International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Strong Key Organization & Protected Statistics Shift System for VANET

[1] Dr. K. Rameshwaraiah, [2] Dr. K. Srinivas Babu, [3] Dr. S. Sree Hari Raju, [4] Ch. Ramya, [5] S. Radhika

Submitted: 07/05/2024 **Revised**: 20/06/2024 **Accepted**: 27/06/2024

Abstract: VANETs are integral to vehicle control systems, allowing vehicles to communicate with one another in a centralized manner. This communication enhances coordination and safety, but also introduces potential cyber security risks. To protect the vehicle infrastructure, it is crucial to develop effective security solutions, as cyber-attacks on VANETs can lead to significant financial losses and safety hazards. Field devices within VANETs, which rely on microcontrollers for processing information, face challenges due to their limited computational capabilities and resources, making it difficult to implement sophisticated security measures. This academic work introduces a novel multi-tiered framework that merges symmetric and asymmetric input cryptographic methods. Our method promise accessibility, reliability, privacy, confirmation. The recommended modified assembly input organization device to merge accidental numeral making by jumble communication confirmation system. Furthermore, we incorporate three distinct symmetric key cryptographic methods inspired by the Vernam cipher, enhancing security with a arbitrary major figure originator, major contradict, plus hash chaining.

Keywords: *enhancing, communication, processing, symmetric*

1. Introduction

VANETs have become increasingly popular due to their ability to improve vehicular safety, alleviate traffic congestion, and offer location-based services. This paper addresses the challenges associated with distributed key management frameworks by proposing a shared key management framework. Roadside units, which monitor road conditions at various locations, play a crucial role in the core VANET architecture, aiming to enhance road safety and optimize traffic management.

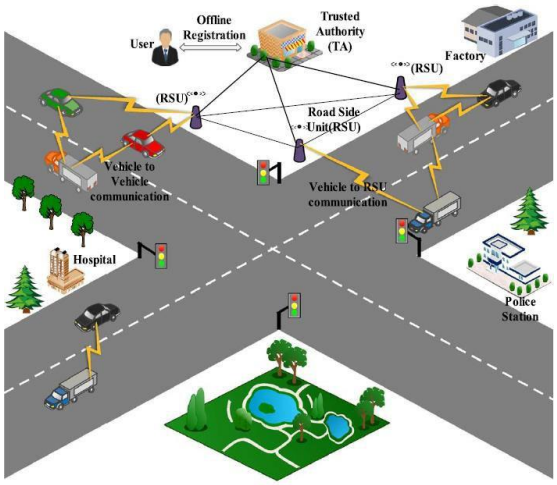
Our projected method tackles key management challenges and meets real-time request response needs in VANETs. This holistic framework aims to enhance the efficiency and safety of contemporary transportation systems while addressing the specific security issues in VANETs.

[1]*Head & Professor,*
[2]*Professor,*
[3]*Associate Professor,*
[4]*Assistant Professor,*
[5]*Assistant Professor,*
Department of Computer Science & Engineering
Nalla Narasimha Reddy Education Society's Group of Institutions

VANETs utilize various communication links such as satellite, radio, microwave, cellular networks, and powerlines, along with geographically distributed field manage procedures. These components create a robust network infrastructure.

To ensure nonstop observing plus manage of apparatus, a difficult structure utilize sensors as well as actuators toward determine a range of constraint with spread numbers toward field procedure. Field organize articles throw digital condition inform toward the Master Terminal Unit, which is usually situated remotely. This data is then communicated back to the field control devices to optimize the system.

Furthermore, status information is stored in a managed database that is synchronized with a Human Machine Interface (HMI) at the control center. This arrangement allows operators to interact with plant operations through visualized data and real-time updates. In extensive VANET networks, like those used in power plants, numerous field devices and dedicated subsystems are essential to alleviate the load on the centralized server.



2. VANET System

VANET communication messages contain sensitive information critical for monitoring and controlling devices on the place base. For example, in water and sewage systems, these messages regulate water tank levels and manage safety valves. Because the campaigns be function plus check slightly, they are prime targets for cyber-attacks aimed at compromising manage schemes, message, plus disaster services. Therefore, ensuring safe program of letters in VANET organization is essential to prevent tampering. Additionally, VANET procedure has to exist genuine as well as sustain in turn privacy throughout program toward avoid illegal admission.

In current days, a range of input organization systems developed toward protected VANET message. Famous processes be classified interested in federal plus decentralized input organization system. Every group exercise unusual move toward intended for assembly input creation plus pulling out, as well as symmetric, asymmetric cryptography, and hybrid methods.

Centralized schemes, while effective, have a significant drawback: if KDC stop working, message be disturbed, which be objectionable intended for VANET schemes. In contrast, decentralized approaches generate keys using keying material, so a failure affects only a single communication link. Symmetric key-based methods excel in ensuring message integrity and availability but fall short in providing authentication and confidentiality. Asymmetric keys, on the other hand, offer reliability, verification, plus isolation except can decrease ease of use. Therefore, hybrid systems that combine both methods are better suited for VANET systems.

Several advanced hybrid input organization methods projected. HSKMA with the purpose of advance ahead the structure projected meant for better effectiveness in addition to protection. This architecture employs a centralized KDC for key distribution. RSA is employ among secondary MTU as well as RTU. Despite their sophistication, these techniques often lack practical implementation evidence, especially in terms of protection against quantum attacks.

Given these challenges, an effective cryptography solution is essential to prevent potential breaches. This paper presents a strong, charge successful protection structure designed for mechanical trade toward tackle a range of protection vulnerabilities and replicated assaults. The projected framework offers a multi coated protection design in favor of vehicle models, integrating both symmetric and asymmetric input cryptographic procedures. The innovative move toward initiate a carefully designed encrusted structure, facilitating seamless communication within the system through hybrid techniques.

The methodology includes generating symmetric keys using the Vernam cipher, moving beyond traditional methods like 3DES and AES. This novel approach introduces new possibilities in cryptographic practices, guarantee genuine instance request-response machines plus sustaining transmit, multicast, with P2P message.

1. Protected assembly input concurrence system concord system associated by VANET procedure values toward guarantee safety amongst MTUs, secondary MTUs, plus RTUs. This scheme employs a accurate casual figure producer supported scheduled the CDT plus a FSRP. These elements be XORed on the way to enhance the privacy of shared secrets. Additionally, HMAC derived from FSRP is used to validate message integrity, improving computational speed for cryptographic operations and strengthening resistance against various attacks.

2. Symmetric Key Generation with Vernam Cipher original technique designed for make symmetric inputs by the Vernam cipher, incorporating major answer plus hash sequencing methods. This approach leverages the non-terminating, non-

repeating properties of FSRP, enhancing security by enabling secure seed exchange.

3. Multi-Layered Framework that merge symmetric and asymmetric input cryptography to provide confirmation, discretion, communication reliability and accessibility designed for VANET organizations. The Vernam cipher-based symmetric input cryptography offers protection against cryptographic assaults, as the NTRU supported situation quantum open input algorithm protect beside quantum plus information produce assaults.

4. Efficient Cipher Suite categorized via estimate a variety of personal as well as unrestricted input algorithms, in view of issues such as conflict toward traditional with quantum assaults, input storage expenses, input chances, plus computational rapidity. The projected set tackle vulnerabilities there inside accessible AGA protection principles.

3. Related Work

VANETs are often established by proprietary procedures, which usually perform not propose protected figures message. The vulnerability of these protocols was illustrated by the Blaster worm, which demonstrated the risks associated with open communication links in remote procedure call (RPC) environments. The availability of various network sniffing tools that can easily capture network traffic further emphasizes the need for secure data transmission in VANETs. Effective key management and encryption are essential for ensuring secure communication within VANETs.

In a typical VANET, the Master Terminal Unit launch organize indication toward RTUs toward manage devices lying on the fix bottom. This engage transmit, multicast, with P2P. MTUs use broadcasting to synchronize control devices during emergencies, multicast for specific substation device operations, and point-to-point communication for routine machinery control. Therefore, a secure framework for VANETs must accommodate all 3 forms of message.

Earlier various input supervision method enclose projected in addition to be able to exist cataloged interested in federal plus decentralized input allocation method. Centralized schemes involve a Key Distribution Center (KDC) that generates and distributes secret keys to secure communication. In contrast, decentralized schemes use pre-shared keying material to create session keys. Some schemes also employ public key methodologies, though these can be time and power-consuming, with Elliptic Curve Cryptography (ECC) being a commonly preferred choice for public-key cryptosystems.

HKMA and AHSKMA architectures projected and may face challenges such as the potential failure of field devices during control device replacements. Choi et al. addressed this with a hybrid input management scheme that applies a federal input allocation procedure among the secondary MTU as well as MTU, along with the LKH procedure among secondary MTU in addition to RTU, though it still lacks high availability.

Various authentication techniques have been developed for VANETs. Johnson et al. proposed the LiSH, which suggest ability designed for input revocation in addition to conflict toward involvement in group communication within VANET systems.

For user authentication, the ECDSA exploit the asymmetric input duo, consisting of a unrestricted as well as confidential input. The unrestricted input is derived from a random multiple of a base point based on the private key. Despite its advantages, ECDSA is vulnerable to assault lying on the ECDLP in addition to potential exploits of hash functions. Wasef et al. introduced the Efficient Certificate Management Scheme for VANETs (ECMV), which utilizes a Public Key Infrastructure (PKI) system where vehicles possess short-lived certificates updated regularly by Road Side Units (RSUs), although this increases system overhead.

Shen et al. proposed the supportive communication confirmation procedure, which aims toward detect and mitigate nasty in sequence in VANETs. CMAP reduces the computational overhead for message verification at vehicles but faces challenges with increased communication overhead due to higher vehicle density and lacks a dedicated verifier for message authentication. Biswas, Misic, and Misic introduced an ID-based signature and verification mechanism, which eliminates the need for certificates in public key verification and enhances message authentication using ID-based proxy signatures, demonstrating robustness against security threats.

Busanelli, Ferrari, and Veltri highlighted the critical need for security in VANETs to mitigate malicious attacks that could increase accident risks.

They proposed a key management strategy tailored for VANET communications, introducing a framework designed for key group multicast to address specific communication requirements in VANETs.

Dhamgaye and Chavhan explored routing protocols and the associated security challenges in VANETs, underscoring the need for secure data routing and the vulnerabilities inherent in wireless communication mediums.

Huang et al. developed the Anonymous Batch Authenticated and Key Agreement (ABAKA) protocol, which efficiently handles multiple vehicle authentication requests and establishes session keys with a single verification step. This approach, utilizing elliptic curve cryptography, aims to reduce delays and transmission overhead.

Mershad and Artail emphasized the importance of inter-vehicle communication for enhancing transportation safety and efficiency, demonstrating its role in improving overall system performance.

Raya and Hubaux examined intelligent transport systems within VANETs, focusing on the exchange of road condition information and addressing security issues to ensure effective data transfer. Hao et al. developed a circulated input supervision construction support taking place assembly signatures, which supports the revocation of malicious vehicles and accommodates diverse security policies. Their framework comprise a helpful point validation procedure designed toward lessen the certification load on vehicles. Shen, Liu, and Cao introduced a Cooperative Message Authentication Protocol (CMAP) aimed at reducing computational overhead in densely populated VANETs, with performance results highlighting its effectiveness. Naranjo, Ramos, and Casado explored the use of the Extended Euclidean algorithm in secure communication contexts, including multicast rekeying and zero-knowledge proofs.

4. Conclusion and Future Enhancements

This study presents a novel dual authentication scheme aimed at improving vehicle security within VANETs. Our approach integrates two key components: the jumble code and the automobile user's fingerprint involved in communication. By combining fingerprint authentication with hash code generation, we effectively prevent unauthorized access to VANET secret keys and protect communication integrity. To counteract the threat of malicious users spoofing authentication codes and sending fraudulent messages, we propose a new dual key management scheme. This scheme ensures computational efficiency and secure data transmission between Trusted Authorities (TAs) and Primary Users (PUs), and between PUs and Secondary Users (SUs) by using two distinct group keys—one for PUs and one for SUs. Additionally, our algorithm incorporates single broadcast messages from the TA to notify group members and facilitate the recovery of updated group keys.

For future improvements, we aim to investigate new approaches to safeguard the privacy of vehicle locations from potential intruders.

References

[1] D.Upadhyay,S.SampalliandB.Plourde,"Vulnerabilities'assessmentandmitigationstrategiesfor the small linux server Onion Omega2", Electronics,vol.9, no.6, pp. 967,2020.

[2] D.UpadhyayandS.Sampalli,"VANET(supervisorycontrol and data acquisition) systems:Vulnerability assessment and security recommendations" ,Comput Security, vol.89,Feb.2020.

[3] Y. Cherdantseva et al., "A review of cyber securityriskassessmentmethodsforVANETsystems" ,Comput.Security, vol.56, pp.1-27,Feb. 2016.

[4] Rezai,P.KeshavarziandZ.Moravej,"Keymanagement issue in VANET networks: A review", Int.J.Eng.Sci. Technol., vol.20,no.1,pp.354-363,2017.

[5] F. M. Salem, E. Ibrahim and O. Elghandour, "Alightweight authenticated key establishment scheme forsecuresmartgridcommunications",Int.J.SafetySecurityEng., vol.10, no. 4,pp. 549-558,2020.

[6] D.Upadhyay,J.Manero,M.ZamanandS.Sampalli,"Gradientboostingfeatureselectionwithmachine learning classifiers for intrusion detection onpower grids", IEEE Trans. Netw. Service Manag., vol.18,no. 1,pp.1104-1116, Mar.2021.

[7] D. Choi, S. Lee, D. Won and S. Kim, "EfficientsecuregroupcommunicationsforVANET", IEEETrans. Power Del., vol. 25, no. 2, pp. 714-722, Apr.2010.

[8] T. C. Pramod and N. R. Sunitha,

"Polynomial basedschemeforsecureVANEToperations",Procedia Technol., vol. 21,pp.474-481, Nov.2015.

[9] Rezai,P.KeshavarziandZ.Moravej,"Secure VANETcommunicationbyusingamodifiedkeymanagement scheme", ISA Trans., vol. 52, no. 4, pp.517-524,2013.

[10] Rezai, P. Keshavarzi and Z. Moravej, "AdvancehybridkeymanagementarchitectureforVANETnetwork security", Security Commun. Netw., vol. 9, no.17,pp. 4358-4368,2016.

[11] D. Choi, H. Jeong, D. Won and S. Kim, "HybridkeymanagementarchitectureforrobustVANETsystems", J. Inf. Sci. Eng., vol. 29, no. 2, pp. 281-298,2013.

[12] R.Jiang,R.Lu,C.Lai,J.LuoandX.Shen,"Robust groupkey managementwith revocation andcollusion resistance for VANET in smart grid", Proc.IEEE Global Commun. Conf. (GLOBECOM), pp. 802-807,2013.

[13] Rezai, P. Keshavarzi and Z. Moravej, "A new keymanagement scheme for VANET networks", Proc. 2ndInt.Symp.Comput.Sci.Eng.,pp.373-378,2011.

[14] S. Ghosh and S. Sampalli, "A survey of security inVANETnetworks:Currentissuesandfuturechallenges", IEEE Access, vol. 7, pp. 135812-135831,2019.

[15] V. Manjunatha, A. Rao and A. Khan, "Complexkey generation with secured seed exchange for vernamcipherinsecurityapplications",Mater.TodayProc.,vol.35, no. 3,pp.497-500, 2021.

[16] R. Chandia, J. Gonzalez, T. Kilpatrick, M. PapaandS.Shenoi,"SecuritystrategiesforVANETnetworks", Proc. Int.Conf.Crit. Infrastruct.Protect.,pp.117-131,2007.

[17] M.F.Moghadam,M.Nikooghadam,A.H.MohajerzadehandB.Movali,"Alightweightkey

managementprotocolforsecurecommunicationinsmart grids", Electr. Power Syst. Res., vol. 178, Jan.2020.

[18] R. Dawson, C. Boyd, E. Dawson and J. M. G.Nieto,"SKMA—AkeymanagementarchitectureforVANET systems", Proc. 4th Aust. Symp. Grid Comput.e-Res.(AusGrid)4thAust.Inf.SecurityWorkshop(Network Security) (AISW-NetSec), vol. 54, pp. 183-192,2006.

[19] D. Choi, H. Kim, D. Won and S. Kim, "Advancedkey-managementarchitectureforsecureVANETcommunications", IEEE Trans. Power Del., vol. 24, no.3,pp.1154-1163, Jul. 2009.

[20] D. Wu and C. Zhou, "Fault-tolerant and scalablekey management for smart grid", IEEE Trans. SmartGrid,vol.2, no.2, pp.375-381, Jun.2011.