Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 6, June -2017

Privacy Preserving of Messages in Vehicular Ad Hoc Network

Gaikwad Priti G.[1], Mrs. Nilam Patil[2]

[1]ME Student, Department of Computer Engineering, DYPCOE, Akurdi, SPPU, Pune, India[1]
[2]Assistant Professor, Department of Computer Engineering, DYPCOE, Akurdi, SPPU, Pune, India[2]

Abstract — *In recent years, the growing needs for increased safety and efficiency of road transportation system have promoted automobile manufacturers to integrate wireless communications and networking into vehicles. The VANETs trustworthiness could be improved by both data trust and node trust. Here data means the sent and received messages by the vehicles and nodes means the vehicles present in that particular VANET area. VANETs uses trust management scheme which is able to detect and cope with malicious attacks and also evaluate the trustworthiness of both data and mobile nodes in VANETs. VANET applications uses the trust management scheme to improve traffic safety, mobility, and environmental protection with enhanced trustworthiness. AES algorithm is used in the proposed system for encrypting the sent messages from sender vehicle to server or vice versa. The SHA3 algorithm is also used for detecting whether sent message by the sender vehicle which is stored on the database and the same message received by the receiver vehicles is in the original format or in the different format which can modified by the attacker. From this the RSU can detect whether the malicious attack is found or not. These algorithms are also used for securing the privacy of the users.*

Keywords- *AES, SHA3, Privacy, trust management, VANET*

I. INTRODUCTION

With the Internet becoming an increasingly significant part of our lives, the dream of a Wi-Fi enabled city is becoming closer and closer to reality. The Vehicular Ad-Hoc Network, or VANET, is a technology that uses moves cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 metres of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes [3].

Vehicular ad hoc networks (VANETs) are created by applying the principles of mobile ad Hoc networks (MANETs) the spontaneous creation of a wireless network for data exchange to the domain of vehicles. It was shown that vehicle-to-vehicle and vehicle-to-roadside communications architectures will co-exist in VANETs to provide road safety, navigation, and other roadside services. VANETs are a key part of the intelligent transportation systems (ITS) framework. Sometimes, VANETs are referred as Intelligent Transportation Networks [4].

VANETs support a wide range of applications from simple one hop information dissemination of, e.g., cooperative awareness messages (CAMs) to multi-hop dissemination of messages over vast distances. Most of the concerns of interest to mobile ad hoc networks (MANETs) are of interest in VANETs, but the details differ. Rather than moving at random, vehicles tend to move in an organized fashion. The interactions with roadside equipment can likewise be characterized fairly accurately. And finally, most vehicles are restricted in their range of motion, for example by being constrained to follow a paved highway [4][5].

The Traffic Estimation and Prediction System (TrEPS) [1] is an application of VANETs, which generally provides the predictive information needed for proactive traffic control and traveller information. For example, It provides input to traffic managers who decide where and when to send the specific messages on variable message signs, such as “Avoid congestion exit here for alternate route”. However, sometimes the TrEPS may encounter confusing or even conflicting traffic information reported by multiple sources.

II. RELATED WORK

A literature review has showed there are many studies mad use of latest Technology using misbehaviour detection, privacy preserving as well as trust management for ad hoc networks.

A. Misbehaviour Detection for Ad hoc Networks

Mahdi Kefayati et al. [2] described Adaptive Path Selection and Loading (APSL) as a multi-path data transmission scheme for mitigating the effects of misbehaving nodes in mobile ad hoc networks. In APSL, misbehaviour resilience is achieved by adaptively loading Reed-Solomon (RS) coded data into multiple node-disjoint paths.

Wenjia Li et al. [3] described a multidimensional framework to evaluate the trustworthiness of MANET node from multiple perspectives such as collaboration trust, behavioural trust, and reference trust. Different types of observations are used to independently derive values for these three trust dimensions.

Sonja Bucheggery et al. [4] described the use of a self-policing mechanism based on reputation to enable mobile ad-hoc networks to keep functioning despite the presence of misbehaving nodes. The reputation system in all nodes makes them detect misbehaviour locally by observation and use of second-hand information. Once a misbehaving node is detected it is automatically isolated from the network.

B. Privacy Preserving for Ad hoc Networks

Genaro Rebolledo-Mendez et al. [7] described an architecture that is able to detect emotions, which can be communicated via the on board unit of a vehicle with city emergency services, VANETs, and roadside units, aimed at improving the drivers experience and at guaranteeing better security measures for the car driver.

Zhengming Li et al. [8] described a VANET based Ambient Ad-Dissemination scheme (VAAD) used to support secure ad disseminations with less cost and effect control. VAAD provides an incentive centred architecture for the involved parties to trade off their conflicting requirements regarding ad dissemination.

Rongxing Lu et al. [10] described a DIKE scheme, which gives a privacy preserving authentication technique that not only provides the vehicle users anonymous authentication but enables double registration detection as well.

Pino Caballero-Gil et. al. [16] proposed authentication based on identity as a way to increase the efficiency and security of communications in vehicular ad-hoc networks. When using identity-based cryptography to achieve certificate less authentication, membership revocation is not a trivial problem. Thus, in order to improve the performance of revocation in such networks, the use of a dynamic authenticated data structure based on perfect k-ary hash trees combined with a duplex version of the new standard SHA-3 is used.

C. Trust Management for Ad hoc Networks

Ing-Ray Chen et al. [17] described a trust-based routing protocol that is able to deal with selfish behaviors and is flexible against trust related attacks and also protocol can be effectively trade off message overhead and message delay for a significant gain in delivery ratio.

R. G. Engoulou et al. [18] describes a survey of the security issues and the challenges generated in VANETs. The various categories of applications in VANETs are introduced, as well as some security requirements, threats and certain architectures that are used to solve the security problem.

Anand Patwardhan et al. [19] described an epidemic data exchange protocol that incorporates reputation and agreement to ensure high reliability of data and stimulate proactive collaboration above and beyond stipulation, to enhance availability and reliability of data.

Zhen Huang et. al. [20] proposed a novel voting scheme to overcome the problem of simple voting for decision making leads to oversampling and gives incorrect results in VANETs. In this scheme, each vehicle has different voting weight according to its distance from the event. The vehicle which is closer to the event possesses higher weight.

III. PROPOSED SYSTEM

Figure 1 shows the proposed system architecture. The Privacy Preserving Trust Management (PPTM) scheme addresses two types of trustworthiness in VANETs such as data trust and node trust. In this first the vehicle user has to install the android application in the mobile device. This app is used for authentication of user which is the main requirement of the system. It is important to authenticate all users through the signing up in the application so that they will be able to communicate with other users present in the VANET by transmitting the messages in the network.

The authorization levels of vehicles is controlled by authentication. It prevents attacks by assigning a specific identity to each vehicle in VANET. For authentication user has to register to the application after that they will get the authorization to send or receive message.

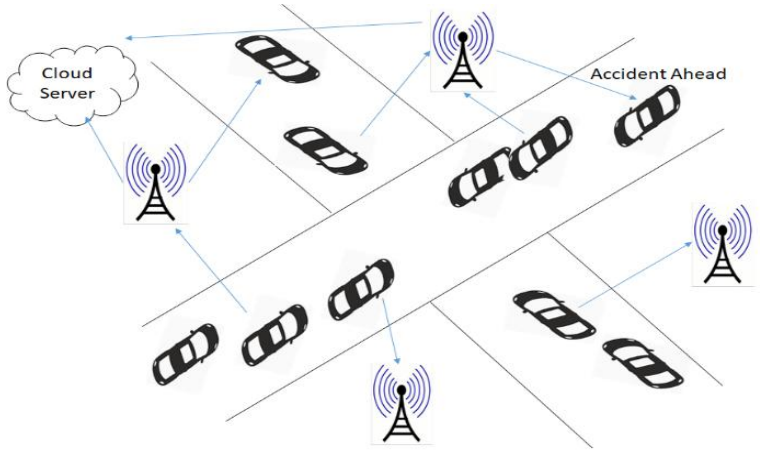

Fig.1. System Architecture in VANETs

The registered user can send the message to the RSU because two vehicles can't communicate with each other directly due to the high mobility. While sending the message from sender vehicle to RSU it is encrypted for security reasons so that original message is stored in the server's database.

The AES algorithm used for encryption of messages which is having the static key so that the users who are having that key are able to decrypt the message. This is used for preserving the privacy of the user who have sent the message and also prevent from getting the false message to avoid the traffic congestion in the network.

At the Cloud Server side it receives all the messages from the RSU which are left and long. The server calculate the distance between the server and sender vehicles for better communication and then server send message to the RSU and then RSU send the same message to the nearest receiver vehicles which are present in that VANET. The cloud server then generate SHA for each message then it shares or stores the SHA and the encryption of each message in the database system.

The receiver vehicles gets the message notification. The message is read by the user and then it send the verification of received message to the RSU. The RSU sends the message verification request to server. The server send the response message to RSU for checking the data or message integrity. Then RSU is storing the status of each messages whether it is malicious or not.

Again at the server side the generated SHA of current received message and the previously stored message is compared for the trustworthiness of nodes as well as data. If the compared SHA is equal then the received message by receiver vehicles and the stored message in database which was send by the sender vehicle is the original message which shows the data integrity, again server sends the successful verification to the RSU. If the compared SHA is not equal then it is shows that attacker is found which shows the node trustworthiness.

IV. ALGORITHM

A. Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) algorithm is used for encrypting the message to preserve the privacy as well as data and node trustworthiness.

Pseudo code:

```
Input: in[4 * Nb], word w[Nb * (Nr+1)])
Output: out[4 * Nb]
begin
        byte state[4,Nb]
        state = in
        AddRoundKey(state, w[0, Nb-1])
        for round = 1 step 1 to Nr1
                SubBytes(state)
                ShiftRows(state)
                MixColumns(state)
        AddRoundKey(state, w[round * Nb, (round+1) * Nb-1])
        end for
                SubBytes(state)
                ShiftRows(state)
                AddRoundKey(state, w[Nr * Nb, (Nr+1) * Nb-1])
                out = state
end
```

B. SHA-3 Cryptographic Hash Algorithms

A cryptographic hash sometimes called 'digest' is a kind of 'signature' for a text or a data file. The SHA-3 family of hash routines generate almost-unique 224-bit, 256-bit, 384-bit, or 512-bit (28-/32-/48-/64-byte) signatures for a text. The algorithm used for generating the hash code is SHA-3 Cryptographic Hash Algorithms.

Pseudo code:

```
String getSHA(String base) {
try {
          MessageDigest digest = MessageDigest.get Instance("SHA-256");
        byte[] hash = digest.digest(base.getBytes(" UTF-8"));
       StringBuffer hexString = new StringBuffer();
        String out = "";
          for (int i = 0; i < hash.length; i++) {
         String hex = Integer.toHexString(0xff & hash[i]);
          if (hex.length() == 1) {
                  hexString.append('0');
            }
```



```
                hexString.append(hex);
            }
            out = hexString.toString();
            System.out.println("SHA-3--->" + out);
            return (out);
            // return hexString.toString();
              } catch (Exception ex) {
              throw new RuntimeException(ex);
              }
    }
```

V. RESULTS

Precision (P) and Recall (R) these two parameters are used to evaluate the accuracy which are both widely used in machine learning and information retrieval to assess the accuracy. In this both P and R values are used to evaluate how accurate the proposed scheme is when it is used to identify untrustworthy nodes in VANETs. These two parameters are defined as follows.

$$P = \frac{Num\ of\ Truly\ Malicious\ Nodes\ Caught}{Total\ Num\ of\ untrustworthy\ nodes\ caught}$$

$$R = \frac{Num\ of\ Truly\ Malicious\ Nodes\ Caught}{Total\ Num\ of\ Truly\ Malicious\ Nodes}$$

The proposed system uses the AES and SHA3 algorithms to reduce the number of malicious nodes present in the VANET which modifies the original message. These algorithms are also used for encryption purpose that can send the message securely in the network. The expected result for the proposed scheme is as shown in the figures.
Fig. 2 and 3 shows the precision and recall values for the PPTM and ART scheme with different percentages of malicious nodes. Both the precision and recall values decrease when there are a higher percentage of malicious nodes. When compared with the ART scheme, the proposed PPTM scheme is better resistant to various attack patterns as well as to the high percentage of malicious nodes in the network.

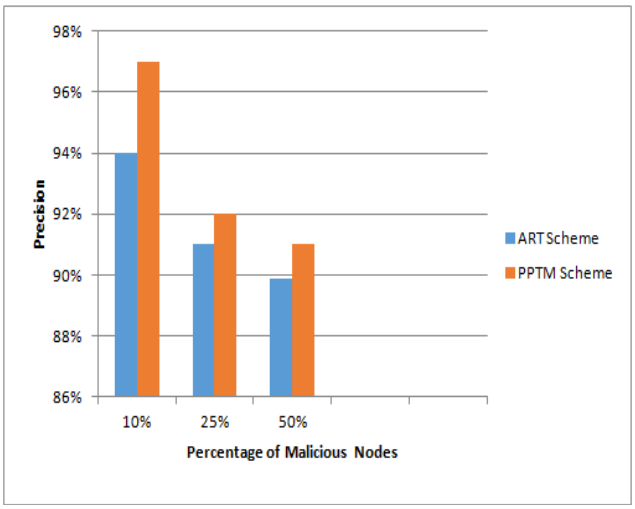

Fig. 2 Effect of adversary percentage on Precision

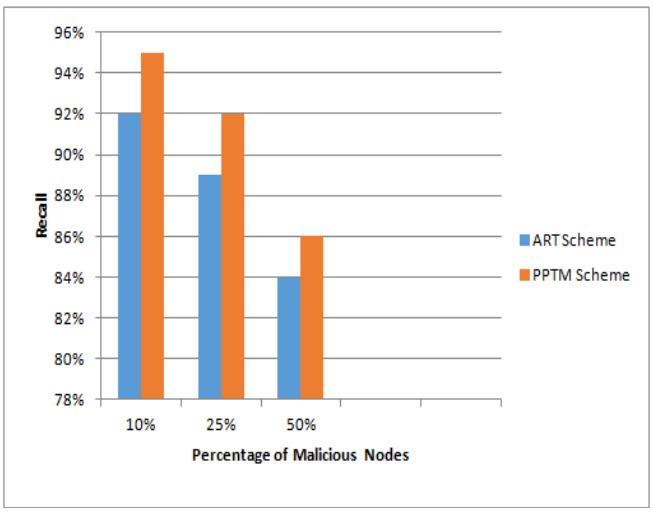

Fig. 3. Effect of adversary percentage on Recall

VI. CONCLUSION AND FUTURE WORK

The Privacy Preserving Trust Management (PPTM) scheme is proposed to evaluate the trustworthiness and privacy of both data and vehicle nodes for VANETs. In the proposed system, data trust and node trust are modelled and evaluated for the trustworthiness of data and nodes. In particular, data trust is used to assess whether or not and to what extent the reported data are trustworthy and node trust indicates how trustworthy the nodes in VANETs are. AES algorithm is used in the proposed system for encrypting the sent messages from sender vehicle to server. The SHA3 algorithm is also used for detecting whether sent message by the sender vehicle which is stored on the database and received messages by the receiver vehicles is the original message or the different message which is modified by the attacker or the malicious attack is found.

The future scope of this proposed system is that the real time cloud and hadoop technology can be used instead of private or public cloud. We can also use the more advance security techniques for node and data trustworthiness.

REFERENCES

1. W. Li and H. Song, "Art: An attack-resistant trust management scheme for securing vehicular ad hoc networks," IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 4, pp. 960-969, 2016.
2. R. G. Engoulou, M. Bellaiche, S. Pierre, and A. Quintero, "Vanet security surveys," Computer Communications, vol. 44, pp. 1-13, 2014.
3. E. Technologies, "Vanet: The vehicular ad hoc network | emerging technologies," 2017. [Online; accessed 15-June-2017].
4. Wikipedia, "Vehicular ad hoc network | wikipedia, the free encyclopaedia," 2017. [Online; accessed 15-June-2017].
5. S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," Journal of network and computer applications, vol. 37, pp. 380-392, 2014.
6. S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (vanets): status, results, and challenges," Telecommunication Systems, vol. 50, no. 4, pp. 217-241, 2012.
7. R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 13, no. 1, pp. 127-139, 2012.
8. R. Chen, F. Bao, M. Chang, and J.-H. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 5, pp. 1200-1210, 2014.
9. G. Rebolledo-Mendez, A. Reyes, S. Paszkowicz, M. C. Domingo, and L. Skrypchuk, "Developing a body sensor network to detect emotions during driving," IEEE transactions on intelligent transportation systems, vol. 15, no. 4, pp. 1850-1854, 2014.
10. Z. Li, C. Liu, and C. Chigan, "On secure vanet-based ad dissemination with pragmatic cost and effect control," IEEE Transactions on Intelligent Transportation Systems, vol. 14, no. 1, pp. 124-135, 2013.
11. S. Taha and X. Shen, "A physical-layer location privacy-preserving scheme for mobile public hotspots in nemo-based vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 14, no. 4, pp. 1665-1680, 2013.
12. W. Li, A. Joshi, and T. Finin, "Coping with node misbehaviors in ad hoc networks: A multi-dimensional trust management approach," in 2010 Eleventh International Conference on Mobile Data Management, pp. 85-94, IEEE, 2010.
13. A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A data intensive reputation management scheme for vehicular ad hoc networks," in 2006 Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, pp. 1-8, IEEE, 2006.
14. M. Kefayati, H. R. Rabiee, S. G. Miremadi, and A. Khonsari, "Misbehaviour resilient multi-path data transmission in mobile ad-hoc networks," in Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks, pp. 91-100, ACM, 2006.
15. S. Buchegger and J.-Y. Le Boudec, "Self-policing mobile ad hoc networks by reputation systems," IEEE communications Magazine, vol. 43, no. 7, pp. 101-107, 2005.
16. H. Deng, Q.-A. Zeng, and D. P. Agrawal, "Svm-based intrusion detection system for wireless ad hoc networks," in Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th, vol. 3, pp. 2147-2151 Vol.3, Oct 2003.
17. S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the confidant protocol," in Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, pp. 226-236, ACM, 2002.
18. T. W. Chim, S.-M. Yiu, L. C. Hui, and V. O. Li, "Opq: Ot-based private querying in vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 12, no. 4, pp. 1413-1422, 2011.
19. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," Wireless networks, vol. 11, no. 1-2, pp. 21-38, 2005.
20. Y.-a. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," in Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pp. 135-147, ACM, 2003.
21. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 255-265, ACM, 2000.
22. *P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Advanced communications and multimedia security, pp. 107-121, Springer, 2002.*

