International Journal of Scientific Research & Engineering Trends
Volume 5, Issue 6, Nov-Dec-2019, ISSN (Online): 2395-566X

# A Survey on Security Attacks in Vehicular Adhoc Networks (Vanets)

**S.Arabindhu Prof K. Prem Kumar S. Vinitha**
Department of Computer Science and Engineering
SMVEC, Puducherry, India

***Abstract* -VANETs have turned into a major part of numerous savvy transportation frameworks. Security is a significant yearning for VANET in perspective on the actualities that improved security which diminishes mishaps and subsequently improves traffic conditions but then spare lives. Creating secure VANET foundations stays most noteworthy test. As verification permits confiding in both client and information, it requires significant consideration in the security structure of VANETs. A large portion of the examination purposeful endeavors' in scholastics and industry are engaged to give productive security engineering to VANET to shield the system from foe hubs and assaults. The issue of VANET is transmitting data to address goal without impact in that data. Bringing up security holes with respect to particular dangers, the arrangement will permit to structured new secure system control strategies. This paper gives different assaults in VANET and potential arrangements by utilizing cryptographic tasks.**

***Keywords*- Vanets, Security attacks.**

## I. INTRODUCTION

Vehicular Ad hoc Network applications require security of utilizations so as to serve clients and make their adventure secure and agreeable. Transmission of information or data among vehicle-to-vehicle exists through remote medium in VANET. So there are odds of different assaults in VANET. Security has consistently been an issue in vehicular systems which must be genuinely considered and a security foundation must be planned and actualized in such organizes. Assailants attempt to have their effect on the system through different methods and the dynamic conduct of these aggressors is erratic.

It is compulsory that every single transmitted datum can be infused or changed by clients who have malignant objectives by aggressor. Then again, by increasing unapproved access to organize, an aggressor can deal with basic parts of a vehicle and cause unsalvageable harm to the vehicle or its travelers. Along these lines, security is compulsory for effective transmission of such data. Other than wellbeing, different administrations, for example, Internet get to, climate figure and geo-area data can advance travel involvement by giving travel solace, accommodation and infotainment. Councils are committing endeavors' to settle benchmarks for VANET.

These guidelines incorporate IEEE 1609.x, 802.11p and Wireless Access in Vehicular Environment (WAVE).WAVE is a layered engineering for gadgets going along IEEE 802.11 to work on Dedicated Short

Range Communication (DSRC) band. The IEEE 1609 family characterizes the engineering and the relating convention set, administrations and interfaces that permit all WAVE stations to interoperate inside the VANET condition. Together the WAVE standard family shapes the premise to actualize a wide scope of VANET applications crosswise over spaces, for example, security, improved route, programmed tolls and traffic cautions, and so on.

So as to accomplish the best security highlights, VANET security issues are arranged as:

1. Security challenges in VANET
2. Security necessities in VANET
3. Attackers on VANET
4. Attacks on VANET

**1. Security Challenges in VANET**

We utilize two methodologies in VANET so as to execute security challenges.

1. Technical Challenges
2. Social and Economic Challenges

In first approach we utilize low intricacy security calculations, for example, RSA, ECC. In second approach we use transport convention decision. So as to accomplish for better security in two approaches, for information encryption AES utilized.

**3. Security Requirements in VANET**

Security is a condition of being or feeling shielded from damage or assault. Security Requirements for VANETs are:

**4. Security Requirements in VANET**

Security is a condition of being or feeling shielded from damage or assault. Security Requirements for VANETs are

**5. Integrity**

Respectability is required between two imparting hubs to ensure information exactness, which is primary security issue attractive in VANETs.

**6. Confidentiality**

The test to shield information content from the enemies is classification.

**7. Non-Repudiation**

To renounce intends to deny. No repudiation is the confirmation that somebody can't deny something. Normally, no repudiation alludes to the capacity to guarantee that involved with an agreement or a correspondence can't prevent the genuineness from claiming their mark on an archive or the sending of a message that they began.

**8. Pseudonymity**

Pseudonymity is the condition of depicting a hidden personality. A holder that is at least one people is recognized however don't reveal their actual names.

**9. Privacy**

The insurance of individual data of drivers inside the system from different hubs however removed by experts in the event of mishaps is a noteworthy protection issue which is alluring for VANETs.

**10. Scalability**

The capacity of a system to deal with developing measure of work in a competent way safely is Scalability, which is the fundamental test in VANETs.

**11. Mobility**

The hubs imparting in VANETs continually change their areas with various headings and rates making the system dynamic in nature. In this way, so as to make correspondence fruitful, it is trying to build up security conventions.

**12. Key-Management**

The key is utilized to scramble and unscramble data during correspondence process. When planning security conventions for systems like VANET, the issue of key administration must be settled.

**13. Location-confirmation**

This is important to anticipate numerous assaults and is useful in information approval process. In thismanner to improve the security of VANETs, a strong strategy is required to confirm the hubs positions.

**14. Data Encryption**

Encryption is the demonstration of encoding content with the goal that others not aware of the unscrambling system (the "key") can't comprehend the substance of the content.

Fig 1: Data Encryption

**3. Attackers on VANET**

Aggressor has different properties which are referenced underneath:

**1. Insider and pariah**

This sort of aggressor is a bona fide client of the system and has detail information of the system. In the event that the assailant is a part hub who can speak with different individuals from the system, it will be known as an Insider and ready to assault in different ways. Insiders are validated individuals from system while outcasts are interlopers

**2. Malicious and Rational**

Malignant aggressors don't much damage to arrange yet they do hurt distinctly to usefulness of system. An insidious aggressor utilizes various techniques to destroy the delegate hubs and the framework without searching for its individual addition. On the unfavorable, a sensible aggressor predicts individual help from the attack. In this way, these assaults are increasingly sure and pursue a few plans.

**3. Active Vs inactive**

A functioning aggressor can accomplish new parcels to degenerate the framework though an inactive assailants dynamic just listen stealthily the remote transporter yet can't make new bundles (i.e., lesser unsafe).

The three primary attributes on which assailant depends to accomplish their objective are spending plan, labour, and apparatuses.

**4. Attacks on VANET**

The security is most unequivocal issues in light of the fact that their data is communicated through remote medium. In this way, there are odds of various potential assaults in VANET because of open nature of remote medium. Assailant objective is the redemption of data from source to goal with altered data in VANET framework. The conceivable order of these assaults is portrayed in following figure

**1. Confidentiality Attacks**

**Eavesdropping**

Spying is the unapproved constant capture attempt of a private correspondence, for example, a telephone call, text, video meeting or fax transmission. The fundamental objective o this assault is access of secret information.

**2. Information get-together assault**

The aggressor performing Bogus Information assault can be untouchable (gate crasher) or insider (authentic client). The thought is to transmit inaccurate or counterfeit data in

the system for individual favourable position. For example, an assailant may transmit a message reporting "Substantial traffic conditions" to the others so as to make its development simpler out and about. ECDSA (Elliptic Curve Digital Signature Algorithm) is probably the best answer for this sort of assaults

**3. Traffic examination**

Aggressors can acknowledge to the traffic on remote connects to decide the area of objective hubs by assessing the correspondence course of action, the volume of information transmitted by hubs and the propensity of the transmission. For instance, in a front line situation, a considerable measure of system traffic regularly streams to and from the home office. Traffic design request thusly enables an interloper to decide the ordering hubs in the system. Regardless of whether the information in a message is verified by encryption, traffic examination can in any case be executed to separate some valuable data. Albeit aloof assaults don't straight influence the system' usefulness, in some VANET use situations, for example, military correspondence, significant data exposure through traffic examination or basically listening stealthily could demonstrate exorbitant.

**4. Integrity Attacks**

**4.1 Message concealment**

The aggressor performing Bogus Information assault can be pariah (interloper) or insider (authentic client). The thought is to transmit off base or counterfeit data in the system for individual favourable position. For example, an assailant may transmit a message reporting "Overwhelming traffic conditions" to the others so as to make its development simpler out and about.

ECDSA (Elliptic Curve Digital Signature Algorithm) is perhaps the best answer for this sort of assaults. In this assault, an assailant specifically drops parcels got from the neighbours these bundles may hold basic wellbeing related data for the recipient, the aggressor smother or square these parcels and can utilize them again at later time. Such kind of assault can forestall cautioning messing to be sent. For example, an assailant may hinder a clog cautioning, so vehicles won't get the notice and compelled to sit tight in the rush hour gridlock for the long time.

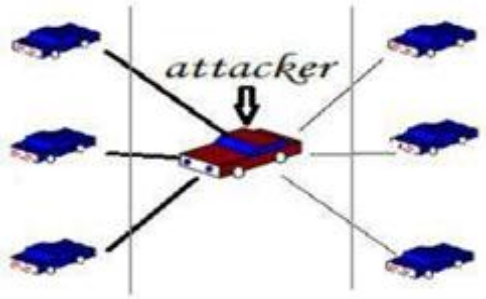


Fig 2: Integrity Attacks

**4.2 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.

**4.3 Fabrication**

In this kind of assault a phony message is embedded into the system by an unapproved client as though it is a legitimate client. This outcome in the loss of privacy, credibility and uprightness of the message.

**4.4 Masquerade**

The aggressor utilizes MAC and IP parodying so as to get character of different hubs and stow away into the system. On the off chance that there is no verification procedure so as to make the system secure from malevolent hubs, a noxious vehicle can send message for different vehicles to pick up its own advantages or make turmoil, automobile overload or mishaps and conceal itself. It is accomplished by utilizing masquerade character and messages manufacture, change and replay. For instance, a malevolent hub may mimic a rescue vehicle to demand others for need path or request close byRSUs to change traffic lights to green. Along these lines, the message from an OBU must be uprightness checked and confirmed before it very well may be depended on.

**4.5 Replay**

An assailant can replay the got bundles separated from going about as a typical hub (advances all the got parcels). In this assault, bundles are falsely rehashed. This activity is completed by a vindictive hub that blocks the wellbeing bundle and retransmits it. This kind of assault is normally performed to imitate a genuine vehicle or RSU. Since, Basic802.11 security does not contain grouping numbers; in this way it gives no assurance against replay. Due to keys can be reused, it is conceivable to replay put away messages with a similar key without discovery to embed false messages into the framework.

**5. Authentication and Identification Attacks**

**5.1 GPS ridiculing**

In VANETs, an area table with the geographic areas and vehicles personalities is a basic component that is kept up because of GPS satellite. Utilizing the GPS satellite test system to create signals, that are more grounded than those produced by the real satellite framework are, an assailant can deliver false readings in the GPS to bamboozle vehicles to imagine that they are in an alternate area. Concealed vehicle is another solid case of bamboozling with situating data.

As Fig. outlines, the vehicle B deludes the vehicle A to accept that it is better set (at B') for sending the notice message, however then keep quietness about the mishap. In light of the transitory vanishing of GPS flag in passages, an assailant is conceivable to infuse false situating data once the vehicle leaves the passage and

before it gets a real position update, as Fig. 10 outlines. This marvel occurs with either a physical passage or a zone stuck by the aggressor that prompts similar impacts.

**5.2 Position faking**

Fashioning of message can be completed by assailant straightforwardly or in a roundabout way through another vehicle.

**5.3 Tunneling**

This sort of assault is additionally called concealed vehicle attainable in a very circumstance any place vehicles flawlessly endeavor to decrease the clog on the remote channel. For instance, a vehicle has sent a notice message to its neighbor and it's anticipating a reaction. Once getting a reaction, the vehicle understands that its neighbor is in an extremely higher position to advance the notice message and quits making this message various hubs.

**6. Availability Attacks**

**6.1DOS assault**

Disavowal of Service Attack: It is the most genuine level assault in vehicular system. In this assault

assailant sticks the fundamental correspondence medium and system is not any more accessible to genuine client.

Above figure demonstrates the entire situation when the aggressor A dispatches DOS assault in vehicular system accordingly it sticks the entire correspondence medium somewhere in the range of V2V and V2I and the genuine clients (B, C, and D) can't speak with one another. One type of DOS assault is Distributed Denial of Service Attack (DDOS Attack).DDOS assaults are those assaults wherein assailant assaults in circulated way from various areas. Aggressor may utilize distinctive timeslots for sending the messages. Nature and schedule vacancy of the message can be differed from vehicle to vehicle of the aggressors. Here, the point of aggressor is same as DOS assault.

**6.2 Jamming assault**

Transmitting of radio sign to upset the entire interchanges by diminishing the sign to-clamour proportion. The term sticking is utilized to separate it from inadvertent sticking which called impedance. In VANET Jamming is a genuine risk to its security. Jammers always send rehashed signals (in influenced zone) to meddle with the correspondence between hubs in the system. The injured individual feels that the condition of the channel is as yet occupied. In this manner, it can't send or get parcels in the stuck region. When sticking is empowered, the sender may effectively send bundles; the recipient can't get every one of the parcels sent by the sender. Subsequently, its parcel conveyance proportion (PDR) is low. These parcels can be conveying significant data (perilous, for example, street conditions, climate, mishaps, and so forth and inability to get or scatter these bundles can prompt fatalities.

**6.3 Malware and Spamming**

Malware and spam assaults, for example, infections and spam messages, can cause genuine interruptions in the typical VANETs tasks. This sort of assault is regularly executed by vindictive insiders as opposed to pariahs. For example, an assailant sends a major measure of spam messages in the system to expend the transfer speed and to expand the transmission dormancy. It is difficult to control such sort of conduct on account of the absence of fundamental framework and brought together organization. In the mean time, malwares are much the same as infections that hamper the ordinary activity of the system. VANET get tainted typically when On Board Units (OBU) of vehicles and Road Side Units (RSUs) perform programming refreshes. Implanted enemy of malware structures are as yet a hazardous issue in VANETs look into network.

**7 Black opening**

A dark opening is a region where the system traffic is diverted. In any case, either there is no hub around there or the hubs dwell here decline to take an interest in the system. In a dark opening assault, a vindictive hub presents itself for having the most brief way to the goal hub and hence, swindles the directing convention. Rather than investigating steering table right off the bat, this threatening hub publicizes quickly that it has a crisp course for the course demand.

In result, assailant hub wins the privilege of answering to the course solicitation and along these lines it can capture the information bundle or hold it. At the point when the manufactured course is effectively settled, it relies upon the malevolent hub whether to drop or advance the parcels to any place it needs. Dark Hole assault is known as a variety of Black Hole assault, in which the malevolent hub deceives the system by consenting to advance the parcels yet it some of the time drops them for some time and after that changes to its ordinary conduct. It is hard to make sense of such sort of assault.Arrangement:

Traditionally in impromptu organizes, there are three sorts of safeguards against Sybil assaults presented, specifically enlistment, position confirmation, and radio asset testing. Enlistment itself isn't sufficient to avoid Sybil assaults, in light of the fact that a vindictive hub has plausibility to enroll with different characters by non-specialized methods, for example, taking. Additionally, a severe enlistment may prompt genuine protection inconveniences.

In position check, the situation of hubs will be confirmed. The objective is to verify that each physical hub alludes to one and just a single character. Radio asset testing depends on the suspicion that every single physical element are constrained in assets.The rest of this paper is composed into as pursues: Part 2, contains an audit of related work. Section 3 clarifies Methodology; Part 4 depicts Conclusion of work. Finally we give affirmations and reference which are utilized for setting up this paper.

## II. RELATED WORK

Merij [1] propose the utilization of a cryptographic based classification that is simple and plain to comprehend since the comparable methodology it takes as done in conventional system security arrangements. Isaac [2] likewise overviews the real security assaults and introduces the comparing countermeasures and cryptographic arrangements. Dynamic guarded systems like the one proposed in Prabhakar [3] are likewise fundamental supplements to the detached components of encryption. Not with standing its dynamic nature and high versatility, the utilization of remote media additionally makes VANET helpless against assaults that endeavour the open and communicate nature of remote correspondence [4].

To adjust the requirement for security and the requirement for speed, specialists in [5] think of a mixture strategy that exploits both uneven and symmetric cryptographic plans. Sun [6] propose a personality based security framework for VANET that can adequately tackle the contentions among protection and tractability. The framework utilizes a nom de plume plan to protect client security. Azogu [7] propose an Asymmetric Profit- Loss Markov (APLM) model that estimates the respectability level of the security plans for VANET content conveyance. Yan [8] propose a novel position discovery plan to avert position-based assaults.

J.T. Isaac, S. Zeadally, and J.S. Camera distributed a paper on "Security assaults and answers for vehicular specially appointed systems" [9].

Irshad Ahmed Sumra proposed five distinct classes of assaults [10] and each class is required to give better points of view to the VANETs security. In [11], the creators attempt to manage the Sybil assault by open key cryptography. A Public Key Infrastructure for VANETs (VPKI) is proposed. The creators outline a total answer for upgrade correspondence security by tending to the key dispersion and key denial. The Sybil assault is constantly distinguished all around right on time since every vehicle is verified correspondingly with its open key. In any case, similar to some other cryptography-based methodologies, the sending of VPKI is an overwhelming and dubious issue that must be tried to evaluate the conceivable usage as a general rule.

ECDSA (Elliptic Curve Digital Signature Algorithm)[12] is named as one of the answers for false data assaults. Customarily in specially appointed systems, there are three sorts of resistances against Sybil assaults presented, to be specific enrolment, position check, and radio asset testing [13].

## III. STRATEGY

**1. Traditional Security Mechanism**

**1.1 Electronic tags**

Electronic tags (ELP), which are cryptographically irrefutable numbers identical to customary tags and help in distinguishing taken autos and monitoring vehicles crossing nation fringe.

**1.2 Asymmetric Encryption utilizing PKI**

An open key cryptosystem depends on the supposition that it may be conceivable to discover a framework where it is computationally infeasible to decide the decoding standard given its encryption rule. Vehicular open key foundation (VPKI) in which a confirmation expert oversees security issues of the system like key circulation, testament denial and so on. To keep a tap on false data assault, information relationship methods are utilized. To recognize false position data, secure situating procedures like unquestionable multi lateration is regularly utilized. Open key encryption has quickly developed in ubiquity since it offers a protected encryption to data. In an open key cryptosystem, the sender encodes a message with the beneficiary's open key. This key is generally posted in a registry like a telephone directory.

After accepting the message, the beneficiary uses his/her very own private key to unscramble the message. For instance, Alice scrambles a message utilizing Bob's open key and sends it to him over an unreliable channel. Sway at that point decodes the message with a private key that is known uniquely to him. RSA is an open key cryptosystem that supports both encryption and advanced marks (authentication).Like all open key cryptography models, the RSA cryptosystem encodes and decodes a message utilizing a couple of keys known as open key and private key. Its security depends on the trouble of considering huge whole numbers.

By and by, most usage of the RSA calculation utilizes the utilization of 512-piece numbers. Splitting such a framework requires the capacity to factor the result of two 512-piece prime numbers. Calculating some of this size is well past the ability of the best current figuring calculations.

**2. Defensive Mechanism**

For contributions as given safety efforts of the VANET, the protective system embraces game theoretic methodologies and is included three phases. The main stage utilizes heuristics dependent on subterranean insect state streamlining to recognize known and obscure rivals. In the subsequent stage, Nash Equilibrium is utilized for choosing the model for a given security issue. The third stage empowers the cautious system.

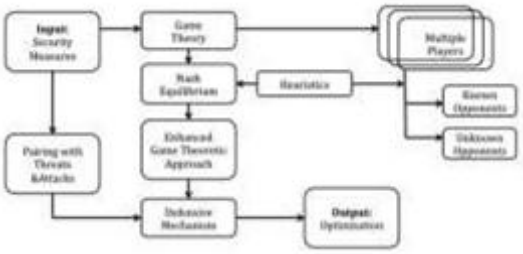

Fig 3:Traditional Security Mechanism

**3. Cryptography Models**

Encryption is the worry of the security of electronic transmissions and carefully put away information. Standard encryption techniques normally have two essential blemishes, (1) A safe channel must build up sooner or later so the sender may trade the disentangling key with the beneficiary; and (2) There is no assurance that who sent a given message. Vehicle Safety Communications Consortium (VSCC) characterized security approaches for security engineering in vehicular systems that are under institutionalization up until this point. It characterizes an open key-framework (PKI) based methodology for verifying messages sent in a vehicle-to-vehicle and vehicle-to-foundation design. We can arrange cryptography strategies into two models:

**4.Conventional Techniques**

**4.1 Tamper-evidence gadget**

Every vehicle conveys a carefully designed gadget. It contains the privileged insights of the vehicle itself. It has its very own battery and its own clock (strikingly so as to have the option to sign timestamps).

**5. Conventional Techniques**

**5.1 Tamper-evidence gadget**

Every vehicle conveys a carefully designed gadget. It contains the privileged insights of the vehicle itself. It has its very own battery and its own clock (strikingly so as to have the option to sign timestamps).

Anonymous keys Safeguard character and area security. Keys can be preloaded at intermittent check-ups. Secrecy is contingent on the situation. The approval to connection keys with ELPs is appropriated.

**5.2 Secure Localization**

This turns out to be all the more testing with regards to vehicular systems, where the topology changes every now and again and rapidly. At whatever point another GeoUnicast correspondence must be started, and the area data of the goal hub is either obscure or obsolete, the LS is utilized to decide the most refreshed area of the goal hub.

**5.3 Certificate Revocation**

Testament repudiation is done when any getting rowdy vehicle having VC is found, where RSU replaces the old VC with new IC, to show that this vehicle must be dodged and this happens when more than one vehicle answering to RSU that a specific vehicle has a VC and broadcasting incorrectly information. See figure 5, this report must be given toRSU each time that any beneficiary gets data from sender and finds that this data isn't right.

**5.4Authentication repudiation method**

The renouncement will be as per the following. A sender can makes an impression on recipient; this message might be from untrusted vehicle, at that point collector makes an impression on RSU to obtain Session Key (SKA), RSU replay message Containing SK Reply (SKR), this message contains the SK appointed to the present association, this key is utilized to keep aggressors from manufacture of messages between two vehicles.

Recipient makes an impression on check legitimacy, this message called "Legitimacy Message", the message employment is to demonstrate if the sender vehicle has a VC or not. A short time later, RSU reports to the beneficiary that the sender has a VC, so collector can think about the data from the sender with no dread

**6. Software Implementation**

A test system demonstrates the conduct of system environment.NS2 is one of the most famous test systems utilized in system examine. It is open source and unreservedly accessible programming and created at the University of Berkeley. In this, organize convention stack is written in C++ language for quick to run, OTCL for quick to information write so as to separate control and information way usage. TCL content is utilized for determining situations, traffic examples and occasions. We can unmistakably examine the follow records in computing the exhibition of system conventions. It bolsters and accessible for adaptations FreeBSD, Linux, Solaris, MAC OSX and all windows renditions. NAM is truncated for Network AniMator and is perception device utilized for parcel level movement. Graph is examination apparatus utilized for seeing recreation results.

**7. Major Attacks and Solutions**

The remote medium utilized in VANET has disadvantages that can render the system powerless against security assaults, for example, impedance, sticking and listening in. Furthermore, the upper layers of VANET convention stack reference the Open System Interconnection (OSI) organize model. Subsequently vehicular systems acquire the vulnerabilities. Fortunately, VANET can likewise profit by the current cryptographic answers for managing security assaults.

## IV. CONCLUSION

Dangers brought about by security assaults are one of the significant security issues for the VANETs that are compelling the arrangement of the vehicular specially appointed systems. VANET is a developing examination zone with promising future just as extraordinary difficulties particularly in its security. It offers general impromptu organize security concerns and faces assaults, for example, spying, traffic examination and animal power assaults. The one of a kind sort of VANET

likewise raises new security issues, for example, position discovery, unlawful following and sticking. General cryptographic methodologies that apply in VANET incorporate open key plans to appropriate one-time symmetric session keys for message encryption, declaration plans for verification and randomizing traffic designs against traffic investigation. The trust-gathering system adopts a half breed strategy of symmetric and symmetric cryptographic plans so as to accomplish both alluring handling rate and security quality.

The pseudo ID-based framework is then secured and it utilizes Threshold-based methods for validation and message marking so as to strike a harmony between the need to protect client security and the prerequisite for discernibility for law implementation specialists. The protective instrument for VANET applies to improve its security. We trust that the characterization of assaults introduced in this paper will be useful in distinguishing assaults and better comprehend the conduct of the assailants.

## 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.Chowdhury, P.; Tornatore, M.; Sarkar, S.;

[5]. 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]. 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. Camara, “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.