International Journal of Future Generation Communication and Networking
Vol. 9, No. 6 (2016), pp. 137-144
http://dx.doi.org/10.14257/ijfgcn.2016.9.6.13

Overview of Trust Management in VANET and Various Cryptography Fundamentals

Pallavi Agarwal[1] and Neha Bhardwaj[2]

[1]*Research Scholar, CSE & IT Dept., Madhav Institute of Technology & Science, Gwalior, India*
[2]*Assistant Professor, CSE & IT Dept., Madhav Institute of Technology & Science, Gwalior, India*
[1]*pallaviagarwal015@gmail.com*, [2]*bhardwaj.neha08@gmail.com*

Abstract

Vehicular Ad Hoc Network (VANET) is a more influential network in which vehicles depend on each other to communicate and for the secure exchange of the messages. With the improvement in the technology, mainly the vehicles are equipped with Wi-Fi and GPS devices to improve the traffic handling and road safety. But many vehicles may broadcast the bogus messages for their own purpose, so it needs a trustful environment and an effective trust management schemes to prevent the network from the various malicious attacks. Trust establishment is very challenging as the network is highly mobile and vehicles may come in or depart at any time. In this paper, we first discuss the VANET model to describe the environment, and then the trust management schemes to secure the network and lastly the various cryptography fundamentals for the fast and safe message transfer.

Keywords: *Vehicular Ad Hoc Network (VANET), VANET model, trust management, cryptography.*

1. Introduction

Vehicular ad hoc networks (VANETs) had been attracted growing attention from both enterprise and academia. In this network, the messages are forward to each other by the vehicle as it plays the roles of a node or a router. The fundamental additives of VANETs are the wireless on-board unit (OBU), the roadside unit (RSU), and authentication server (AS). OBUs are mounted in the vehicle to provide an interface to drivers, RSUs are deployed on intersections or hotspots as an infrastructure to offer data or provide the facility of the internet for cars inside their radio coverage and AS is responsible for security by installing the suitable parameters in the OBU to authenticate the user. The key focus is to enhance the road safety and reduce the loss of life by increasing the driver comfort [1]. It is vital for vehicular ad hoc environments ensure traffic safety, by delivering the correct info to drivers in an exceedingly measurable effective time. This can be not always straightforward thanks to the presence of malicious or greedy nodes [2], wherever false information may be broadcasted misleading nodes within the scene. Thus, establishing trust between nodes is a necessary think about order to work out whether their claimed sent information is reliable [3].

ISSN: 2233-7857 IJFGCN
Copyright ⓒ 2016 SERSC

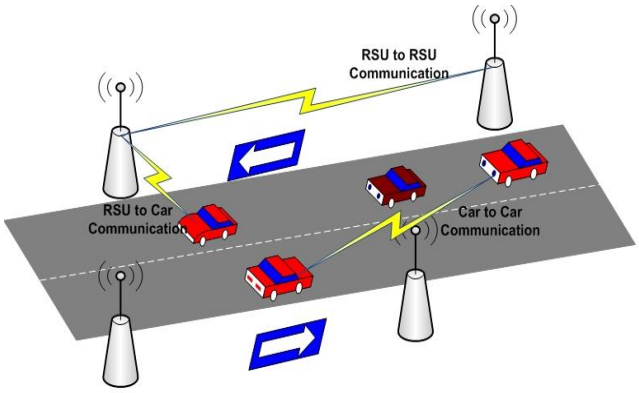

Figure 1. VANET Structure

The paper contribution will be summarized as follows; the trust management scheme of node is introduced in a classified decentralized system, introducing cryptography basics for detecting malicious data. The foundation of network for V2I and V2V communications to provide efficient message delivery. Efficient message authentication is practiced to broadcasting functions by the RSU.

The trust management scheme presented in this paper is predicated on a classified decentralized estimation scheme for drivers and vehicles. Every driver license Id (node) is concatenated to the vehicle Id number, before causing a message, solely discovered once needed by licensed entities.

2. Related Work

Raya and Hubaux [3], proposed a method that preloaded every vehicle with an oversize range of a pair of public and private key and the related public key certificate. Every key pairs are used to preserve the privateness and for this they have a limited lifespan. The traffic messages are always signed with a scheme of public key-based. But this method required excessive storage price, high communication overhead and high computational cost.

Freudiger et al. [7], proposed the method to enhance the location privateness by using the cryptography method MIXzone, and Sampigethava et al. [8], supplied location privacy by way of utilizing the organization navigation of vehicles. But, these processes do now not work nicely with such type of highly dynamic surroundings like VANETs because they use uneven cryptography or a digital signature verification scheme, which outcomes in excessive computation fees, long authentication latency.

Zhang et al. [9], proposed a scheme in which symmetric key hash message authentication code used as a replacement of a public key infrastructure-based message signature to reduce the signature cost and the scheme is known as RSU-aided message authentication scheme (RAISE). However, in RAISE, the important thing settlement system still executes the exponent operation, which ends up in a high computational cost. Moreover, the RSU wishes to maintain the greater identification-Key table, ensuing in greater storage price. As a result, there is still a want for an efficient scheme of authentication for VANETs with low computation and low storage cost.

Jorge h. et al. [10], proposed a watch dog algorithmic rule with an intermission identification system for building the trust administration. In this source node sends messages to the neighbor's node and shows that node with ids. It forwards those messages and keeps its trust price in trust table typically that decreasing trust estimation of that node. The disadvantage of this strategy is to form crash within the system, and show that node till that forward or drop. It contained the large record of checking the history of the

 Copyright ⓒ 2016 SERSC

neighbor's node within the event that it's enlarged the amount of neighbor nodes.

Chaung et al. [6], the primary mistrustful node becomes trustful and authenticated, it obtains the spare approved parameter, and therefore it will authorize alternative mistrustful nodes. The matter is, if the associate opposes node was authenticated as trustful, it should misuse this trust gained to authorize and authenticate alternative misbehaving nodes. A user is allowed over one identity within the network.

Ming et al. [6], in this paper proposed a scheme known as TEAM which is decentralized lightweight authentication scheme to protect valid users in VANETs from malicious attacks. It used an XOR operation and a hash function which has a substantially less amount of cryptographic calculation. Moreover, TEAM is predicated on the idea of transitive trust relationships to boost the performance of the authentication procedure. Additionally, TEAM features a few storage areas to store the authentication parameters.

3. VANET Model Overview

There are various entities available for the VANET deployment. Some necessary operations are used in VANET which are performed by the vehicles and other entities. There are several ways to communicate with each other. Two types of environment are provided in the network such as infrastructure and ad hoc environment [4].

3.1. Infrastructure environments

The entities are permanently connected and are responsible for the traffic or external services. It consists of M**anufacturer** which is used to uniquely identify the vehicles, **Trusted Third Parties** (TTP) offer many services like credential management or time stamping, **Legal authority** which is for registration of vehicles and reporting of offenses as different rules or regulations of each country and **Service providers** offer services like Digital Video Broadcasting (DVB) or Location-Based Services (LBS).

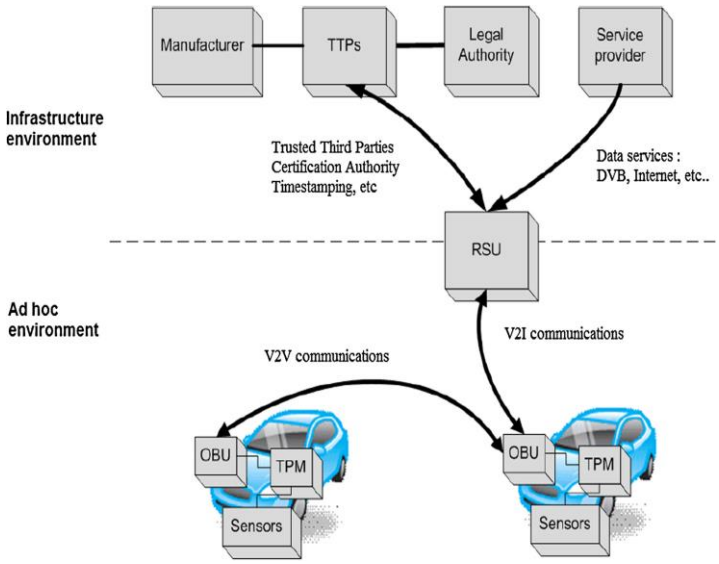

Figure 2. VANET Model

3.2. Ad-hoc Environment

In this environment, vehicles are communicating. There are three devices such as **OBU, which** enables communication among V2V, V2I and I2I, **Sensors** which is used to sense the environment and improve the road safety and **TPM** (Trusted Platform Module)

which is used for computation and storage provide the security.

4. Trust

Trust is a very challenging task to achieve in VANET as the network is decentralized and there is no central authorized structure to manage all the nodes [5]. The nodes can come in or depart the network anytime. There should be a trust table in every vehicle which stores all the trust values of neighboring vehicles.

4.1. Trust Management for VANET

Trust management should be effective to maintain the trust in VANET. There have desired properties to manage the trust that should incorporate in the network.

4.1.1. Decentralized Trust Establishment: VANET is fully decentralized and there is no central authority to manage the highly dynamic network. There is a direct communication between the vehicles to update the value of trustworthiness of the other vehicles. This kind of matched interaction in a distributed will simply enforced manner. Some trust models also allow a peer a to model the name of another peer b by seeking several different peers' opinions concerning b and mixing these opinions along.

In any case, peer a might not recognize that other peers have had direct intercommunication with b as a result of there is no a central authority to gather such information. The models in [14] distributed peer-to-peer environments so conjointly allow peer a to follow a suggestion from different peers known as referrals about that peers could have information concerning peer b. Once the peers have the specified information are identified, reputation of peer b are often inbuilt a distributed manner.

4.1.2. Coping with Sparsity: The effectiveness of the trust establishment of direct communications must not be
dependent upon a minimum threshold. In VANET, there are fewer expectations that a peer would possibly contact more than once with the same peer. However, the trust models should be effectively able to access every data should be taken into consideration by the direct communication even although it may happen simply once. Thus, in a very situation wherever the quantity of peers that are able to unfold information has gone all the way down to the extent that the condition of data inadequacy or a complete lack of data is prevalent, any information may be termed precious. Within the trust calculation, the load for the information will be raised during this situation, whereas it's going to have a lower default value to take care of the information sparseness problem in VANET.

4.1.3. Event/Task and Location/Time Specific: VANET environment is ever-changing constantly, so an honest trust model ought to introduce certain dynamic metrics of trust, capturing this dynamism by allowing a peer to manage trust management looking at the situation. Here, we tend to discuss two notably necessary dynamic factors within the perspective of VANETs, such as event/task and location/time.

Peers normally will report completely different events, e.g., automobile crashes, collision warnings and atmospheric condition, etc. Trust management should thus be event/task specific. As an instance, some of these tasks could also be time sensitive and need fast reaction from the peer that receives them. During this case, this peer can solely consult a really restricted range of different peers to verify whether or not the reportable information is true. In another case, coverage peers having completely different roles in VANET could have a lot of or less data in several varieties of tasks. Additionally, a peer ought to update the coverage peer's trust by taking into consideration the kind of the reportable event. As an instance, life-critical events will definitely have a lot of impact on

 Copyright ⓒ 2016 SERSC

the coverage peer's trust.

We conjointly note that location and time are another 2 particularly vital dynamic metrics. To Illustrate, the data of the reported event have given the priority if it is nearer to the origin of a particular message, wishing on the underlying assumption that a peer nearer to the event is probably going to report a lot of realistic knowledge regarding [11] the event. For better weight in trust calculation, the message of a certain event is received nearer to the time once the reportable event has taken place. Another proposal are also there from trust technique time based trust, since the connection of information in VANET is extremely passionate about once it had been received, it would make sense to assign a decay issue with the message. The message with more delay from the time of evaluating trust would be allotted a lower weight.

4.1.4. Scalable: It is a very essential characteristic in trust management in VANET environments. In a very dense environment, the amount of peers who reporting the data or passing through the network is doubtless very huge. On the other hand, a peer has a power to decide in serious circumstances. For this condition, every peer has to consult or accept data from a solely variety of different trustworthy peers. This range can be varied or updated with the changes in VANET. However, this value is not large enough for the scalability in the network.

Trust establishment should be scalable in VANETs. For example, every peer has to store the data of all past connections to maintain experience based trust and to calculate the trust with different peers. To maintain the scalability, trust models have to update the trust value of peers by considering the past connections in a very algorithmic manner. The peer trust increase with the increasing number of interactions and only the recent trust values are to be hold on and used in the computation. This strategy will build scalable trust management.

4.1.5. Integrated Confidence Measure: Complete details of other peers should be available to establish the trusted model. It is so necessary to incorporate a confidence measure in trust management for capturing the ambiguity. Confidence is used as correctness of trust value and frequently lies within the interval [0,1]. The worth of confidence would rely on the amount of different metrics that were obtainable within the calculation of the associated trust worth.

In general, a higher worth of confidence i.e. a price nearer to one would result from considering a lot of evidence or metrics having high dependableness. Confidence is viewed as a parameter that adds spatiality to the output which is generated by the model permitting the peer applications to have a richer notion of trust and eventually decide a way to react on the according event. Many researchers have planned trust and reputation models with the concept of confidence.

4.1.6. System Level Security: Security techniques have to work with protocols at the system level to permit the authentication of the peers i.e. verify their identity. This can be necessary as a result of most of the trust building models assume that a peer may be uniquely known to the present finish, sure security needs identified to be essential for trust are known which can be enforced through the public-private key infrastructure (PKI) that creates use of public key secret writing and certificates. A trustworthy certification [15] authority (CA) problems a public key certificate validating that an exact public secret is owned by a selected peer, which may simply be a document containing the information about the name of peer or driver license with its public key. The common public key then may be wants to code and sign a message that enables solely the owner to look at the contents and validate its integrity. A lot of specifics, that CA signed the entire document (with the certificate authority's non-public key) to become the peer's public key certificate. Everybody will verify the authority's signature by exploitation the authority's

Copyright ⓒ 2016 SERSC

public key. Now, once peer a sends a message to see b, a requirement sign the message together with his non-public key b then will verify (using a's public key) that the message was really directed by a.

4.1.7. Sensitive to Privacy Concerns: Privacy is a crucial concern during a VANET atmosphere. In this atmosphere, the disclosing of an identity vehicle owner's (e.g. The house address of the owner) might permit a probably malicious party to cause injury to the owner. Trust management allows peers to certify one another that make use of a public key infrastructure (PKI). Once a peer sends a report to another peer, the sender has to certify itself to the receiver. Though these keys don't contain any sensitive identities of the sender, the receiver is also able to track them by work the messages containing the key of the sender. For example, the receiver will track the probably senders' home address by looking for the route of the sender if the receiver has sufficient info regarding completely different locations that the sender has been to, and so alternative identities. This issue may be addressed by ever-changing keys. Each peer in VANET can store an outsized set of pre-generated keys and certificates. The keys will be changed to protect the sensitive and some private details about the senders' location while the data is sending to the other peer, so others don't acknowledge this sender together of the previous senders that they need to interact with. During this means, others won't be able to find out the sender's privacy sensitive identities, whereas they're going to still be able to keep track of expertise with this sender concerning some insensitive senders' locations.

4.1.8. Robustness: Trust management will effectively share information to develop peer connection in VANETs and observe malicious peers to protect the network from various attacks. But sometime the trust management compromised and might become the target of attacks.

5. Cryptographic Fundamentals

Cryptographic fundamentals provide all the security services of the cryptography. Cryptography is used to encrypt the messages to protect it from various attacks. Some methods are used to convert the messages from plaintext to ciphertext like encryption and decryption which makes them unable to be read by an attacker. There are many techniques provided by the modern cryptography such as confidentiality, integrity, authentication, non-repudiation etc. There are various techniques which are used in cryptography to verify the data. Some are used during the transmission of the data in the network while others are used at the user end side.

1. Confidentiality: It is used to encrypt the message so that it cannot be read by an unauthorized person. In a VANET, the information changed is usually public, except those connected to the privacy of users.

2. Integrity: The message should not modify during the transmission. It means the receiver is in a position to confirm that the received message is that the message that has been issued and it has not been changed in transit. A method hash functions type the basis solutions set of integrity issues.

3. Authentication: It is to ensure that the sender and receiver are the one who claims to be. The Digital signature is used for the authentication purpose. A VANET user must not be ready to pass for somebody else.

4. Non-repudiation: It is to ensure that a vehicle should not deny to send the messages. During a VANET context, a vehicle must not be ready to deny sending a warning e.g. or

 Copyright ⓒ 2016 SERSC

having made an attack.

5.1. Encryption/Decryption

The principle of encryption and decryption of a message means the algorithm is used to protect the data by applying a set of mathematical functions. It receives the message as a plaintext and then applies an encryption key then produce the output as a ciphertext and vice versa. Data encryption required the keys which is generated by the certificate authority and every vehicles have their own key which is used during the encryption and decryption process. There are two methods applied in cryptography, which used a different process to convert the data.

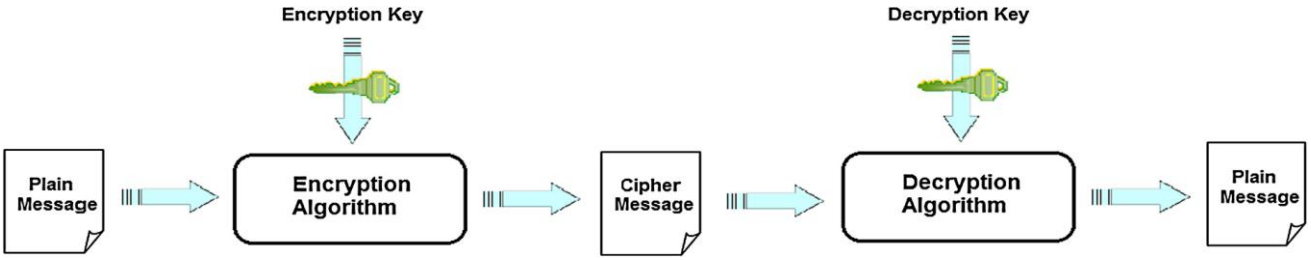

Figure 3. The principle of Encryption/ Decryption

5.1.1. Symmetric Cryptography: This type of cryptography is also known as secret key cryptography. In this technique, there is a single key for the encryption or decryption. So the key should be kept protected as if it compromised then the security is affected. The requirement that each party have access to the key secret's one of the most drawbacks of symmetric cryptography as compared to uneven one.

5.1.2. Asymmetric Cryptography: This type of cryptography is also known as public key cryptography. There is a key pair for each user; one private key that should be kept secret and other is public which should be available publicly. It is comparatively slower but more secure than symmetric cryptography [12].

Asymmetric cryptography also can be utilized in coding, but it's primarily used in the key exchange procedures and in the digital signature authentication tool through digital certificates. The general public key cryptography solves many issues that secret key cryptography does not succeed.

5. Conclusion

Vehicular Ad hoc NETworks (VANETs) designed to provide comforts of the passengers and improve the road safety. As the transportation system are have become the intelligent transportation system which generate the warning messages to the driver to reduce the accidents. The data plays a very important role in VANET so the trustworthiness of data must be protected from the attackers. We presented some trust management methods which is useful in creating a trustful network. There are many cryptographic solutions are available to prevent the vehicles from getting the data and increase the efficiency of the network. Many attacks are performed in VANET and it should be reduced by applying different techniques according to the needs of driver.

Copyright ⓒ 2016 SERSC

References

[1] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," IEEE Security Privacy Mag., vol. 2, no. 3, **(2004)** May–June**,** pp. 49–55.
[2] Ghassan Samara, Wafaa A.H. Al-Salihy and R. Sures, "Security Analysis of Vehicular Ad Hoc Networks (VANET)," Second International Conference on Network Applications, Protocols and Services, **(2010)**.
[3] J. Zhao, Y. Zhang and G. Cao, "Data pouring and buffering on the road: A new data dissemination paradigm for vehicular ad hoc networks," IEEE Trans. Vehicular Technol., vol. 56, no. 6, **(2007)** November, pp. 3266–3277.
[4] M. d. Fuentes, A.I. González-Tablas and A. Ribagorda, "Overview of security issues in vehicular ad-hoc networks," in: Maria Manuela Cruz-Cunha, Fernando Moreira (Eds.), Handbook of Research on Mobility and Computing, IGI Global, **(2010)**.
[5] S. Eichler, C. Schroth, and J. Eberspacher, "Car-to-car communication."
[6] Ming-Chin Chuang and Jeng-Farn Le "TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks," 1932-8184/$31.00 c IEEE, **(2013)**.
[7] J. Freudiger, M. Raya and M. Feleghhazi, "Mix zones for location privacy in vehicular networks," in Proc. First Int. Workshop Wireless Network Intelligent Transportation System, **(2007**) August, pp. 1–7.
[8] K. Sampigethaya, M. Li, L. Huang and R. Poovendran, "AMOEBA: Robust location privacy scheme for VANET," IEEE J. Selected Areas Communication, vol. 25, no. 8, **(2007)** October, pp. 1569–1589.
[9] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in Proc. IEEE International Conference Communication, **(2008)** May, pp. 1451–1457.
[10] Hortelano, Jorge, Juan Carlos Ruiz, and Pietro Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in VANETs", International Conference on Communications Workshops (ICC), IEEE, **(2010)**, pp- 1-5.
[11] Brouce Schneier, "Applied Cryptography. Protocols, Algorithms, and Source Code in C, " John Wiley & Sons, Inc, **(1996)**.
[12] Mohamed Nidhal Mejri, Jalel Ben-Othman and Mohamed Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," Vehicular Communications 1, **(2014)**, pp. 53–66.
[13] B. Yu and M. P. Singh, "A social mechanism of reputation management in electronic communities," in Proceedings of the 4th International Workshop on Cooperative Information Agents, **(2000)**, pp. 154–165.
[14] M. Raya, P. Papadimitratos, V. Gligor and J. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," Technical Report, LCA-REPORT-2007-003, **(2007)**.

 Copyright ⓒ 2016 SERSC