DOIs:10.2017/IJRCS/202405004 --:-- Research Paper / Article / Review

A Secure Data Delivery in Vehicular Ad hoc Networks

Mohan Kumar Patel
Assistant Professor, CSE, Madhyanchal Professional University, Bhopal, India
Email- patel.mohan67@gmail.com

***Abstract**: Vehicular Ad Hoc Networks (VANETs) constitute a distinct subset of Mobile Ad Hoc Networks (MANETs), tailored to vehicular communication. In this paper, we introduce a Secure Data Delivery scheme specifically crafted for VANETs. The proposed scheme comprises two primary phases: 1) identification of encouraging and anticipated zones, and 2) establishment of connectivity between source and destination vehicles within the anticipated zone to ensure reliable data delivery. In the forwarding zone, vehicles with high mobility are utilized to transport data packets. However, within the anticipated zone, data packets are broadcasted until reaching the destination vehicle if it is not within the forwarding zone. To evaluate the performance effectiveness of the proposed scheme, we conduct a thorough analysis focusing on key performance metrics including latency, packet delivery rate, route lifetime, and control overhead. Keywords: VANETs, MANETs, packet rate, detention, route lifetime.*

***Key Words:** VANETs, MANETs, packet, ratio,*

1. INTRODUCTION :

Vehicular ad hoc networks (VANETs) represent a crucial component of the Intelligent Transportation System (ITS), facilitating communication among vehicles and between vehicles and roadside infrastructure. However, the security and privacy challenges encountered by VANETs are significant and complex, posing a formidable hurdle in contemporary research. Consequently, mitigating these security threats and addressing privacy concerns is imperative for the advancement of wireless communication in VANETs.

2. PROPOSED WORK FOR ENCRYPTION AND DECRYPTION:

This paper introduces an efficient scheme aimed at identifying malicious behaviour and ensuring data security for dynamic nodes. We present a streamlined framework specifically tailored for this purpose. The framework is structured to accommodate any node within the dynamic path, prioritizing inclusivity while considering potential security risks associated with multiple nodes. To mitigate these risks, we implement two distinct types of security measures, particularly focusing on the communication medium where security breaches are most likely to occur. In our system, nodes are categorized into two types: IN nodes and OUT nodes. Nodes of the same category can communicate directly, but they share data with varying levels of key filtration implemented using RSA and RC6 mechanisms. However, for OUT nodes, there's an additional condition where an OUT node may act as an IN node but only upon acceptance from the other side. When files are processed in this manner, they undergo the aforementioned steps along with the addition of an extra hash code designed to identify malicious behaviour.

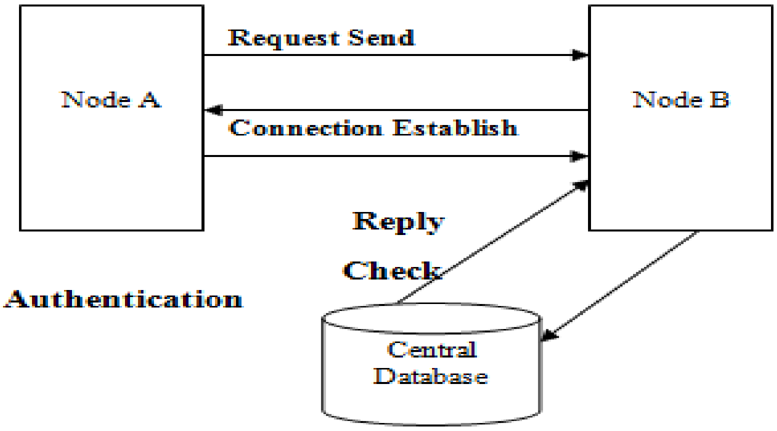

Fig. 1

Proposed algorithm

1. In RSA, encryption is performed using a key pair (e, n), with the following steps:
2. Represent the message as a number between 0 and (n-1). For large messages, break them into smaller chunks, each represented by a number within the same range.
3. Encrypt the message by raising it to the power of e modulo n. The resulting ciphertext is denoted as C.
4. To decrypt the ciphertext C, raise it to another power d modulo n.
5. The encryption key (e, n) is made public, while the decryption key (d, n) remains private.
6. Determining appropriate values for e, d, and n involves the following steps:
7. Select two large prime numbers (each with 100+ digits) and denote them as p and q.
8. Set n equal to the product of p and q.
9. Choose a large integer d such that the greatest common divisor (GCD) of d and ((p-1) * (q-1)) equals 1.
10. Find e such that e * d = 1 (mod ((p-1) * (q-1))).
11. The RC6 algorithm, which was a finalist in the Advanced Encryption Standard (AES) competition, is a block cipher.
12. RC6 evolved from its predecessor RC5, which was a simple and parameterized family of encryption algorithms.
13. It is based on RC5 and features variable block size, key size, and number of rounds.
14. RC6 has a maximum key size of 2040 bits and includes integer multiplication and four 4-bit working registers, in contrast to RC5's two 2-bit registers.

Encryption with RC6

- Input:
- Plaintext stored in four w-bit input registers A; B ; C; D Number r of rounds w-bit round keys S[0;:::; 2r + 3]
- Output: Cipher text stored in A; B ; C; D
- Procedure:
- B = B + S[0]
- D = D + S [1]
- for i = 1 to r do
- {
- t = (B * (2B + 1)) << lg w
- u = (D * (2D + 1)) << lg w
- A = ((A ʘ t) << u) + S[2i]
- C = ((C ʘ u) << t) + S[2i + 1]
- (A; B ; C; D)=(B; C; D; A)
- }
- A = A + S[2r + 2]
- C = C + S[2r + 3]

- Input: Cipher text stored in four w-bit input registers A; B ; C; D Number r of rounds w-bit round keys S[0;:::; 2r + 3]
- Output: Plaintext stored in A; B; C; D
- Procedure:
- C = C- S[2r + 3]
- A = A- S[2r + 2]
- for i = r down to 1 do
- {
- (A; B ; C; D)=(D; A; B ; C)
- u = (D* (2D + 1)) << lg w
- t = (B *(2B + 1))<< lg w
- C = ((C- S[2i + 1]) >> t) Ꙩ u
- A = ((A -S[2i]) >> u) Ꙩ t
- }
- D = D- S[1]
- B = B – s[0]
- INPUT: (Text, character, Random-Seed)
- OUTPUT: random_data, (Final-Seed)
- random_data = F(Text, character, Random-Seed)
- Key' = Math.random(Text, character, Random-Seed)
- Final-Seed' = F(Key', Random-Seed)
- Return random data

3. OUTPUT AND EXPERIMENTAL RESULT :

Result Evaluation

Info					
Node name	**ID**	**TCP**	**IP**	**key**	**Node status**
Node1	**ID1**	**80**	**192.168.1.101**	**iS3Rc1f6**	**IN**
Node2	**ID2**	**80**	**192.168.1.101**	**xH2Ub1u1**	**IN**
Node3	**ID3**	**80**	**192.168.1.101**	**kG2Wc7e9**	**IN**
Node4	**ID4**	**80**	**192.168.1.101**	**pG9Hq3e4**	**OUT**
Node5	**ID5**	**80**	**192.168.1.101**	**eB6Na6t6**	**OUT**
Node6	**ID6**	**80**	**192.168.1.101**	**zU4Bq3l3**	**OUT**

table 1

4. CONCLUSION AND FUTURE WORK :

In this paper, we propose a hybrid encryption method that combines the strengths of Ron Rivest, Adi Shamir, and Leonard Adleman (RSA) and Rivest Cipher (RC6) to ensure robust data protection. Additionally, we integrate a listener component to detect malicious behavior promptly, enabling timely intervention. To further enhance data security, we employ a Java-based Base 256 expandable overlapping mechanism during data sharing, ensuring that only authenticated users can access and modify the files. Our experimental results demonstrate the effectiveness of our approach, showing superior performance compared to using individual algorithms separately. Moreover, our method exhibits minimal data loss, as evidenced by data loss comparison, thus ensuring high data integrity. Based on the comprehensive analysis of our results, our proposed method emerges as a valuable and effective solution for ensuring data security and integrity

REFERENCES:

1. S. Noguchi, M. Tsukada, T. Ernst, A. Inomata, and K. Fujikawa, “Location-aware Service Discovery on IPv6 GeoNetworking for VANET,” in Proceedings of the 11th International ITS Telecommunications (ITST), pp. 224-229, Aug. 2011.
2. Z. Ou, M. Song, H. Chen, and J. Song, “Layered Peer-to-Peer Architecture for Mobile Web Services via Converged Cellular and Ad Hoc Networks,” in Proceedings of the 3rd International Conference on Grid and Pervasive Computing Workshops, pp. 195 – 200, May 2008.Rowstron and P. Druschel, “Pastry: Scalable, Decentralized Object Location, and Routing for Large-scale Peer-to-Peer Systems,” in Proceedings of the 2001 IFIP/ACM International Conference on Distributed Systems Platforms Heidelberg, pp. 329-350, Nov. 2001.
3. T. Fujii, K. Yamori, and Y. Tanaka, “Ad hoc Network Service with Relay Reward and Its Routing Performance,” in Proceedings of the 2010 8th Asia-Pacific Symposium on Information and Telecommunication Technologies (APSITT), pp. 1-6, Jun. 2010.
4. Wongdeethai, Singha, and Peerapon Siripongwutikorn. "Multipath query spreading over vehicular ad-hoc networks." In Computer Science and Engineering Conference (ICSEC), 2013 International, pp. 255-260. IEEE, 2013.
5. K.V.Kulhalli, Prajakta Rane, “On Demand Multipath Routing Algorithm for Adhoc Wireless Networks ", International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-14, March-2014, pp.357-363.
6. Aruna Rao S.L, K.V.N.Sunitha, “Secure Geographical routing in MANET using the Adaptive Position Update", International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-16, September-2014, pp.785-794.
7. Kambalimath, Mahantesh G., S. K. Mahabaleshwar, and S. S. Manvi. "Reliable Data Delivery in Vehicular Ad Hoc Networks." In Broadband and Wireless Computing, Communication and Applications (BWCCA), 2013 Eighth International Conference on, pp. 316-322. IEEE, 2013.
8. T. Leinmuller, E. Schoch, and C. Maihofer, “Security Requirements and Solution Concepts in Vehicular Ad Hoc Networks,” IEEE 4th Annual Conference on Wireless on Demand Network Systems and Services, pp. 84-91, 2007.
9. H. Hartenstein, and K. P. Laberteaux, “A Tutorial Survey on Vehicular Ad Hoc Networks,” IEEE Communications Magazine, pp. 164-171, Jun 2008.
10. C. Langley, R. Lucas, and H. Fu, “Key Management in Vehicular Ad-Hoc Networks,” IEEE International Conference on Electro/Information Technology, pp.223-226, 18-20 May 2008.
11. M. Burmester, E. Magkos, and V. Chrissikopoulos, “Strengthening Privacy Protection in VANETs,” IEEE International Conference on Wireless & Mobile Computing, Networking & Communication, pp. 508-513, 2008.T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, “Security and Privacy Issues for Inter-vehicle Communications in VANETs,” IEEE Sensor, Mesh and Ad Hoc Communications and Networks Workshops, pp. 1-3