Sumra *et al.LGU (IJECI)*2018

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 2 issue 3 July-September 2018

Security in Vehicular Ad hoc Network (VANET) using Trusted Platform Module (TPM): A Survey

Irshad Ahmed Sumra[1], Zahid Adeel Hashmat[2]
Computer Science Department
University of South Asia
47-Tufail Road, Lahore.
Sector C, DHA Phase-VI Lahore.
zahidadeelhashmat@gmail.com[2] ,irshad.ahmed@usa.edu.pk[1]

Abstract:

Vehicular Ad hoc Networks (VANETs) are gaining more attention from automobile industries due to user safety on highway. However, security and safety critical issues need to be resolved before deployment of VANET in real environment. In this paper, we are providing a comprehensive survey on the usage of trusted platform module (TPM) in VANET. VANET is a open wireless environment where vehicle can communicate with other vehicles and also with roadside unit where any infected rogue vehicle can perform malicious actions on fellow vehicles. Security threats caused by rogue vehicles can endanger life of passengers. Trust is an important key factor and it can be introduced inside VANET environment using TPM hardware. The core purpose of this survey is to highlight the security threats in VANET and provide security architecture built upon TPM to mitigate all discussed threats.

Keywords: Vehicular ad hoc network (VANET), Security, trusted platform module (TPM), dedicated short range communication (DSRC).

1. Introduction

Traffic accidents impact our life directly or indirectly and are considered a major challenge in traffic management. According to the global status report on road safety 2015, it is indicated that the global road accident deaths has platitude at 1.25 million per year [1] and it will increase 60% more in next few years if it is not controlled somehow. An ideal solution to avoid road accidents and improve traffic management is VANET. It is a sub category of mobile ad hoc network (MANET) where nodes can be Road Side Units (RSUs) or vehicles [2]. It uses Dedicated Short Range Communication (DSRC) channels in vehicle to vehicle (V2V) and vehicle to road side unit (V2R) communication [3]. DSRC are short to medium range wireless communication channels which are specifically designed for automobiles to guarantee active safety applications [1]. In

safety applications, warning messages are sent to network vehicles to prevent road accidents. Non-safety applications may include comfortable driving experience of passengers and availability of parking slots. Inside VANET, trust is key importance parameter between vehicles and RSUs. So, information and data exchange happens between vehicles and RSUs assuming that security, trust, privacy triad is ensured. Vehicle is a private property of a user and it may disclose very sensitive information about its owner if somehow a malicious attacker exploits it. In short, VANET faces some serious security challenges where a malicious attacker can change the behavior of network nodes and launch attacks against safety and non-safety applications. Therefore, network security must be ensured before deployment in order to avoid any life critical situations. High mobility nature of VANET makes it very challenging task to monitor [4] and identify attacks. In order to make a reliable network these mobile nodes have to trust each other which is technically possible using trusted platform module (TPM). Trusted computing group (TCG) defines trust as "Any entity that behaves in an expected manner for that intended purpose"[5]. Core entities of VANET are user, vehicle and RSU where unexpected behavior from either of them can highly affect the behavior of other entities. So, in this paper we will discuss that how TPM can introduce 'TRUST' factor among VANET nodes and how it can help us to improve security against attacks.

The rest of the paper is divided into VI sections where section II discusses essential security requirements for VANET. Section III discusses the TPM architecture and proposed TPM model for VANET. Section IV discusses in details the about the nature of attacks on VANET. Section V discuss about possible usage of TPM and some other trusted hardware modules in VANET for defensive countermeasure of attacks and in the end section VI concludes the paper.

2. Essential Security Requirements

VANET infrastructure highly relies on communication and messages among its nodes. So, it is very important to make sure authenticity and integrity of the exchanged communication data. As VANET is a real-time network and little delay in communication messages can endanger the life of passengers especially when messages are meant for safety applications. So, it is very possible that a malicious intent attacker may try to delay or drop the safety concerned communication messages. Taking above mentioned scenarios into consideration, we need some proper security measures which may define and measure the security of VANET nodes [6]. So, we will discuss following five parameters to address all these security and privacy issues [13]. In simple words, a network will be considered well secured if it implements following parameters in its topology.

2.1 Authenticity:

Inside VANET, there may be legitimate and non-legitimate (malicious) nodes. So, first of all it is important to ensure that the communication nodes are authenticated by a trusted authority. A third party certificate authority (CA) module manages and verifies the identities of VANET nodes. So, it will ensure that the messages are received from legitimate users [7]. Authenticity will provide a trustworthy environment for exchanged messages by keeping un-authorized nodes away from private communication channels.

2.2 Confidentiality:

Confidential user data such as vehicle's

registration number, global position and route plan of VANET nodes is shared with concerned authorities for safety or non-safety applications [6]. Confidentiality parameter demands that the data must be shared and stored in secure way in order to avoid any un-authorized access. Confidentiality is achieved using encryption algorithms.

2.3 Availability:

VANET safety applications require real-time message exchanging. So, the network should be highly available and operational for authenticated users. VANET real-time applications exchange messages at very high data rate where there is not even a margin of milliseconds delay. In VANET safety applications, a milliseconds delay may endanger someone's life.

2.4 Integrity:

It makes sure that the message sent from sender side has been received successfully on receiver side without any alteration or modification on its way [10]. A malicious intent attacker can do attack against integrity in which case receiving node will receive tempered message which may cause serious problems. This kind of attack is used to spread misinformation. To ensure data integrity, sender node digitally signs its message with certificate before sending which is verified on receiving end to make sure that data is not tempered.

2.5 Non-Repudiation:

Nodes involved in message sending process must send that message at any cost and they must not be able to deny it. Similarly, nodes involved in reception process must receive it and should not have the ability to deny it. Non-repudiation is often used to detect and unveil the criminals. Particularly, it can be useful in accident's investigations by re construction of exchanged messages [10].

3. TPM Based Trust model for VANET

TPM hardware module is specifically designed for computing purposes where security and trust is main concern and now it is being integrated into many computer devices. In laptops, mostly TPM chips are being integrated for business class like Dell's latitude series [9]. The infrastructure on which TPM is deployed, a piece of software is needed to communicate with TPM. TPM communicates with this software to store data on secure locations. It has built-in cryptographic functionalities which are used to enforce trust. Though TPM seems quite good against software attacks but it doesn't have any mechanism to avoid hardware tampering. It can be introduced inside VANET to ensure a secure and trusted V2V and V2I communication. An architectural diagram of TPM is shown in Figure 1.

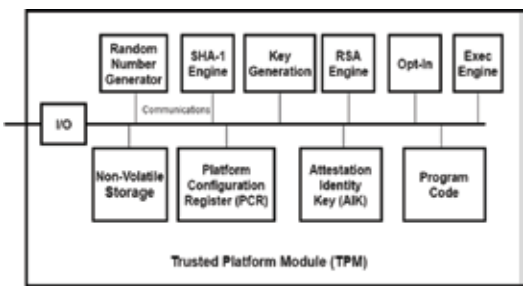

Figure 1. TPM Architecture [20]

F. Stumpf et al. [19] proposed a multi-layered C2C communication protocol named SRAAC for VANETs in order to ensure trust, security and privacy of nodes. Secure Revocable Anonymous Authenticated inter-vehicle Communication (SRAAC) protocol facilitate vehicles in inter-vehicle communication by sending or receiving safety messages. Proposed SAARC protocol will contain authentication authority (AA), inter-vehicle

communication certificate server (ICS) and onboard unit (OBU) components. Author discussed some potential attacks to SRAAC which are OBU collision attacks, false safety message injection and arbitrary validation time. Author not only discussed these attacks but also proposed a solution to prevent from these attacks which involves the usage of trusted inter-vehicle communication (T-IVC) certificate.

G. Guette et al. [20] discussed in detail that how TPM can be useful in VANET security. They highlighted some essential security parameters and proposed two applications [5] (event reporting and platoons) for VANET. Their research circles around some essential security parameters in VANET (authenticity, confidentiality, integrity) which are highlighted in section II of this paper. Their key objective was to ensure a secure and anonymous V2V communication using cryptographic keys. José María de Fuentes [21] highlighted some serious security issues in VANET and proposed some solutions related to those issues.

G. Guette et al.[22] proposed TPM based security and privacy solutions. Cryptographic key management was main focus point of their discussion. TPM module is used as an integrated part of the vehicle for all this solution. Privacy Certification Authority (PCA) is a third party modules which issues a certificate for Attestation Identity Key (AIK). AIK is used for attestation of current platform and its configuration. PCA also verifies different AIKs which are being used by different network applications. AIK certificates were proposed to be saved on a memory stick. The proposed mechanism creates some dependencies such as PCA and memory stick needs to communicate through a computer, and to connect with certification authority an internet connection is needed.

Sumra et al. [23] discussed in detail about a new card based scheme for VANET which focus on trust and security related issues. Sumra et al. [30] provided solution of security, trust and privacy using TPM in VANET.

For authentication purpose TPM used many key and here is mentioned two important keys which are given below:-

1) **Attestation Identity Keys (AiK):** This key generated by the TPM and the Privacy Certification Authority (PCA) authenticate the key and secure the end user information. AiK does not disclose the identity of the TPM and this is the main advantage of this key.

2) **Endorsement Key (EK):** this key is generated by the TPM manufacturer and unique feature of this key is securely stored inside the TPM.

A TPM root of trust architecture is showed in a Figure 2 and details about each module is given after that.

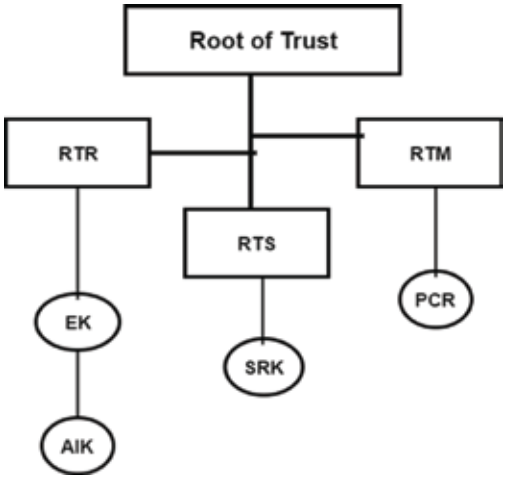

Figure 2. TPM based Root of Trust [24]

Root of Trust: TPM hardware provides following three types of root of trust [24]:

- Root of trust for measurement (RTM)
- Root of trust for reporting (RTR)
- Root of Trust for Storage (RTS)

TPM hardware communicates with onboard unit (OBU) and other embedded sensors of the vehicles and ensure root of trust. Figure 3 shows a high level working of TPM with OBU and other sensors and its application in VANET.

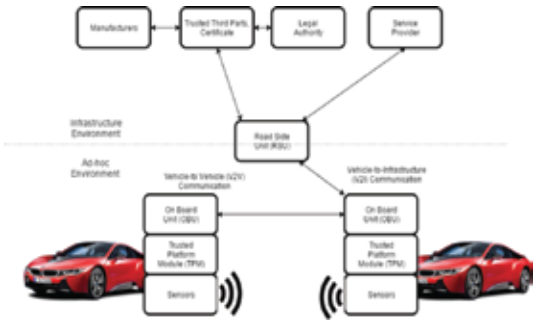

Figure 3. Trusted communication with TPM [28]

Root of Trust for Measurement (RTM): RTM is the module of TPM which measures current system state and saves it in Platform Configuration Register (PCR). TPM uses internal secure storage registers which are shielded from external attacks and data tampering attempts. So, PCR ensures data integrity of stored system state. PCR storage is non-volatile and it persists even when system is powered off.PCR basic purpose is storage of 20 byte digest hash values of system states and representation of hardware and software configuration metrics. Configuration Metrics are very important as they are defined before system is developed and then monitored in entire lifetime of system. If system finds any change in hardware and software configuration metrics, it logs it and takes appropriate actions.

Root of Trust for Reporting (RTR): RTR generates reports about current platform and securely provide generated reports to third parties. RTR ensures data integrity and privacy using digital certificates. RTR digitally signs PCR values with private key and send them to requesting third party. Third party can verify that digitally signed values using Endorsement Key (EK) [25] which is a public key.

Root of Trust for Storage (RTS): R T S does encryption and decryption of data and keys. Besides this, it also provides keys list and their respective unique functionalities. RTS utilizes a Storage Root Key (SRK) which uses asymmetric encryption to encrypt data and keys. RTS is embedded into TPM and its core purpose is to wrap TPM protected keys.

4. Attacks in VANET

A malicious intent attacker can launch different attacks in VANET. In this section, five major classes of attacks are discussed in VANET security perspective [24, 25]. In section VI, some proposed solutions to mitigate these attacks are discussed. Each attack class gives an insight to threat severity and attack type. The purpose of this section is to identify the attacks on based of their behavior or signatures and take appropriate measures accordingly. Figure. 4 lists down five classes of different types of attacks in VANET [29].

Figure 4. Classes of attacks in VANET [29]

First Class - Application Attack

This attack mainly targets VANET safety and non-safety applications. In this attack, attacker intercepts messages from one vehicle, tampers it and then spread it to other vehicles. In safety applications, warning messages are passed from one vehicle to other vehicles. If an attacker modifies it, it will give rise to some serious consequences. In bogus information attack [12] attacker spreads misinformation inside network which highly affects the behavior of network users.

In safety application attack, an attacker may spread wrong information that road is clear while there is a work zone ahead. So, in such case a road accident is obvious. In non-safety application attack, attacker may spread messages to other vehicles that parking slots are not available while actually there is parking slots are available [7].

Second Class - Network Attack

Network attack directly affect VANET infrastructure which in turn affect V2V and V2I communications. This attack is considered of high priority and might create serious problems for users.

a. Sybil Attack:

Sybil attack [16] belongs to the network attacks class. In this attack, attacker fabricates VANET communication messages with fake source identities and broadcast them inside network. When the fabricated messages [15] are received by legitimate users, they believe that there is more than one vehicle in the surrounding or there is some serious traffic jam situation. Attacker will benefit when other vehicles would believe that road is blocked because of traffic jam.

b. Denial of Service (DOS) Attack [32]:

DOS attack is attack on availability of some service. Inside VANET environment, all vehicles rely on network communication messages and if some attacker somehow jams this network, it will be serious problem. All V2V and V2I communication will get down, so authentic users won't be able to communicate with one another and it will create serious traffic jam or other life critical situations.

Third Class - Social Attack

In these attacks, social engineering attacks may be involved and it may also have attacks where immoral and abusive messages can be shared with network nodes. The main objective of this attack type is to create disturbance inside network. For example, a malicious intent driver send message to other vehicle death of his/her siblings. It will highly affect the behavior of driver which may lead to road accidents. Social attacks are totally based on social messages where one vehicle can lie to other fellow VANET nodes to create havoc.

Fourth Class - Timing Attack

This attack [31] is also on VANET safety and non-safety applications but in this attack warning messages are not altered by attacker. Instead, attacker creates a delay in message delivery. As VANET is a real-time network where warning messages should be sent and received in real-time otherwise it may cause some serious problems in life critical situations. For example, if a warning message is going to tell vehicle that there is a work zone ahead and user doesn't receive it in time, it may cause an accident.

Fifth Class - Monitoring Attack

In this class of attack, attacker only monitors or sniffs network traffic in passive mode without

creating any disturbance. In this attack, attack may find some valuable information from V2V and V2I communication which may be used for attacker's benefit. For example, if some police operation is going to happen somewhere inside VANET and attacker somehow intercept the operation details; he may use it for his benefit. Attacker may track user location in a specific region using ID disclosure attacks [17].

5. TPM based Proposed Mechanisms

VANET security threat has been under considerations in last few years and many solutions were proposed to mitigate those risks. In this section, countermeasures for attacks discussed in previous section are highlighted. In this section five basic trust entities will be discussed along with how they coordinate to create a chain of trust on platform. Figure 3 also elaborates that how TPM can be useful in VANET V2V and V2I communication. Trust entities (user, vehicle, application, routing, medium and infrastructure) are given below:[14]

a) Trusted User

There are basically two types of users inside VANET which are trusted users and non-trusted users. Trusted users are those who show the normal and non-malicious behavior. On the other hand, non-trusted users can tamper with VANET safety and non-safety applications. VANET warning messages are passed by trusted user to other users and data integrity is ensured while non-trusted users will tamper data on the way and compromise privacy of others. This way a chain of trust will be affected.

b) Trusted Vehicle

Vehicle is an important node of VANET so it is very important to make sure that vehicle is trusted or non-trusted (compromised) because vehicle is an integral part of V2V and V2I communication and if it is compromised, whole chain of trust will be affected. Trust factor in vehicles is introduced by integrating TPM with sensors and OBU. Figure 3 is elaborating this concept very well.

c) Trusted Applications

VANET safety and non-safety applications should have proper security measures within them so that an attacker may not use them to others and applications should perform their activities in the way they are designed to work. M.Gerlach et al. [11] proposed and discussed a model for trusted applications inside VANET. Proposed model discusses the situations where the attributes of the trust and trustee are relevant.

d) Trusted Routing

Routing is very integral part of network communications which involves hop to hop and hop communication. T. Chen et al. [26] proposed his own trusted routing framework which authenticates communication messages, ensures trust between vehicles and routing verification with depending on any third party CA. Trusted framework works on Optimized Link State Routing (OLSR) protocol.

e) Trusted Medium

VANET uses dedicated short range communication (DSRC) band for communication channels. It provides multiple channels on high bandwidth which ranges from 5.850 to 5.925 GHz. Attacker will try to monitor or tamper data of VANET nodes so there should be a secure and trusted communication channel. Communication channel should continuously hop to avoid any

data sniffing. C. Laurendeau et al. [27] discussed some security threats in DSRC which can be minimized to make communication channels secure and trusted.

f) Trusted Infrastructure

VANET infrastructure should be trusted and highly available to VANET nodes. V2I communication is an integral part of VANET applications and if somehow a malicious intent attacker performs a DOS attack against infrastructure and takes it down, it will raise some serious problem for VANET nodes because network nodes trust on infrastructure and if infrastructure is not responding it will break chain of trust.

6. Conclusion

Authenticity, confidentiality and availability are some essential security requirements and all of these can be achieved inside VANET if somehow 'TRUST' is introduced inside infrastructure and vehicles. TPM module is used to develop this trust. VANET safety and non-safety applications share messages in V2V and V2I communication so it is very important that all those messages are authenticated and generated by trusted network nodes. For this purpose, TPM digitally signs messages and receiving person verifies those with their key which verifies the authenticity of messages. TPM is integrated with onboard-unit and sensors of vehicle where it authenticates all incoming and outgoing communications. A chain of trust can be developed with trusted user, vehicle, applications and purpose of this chain of trust to handle with different types of attacks in VANET and secure the vehicle to vehicle and vehicle to road side communication.

7. References

[1] World health organization http://www.who.int/violence_injury_prevention/road_safety_status/2015/en/.

[2] Samara, G., Al-Salihy, W. and Sures, R. (2010) Security Analysis of Vehicular Ad Hoc Nerworks (VANET). Proceedings of Second International Conference on Network Applications Protocols and Services (NETAPPS), IEEE, Kedah, 22-23 September 2010, 55-60.

[3] International transportation system http://www.its.dot.gov/factsheets/dsrc_factsheet.htm.

[4] Al-Raba'nah, Y. and Samara, G. (2015) Security Issues in Vehicular Ad Hoc Networks (VANET): A Survey. International Journal of Sciences & Applied Research (IJSAR) , 2, 50-55.

[5] B.Balacheff,L.Chen,S.Pearson, D.Plaquin,G.Proudler. In, S.Pearsoned, "Trusted Computing Platform: TCPA technology in context", Prentice Hall PTR, Upper saddle river, NJ, 2003.

[6] Engoulou, R.G., Bellaïche, M., Pierre, S. and Quintero, A. (2014) VANET Security Surveys. Computer Communications, 44, 1-13. https://doi.org/10.1016/j.comcom.2014.02.020

[7] Raya, M. and Hubaux, J.P. (2007) Securing Vehicular Ad Hoc Networks. Journal of Computer Security, 15, 39-68. https://doi.org/10.3233/jcs-2007-15103

[8] I.AhmedSumra, H.B. Hasbullah, J.AbManan,"User requirements model for vehicular ad hoc network applications", International Symposium on Information Technology 2010

(ITSim 2010), Malaysia.C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.

[9] http://www.dell.com/us/business/p/latitude-laptops

[10] Mejri, M.N. and Hamdi, M. (2015) Recent Advances in Cryptographic Solutions for Vehicular Networks. IEEE Proceedings of International Symposium on Networks , Computers and Communications (ISNCC), Hammamet, 13-15 May 2015, 1-7.

[11] M.Gerlach, F. FOKUS,"Trust for Vehicular Applications" IEEE Computer Society, Proceedings of the Eighth International Symposium on Autonomous Decentralized Systems, p: 295-304, year of publication: 2007.

[12] M. Raya,J. Pierre, Hubaux,"Securing vehicular ad hoc Networks" Journal of Computer Security,vol.15,Issue no.1 January 2007, pp: 39-68.

[13] Razzaque, M.A., Salehi, A. and Cheraghi, S.M. (2013) Security and Privacy in Vehicular Ad-Hoc Networks: Survey and the Road Ahead. In: Khan, S. and Khan Pathan, A.-S., Eds., Wireless Networks and Security , Springer, Berlin Heidelberg, 107-132.

[14] Irshad Ahmed Sumra1,Halabi Hasbullah1,Jamalul-lail2,Masood-ur-Rehman1,Trust and Trusted Computing in VANET. Computer Science Journal 2011.

[15] J. Douceur,"Thesybil Attack", First international workshop on peer topeer(P2P) system,march 2002,pp: 251-260.

[16] G. Guette, B.Ducourthial," On the sybilattackdetection in VANET",

[17] M. Raya, P. Papadimitratos, J.P. Hubaux," Secure vehicular communications", IEEE Wireless Communication Magazine,specail issue on inter-vehicular communication, Oct 2006.

[18] Al-Raban'nah, Y. and Al-Refai, M. (2016) Toward Secure Vehicular Ad Hoc Networks an Overview and Comparative Study. Journal of Computer and Communications, 4, 12-27.

[19] F. Stumpf, L. Fischer and C.Eckert," Trust, Security and Privacy in VANETsMultilayered Security Architecture for C2C-Communication", Automotive Security, pp. 55-70, Wolfsburg, Germany, VDI-Verlag, 200.

[20] G.Guette,O.Heen, "A TPM-based Architecture for improvedsecuirty and Anonoymity in vehicular ad hoc networks" ,IRIS France.

[21] J.M. d. Fuentes, A.I. González-Tablas, A. Ribagorda, "Overview of security issues in vehicular ad-hoc networks", Maria Manuela Cruz-Cunha, Fernando Moreira (Eds.), Handbook of Research on Mobility and Computing, IGI Global (2010)

[22] G. Guette, C. Bryce, "Using TPMS to securevehicular ad-hoc networks (VANETS)", in: Information Security Theory and Practices. Smart Devices, Convergence and NextGeneration Networks, 2008, pp. 106–116.

[23] IA,Sumra, H.Hasbullah, iftikharahmed, Jamalul-lail," New CardBasedScheme to Ensure Security and Trust in Vehicular Communications", Saudi

International Electronics, Communications and Photonics Conference Riyadh, Saudi Arabia April 23rd - 26th 2011.

[24] K. N. McGill.” Trusted mobile devices: Requirements for a mobile trustedplatform module”, Johns hopkinsapltechnical digest 32(2):544, 2013.

[25] S. Kinney,” Endorsement Key (EK)”,Trusted Platform Module Basics Using TPM in Embedded Systems , chapter No.04, , pp No.32.

[26] T. Chen, O. Mehani and R. Boreli, ”TrustedRouting for VANET” 9th International Conference on Intelligent Transport SystemsTelecommunications (20 October 2009), pp. 647-652.

[27] C. Laurendeau, M. Barbeau,”Theat to security in DSRC/WAVE”, 5th International Conference on Ad Hoc Networks and Wireless (ADHOCNOW). LNCS 4104, pp.226-279, 2006.

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

[29] I. A. Sumra, I. Ahmad, H. Hasbullah and J. l. bin Ab Manan, "Classes of attacks in VANET," 2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC), Riyadh, 2011, pp. 1-5.

[30] I. A. Sumra, H. B. Hasbullah and J. l. A. Manan, "Using TPM to ensure security, trust and privacy (STP) in VANET," 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), Riyadh, 2015, pp. 1-6.

[31] I. A. Sumra, J.-L. A. Manan, and H. Hasbullah, “Timing attack in vehicular network,” in Proc. of the 15th WSEAS International Conference on Computers, Corfu Island, Greece, July 2011, pp. 151–155.

[32] I.A. Sumra, H.B. Hasbullah, J. lb. Ab Manan, ”Denial of Service (DOS) Attack and Its Possible Solutions in VANET”,WASET issue 65, april 2010 ISSN 2070-3724.