EAI Endorsed Transactions
on Internet of Things

Research Article EAI.EU

Enhanced security based on Context Aware Proactive Trust Aware Routing Protocol using secure Preemptive Verifiable Key Handover Policy for VANET Environment

K. N. Anupama[1],R. Nagaraj[2,*]

[1]Kaamadhenu Arts and Science College Sathyamangalam, Erode, Tamil Nadu, India
[2]Government Arts and Science College Sathyamangalam, Erode, Tamil Nadu, India

Abstract

INTRODUCTION: Road safety improvements through Vehicular Ad-hoc Networks (VANETs) occur because these networks enable vehicles to exchange messages with Road Side Units (RSUs). The secure exchange of data in VANET evolves as a fundamental challenge in practical systems because nature-based implementation problems combine with protection threats from both data failure and sabotage-based message releases.
OBJECTIVES: This research develops a new routing protocol to strengthen VANET communication security processes by filling existing vulnerabilities and building reliable data transmission methods.
METHODS: CAPTARP represents a routing protocol which integrates PVKHP as its Secure Preemptive Verifiable Key Handover Policy. Data from RSU communications first needs collection before the lookup environment can be established. The Payload Data Impact Rate (PDIR) detects both transmission defects and congestion through analysis. The Transmission Behavioral Delay Tolerance Rate detects the patterns of deliberate transmission anomalies. SRSU-FIS operates as a security enhancement mechanism for routing decisions while maintaining context-based security protection capabilities.
RESULTS: Test simulations show that the proposed system delivers better results than current approaches by achieving 94.19% throughput alongside 96.03% packet delivery ratio while reaching 95.03% security performance and 95.24% authentication level and maintaining 18.06 ms end-to-end delay.
CONCLUSION: The combination of CAPTARP protocol with PVKHP protocol effectively strengthens VANET security by providing better authentication coupled with trust validation and rapid communication procedures. The security performance surpasses traditional methods because this innovative approach represents a strong solution for protecting vehicular communication networks.

Received on 24 October 2024; accepted on 18 December 2024; published on 28 May 2025

Keywords: Authentication, routing protocol, delay, RSU, Secure communication, VANET

doi:10.4108/eetiot.7648

1. Introduction

Security protocols are necessary for recent vehicular ad hoc network (VANET) communication developments to provide impenetrable security for vehicles and VANET components. Because VANET's infrastructure is open, it is vulnerable to various security risks related to information. Along with them, VANETs can improve urban transport and road safety management. Early warning systems capable of alerting drivers about road construction, collisions, and weather-related hazards can be implemented in vehicular ad hoc networks for widespread use. Moreover, drivers in VANET can provide infotainment to the passengers, which can help maintain safe driving practices and enhance the overall driving experience [1-2].

For instance, a malicious actor can pose as an ambulance and request or grant permission for a traffic

[*]Corresponding author. Email: anupama.kn@gmail.com

light to turn green. Additionally, shared public media platforms employ wireless communication channels to protect user's data security. Recipients can avoid potential collisions by recognizing parallel attacks in all messages before taking further action. Moreover, these messages enable drivers to comprehend road conditions and traffic information and adjust their lanes and speeds for safer and faster driving. Once these safety measures have been taken, advertisements for restaurants and nearby gas stations can be added to enhance the value of the services provided by VANET reports [3-4].

VANET is a communication environment open to attacks due to its lack of security measures. Attackers can exploit this vulnerability by spoofing messages. However, since there is limited communication time between cars in VANETs, and they typically move very quickly, it is necessary to identify vehicles rapidly. It is difficult for a single vehicle to receive messages from dozens or hundreds of other vehicles simultaneously in a densely populated area. Authentication of multiple messages within a short period causes rush issues. However, current authentication schemes are inadequate to meet VANET's strict time requirements, resulting in lost information [5].

Contribution of this research

- To propose a CAPTARP based on secure Preemptive Verifiable Key Handover Policy (PVKHP) in improve the security in VANET Environment.
- Using SRSU-FIS creates the logical decision for security enhancement in transmission defects routing.
- By intending CAPTARP to improve the secure transmission along with the sharable communication nodes.
- Finally the PVKHP verifies the distinctive node to securely handover the data.

2. Literature Survey

The author suggested a Trust Management Scheme Based on Hybrid Cryptography (TMHC) to enable safe communication and identify areas between vehicles. On the other hand, malicious entities can launch many security attacks against VANETs [6]. The novel aimed to distribute network parameters by establishing links between vehicles and infrastructure using Chebyshev confusion maps [7]. However, several security features cannot be used because of the environment's poor wireless performance. The author suggested a lightweight protocol for privacy-preserving authentication in VANETs that ensures secure and efficient data transfer over public channels, a critical task in VANETs [8]. The novel suggested a VPCS (VANET-Based Privacy-Preserving Communication Scheme) could be deployed to fulfil content a d context privacy needs. Nevertheless, VANET poses the most difficult challenge in privacy protection [9]. The novel proposes achieving mutual authentication through VANETs by combining nickname and group-based approaches using vehicles and Roadside Units (RSUs) [10].

The author suggested implementing bulk signatures without certificates to offer a new authentication scheme for VANETS. However, high vehicular mobility density and scalability pose critical challenges in these contexts [11]. The author proposed combining the short-term mutual features of wireless channels into a cross-layer authentication system for vehicular communication [12]. The author proposed implementing a signature scheme called Conditional Privacy Protection Authorization (CPPA) to provide a discrete logarithmic inference of message retrieval [13]. The novel proposes a modification to improve VANET by using the split lemma temporarily or incorrectly in security proofs based on the Certificate Less Aggregate Signature (CLAS) scheme [14]. The author suggested that Elliptic Curve Cryptography (ECC) can handle message signatures by using addition operations and dot multiplication during verification [15]. However, implementing message return validation approaches increases their costs while reducing overhead.

The author suggested using bilinear connectivity in conjunction with Conditional Privacy-Preserving Hybrid Encryption (CPP-HSC) to assemble the security requirements of multimodal vehicle communication [16]. The novel proposed that traffic-related data can be obtained, intercepted and replicated through VANETs based on compromising their security [17]. However, in VANETs, information privacy protection in the radio access medium is critical. The author presented an authentication protocol based on the designed ECC. However, current authentication protocols focus either on lightweight functionality or on security [18]. The author proposed implementing an Identity-based CPPA (ID-CPPA) signature scheme for handling bilinear mapping for Vehicle-To-Infrastructure (V2I) communication [19]. The author suggested using a lightweight protocol for vehicle dynamics to manage segments and analyze overhead. However, V2V communication is insufficient for managing a large number of vehicles [20].

Table 1 demonstrates that secure, authenticated communication can be used to learn about VANET technology and its benefits.

Table 2. Implementation of VANET-based secure privacy protection and highlighting its limitations and techniques.

Author	Year	Technique	Advantage
M. A. Saleem [21]	2023	Trusted Authority (TA)	It defends against various known VANET attacks.
M. A. Al-Shareeda [22]	2021	VANETs	VANET can fulfil all security and privacy requirements for proprietary programs.
L. Wei [23]	2022	Authenticated Key Agreement (AKA)	Mechanism for Securing Communication Channels in VANET.
Q. Xie [24]	2023	ECC	The module can be verified through the Vehicle-to-Vehicle (V2V) authentication protocol.
J. Cui [25]	2020	TA	Enable faster and more efficient authentication.

Table 1. Proven Secure Authenticated Communication over VANET

Year	Author	Method	Limitation
2019	Y. Wang [26]	Road Condition Monitoring (RCM)	Privacy protection is required in VANET applications.
2020	I. Ali [27]	Identity-Based Signature with Conditional Privacy-Preserving Authentication (IBS-CPPA)	However, addressing multiple message authentication is challenging in VANET.
2020	Z. Xu [28]	CLAS	Challenges can arise from network topology and lack of centralized management capabilities.
2021	W. Xiong [29]	Tamper-Proof Device (TPD)	Predicting conditional privacy-preserving authorization is a difficult task

Table 2. A Secure Privacy-Preserving Based on VANET

3. Proposed methodology

This section outlines VANET's secure communication based on authentication policy. Figure 1 illustrates the proposed diagram for proficient communication in the VANET environment. Our proposed system consists of two stages for vehicle communication.

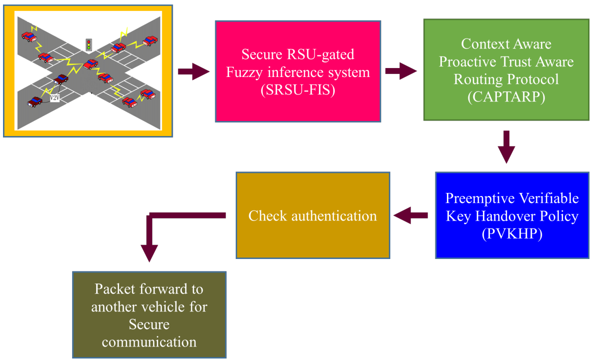
Secure RSU-gated Fuzzy inference system (SRSU-FIS)
Context Aware Proactive Trust Aware Routing Protocol (CAPTARP)
Preemptive Verifiable Key Handover Policy (PVKHP)
Check authentication
Packet forward to another vehicle for Secure communication

Figure 1. Proposed diagram

From the figure, the proposed SRSU-FIS creates the logical decision for security enhancement in transmission defects routing. By intending CAPTARP to improve the secure transmission along with the sharable communication nodes. Finally the PVKHP verifies the distinctive node to securely handover the data. The detailed description is illustrates in the following sub-sections.

3.1. Secure RSU-gated Fuzzy inference system (SRSU-FIS)

VANET relies on the SRSU-FIS technique to maintain secure communication among vehicles in the network. Additionally, SRSU-FIS can be employed to determine the safety of communication within the network. By using a gated fuzzy logic system, SRSU-FIS considers various factors, such as the reliability of communication nodes, the content of communication, and the current state of the network. The SRSU-FIS method has numerous applications, one of which is communication security. As the average speed of vehicles increases, the distance for communication security between them also increases. To indicate the potential distance between each vehicle, an average distance is defined. If a transmission path edge is crossed for a specific period, the path continues to the most distant destination node.

Calculate the transmission path for the average vehicle density on the road segment, as depicted in Equation 1. Where a-road segment, u-time stamp, QE-vehicle distance, $Q_E^{a,u}$ – vehicle network connectivity model, U_K – transmission range, $U_K(max)$ – maximum transmission range, $S^{a,u}$ – numer of road segment, and z_a – length of road segment.

$$Q_E^{a,u} = \frac{U_K(maX) \times S^{a,u}}{z_a} \qquad (1)$$

Calculate the average distance of the transmission path between the vehicles as shown in equation 2.

Where Q^0 – vehicle velocity, $I_E^{a,u}$ – average distance, u_e – breaking time delay and value, 2_i^p – maximum reduction and general value, and e–safety distance.

$$I_E^{a,u} = Q^0 u_e + \frac{Q_0^2}{2_i^p} + e\ldots \tag{2}$$

Calculate the transfer path opposite ratio of vehicles on the road segment as shown in Equation 3. Let's assume $g_K^{a,u}$ – opposite ratio, S_a, E^1, S_a, E^2 – both direction road segment, i-segment.

$$g_K^{a_u} = \begin{cases} \frac{M_{in}(s_a,E_1,S^a,E_2)}{M_{ax}(s_a,E^1,s_a,E^2)}, & M_{ax}(s_a, E^1, s_a, E^2) \neq 0 \\ 1, & M_{in}(s_a, E_1, S^a, E_2) = 0 \end{cases} \tag{3}$$

The fuzzy network connectivity ratio of the transmission path is calculated as shown in Equation 4.

$$F_k^a = \frac{\sum_{y=1}^{s} x \times \mu^y(x)}{\sum_{y=1}^{s} \mu^y(x)}, \ldots \tag{4}$$

Compute the fuzzy network connectivity ratio of the current node using Equation 5 to 8. Let's assume s_{cur} – current node, A^u – information table, S-node, u-time, Q^u – vector time,

$$\forall s \in A^u(s_{cur}), \ldots \tag{5}$$

$$s \in S_{sec}(m^u), \ldots \tag{6}$$

$$\|Q^u(\bar{s}_{cur}, s)\| \leq U_k(maX) \tag{7}$$

$$max(\|Q^u(\bar{s}_{cur}, s)\|) \tag{8}$$

Equations 9 and 10 calculate the fuzzy network connectivity ratio of the primary and secondary transmission paths. Where $Q^{(u+a,u)}(s_{cur}, S)$, $Q_t(s)$ – dot product vector, M^s, M^u – matching degree.

$$\begin{cases} \forall s \in A^u(s_{cur}), \ldots \\ s \in S_{sec}(m^u), \ldots \\ \|Q^u(\bar{s}_{cur}, s)\| \leq U_k(maX) \\ Q^{(u+a,u)}(s_{cur}, S), Q_t(s) > 0, \ldots \end{cases} \tag{9}$$

$$m_{ax}(P(m^s, m^u)) \times (\|Q_{(u+\Delta u)}(\vec{s}_{cur}, S)\| - \|Q_{(t)}(\vec{s}_{cur}, S)\|) \ldots \tag{10}$$

Therefore, it is possible to estimate the road segment compatible with the current node transmission path and estimate the distance path time of the node in the transmission path moving to the destination node.

3.2. Context Aware Proactive Trust Aware Routing Protocol (CAPTARP)

In secure routing cooperation, the CAPTARP method is used to communicate nodes. This method relies on nodes having larger values to be selected as communication nodes in the routing path. CAPTARP technology estimates the explicit trust value based on direct and indirect trust weights, as well as the residual energy of the communication nodes. If a communication node's precise trust value is less than a preset threshold, it is considered untrustworthy. The current node weight in the communication trust value depends on the specific application of the VANET. Implicit trust values permit related party nodes to evaluate the target based on their communication protocol.

Calculate the current direct trust value of the communication node as shown in Equation 11. Let's assume a-node, b-neighbour, E_{ab} direct trust value, γ weight of historical value, u total number of packet, $K_u + N_u$ send and received node,

$$EU_{ab}^s = Q_{(t)}\gamma * (\omega_1 K_1 + \omega_2 N_1)^{s-1} + (1 - \gamma) * (K_u + N_u)^s$$

Calculate the ratio of total communications sent and received node as shown in Equations 12 and 13. Where K_p = receive message, N_p = send message,

$$K_u = \frac{K_p^{(b)}}{p_b} \tag{12}$$

$$N_u = \frac{N_p^{(b)}}{p_b} \tag{13}$$

As shown in Equation 14 and 15, calculate the high trust value of nodes corresponding to the transition path. Let's assume U-current time of node, f_1 and f_2 change trust value, τ time threshold,

$$\omega^1 = d^{-f_1} m_{OD}(U, \tau) \tag{14}$$

$$\omega^2 = d^{-f_1} m_{OD}(U, \tau) \tag{15}$$

Calculate the implicit trust value of the node using Equation 16. Let's assume a-node,$EU_{aJ_a}^s * Eu_{J_a b}^s$ direct trust value, a and b- trust neighbour node.

$$AU_{ab}^s = \frac{1}{p} \sum_{J_a \in J_w} (EU_{aJ_a}^s * Eu_{J_a b}^s) \tag{16}$$

Calculate the energy used for receiving and sending the transmitting node, as indicated in Equation 17 to 19. Where D_k^b = energy receive node, D^{Nb} = energy send node, D_{etc} = energy electronics, e_0 = threshold value, e-distance, d_{cn} and d_{pm} energy consumption free path and multipath model.

$$D^{p} = Z * D_{etc} \tag{17}$$

$$D^{Nb} = \begin{cases} z * D_{\mathcal{E}lc} + z * d_{cn}, & E^2E < e_0 \\ z * D_{\mathcal{E}lc} + z * d_{pm}, & E^2E < e_0 \end{cases} \tag{18}$$

$$e_0 = \sqrt{\frac{d_{cn}}{d_{pm}}} \tag{19}$$

Compute the initial and residual energy transfer paths as shown in Equation 20 and 21.Where KD_b-resudial energy node, b-energy of trust value.

$$KD_b = D_0 - D_{K^b} - E^{Nb} \tag{20}$$

$$D^b = \frac{KD_b}{D_0} \tag{21}$$

Calculate the security and energy consumption of the node trust values as shown in Equation 22. Let's assume η_1, η_2, η_3 = energy trust value, A and B-trust value of the node.

$$FU^{s}_{ab} = \eta_1 * EU^{s}_{ab} + \eta_2 * AU^{s}_{ab} + \eta_3 * D^b \tag{22}$$

4. Preemptive Verifiable Key Handover Policy (PVKHP)

The proposed PVKHP algorithm aims to authenticate V2V communications based on legitimate vehicles. In other words, only authorized vehicles will be allowed to interact with other vehicles. When a vehicle user moves from the previous RSU coverage area to the current RSU coverage area, handover authentication is conducted to transfer the packet and the authentication data from the previous RSU to the next RSU. To ensure the security of data transmission, the communication entity must be verified before the information is ready for transmission. Accordingly, when vehicle V_Q wants to send a message to V_R, it sends a request message and records the timestamp of the request. Next, vehicle V_R records the timestamp of the received request, and if it takes too long, the request will be invalidated. Moreover, our proposed algorithm checks the authentication in each vehicle, and if it is correct, the data is shared; otherwise, it is considered a malicious node. Then the proposed method perform the following steps.

Each vehicle is assigned a distinct identity and secret key in our proposed algorithm. Hither, $\mathcal{V}_{v_q}$ is a unique identity $(\mathcal{J}_d)$ of the vehicle $\mathcal{V}_q$. Then, the proposed trust authority $(T_{\mathcal{A}})$ generates their own secret key $\mathcal{S}$, as shown in equation,

$$\mathfrak{G}_{\mathbb{T}a} = \mathfrak{G}\left(\mathfrak{Ib} \parallel \mathfrak{R}_{\mathbb{T}_a}\right) \tag{23}$$

Assuming that, $\mathbb{G}$ is a hash function and $\mathbb{R}$ is a random number created by the trust authority. Then we register the vehicle unique ID and secret key parameters in the table it will estimate the following equation,

$$\beta_{\mathcal{V}_q} = \mathbb{G}(\mathcal{J}_{\mathcal{V}_q} \parallel \mathbb{G}_{\mathcal{V}_q}) \tag{24}$$

Assuming that, $\mathbb{G}_{\mathcal{V}_q}$ denotes secret key for $\mathcal{V}_q$. Then $\mathcal{V}_q$ calculates the parameter $\vartheta_{\mathcal{V}_q}$ in below equation:

$$\beta_{\mathbb{V}_Q} = S\left(\mathcal{J}\mathfrak{b}_{\mathbb{V}_Q} \parallel \mathfrak{G}_{\mathbb{V}_Q}\right) \tag{25}$$

Let us assume that, ⊕ is a XOR operation. Then $\mathbb{G}_{\mathcal{V}_q}$ and $\mathbb{R}_{\mathcal{V}_q}$ parameters are estimated in below equation.

$$\mathcal{Q}_{\mathbb{V}_Q} = S\left(\mathcal{I}\mathfrak{d}_{\mathbb{V}_Q} \parallel \beta_{\mathbb{V}_Q}\right) \tag{26}$$

$$\mathfrak{R}_{V_Q} = \mathfrak{G}(\mathfrak{S}_{V_Q} \| \beta_{V_Q}) \tag{27}$$

Further, trusted authorities calculate the parameter $\mu_{T_{\mathcal{A}}}$,

$$\mu_{T_a} = \mathfrak{G}(\vartheta_{V_Q} \| \rho_{T_a}) \oplus \mathfrak{S}_{T_a} \tag{28}$$

Afterwards, the parameters $\mu_{T_{\mathcal{A}}}$ and $\mathbb{R}_{\pi_d}$ are transmitted to the $\mathcal{V}_q$ vehicle. Once the $\mathcal{V}_q$ vehicle receives the parameters, it reserves them in the tamper-resistant device within the table. The vehicle stored own parameters is $\{\beta_{\mathcal{V}_q}, \mu_{T_{\mathcal{A}}}, \mathbb{R}_{\pi_d}\}$ called tamper proof device.

Then $\mathcal{V}_q$ computes the subsequent parameters to transmit the request,

$$\mathcal{P}_c = \mathbb{G}(\mathbb{G}_{T_{\mathcal{A}}} \parallel t_{\mathcal{S}}) \oplus \mathbb{R}_{T_{\mathcal{A}}} \tag{29}$$

The above equation creates the broadcasting message format based on the timestamp for transmission. Then, the transmission request is formulatted below the equation.

$$T_{\text{req}} = \mathcal{G}_{\text{req}} \oplus \mathcal{P}_c \oplus \mathbb{G}_{T_{\mathcal{A}}} \oplus t_{\mathcal{S}} \tag{30}$$

Lastly, the vehicle $\mathcal{V}_q$ communicates parameters $\{\mathcal{P}_c, T_{\text{req}}, t_{\mathcal{S}}\}$ towards the $\mathcal{V}_R$. Hither, $t_{\mathcal{S}}$ denotes timestamp that communicated request.

Vehicle $\mathcal{V}_R$ collects the incoming request parameters $\{\mathcal{P}_c, T_{\text{req}}, t_{\mathcal{S}}\}$ to replay the message which is called $\mathcal{T}$. If $\mathcal{T}$ is delayed, the following inequality is computed.

$$\mathcal{T} - t_{\mathcal{S}} \geq \Sigma_t \tag{31}$$

Assuming that, Σ_t denotes total time for message request. Perhaps if the delay is too long, the received parameters will expire. So, our proposed method instantly stops their vehicle communication.

Perhaps if the delay is too long, the received parameters will expire. So, our proposed method stops its vehicle communication. If the delay is fewer, it goes to the next step, i.e. node (vehicle) $\mathcal{V}_R$ sends a reply to node (vehicle) $\mathcal{V}_q$. For security reasons, the reply is encrypted when it is sent. It is calculated by the equation below,

$$\mathbb{M}_{\nabla} = \mathfrak{Z}(\mathbb{V}_{\mathcal{R}} reply + \mathfrak{S}_{\mathbb{T}} \dashv) \tag{32}$$

Finally, the vehicle $\mathcal{V}_R$ transmits the parameters $\{\mathcal{T}, M_r\}$ towards $\mathcal{V}_q$. Let us assume that, 3 denotes encryption for vehicle $\mathcal{V}_R$ reply.

Vehicles $\mathcal{V}_q$ and $\mathcal{V}_R$ exchange control packets (request, reply) to obtain each other's information. Once vehicle $\mathcal{V}_q$ gets a reply, it calculates the delay, and if the delay is too high, vehicle $\mathcal{V}_R$ stops the transmission. Moreover, if the response delay is less, our proposed method can authenticate the vehicle and transfer data from vehicle $\mathcal{V}_q$ to vehicle $\mathcal{V}_R$.

$$\mathcal{A}_{code} = \sum_{i=1}^{\mathfrak{n}} \frac{\mathbb{V}_{\mathcal{Q}} \mathbb{J} \mathfrak{b}_i}{\mathfrak{n}} \tag{33}$$

The above equation is used to analyze each vehicle's unique authentication code ($\mathcal{A}_{\text{code}}$). Let us assume, n denotes number of vehicles. Then compute the handover policy for data communication. Assuming that, handover policy is denoted as $\mathbb{G}_{\beta_{q1}}$ and $\mathbb{G}_{\beta_{q2}}$.

$$\mathfrak{G}_{\beta_1} = \mathfrak{G}_{rece}(\mathbb{J}_b || \mathfrak{S} || \mathcal{A}_{code}) \tag{34}$$

$$\mathfrak{G}_{\mathfrak{p}2} = \mathfrak{p}k^{(\mathfrak{I}\mathfrak{b}||\mathfrak{G})}$$

Then, handover receiver kept the secret key and vehicle $\mathcal{V}_q$ is sent to the user hand over authentication policy to authorized vehicle $\mathcal{V}_R$. By receipt $\mathbb{G}_{\text{req}}$ and $\mathbb{G}_{\mathcal{V}_q}$, vehicle calculates,

$$0\mathfrak{F}_{\mathfrak{p}\mathfrak{v}_{\mathcal{Q}}} = \mathfrak{G}_{\mathfrak{p}2}^{\mathbb{V}_{\mathcal{R}}, \mathfrak{G}(\mathfrak{I}\mathfrak{b}||\mathcal{A}_{code}||\mathfrak{S})} \tag{35}$$

The above equation is efficiently authenticate the new vehicle $\mathcal{V}_R$ for proficient and secure data transmission in VANET. Figures explain the flow chart for handover authentication with efficient data transmission.

5. Performance analysis

This section presents the results obtained considering security, authentication, throughput, end-to-end delay, reliability of packet delivery ratio, and time complexity parameters. The computer specifications for this performance analysis are Intel(R) Core(TM) i7 CPU @ 3.40GHz and 16 GB of RAM with Windows 10 OS (64-bit).

Table 3 depicts the implementation parameters for secure communication in VANET.

Comparison performance

This section discuss the comparison result of the proposed approach with existing algorithms such as

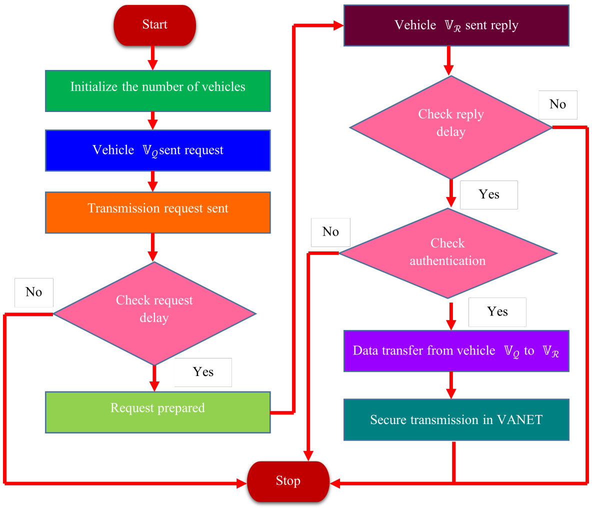
Start
Initialize the number of vehicles
Vehicle $\mathbb{V}_Q$ sent request
Transmission request sent
Check request delay
No
Yes
Request prepared
Vehicle $\mathbb{V}_{\mathcal{R}}$ sent reply
Check reply delay
No
Yes
Check authentication
No
Yes
Data transfer from vehicle $\mathbb{V}_Q$ to $\mathbb{V}_{\mathcal{R}}$
Secure transmission in VANET
Stop

Figure 2. Flow diagram for secure communication

Parameters	Range
Area	900*900m
Structure	VANET
Transmission rate	3 Mbps
Number of vehicle	100
Traffic source	CBR
Packet size	512 bytes
Transmission range	300m

Table 3. Implementation parameters

Certificate-Less Unified Signature (CLAS) is developed by Y. Zhou et al. (2023) and Authenticated Key Agreement (AKA) designed by L. Wei et al. (2022).

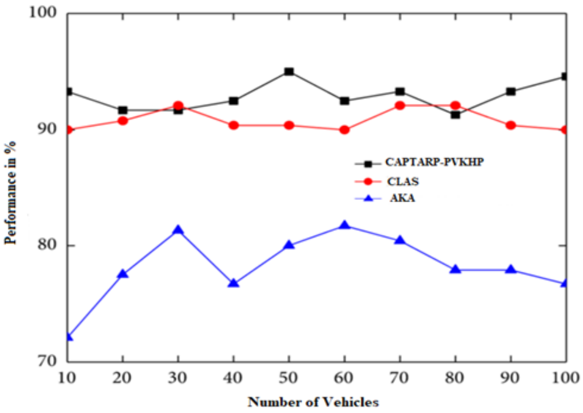

Figure 3. Comparative analysis of throughput performance

Figure 3 clearly shows that result of throughput performance the proposed gradually increase the performance than other methods. This implies that the packet will be processed and sent quickly. As a result, our proposed systems instantly determine authorized vehicles to ensure dependable packet communication in the VANET. The proposed achieved throughput performance is 94.19%.

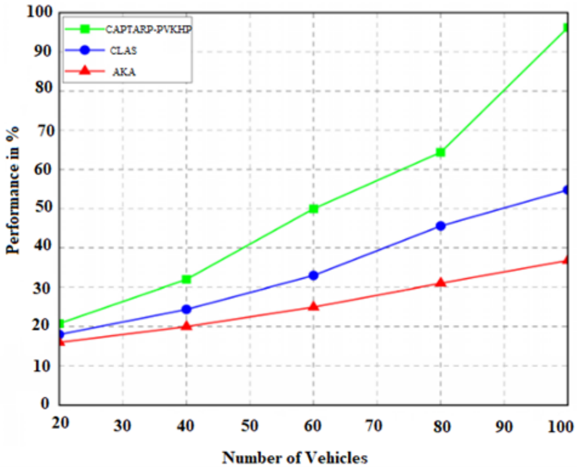

Figure 4. Comparative analysis of Packet delivery ratio

Figure 4 clearly shows that result of Packet delivery ratio performance the proposed gradually increase the performance than other methods. This implies that the packet will be processed and sent quickly. As a result, our proposed systems instantly determine authorized vehicles to ensure dependable packet communication in the VANET. The proposed achieved Packet delivery ratio performance is 96.03%.

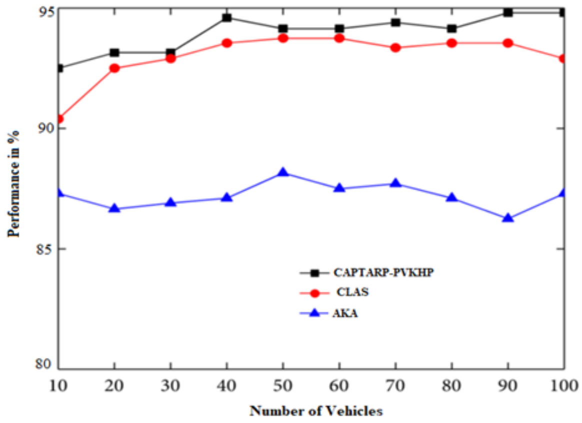

Figure 5. Comparative analysis of Security performance

Figure 5 clearly shows that result of Security performance the proposed gradually increase the performance than other methods. This implies that the packet will be processed and sent quickly. As a result, our proposed systems instantly determine authorized vehicles to ensure dependable packet communication in the VANET. The proposed achieved Security performance is 95.03%.

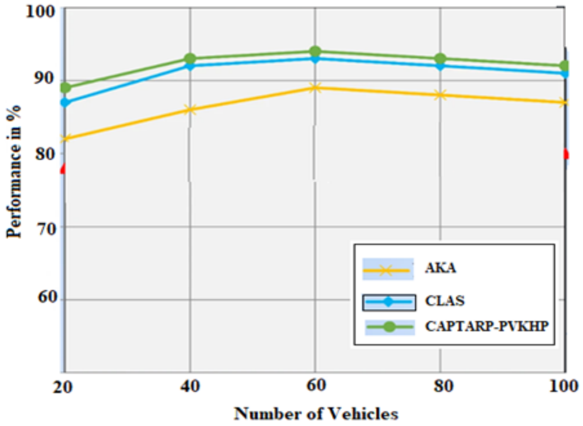

Figure 6. Comparative analysis of Authentication performance

Figure 6 clearly shows that result of Authentication performance the proposed gradually increase the performance than other methods. This implies that the packet will be processed and sent quickly. As a result, our proposed systems instantly determine authorized vehicles to ensure dependable packet communication in the VANET. The proposed achieved Authentication performance is 95.24%.

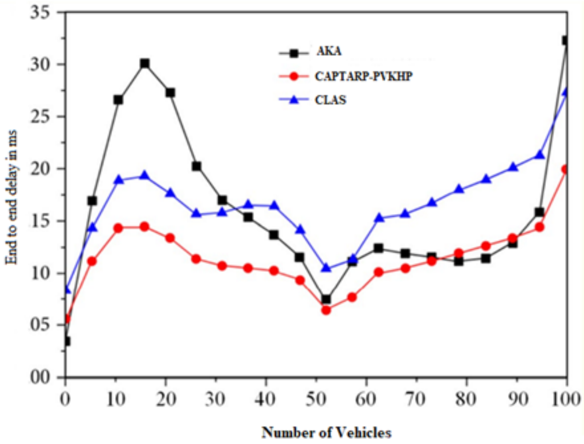

Figure 7. Comparative analysis of End to End delay

As shown in figure 7 describes the end to end delay for secure communication in VANET. The graphical representation of the proposed work attained a fewer end to end delay performance than other conventional methods like AKA and CLAS. The proposed has 18.06ms, while the existing AKA and CLAS algorithm delay performance is 26.05ms and 30.48ms, respectively.

6. Conclusion

To conclude, this paper introduced Context Aware Proactive Trust Aware Routing Protocol (CAPTARP) based on secure Preemptive Verifiable Key Handover Policy (PVKHP) algorithm to solve security issues in VANET environment. The proposed contains mainly two stages are firstly Secure RSU-gated Fuzzy inference system (SRSU-FIS) algorithm is used to find the routing for packet communication. Secondly, Context Aware Proactive Trust Aware Routing Protocol (CAPTARP) is used to improve the secure transmission. Therefore, the proposed simulation result achieved results are throughput is 94.19%, packet delivery ratio is 96.03%, security performance is 95.03%, Authentication performance is 95.24%, and end to end delay performance is 18.06ms. The proposed method attains the efficient results for secure communication in VANET than other methods.

Acknowledgement. The authors wish to express their heartfelt gratitude to the Department of Computer Science, Kaamadhenu Arts and Science College Sathyamangalam, for providing the essential resources and infrastructure to carry out this research. We extend our sincere thanks to our colleagues and mentors for their invaluable feedback and guidance, which significantly contributed to the success of this work.

References

[1] Mahmood J., Duan Z., and Xue H. (2021) *Secure Message Transmission for V2V Based on Mutual Authentication for VANETs*, Volume 2021, Article ID 3400558. https://doi.org/10.1155/2021/3400558.

[2] Manivannan D., Moni S.S., and Zeadally S. (2020) *Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)*, Vehicular Communications, Volume 25, 100247. https://doi.org/10.1016/j.vehcom.2020.100247.

[3] Al-shareeda M.A., Anbar M., Manickam S., and Hasbullah I.H. (2020) *An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Secure Communication in a Vehicular Ad Hoc Network*, Symmetry, 12(10), 1687. https://doi.org/10.3390/sym12101687.

[4] Jing T., Pei Y., Zhang B., et al. (2018) *An efficient anonymous batch authentication scheme based on priority and cooperation for VANETs*, Journal of Wireless Communications and Networking, 2018(277). https://doi.org/10.1186/s13638-018-1294-z.

[5] Xu H., Zeng M., and Hu W. (2019) *Authentication-Based Vehicle-to-Vehicle Secure Communication for VANETs*, Volume 2019, Article ID 7016460. https://doi.org/10.1155/2019/7016460.

[6] Tangade S., Manvi S.S., and Lorenz P. (2020) *Trust Management Scheme Based on Hybrid Cryptography for Secure Communications in VANETs*, IEEE Transactions on Vehicular Technology, 69(5), 5232–5243. https://doi.org/10.1109/TVT.2020.2981127.

[7] Abdelfatah R.I., Abdal-Ghafour N.M., and Nasr M.E. (2022) *Secure VANET Authentication Protocol (SVAP) Using Chebyshev Chaotic Maps for Emergency Conditions*, IEEE Access, 10, 1096–1115. https://doi.org/10.1109/ACCESS.2021.3137877.

[8] Umar M., Islam S.H., Mahmood K., Ahmed S., Ghaffar Z., and Saleem M.A. (2021) *Provable Secure Identity-Based Anonymous and Privacy-Preserving Inter-Vehicular Authentication Protocol for VANETS Using PUF*, IEEE Transactions on Vehicular Technology, 70(11), 12158–12167. https://doi.org/10.1109/TVT.2021.3118892.

[9] Al-Shareeda M.A., Anbar M., Manickam S., and Yassin A.A. (2020) *VPPCS: VANET-Based Privacy-Preserving Communication Scheme*, IEEE Access, 8, 150914–150928. https://doi.org/10.1109/ACCESS.2020.3017018.

[10] Wang P. and Liu Y. (2021) *SEMA: Secure and Efficient Message Authentication Protocol for VANETs*, IEEE Systems Journal, 15(1), 846–855. https://doi.org/10.1109/JSYST.2021.3051435.

[11] Thumbur G., Rao G.S., Reddy P.V., Gayathri N.B., Reddy D.V.R.K., and Padmavathamma M. (2021) *Efficient and Secure Certificateless Aggregate Signature-Based Authentication Scheme for Vehicular Ad Hoc Networks*, IEEE Internet of Things Journal, 8(3), 1908–1920. https://doi.org/10.1109/JIOT.2020.3019304.

[12] Shawky M.A., Bottarelli M., Epiphaniou G., and Karadimas P. (2023) *An Efficient Cross-Layer Authentication Scheme for Secure Communication in Vehicular Ad-Hoc Networks*, IEEE Transactions on Vehicular Technology, 72(7), 8738–8754. https://doi.org/10.1109/TVT.2023.3244077.

[13] Wei L., Cui J., Xu Y., Cheng J., and Zhong H. (2021) *Secure and Lightweight Conditional Privacy-Preserving Authentication for Securing Traffic Emergency Messages in VANETs*, IEEE Transactions on Information Forensics and Security, 16, 1681–1695. https://doi.org/10.1109/TIFS.2020.3040876.

[14] Zhou Y., Wang Z., Qiao Z., Yang B., and Zhang M. (2023) *An Efficient and Provably Secure Identity Authentication Scheme for VANET*, IEEE Internet of Things Journal, 10(19), 17170–17183. https://doi.org/10.1109/JIOT.2023.3273234.

[15] Alshudukhi J.S., Mohammed B.A., and Al-Mekhlafi Z.G. (2020) *Conditional Privacy-Preserving Authentication Scheme Without Using Point Multiplication Operations Based on Elliptic Curve Cryptography (ECC)*, IEEE Access, 8, 222032–222040. https://doi.org/10.1109/ACCESS.2020.3044961.

[16] Ali I., Lawrence T., Omala A.A., and Li F. (2020) *An Efficient Hybrid Signcryption Scheme With Conditional Privacy-Preservation for Heterogeneous Vehicular Communication in VANETs*, IEEE Transactions on Vehicular Technology, 69(10), 11266–11280. https://doi.org/10.1109/TVT.2020.3008781.

[17] Ali I., Hassan A., and Li F. (2019) *Authentication and privacy schemes for vehicular Ad Hoc networks (VANETs): A survey*, Vehicular Communications, 16, 45–61.https://doi.org/10.1016/j.vehcom.2019.02.002.

[18] Nandy T., et al. (2021) *A Secure, Privacy-Preserving, and Lightweight Authentication Scheme for VANETs*, IEEE Sensors Journal, 21(18), 20998–21011. https://doi.org/10.1109/JSEN.2021.3097172.

[19] Ali I. and Li F. (2020) *An efficient conditional privacy-preserving authentication scheme for vehicle-to-infrastructure communication*

in VANETs, Vehicular Communications, 22.https://doi.org/10.1109/TVT.2020.3008781.

[20] Lee J., Kim G., Das A.K., and Park Y. (2021) *Secure and Efficient Honey List-Based Authentication Protocol for Vehicular Ad Hoc Networks*, IEEE Transactions on Network Science and Engineering, 8(3), 2412–2425. https://doi.org/10.1109/TNSE.2021.3093435.

[21] Saleem M.A., Al-Shareeda M.A., Anbar M., Hasbullah I.H., and Manickam S. (2023) *Provably Secure Conditional-Privacy Access Control Protocol for Intelligent Customers-centric Communication in VANET* IEEE Transactions on Consumer Electronics, doi: 10.1109/TCE.2023.3324273.

[22] Al-Shareeda M.A., Anbar M., Hasbullah I.H., and Manickam S. (2021) *Survey of Authentication and Privacy Schemes in Vehicular ad hoc Networks* IEEE Sensors Journal, vol. 21, no. 2, pp. 2422-2433, doi: 10.1109/JSEN.2020.3021731.

[23] Wei L., Cui J., Zhong H., Xu Y., and Liu L. (2022) *Proven Secure Tree-Based Authenticated Key Agreement for Securing V2V and V2I Communications in VANETs* IEEE Transactions on Mobile Computing, vol. 21, no. 9, pp. 3280-3297, doi: 10.1109/TMC.2021.3056712.

[24] Xie Q., Ding Z., and Zheng P. (2023) *Provably Secure and Anonymous V2I and V2V Authentication Protocol for VANETs* IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 7, pp. 7318-7327, doi: 10.1109/TITS.2023.3253710.

[25] Cui J., Zhang X., Zhong H., Zhang J., and Liu L. (2020) *Extensible Conditional Privacy Protection Authentication Scheme for Secure Vehicular Networks in a Multi-Cloud Environment* IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1654-1667, doi: 10.1109/TIFS.2019.2946933.

[26] Wang Y., Ding Y., Wu Q., Wei Y., Qin B., and Wang H. (2019) *Privacy-preserving cloud-based road condition monitoring with source authentication in VANETs* IEEE Transactions on Information Forensics and Security, vol. 14, no. 7, pp. 1779-1790.

[27] Ali I., Lawrence T., and Li F. (2020) *An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs* Journal of Systems Architecture, vol. 103, pp. [online] Available: https://doi.org/10.1016/j.sysarc.2019.101692.

[28] Xu Z., He D., Kumar N., and Choo K.-K.R. (2020) *Efficient certificateless aggregate signature scheme for performing secure routing in VANETs* Security and Communication Networks, vol. 2020.doi: 10.1155/2020/5276813.

[29] Xiong W., Wang R., Wang Y., Zhou F., and Luo X. (2021) *CPPA-D: Efficient conditional privacy-preserving authentication scheme with double-insurance in VANETs* IEEE Transactions on Vehicular Technology, vol. 70, no. 4, pp. 3456-3468.