to drop or forward the packets to wherever it wants. Gray Hole attack is known as a variation of Black Hole attack, in which the malicious node misleads the network by agreeing to forward the packets but it sometimes drops them for a while and then switches to its normal behaviour. It is very difficult to figure out such kind of attack.

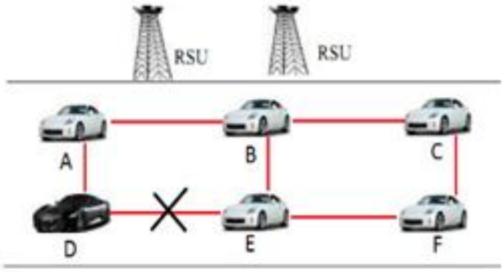


Figure 12: Black hole attack

1.4.4.5 Sybil attack

It is a critical attack. In this kind of attack attacker sends multiple messages to other vehicles. Each message contains different source identity. It creates confusion to other vehicles by sending wrong messages like traffic jam. So there is jam further and vehicles are forced to take another route. The main aim of the attacker is to provide an illusion of multiple vehicles to other vehicles so that vehicles can choose another route.

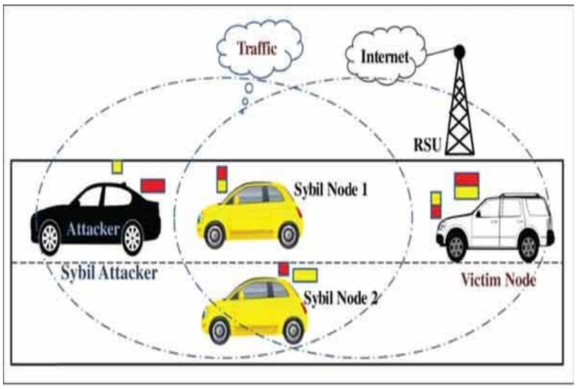


Figure 13: Sybil attack

Solution: Traditionally in ad hoc networks, there are three types of defences against Sybil attacks introduced, namely registration, position verification, and radio resource testing. Registration itself is not enough to prevent Sybil attacks, because a malicious node has possibility to register with multiple identities by non-technical means such as stealing. Moreover, a strict registration may lead to serious privacy troubles. In position verification, the position of nodes will be verified. The goal is to make certain that each physical node refers to one and only one identity. Radio resource testing is based on the assumption that all physical entities are limited in resources.

The remainder of this paper is organized into as follows: Part 2, contains a review of related work. Part 3 explains Methodology; Part 4 describes Conclusion of work. At last we give acknowledgements and reference which are used for preparing this paper.

2. Related Work

Merij [1] propose the use of a cryptographic based categorization that is easy and plain to understand since the similar approach it takes as done in traditional network security solutions. Issac [2] also surveys the major security attacks and presents the corresponding countermeasures and cryptographic solutions. Active defensive mechanisms like the one proposed in Prabhakar [3] are also essential complements to the passive mechanisms of encryption. In addition to its dynamic nature and high mobility, the use of wireless media also makes VANET vulnerable to attacks that exploit the open and broadcast nature of wireless communication [4]. To balance the need for security and the need for speed, researchers in [5] come up with a hybrid method that takes advantage of both asymmetric and symmetric cryptographic schemes. Sun [6] propose an identity-based security system for VANET that can effectively solve the conflicts between privacy and tractability. The system uses a pseudonym-based scheme to preserve user privacy. Azogu [7] propose an Asymmetric Profit-Loss Markov (APLM) model that measures the integrity level of the security schemes for VANET content delivery. Yan [8] propose a novel position detection scheme to prevent position-based attacks. J.T. Isaac, S. Zeadally, and J.S. Camara published a paper on "Security attacks and solutions for vehicular ad hoc networks" [9]. Irshad Ahmed Sumra proposed five different classes of attacks [10] and every class is expected to provide better perspectives for the VANETs security. In [11], the authors try to deal with the Sybil attack by public key cryptography. A Public Key Infrastructure for VANETs (VPKI) is proposed. The authors illustrate a complete solution to enhance communication security by addressing the key distribution and key revocation. The Sybil attack is always detected very early since each vehicle is authenticated correspondingly with its public key. Nonetheless, like any other cryptography-based approaches, the deployment of VPKI is a heavy and uncertain issue that must be tested to assess the possible utilization in reality. ECDSA (Elliptic Curve Digital Signature Algorithm) [12] is named as one of the solutions for bogus information attacks. Traditionally in ad hoc networks, there are three types of defences against Sybil attacks introduced, namely registration, position verification, and radio resource testing [13].

3. Methodology

3.1. Classical Security Mechanism

3.1.1 Electronic license plates

Electronic license plates (ELP), which are cryptographically verifiable numbers equivalent to traditional license plates and help in identifying stolen cars and keeping track of vehicles crossing country border.

3.1.2 Asymmetric Encryption using PKI

A public-key cryptosystem is based on the assumption that it might be possible to find a system where it is computationally infeasible to determine the decryption rule given its encryption rule. Vehicular public key infrastructure (VPKI) in which a certification authority manages security issues of the network like key distribution, certificate revocation etc. To keep a tap on bogus information attack, data correlation techniques are used. To identify false position information, secure positioning techniques like verifiable multilateration is commonly used. Public key encryption has rapidly grown in popularity because it offers a very secure encryption to information. In a public-key cryptosystem, the sender encrypts a message with the recipient's public key. This key is usually posted in a directory similar to a phone book. Upon receiving the message, the recipient uses his/her own private key to decrypt the message. For example, Alice encrypts a message using Bob's public key and sends it to him over an insecure channel. Bob then decrypts the message with a private key that is known only to him. RSA is a public-key cryptosystem that supports both encryption and digital signatures (authentication).Like all public key cryptography models, the RSA cryptosystem encrypts and decrypts a message using a pair of keys known as public key and private key. Its security is based on the difficulty of factoring large integers. Presently, most implementations of the RSA algorithm employ the use of 512-bit numbers. Cracking such a system requires the ability to factor the product of two 512-bit prime numbers. Factoring a number of this size is well beyond the capability of the best current factoring algorithms.

3.2 Defensive Mechanism

For inputs as given security measures of the VANET, the defensive mechanism adopts game theoretic approaches and is comprised of three stages. The first stage uses heuristics based on ant colony optimization to identify known and unknown opponents. In the second stage, Nash Equilibrium is employed for selecting the model for a given security problem. The third stage enables the defensive mechanism.

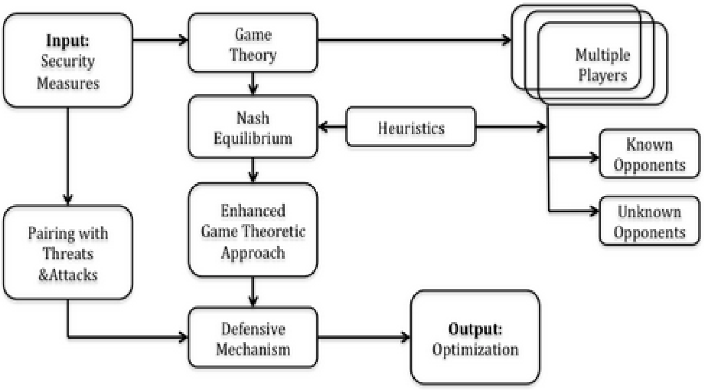


Figure 14: Defensive mechanism

3.3 Cryptography Models

Encryption is the concern of the protection of electronic transmissions and digitally stored data. Standard encryption methods usually have two basic flaws, (1) A secure channel must establish at some point so that the sender may exchange the decoding key with the receiver; and (2) There is no guarantee that who sent a given message. Vehicle Safety Communications Consortium (VSCC) defined security approaches for a security architecture in vehicular networks that is under standardization so far. It defines a public-key-infrastructure (PKI)-based approach for securing messages sent in a vehicle-to-vehicle and vehicle-to-infrastructure fashion. We can categorize cryptography techniques into two models:

3.3.1 Conventional Techniques

3.3.1.1 Tamper-proof device

Each vehicle carries a tamper-proof device. It contains the secrets of the vehicle itself. It has its own battery and its own clock (notably in order to be able to sign timestamps).

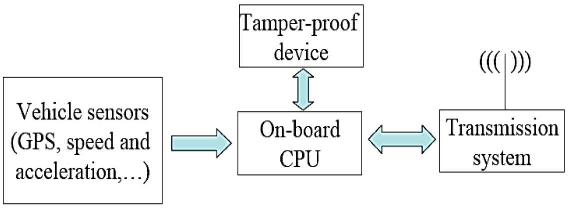


Figure 15: Tamper proof device in VANET

3.3.1.2 V-PKI (vehicular PKI)

Each vehicle carries in its Tamper-Proof Device (TPD). Mutual authentication can be done without involving a server authority (national or regional) is cross certified.

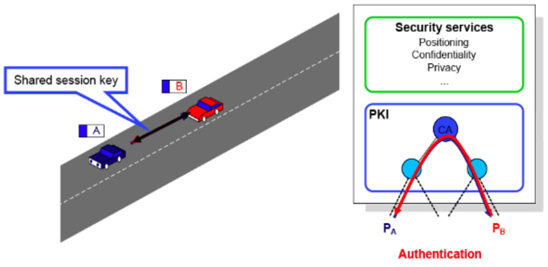


Figure 16: PKI in VANET

3.3.1.3 Anonymous keys

Preserve identity and location privacy. Keys can be preloaded at periodic checkups. Anonymity is conditional on the scenario. The authorization to link keys with ELPs is distributed.

3.3.1.4 Secure Localization

This becomes more challenging in the context of vehicular networks, where the topology changes frequently and quickly. Whenever a new GeoUnicast communication has to be initiated, and the location information of the destination node is either unknown or outdated, the LS is used to determine the most updated location of the destination node.

3.3.1.5 Certificate Revocation

Certificate revocation is done when any misbehaving vehicle having VC is discovered, where RSU replaces the old VC with new IC, to indicate that this vehicle has to be avoided and this happens when more than one vehicle reporting to RSU that a certain vehicle has a VC and broadcasting wrong data. See figure 5, this report must be given to RSU each time that any receiver receives information from sender and finds that this information is wrong.

Certificate revocation procedure

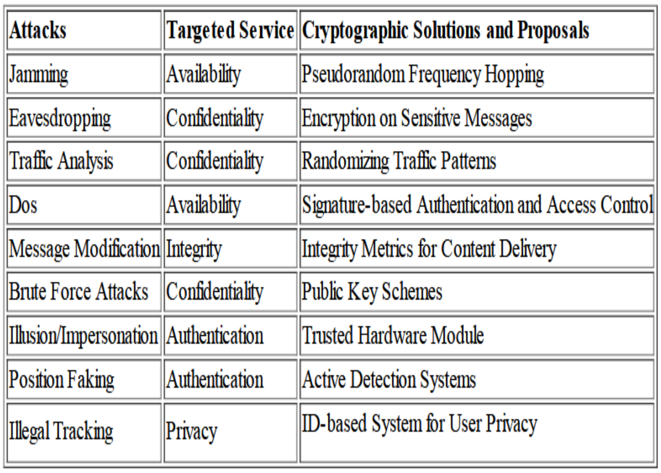
The revocation will be as follows. A sender can sends a message to receiver; this message may be from untrusted vehicle, then receiver sends a message to RSU to acquire Session Key (SKA), RSU replay message Containing SK Reply (SKR), this message contains the SK assigned to the current connection, this key is used to prevent attackers from fabrication of messages between two vehicles. Receiver sends a message to check validity, this message called “Validity Message”, the message job is to indicate if the sender vehicle has a VC or not. Afterwards, RSU reports to the receiver that the sender has a VC, so receiver can consider the information from the sender with no fear.

3.4 Software Implementation

A simulator shows the behaviour of network environment.NS2 is one of the most popular simulators used in network research. It is open source and freely available software and developed at the University of Berkeley. In this, network protocol stack is written in C++ language for fast to run, OTCL for fast to data write in order to differentiate control and data path implementations. TCL script is used for specifying scenarios, traffic patterns and events. We can clearly analyse the trace files in calculating the performance of network protocols. It supports and available for versions FreeBSD, Linux, Solaris, MAC OSX and all windows versions. NAM is abbreviated for Network AniMator and is visualization tool used for packet level animation. Xgraph is analysis tool used for seeing simulation results.

3.5 Major Attacks and Solutions

The wireless medium used in VANET has drawbacks that can render the network vulnerable to security attacks such as interference, jamming and eavesdropping. In addition, the upper layers of VANET protocol stack reference the Open System Interconnection (OSI) network model. Therefore vehicular networks inherit the vulnerabilities. Luckily, VANET can also benefit from the existing cryptographic solutions for dealing security attacks.



Attacks	Targeted Service	Cryptographic Solutions and Proposals
Jamming	Availability	Pseudorandom Frequency Hopping
Eavesdropping	Confidentiality	Encryption on Sensitive Messages
Traffic Analysis	Confidentiality	Randomizing Traffic Patterns
Dos	Availability	Signature-based Authentication and Access Control
Message Modification	Integrity	Integrity Metrics for Content Delivery
Brute Force Attacks	Confidentiality	Public Key Schemes
Illusion/Impersonation	Authentication	Trusted Hardware Module
Position Faking	Authentication	Active Detection Systems
Illegal Tracking	Privacy	ID-based System for User Privacy

Figure 17: Possible major attacks and solutions in VANET

4. Conclusion

Risks caused by security attacks are one of the major security issues for the VANETs that are constraining the deployment of the vehicular ad hoc networks. VANET is an emerging research area with promising future as well as great challenges especially in its security. It shares general ad-hoc network security concerns and faces attacks such as eavesdropping, traffic analysis and brute-force attacks. The unique nature of VANET also raises new security issues such as position detection, illegal tracking and jamming. General cryptographic approaches that apply in VANET include public key schemes to distribute one-time symmetric session keys for message encryption, certificate schemes for authentication and randomizing traffic patterns against traffic analysis. The trust-grouping framework takes a hybrid approach of symmetric and symmetric cryptographic schemes in order to achieve both desirable processing speed and security strength. The pseudo ID-based system is then covered and it uses Threshold-based techniques for authentication and message signing in order to strike a balance between the need to preserve user privacy and the requirement for traceability for law enforcement authorities. The defensive mechanism for VANET applies to improve its security. We hope that the classification of attacks presented in this paper will be helpful in identifying attacks and better understand the behaviour of the attackers.

Acknowledgement

I will be thankful forever to the LORD BAJARANGBALI for his boundless blessings showered on me. I am very grateful and express my heartfelt countless Namaste to most respectable and my M.Phil. Guide and supervisor who are Dr. S. Ananthi madam ji,B.E.,M.Tech.(IISC),Ph.D., Associate Professor, Department of Network Systems and Information Technology, University of Madras, Guindy Campus, Chennai for their constant support, invaluable and inspiring guidance to the progress of my paper work. Without madam ji, and Sir K. Padmanabhan inspiration, definitely this paper work would not have been possible. I would like to express my heartfelt special thanks to most respectable, emeritus and senior Prof. (ret.) Dr.K.Padmanabhan, Former Head, CISL and Emeritus Professor in AC Technology College, Anna University for their kind support for carrying out this paper work. I would like to express special thanks to Prof. (ret.) Ramana Murthy M. V., Department of Mathematics & Computer Science, University College of Science, Osmania University, Hyderabad, Telangana, and Prof. (ret.) Shankar B., Department of Mathematics, University College of Science, Osmania University, Hyderabad, Telangana and Radhakrishna Peddiraju sir for clarifying my doubts On NS2 software to run on windows 7. I take this opportunity to express my heartfelt thanks to Dr. K.R.Balaji M.Sc.,M.Phil.,Ph.D. Department of NS & IT, University of Madras, Guindy Campus, Chennai, and Arun Ananthanarayanan, UGC research scholar, Department of NS & IT, University of Madras, Guindy Campus, Chennai for giving their constant support and valuable help.

References

[1] Mohamed Nidhal Mejri, Jalel Ben-Othman, Mohamed Hamdi, "a Survey on VANET security challenges and possible cryptographic solutions",Vehicular Communications, Volume 1, Issue 2, April 2014, Pages 53-66, ISSN 2214-2096.

[2] Isaac, J.T.; Zeadally, S.; Camara, J.S., "Security attacks and solutions for vehicular ad hoc networks," Communications, IET , vol.4, no.7, pp.894,903, April 30 2010. doi: 10.1049/iet-com.2009.0191.

[3] Prabhakar, M.; Singh, J.N.; Mahadevan, G., "Defensive mechanism for VANET security in game theoretic approach using heuristic based ant colony optimization," Computer Communication and Informatics (ICCCI), 2013 International Conference on, vol., no., pp.1,7, 4-6 Jan. 2013. doi: 10.1109/ICCCI.2013.6466118.

[4] Sumra, I.A.; Hasbullah, H.; Manan, J.A., "VANET security research and development ecosystem," National Postgraduate Conference (NPC), 2011, vol., no., pp.1,4, 19-20 Sept. 2011. doi: 10.1109/NatPC.2011.6136344.

[5] Chowdhury, P.; Tornatore, M.; Sarkar, S.; Mukherjee, B., Wagan, AA; Mughal, B.M.; Hasbullah, H., "VANET Security Framework for Trusted Grouping Using TPM Hardware," Communication Software and Networks, 2010. ICCSN '10. Second International Conference on, vol., no., pp.309, 312, 26-28 Feb. 2010. doi: 10.1109/ICCSN.2010.115.

[6] Jinyuan Sun; Chi Zhang; Yanchao Zhang; Yuguang Fang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," Parallel and Distributed Systems, IEEE Transactions on, vol.21, no.9, pp.1227,1239, Sept. 2010. doi: 10.1109/TPDS.2010.14.

[7] Azogu, I.K.; Ferreira, M.T.; Hong Liu, "A security metric for VANET content delivery," Global Communications Conference (GLOBECOM), 2012 IEEE , vol., no., pp.991,996, 3-7 Dec. 2012. doi: 10.1109/GLOCOM.2012.6503242.

[8] Gongjun Yan; Bista, B.B.; Rawat, D.B.; Shaner, E.F., "General Active Position Detectors Protect VANET Security," Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on , vol., no., pp.11,17, 26-28 Oct. 2011. doi: 10.1109/BWCCA.2011.12.

[9] J.T. Isaac, S. Zeadally, and J.S. Cmara, "Security attacks and solutions for vehicular ad hoc networks", in IET Communications, pp. 894-903, 2009.

[10] Irshad Ahmed Sumra, Iftikhar Ahmad, Halabi Hasbullah, Jamalul-lail bin Ab Manan, "Classes of attacks in VANET", in Tenth International Conference on Wireless and Optical Communications Networks (WOCN), pp 1 - 5, 2013.

[11] M.Raya, P. Papadimitratos, and JP. Hubaux, "Securing Vehicular Communications", in IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, 2006, pp. 8-15.

[12] S. S. Manvi, M. S. Kakkasageri, D. G. Adiga, " Message Authentication in Vehicular Ad hoc Networks: ECDSA Based Approach", in International Conference on Future Computer and Communication, 2009, pp. 16-20.

[13] Bin Xiao, Bo Yu, Chuanshan Gao, "Detection andlocalization of Sybil nodes in VANETs", in DIWANS '06, pp. 1-8

AUTHORS

Dr. M. Raghavender Sharma (drmrsstatou@gmail.com) pursed Bachelor of Science in Mathematics, Master of Science in Statistics, and achieved Doctoral Degree in Statistics, all degrees from Osmania University, Hyderabad, Telangana, India, and currently he is working as an Assistant Professor and Head of Department, Department of Statistics at University College of Science, Saifabad, Osmania University, Hyderabad, Telangana, India. He is supervising many Ph. D.'s. He has excellent teaching track record with 25 years teaching experience.

Mr. Venkatamangarao Nampally (n.venkat018@gmail.com) pursed Bachelor of Science in Computer Science, Master of Science in Computer Science and Master of Technology in Computer Science & Engineering, all degrees from Osmania University, Hyderabad, Telangana, India, and pursed Master of Philosophy from University of madras, Chennai, Tamil Nadu, India. His main research work focuses on VANET communication. He has 7 years of teaching experience and 2 year of Research Experience.