AN EFFICIENT VEHICLE AUTHENTICATION USING BLOCK AUTHENTICATION CODE FOR VANET

Dr. M. LALLI[1], RASIKA. R[2]

***

Abstract - *In city areas, use of vehicles are increased exponentially day-by-day. Therefore, it's very robust to discipline and maintain city traffic caused by tons of vehicles. Therefore, the traffic potency and safety of the vehicles are often improved with the assistance of VANET. To cope with this scenario, several conditional privacy preserving authentication (CPPA) protocols and password-based conditional privacy preserving authentication and group-key generation (PW-CPPA-GKA) protocol for VANETs have been proposed. Hence, all the protocols proposed until now suffer from high security weakness. Additionally, a number of these CPPA protocols use elliptic curve or bilinear-pairing which has high computation price in contrast to the cryptographic hash functions. The Proposed work presents a block authentication code (BAC) algorithm for VANETs. The protocol affords group-key which is generated, user effort, user join, and countersign modification facilities. We tend to assess the proposed work in terms of routing cost, packet delivery ratio (PDR), packet delivery time, and usefulness of mobile nodes supported by network level simulations. Simulation outcome shows that the planned formula completely exploits the remaining time till packet purpose to point out into networking satisfaction of reducing the routing price and boost packet delivery performance.*

***Key Words*: BAC, VANET, CPPA, GKA**

1. INTRODUCTION

Wireless Ad-Hoc Network (WANET) could be a distributed form of remote system. They are self-arranging and won't have a pre-existing foundation, not like the switches in wired networks or passages in managed remote networks. It is referred as ad-hoc for the rationale that it is not structured. The nodes during this network progress information to different nodes by participating in routing, and also the progressed information are settled smartly on the support of system connectedness and the routing rule in use.

Thus, during this span, wireless communication plays a very important part, which provides a religion of a Wi-Fi surrounding. The trust in the Wi-Fi environment dragged to the emergence of Vehicular Ad hoc Network (VANET). VANETs are said as a structure of Mobile Ad hoc Network (MANET). So VANET is treated as a section of MANET, that is employed to share data between vehicles and alternative road aspect environments. VANETs are basically developed for providing safety along the roadside environments and to prevent vehicles from getting into accidents. VANET reports information for vehicles regarding traffic issues, weather conditions, traffic collision, and other roadside information. VANETs also helps the users to communicate among vehicles and also with the roadside units. VANET instill adequate potential in vehicles to transmit alerts about environmental risks, traffic and road conditions and territorial data to different vehicles.

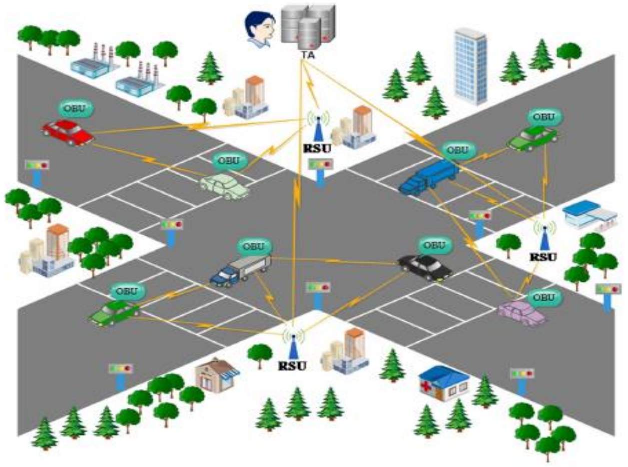

Fig -1: Communication model in VANET

The major expect of VANETs is to supreme the client's decision out and fabricate their drive intact and intimate. Vehicles move at such a rapid, that it is more earnestly to keep up a consistent handoff and an enduring network to the Internet. In VANET the vehicles communicate with one another and also with the road side unit, these communication are characterized into two types[12].

Vehicle to Vehicle Communications (V2V): Vehicles belonging to the same RSU share the private information regarding their status such as their current location, speed, direction.

Vehicle to Infrastructure Communication (V2I): Vehicles communicate with the Road Side Unit(RSU) in order to share information about the traffic congestion. Landmarks, traffic collisions etc.

2. RELATED WORK

Many research works have been carried out to preserve the authentication and privacy of VANET. Many papers have also been published by researchers regarding VANET security.

D.He.S et al [1], have proposed a Identity-based conditional privacy-preserving authentication scheme. This was proposed to improve the security and privacy preserving problems of VANET without using bilinear pairing. The proposed scheme rapidly reduced the computational and communication cost providing better performance.

M.Bayat et al [2], have analyzed and proposed an improved authentication scheme for VANETs introduced by Lee et al, where Lee et al 's work proves to be vulnerable to Impersonation attack. So the proposed work has been introduced with an improved scheme and also with a simulation expressing the proposed works efficiency when compared with the existing work.

Y. Liu et al [3], have introduced a proxy-based scheme where the Proxy vehicles are used to verify many messages with an verification function at the same time, where the RSU has the capability to verify the results without being dependent. Thus this paper shows that how fast an RSU can verify signatures per second with the help of proxy vehicles.

C. Zhang et al [4], have submitted a scheme for verifying the signatures using the identity-based batch verification process. This paper deals with explaining how the vehicles verify signatures in batch instead of verifying them in an one-by-one manner, thus increasing the verification speed. The authors have also suggested a technique called group testing to find the invalid signatures. The proposed model doesn't require certificates because, this paper is proposed with ID based cryptography to generate private keys for pseudo identities, thus reducing transmission overhead.

S.H. Islam et al [5], have proposed a pairing free identity based authenticated group key agreement protocol using elliptic curve cryptosystem for imbalanced mobile networks which enhances the security as well as improves the computational efficiency whereas, the earlier protocols used bilinear pairing and map-to-point hash function which is found to have a triple time higher computational cost when compared to the ECPM. The proposed protocol has also improved the other problems of the earlier protocols such as limitation of bandwidth and the storage space.

3. PROPOSED SYSTEM

A novel block authentication code (BAC) protocol based on hash function for VANETs is proposed in this work. The proposed protocol furnishes sufficient protection, and privateness which are given the topmost priority in VANET application. The comprehensive comparative analysis of the projected BAC protocol showed that it's sturdy and economical than the PW-CPPA-GKA and other CPPA protocol projected for VANETs. The hash function's domain is of irregular size, while the co-domain's size is unchanged. For instance, consider SHA-512, that converts a random size data to 512 bits data. It is not possible to calculate the input of hash function once the output is given, because hash functions in general aren't feasible to reverse. Added to that, every vehicle in the protocol is attached to an On Board Unit (OBU). There is a memory in OBU to hold private data, a clock for synchronization and a battery. The proposed protocol is divided into following phases:

- Initialization
- RSU and Vehicle registration
- Message generation and verification
- Group-key generation
- Vehicle leaving and joining
- Password change

4. BAC ALGORITHM

The Proposed algorithm eventually decreases the consumption of energy, by sending the packets in block which also prevents packet loss. The hash function with secret key generates the BAC from the sender side. The receiver extracts the BAC after it is generated. The receiver then uses the hash function and key that is used for generating BAC on received packets where content based BAC is produced.

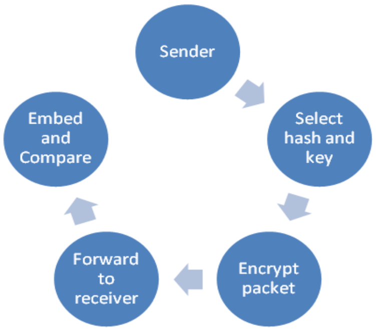

Fig -2: BAC

Psuedo Code

```
Sender
1. Select a packet, choose hash function H(x) and key k
2. With the hash function and key generate BAC
Receiver
3. Calculate Yr;d to extract BAC
3. Check Yr;d is lesser or greater than zero
        Ye;d <> 0
4. If Yr;d >0 Then
      Extracted Bit is 1
   else
```

Extracted Bit is 0

5. Apply Hash (H) and key k on received packets to produce Content based BAC

6. Compare Extracted and Generated BAC

The Proposed algorithm reduces Energy Consumption and Average Delay and hence increases the throughput.

The Throughput has been gradually increased in the proposed work in contrast to the Existing work

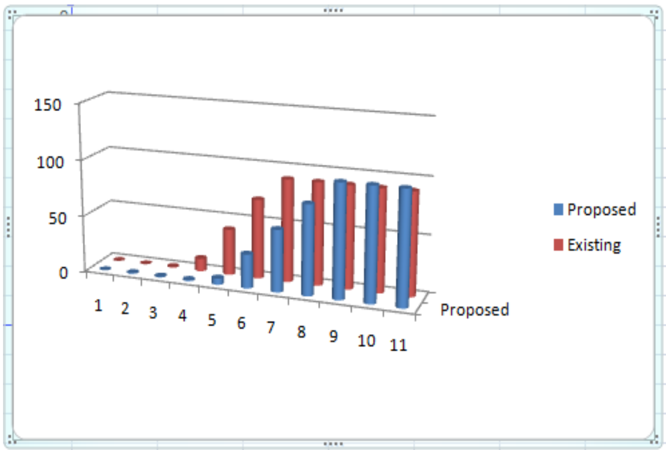

Chart -1: Throughput

The Packet drop is zero in the proposed work, which confirms the safety, security and the efficiency of the Proposed algorithm

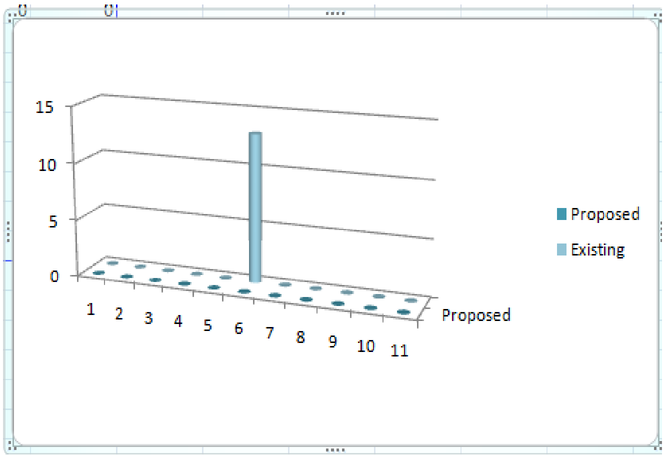

Chart -2: Packet Drop

The average delay is gradually low in the Proposed system than the Existing system. It proves there is no packet loss.

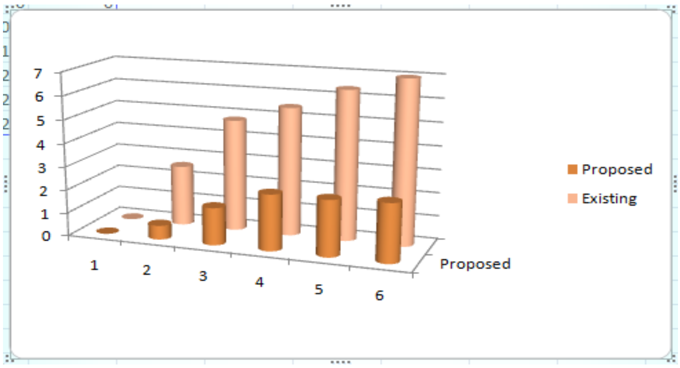

Chart -3: Average Delay

The Proposed work proves to consume less energy when compared to the Existing work which proves that the Proposed algorithm works well.

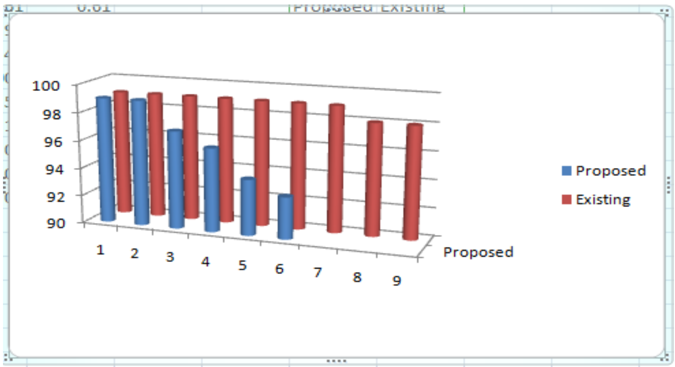

Chart -4: Energy Consumption

6. PERFORMANCE METRICS

Energy Consumption

The nodes consuming energy during node communication and transmission in the given execution time in Joules (J)

Average Delay

The delay or the time taken by the packet to reach from source to destination

Packet Loss

The number of packets lost or missed during transmission due to different time swapping

Packet Delivery Ratio

The ratio of packets that reached the destination to the packets sent from source

Throughput

The total number of successful packets sent during the transmission in kB/s. If throughput increases mean the number of successful packets delivered is high

5. SIMULATION RESULTS

The Simulation results are carried out in Network Simulator 2.35 (NS 2.35). The scenario consists of 7 Nodes. The Proposed algorithm is used to send data securely and without any packet loss

Table -1: Simulation Parameter

PARAMETER	VALUE
Number of Nodes	7
Area Size	500x500
MAC Protocol	802.11
Packet Size	512 Bytes
Protocol	DSDV

The Proposed work produces better results when compared to the existing works. The BAC and Group key agreement protocol provides increased throughput and decreased energy efficiency and packet drop. Thus, the proposed system proves to be high secured in contrast to the other protocols and also low in terms of computational and communication cost.

3. CONCLUSIONS

In this work a block authentication code for VANETs is introduced. Comparing our protocol with the existing CPPA protocols it has been found out that the proposed work is lesser in terms of computation and communication cost. The proposed BAC protocol assimilate a secured and authenticated generation of group-key and management between the vehicles, both in joining and leaving process and also a changeable password. Thus, the efficiency and energy, throughput, delay performance of our proposed protocol is better than the other existing CPPA protocols. We evaluate our proposed work in terms of routing cost, packet delivery ratio, and packet delivery time.

4. FUTURE WORK

We can further develop two new batch signature schemes based on Boneh–Lynn–Shacham (BLS) and digital signature algorithm (DSA), which are more efficient than the batch RSA signature scheme.

REFERENCES

[1] D. He, S. Aeadally, B. Xu, X. Huang, (2015). An efficient identity-based conditional privacy- preserving authentication scheme for vehicular ad hoc networks, IEEE Trans. Inf. Forensics Secure. 10 (12) 2681–2690, DOI: 10.1109/TIFS.2015.2473820.

[2] M. Bayat, M. Barmshoory, M. Rahim, M.R. Aref, (2014). A secure authentication scheme for vehicular ad hoc networks with batch verification, Wireless Network. 21 (5) 1733–1743, https://doi.org/10.1504/IJES.2019.099404.

[3] Y. Liu, L. Wang, H.H. Chen, (2015). Message authentication using proxy vehicles in vehicular ad hoc networks, IEEE Transactions on Vehicular Technology 64 (8) 3697–3710, DOI:10.1109/TVT.2014.2358633

[4] C. Zhang, P-H. Ho, J. Tapolcai, (2011). On batch verification with group testing for vehicular communications, Wireless Network 17 (8) 1851– 1865, doi>10.1007/s11276-011-0383-2.

[5] S.H. Islam, G.P. Biswas, (2012). A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks, Ann. Telecommun.67 (11) 547–558, https://doi.org/10.1007/s12243-012-0296-9.

[6] P. Vijayakumar, M. Azees, A. Kannam, L.J. Deborah, (2015). Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst. 17 (4) 1–13,
DOI: 10.1109/TITS.2015.2492981.

[7] P. Vijayakumar, M. Azees, V. Chang, J. Deborah, B. Balusamy, (2017). Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks, http://dx.doi.org/10.1007/s10586-017- 0848-x.

[8] P. Vijayakumar, V. Chang, L.J. Deborah, B. Balusamy, P.G. Shynu, (2016). Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks, Future Gener. Comput. Syst.. http://dx.doi.org/10.1016/j.future.2016.11.024.0

[9] K.A. Shim, (2012). An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks, IEEE Trans. Veh. Technol. 61 (4) 1874–1883, DOI: 10.1109/TVT.2012.2186992.

[10] S.K.H. Islam, M.S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li , M.K. Chaitanya, (2017), A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs, Future Generation Computer Systems 84 (19) 216-227, https://doi.org/10.1016/j.future.2017.07.002.

[11] S Gillani, F Shahzad, A Qayyum, R Mehmood, (2013). A Survey on Security in Vehicular Ad Hoc Networks, Communication Technologies for Vehicles, 59-74.

[12] B Mishra, P Nayak, S Behera, D Jena, (2011). Security in Vehicular Ad-hoc Networks: A Survey, International Conference on Communication, Computing ..., 53, doi>10.1145/1947940.1948063.

[13] H La Vinh, AR Cavalli, (2014). Security attacks and solutions in Vehicular ad hoc networks: A Survey, International journal on Ad Hoc networking systems, 4

(2), 1-20, doi: 10.5121/ijans.2014.4201.

[14] MA Elsadig, YA Fadlalla, (2016). VANETs Security Issues and Challenges: A Survey, Indian Journal of Science and Technology 9 (28), DOI:10.17485/ijst/2016/v-9i28/97782.

[15] J Jain, N Chahal, (2016). A Review On Vanet, Types, Characteristics And Various Approaches, International Journal Of Eng Sci & Research Tech, 5(9), 2277-9655, DOI: 10.5281/zenodo.61605.

[16] D. He, N. Kumar, M.K. Khan, L. Wang, J. Shen, Efficient privacy-aware authentication scheme for mobile cloud computing services, IEEE Syst. J. PP (99) (2016) 1–11.

[17] S.H. Islam, G.P. Biswas, A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks, Ann. Telecommun. 67 (11) (2012) 547–558.

[18] S. Rehman, M.A. Khan, Tanveer A. Zia, L. Zheng, Vehicular Ad-Hoc Networks (VANETs) — an overview and challenges, J. Wirel. Netw. Commun. 3 (3) (2013) 29–38.

[19] M. Raya, J.-P. Hubaux, Securing vehicular ad hoc networks, J. Comput. Secur. 15 (1) (2007) 39–68.

[20] J Jain, N Chahal, A Review On Vanet, Types, Characteristics And Various Approaches, International Journal Of Eng Sci & Research Tech, 5(9), (2016). 2277-9655, -

[21] B Mishra, P Nayak, S Behera, D Jena. Security in Vehicular Ad-hoc Networks: A Survey, International Conference on Communication, Computing ..., 53, (2011).

[22] S.H. Islam, G.P. Biswas, (2012). A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks, Ann. Telecommun.67 (11) 547–558, https://doi.org/10.1007/s12243-012-0296-9.

[23] S. Rehman, M.A. Khan, Tanveer A. Zia, L. Zheng, Vehicular Ad-Hoc Networks (VANETs) — an overview and challenges, J. Wirel. Netw. Commun. 3 (3) (2013) 29–38.

[24] M. Raya, J.-P. Hubaux, Securing vehicular ad hoc networks, J. Comput. Secur. 15 (1) (2007) 39–68.

[25] D. He, N. Kumar, H. Shen, J-H. Lee, One-to-many authentication for access control in mobile pay-TV systems, Sci. China Inf. Sci. 59 (5) (2016) 1–14.