International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2024/34 Volume 11, Issue 4, July – August (2024)

RESEARCH ARTICLE

A Trust-Aware Framework for Reliable Content Dissemination in NDN-Based VANETs Using Hidden Markov Models

Padma Devi S
Department of Computer Science and Engineering, Velammal College of Engineering and Technology, Madurai, Tamil Nadu, India.
paddevima@gmail.com

Dhanalakshmi K
Department of Computer Science and Engineering, PSNA College of Engineering and Technology, Dindigul, Tamil Nadu, India.
dhanalakshmikrs@gmail.com

Received: 05 June 2024 / Revised: 14 August 2024 / Accepted: 21 August 2024 / Published: 31 August 2024

Abstract – Vehicular Ad Hoc Networks (VANETs) play a vital role in intelligent transportation systems where dissemination of trustworthy information is very crucial. Existing trust management schemes and cryptographic techniques in VANET are computationally expensive, which increases latency. To ensure trusted content dissemination in the VANET, the proposed work combines Named Data Networking (NDN) with the Hidden Markov Model (HMM). In NDN, content is searched based on content name rather than IP address which eliminates the need for centralized servers and reduces the latency. HMM is employed to model trustworthiness and improve the authenticity of the content. The Trust-Aware Framework for Reliable Content Dissemination (TAFRCD) consists of four phases, such as trust modeling, trust establishment, trust-based content dissemination, and performance evaluation. Extensive simulation is conducted to assess the efficiency of this strategy by comparing it with existing approaches like NOTRINO and TROVE in terms of trust detection accuracy, content retrieval latency, network overhead, and dissemination efficiency. The results reveal that TAFRCD ensures trustworthy communication in VANET better than existing content distribution and trust management schemes.

Index Terms – Vehicular Ad Hoc Networking (VANET), Named Data Networking (NDN), Content Dissemination, Intelligent Transportation Systems (ITS), Machine Learning, Hidden Markov Model (HMM).

1. INTRODUCTION

In the realm of Intelligent transportation systems, VANET plays a pivotal role. VANETs enable real-time communication between vehicles which is useful in many applications like infotainment, exchanging roadside information, parking-related information, traffic congestion, etc. Due to the high mobility nature of VANET, it is difficult to disseminate the content, get the required content within the stipulated time, and check whether the content comes from a trusted source or not.

As an indispensable component of the intelligent transportation system, VANET mandates content disseminated in the network must be dependable and trustworthy. Several techniques such as encryption, Digital Signatures, and Trust management techniques have been proposed to address the issues. They ensure the accuracy and authenticity of the content, but they are computationally expensive and resource-intensive which increases the latency in disseminating the content. VANET's dynamic environment necessitates the deployment of effective and adaptive content dissemination mechanisms in the network. Besides, the trustworthiness of the information disseminated can be compromised by cryptographic techniques which are vulnerable to attacks like replay and man-in-the-middle attack. For example, Cooperative collision avoidance systems rely on vehicles exchanging their positions and speed to detect potential collisions and take preventive actions. Existing trust management techniques struggle to ensure the integrity and accuracy of the exchanged data. Malicious vehicles could manipulate their reported positions or velocities without reliable trust mechanisms, leading to false collision warnings or ineffective collision avoidance maneuvers.

The rationale for this study stems from the advantages and disadvantages of the current trust management techniques in VANETs. Current schemes such as reputation-based trust, blockchain-based trust, and machine learning-based models offer various advantages including enhanced security and privacy preservation. The study reveals constraints such as higher complexity overhead, scalability challenges, and reliance on centralized authorities for efficient functioning. These drawbacks highlight the need for an innovative approach that considers the unique challenges associated with VANET communication.

Instead of the IP address of devices or locations, NDN content is located using the content name. This eliminates the need for the usage of centralized servers, but it enables a caching mechanism that enhances the efficiency of content dissemination. When a vehicle needs content, it sends the request with the content name. The vehicle which has the required content in its cache sends the data packet to the requesting vehicle.

NDN possesses an inherent security mechanism (i.e.) each data packet is signed, ensuring the content's authenticity and integrity [1]. Therefore, it eliminates the need for more complex or resource-intensive cryptographic techniques. Further, NDN enables the vehicle to retrieve the content cached in a nearby vehicle, eliminating the need to find the precise location of the content. Therefore, it is more suitable for VANET, where topology changes frequently.

This research paper unveils an innovative strategy for securing trusted content dissemination in VANETs based on Named Data Networking (NDN), employing the Hidden Markov Model (HMM). Incorporating the HMM is intended to enhance the reliability and authenticity of the content. Through a series of trust evaluation techniques using HMM, reliable content sources are identified, and trustworthy communication is established.

Through this research, we aim to establish a foundation for enhancing the trustworthiness and security of content dissemination in NDN-based VANETs, thereby contributing to the advancement of intelligent transportation systems, and enabling a safer and more efficient vehicular environment.

This paper's primary contributions include,

1. Development of a conceptual framework for trusted content dissemination in NDN-based VANET.
2. Integration of Hidden Markov Model (HMM) in content-centric NDN to model trustworthiness.
3. Evaluation of the proposed work through extensive simulation and performance analysis with existing trust management schemes.

The article is organized as follows in its subsequent sections: A thorough review of the relevant studies on trust management and content distribution in VANETs is provided in Section 2. Section 3 presents the system model and architecture, outlining the design principles and components of our proposed approach and details the implementation. Section 4 presents the simulation results and performance analysis. Section 5 concludes the article by summarizing key findings and outlining potential avenues for future research.

2. RELATED WORKS

In the contemporary era, VANETs have emerged as a key contributor to the Intelligent transportation system, striving to elevate road safety and effective communication in the roadside environment. However, ensuring trusted communication in VANET is a challenging task since they are highly dynamic and susceptible to security threats. This section aims to review existing research on trusted content dissemination in VANET, focusing on approaches that incorporate machine learning models within the Named Data Networking (NDN) framework.

2.1. VANETs & Content Dissemination

The main objective of routing in Named data networking (NDN) is to address the inefficiencies that are prevalent in IP-based networks. The main advantages of stateful and adaptive forwarding operations are simplified vehicle configuration, elimination of the need for network configuration changes, and use of unique names to seek and locate the content [2]. Since content names do not require prior IP setting, they are a good option for location- and time-sensitive applications in the VANET situation. Various strategies have been proposed for content dissemination in VANET.

- Epidemic Routing: It is a broadcast-based routing technique where each vehicle broadcasts a message to all its neighbors and each neighbor does the same until the message is broadcast to all the vehicles in the network. Though this method ensures a higher content delivery ratio, it leads to high network overhead in dense traffic scenarios [3].
- Geographic Routing: Geographic routing [4]–[7] utilizes only geographical information of vehicles to disseminate the content. Messages are forwarded only to the specific geographical region. Nevertheless, the success of this routing approach solely depends on the precise location information, posing challenges in a highly dynamic and unpredictable vehicular environment.
- Probabilistic-Based Routing: Probabilistic-based routing [8]–[11] is a balance between epidemic and controlled dissemination. It decides whether the vehicle must broadcast the content or not based on the probability. It can achieve controlled dissemination and reduced overhead but there is a trade-off between coverage and efficiency.
- Cache-Based Dissemination: This technique [12]–[14] leverages the storage capabilities of vehicles to store and forward the content. Caching enhances content availability

and reduces network congestion. However, it has certain limitations such as cache management overhead, stale and inconsistent cache content, and limited cache size.

2.2. Trusted Content Dissemination

VANET faces several security challenges [15], [16] in content dissemination due to its dynamic and open nature. Ensuring content security is crucial to maintaining the integrity, privacy, and reliability of vehicular communication.

The main security challenges in VANET are data integrity, authenticity, privacy, message authentication, DoS attacks, Sybil attacks, content pollution, trust management, certificate issues, secure routing, and key management.

- Privacy-Preserving Techniques: Privacy-preserving techniques such as Message Authentication Acceleration Protocol (MAAC), proxy signatures, and privacy-preserving data forwarding schemes aim to protect the privacy of the vehicles and location information while still allowing for secure communication and authentication in VANET. The main strengths of these techniques are the protection of location privacy, secure communication, Anonymity, and Resilience to attacks. It makes content dissemination more trustworthy to drivers and stakeholders. But these techniques also have several weaknesses such as increased complexity overhead, limited scalability, trade-off between privacy and security, and need for trusted authorities [17].

- Reputation-Based Trust: In the realm of reputation-based trust [18], agents make trust decisions about other agents based on records of their prior actions based on legitimate sources, rather than relying on credentials. Reputation values are mapped to producers or connected to individual content objects, which enables proactive decision-making on the reliability of a producer's future content. The challenges in implementing reputation-based trust in NDN include the need to explore distinctive design options and quantify performance trade-offs, develop incentive-based mechanisms to encourage accurate rating, and prevent malicious behavior. They also address privacy concerns related to the dissemination of reputation information.

- Blockchain-Based Trust Management: Blockchain-based trust management scheme [19] allows vehicles to use certificates to request location-based services without revealing their confidential information, ensuring the privacy and security of the vehicles. It also includes a reputation-based incentive mechanism to encourage honesty and discourage malicious behavior. Yet, the incorporation of blockchain systems may introduce complexity and resource-intensive demands which may pose challenges in terms of reliability and efficiency.

- Machine Learning-Based Trust Models: In Machine learning-based trust model [20], the trust assessment model calculates individual trust attributes numerically by combining mathematical techniques with intelligent machine learning techniques. This method, which uses minimum outliers and maximum border separation, can distinguish between trustworthy and malevolent contact. It provides a systematic approach to looking at the information and analyzing every aspect of trust. Despite these considerations, the centralization of the trust computation platform is the primary premise of this study.

- Misbehaviour Detection Using Entropy and Threshold Analysis: The authors of [21]suggest an approach for detecting misbehavior, employing entropy and threshold analysis for node-level examination. A binary classification model is created through the utilization of machine learning and logistic regression in this context. This approach reduces monitoring and processing overheads by using flow sampling and processing instead of traditional packet processing. But here the need for a large dataset of flow samples to train the binary classification model which may be difficult to obtain in some scenarios.

- Fuzzy Rule-Based Neural Networks for Intruder Detection: In this work [22], the authors mention the use of fuzzy rule-based encoder perceptron neural networks for intruder detection in VANET. This technique improves communication and intruder detection in VANET, but it may incur some processing overhead.

Table 1Comparison of Existing Approaches

Ref . No	Approach	Pros	Cons
3	Epidemic Routing	High content delivery ratio	High network overhead in dense traffic
4	Geographic Routing	Efficient for location-based services	Depends on precise location information
11	Probabilistic-Based Routing [8]-[11]	Controlled dissemination, reduced overhead	Trade-off between coverage and efficiency
14	Cache-Based Dissemination [12]-[14]	Enhances content availability	Cache management overhead, inconsistent content
17	Privacy-	Secure	Increased

	Preserving Techniques [17]	communication, anonymity	complexity, limited scalability
18	Reputation-Based Trust [18]	Proactive decision-making on reliability	Design complexity, privacy concerns
19	Blockchain-Based Trust Management [19]	Ensures privacy and security	Complexity, resource-intensive
20	Machine Learning-Based Trust Models [20]	Systematic trust analysis	Centralization concerns
21	Misbehavior Detection [21]	Reduces monitoring overheads	Requires large dataset
22	Fuzzy Rule-Based Neural Networks [22]	Improves communication and detection	Processing overhead

Existing approaches to content dissemination and trust management in VANETs, including epidemic, geographic, probabilistic-based, and cache-based techniques, each have advantages but also suffer from drawbacks like high network overhead, reliance on precise location data, and cache management issues (Table 1). Current security measures such as privacy-preserving techniques, reputation-based trust, and blockchain-based models introduce complexity, demand substantial computational resources, and struggle with scalability in the dynamic environment of VANETs. To address these challenges, the proposed Trust-Aware Framework for Reliable Content Dissemination (TAFRCD) integrates Named Data Networking (NDN) with the Hidden Markov Model (HMM), combining NDN's low latency and decentralized nature with HMM's capability to model trust and ensure content authenticity. TAFRCD offers a structured and efficient solution for trustworthy communication in VANETs, aiming to overcome the limitations of existing methods and significantly enhance network performance.

2.3. Problem Statement

Vehicular Ad hoc Networks (VANETs) are essential for intelligent transportation systems, but their dynamic and decentralized nature makes them vulnerable to security threats, including data breaches and malicious attacks. Existing trust management and cryptographic techniques are often computationally intensive, leading to latency that impedes real-time applications. Additionally, current content dissemination strategies face challenges such as high network overhead and inefficient trade-offs between coverage and efficiency. This research proposes a Trust-Aware Framework for Reliable Content Dissemination (TAFRCD) that integrates Named Data Networking (NDN) with the Hidden Markov Model (HMM) to enhance trust, reduce latency, and improve overall network performance.

3. PROPOSED WORK

In this Proposed Work, NDN and HMM are combined to improve the efficiency of trusted content dissemination in VANET. Since VANET is highly dynamic, NDN is more suitable for content dissemination. In NDN, content is searched based on the content name rather than an IP address. Therefore, when NDN is used along with VANET, it eliminates the need for allocating IP addresses for vehicles for identification. HMM uses a statistical modeling technique where the underlying system uses a Markov process with hidden states. Vehicle needs more reliable and trusted data on the move, hence HMM is used to assess the trustworthiness of the data. HMM uses probabilities to assess how trustworthiness changes over a while. It helps to identify the patterns that are not visible in a dynamic environment. HMM models are constructed by analyzing the data from the past. Once HMM is trained using these data, it tries to predict the trustworthiness of the incoming content. By integrating HMM and NDN, the proposed framework creates a reliable and secure environment for sharing information among vehicles. Trust is a complex concept in a dynamic environment. It is affected by numerous factors such as reputation, security measures, reliability of content, context, social influence, transparency, accountability, and user experience. Trust also changes over time which becomes difficult to assess. HMM is a suitable modeling technique for trust because it models trust using hidden states which means it can capture and understand the unseen aspect of the trust.

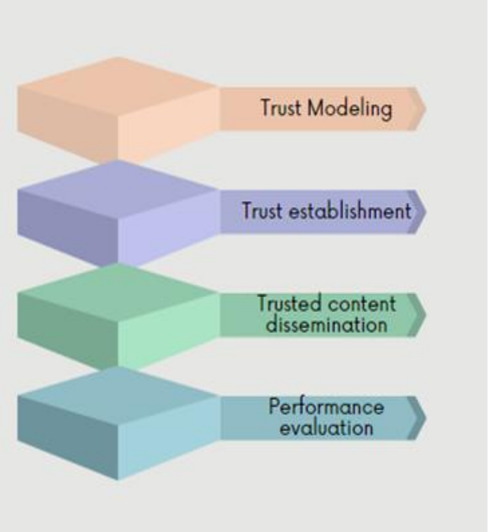

Figure 1 Key Steps in TAFRCD

The proposed framework consists of four phases (Figure 1)

1. Trust Modelling – A Trust model (Algorithm 1) is created using HMM. It captures the dynamic trustworthiness of the producers using past interactions, reputation, and context. It provides a comprehensive way to evaluate trust.
2. Trust Establishment **-** In this phase, a trust establishment algorithm (Algorithm 2) is implemented which is developed based on the trust model to establish trustworthy communication. It involves the exchange of trust-related information and trust scores to verify the authenticity and reliability of content sources. It ensures that only reliable content is disseminated in the network.
3. Trust-based content dissemination – This phase combines the advantages of NDN which focuses on the content with the trust model. It prioritizes content from various sources based on the trust level and facilitates content caching and retrieval (Algorithm 3).
4. Performance Evaluation – Here the performance of TAFRCD is evaluated by conducting extensive simulation using the mobility model and content semination scenario. Then the results are compared with existing approaches like NOTRINO [23] and TROVE [24].

```
Input: Interaction history between vehicles in the VANET
Output: Trust scores for content producers and consumers
1. InitializeHMMParameters ():
   - Set the number of hidden states, H
   - Set the number of observable events, O
   - Initialize transition matrix A with dimensions H x H
   - Initialize emission matrix B with dimensions H x O
   - Initialize initial state distribution $\pi$ with dimensions 1 x H
2. ConstructInteractionHistory ():
   - Gather and organize the interaction history between vehicles in the VANET
3. InitializeHMM ():
   - Assign initial probabilities to the hidden states in $\pi$
   - Randomly initialize the transition(A) and the emission matrix(B).
4. TrainHMM ():
   - Use the interaction history to estimate the transition (A) and emission matrix (B).
   - Apply Baum-Welch algorithm to update the parameters based on observed interactions
5. EvaluateTrust(entity):
   - Create a sequence of observed trust factors for the given entity
   - Implement the Viterbi algorithm to determine the possible sequence of hidden states (trust levels)
   - Calculate the trust score by aggregating the probabilities of the hidden states associated with trustworthy or untrustworthy levels
6. UpdateHMM ():
   - Update the HMM parameters based on new interaction data
   - Incorporate the newly observed trust factors into the emission matrix B
   - Adjust the transition probabilities in the transition matrix A based on the updated trust levels
7. Repeat steps 5 and 6 as new interaction data becomes available to continuously update and refine the trust model.
```

Algorithm 1 Trust Modelling Using Hidden Markov Models

3.1. Hidden States

In the proposed work, we have defined three hidden states to represent distinct levels of trust: "High Trust" (H), "Medium Trust" (M), and "Low Trust" (L). These states capture the varying degrees of trustworthiness that a vehicle can possess in the VANET.

3.2. Observable Events

3.2.1. Interaction Types

- Content Request (CR): Vehicle V sends a request to vehicle S for specific content.
- Content Response (CRes): Vehicle S responds to Vehicle V's content request.
- Content Forwarding (CF): Vehicle V forwards content received from another vehicle-to-vehicle S.
- Content Verification (CV): Vehicle V verifies the authenticity or integrity of content received from vehicle S.

3.2.2. Communication Metrics

- Signal Strength (SS): The signal strength value indicates the quality of the communication between vehicles V and S.
- Packet Loss (PL): The percentage of lost packets during the communication between vehicles V and S.
- Latency (LT): The time delay experienced during the communication between vehicles V and S.

3.2.3. Reputation Feedback

- Positive Feedback (PF): Feedback received from other vehicles indicating the trustworthiness of vehicle S.
- Negative Feedback (NF): Feedback received from other vehicles indicating the untrustworthiness of vehicle S.

3.2.4. Content Verification Results

- Successful Verification (SV): The content received from vehicle S is successfully verified.
- Tampering Detected (TD): The content received from vehicle S is detected to have been tampered with or modified.

Table 2 Transition Matrix (A)

	High Trust	Medium Trust	Low Trust
High Trust	0.7	0.2	0.1
Medium Trust	0.3	0.5	0.2
Low Trust	0.1	0.3	0.6

Table 3 Emission Matrix for Observable Events and Content Verification Results

	Successful Verification	Tampering Detected
High Trust	0.03	0.02
Medium Trust	0.03	0.02
Low Trust	0.02	0.08

Table 2 shows a sample transition matrix. Table 3 shows a sample emission matrix for the observable event and content Verification results. Here, the emission probability of observing Successful Verification when in a High Trust state is 0.03, indicating a higher likelihood of successful verification for content received from vehicles with a higher trust level. Similarly, the emission probability of observing Tampering Detected when in a Low Trust state is 0.08, suggesting a higher likelihood of detecting tampering or modification in content received from vehicles with a lower trust level.

```
Input: Vehicle V requesting content C from vehicle S
Output: Trust score and trust certificate for vehicle S
function TrustEstablishment (V, S):
    trustScore = TrustModel.GetTrustScore(V, S)  // Get trust score for vehicle V from trust model for vehicle S
    if trustScore < threshold:
        trustChallenge = GenerateTrustChallenge()  // Generate a trust challenge for vehicle V
        response = SendTrustChallenge(V, S, trustChallenge)  // Send the trust challenge to vehicle S
        trustScore = EvaluateTrustResponse(S, V, response)  // Evaluate the response and update trust score
        trustModel.UpdateTrustScore(V, S, trustScore)  // Update trust score in trust model for vehicle S
    trustCertificate = GenerateTrustCertificate(S, trustScore)  // Generate trust certificate for vehicle S
    if VerifyTrustCertificate(V, S, trustCertificate):  // Verify the trust certificate by vehicle V
        trustModel.UpdateTrustScore(S, V, trustScore)  // Update trust score in trust model for vehicle V
        return trustScore, trustCertificate
    else:
        return null, null  // Trust certificate verification failed
end function
```

Algorithm 2 Trust Establishment in NDN-Based VANETs Using HMMs

Trust modelling is implemented in a VANET scenario with three hidden states (High Trust, Medium Trust, and Low Trust) and four observable events (Content Request, Content Response, Content Forwarding, and Content Verification).
The Trust Establishment algorithm aims to establish trust between two vehicles, V(Requesting Vehicle) and S(Source Vehicle), in an NDN-based VANET.

The algorithm begins by obtaining the trust score for vehicle V from the trust model associated with vehicle S. If the trust score falls below the trust threshold, a trust challenge is generated by vehicle V and sent to vehicle S. Vehicle S sends the response of trust challenge to vehicle V.

If the vehicle V is satisfied with the response, it updates the trust score in the trust model of both V and S. Based on the trust score, vehicle S generates a trust certificate which is verified by vehicle V. If the trust certificate verification process fails, the algorithm returns null values (Figure 2).

3.3. Trust Score Calculation

The trust score for vehicle V is calculated by vehicle S based on the interaction history.

- Set up the HMM parameters including trust levels (Low, Medium, High), Observable events (interaction history), transition probabilities, and emission probabilities.
- Assume the observation sequence (i.e., interaction history is denoted by O (equation 1) which includes events like Successful communication, reputation feedback, etc.)

$$\mathrm{O} = \left[\mathrm{E}_{1,}\mathrm{E}_{2,}\mathrm{E}_{3,}\ldots\ldots\mathrm{E}_{n,}\right] \quad (1)$$

- Use the Viterbi algorithm to calculate the probabilities for each trust level at each step in the interaction history (using equation 2).

$$\mathrm{V[t,j]} = \mathrm{max}_{\mathrm{k}}\left(\mathrm{V[t-1,k]} \times \mathrm{P(j|k)} \times \mathrm{P(E_1|j)}\right) \quad (2)$$

Here $V[t,j]$ denotes the likelihood of being in state j at time t, $V[t-1,k]$ is the likelihood of being in state k at the previous time step (t-1), $P(j|k)$ is the transition probability from state k to state j, $P(E_1|j)$ is the emission probability of the current observation E_1 given the system is in state j in the context of trust and max_k denotes the maximum value of overall possible states.

In simple terms, given the past trust level and current trust level, what is the probability of being in the current trust level?

- While doing the forward pass, the trust level with the highest probability is stored using the back pointer.
- After processing the entire interaction history, the back pointer is used to trace back and find the most likely sequence of trust levels (as mentioned in equation 3).

$$\boldsymbol{Most\ Likely\ Sequence} = [\boldsymbol{H_1}, \boldsymbol{H_2}, \boldsymbol{H_3}, \ldots\ldots \boldsymbol{H_n}] \quad (3)$$

- Then, the trust score (equation 4) is calculated as

$$\boldsymbol{Trust\ Score} = \mathbf{max}(\boldsymbol{P}(\boldsymbol{H}|\boldsymbol{O}) \quad (4)$$

It means finding the trust level with the highest probability in the most likely sequence obtained from the Viterbi algorithm.

Finally, Trust based content dissemination process starts when a vehicle in the network requests some content. When a vehicle receives the request, it checks whether the requesting vehicle is trustworthy based on HMM. If the requesting vehicle is found to be trustworthy, it checks whether the content is in the cache, if not it rejects the request.

If the content is cached, the content will be sent to the requesting vehicle else the request will be broadcast to the neighbours. When the content is found, the trustworthiness of the source vehicle is also calculated based on the same process. This process ensures that only trusted content is disseminated within the VANET while continuously monitoring and updating the trust scores.

```
procedure TrustBasedContentDissemination(ContentRequest):
    VehicleTrustModel = RetrieveTrustModel(ContentRequest.RequestingVehicle)
    TrustThreshold = 0.7
    TrustScore = CalculateTrustScore(VehicleTrustModel)
    if TrustScore < TrustThreshold:
        MarkVehicleAsUntrusted(ContentRequest.RequestingVehicle)
        DiscardContentRequest(ContentRequest)
    else:
        Content = SearchLocalContentCache(ContentRequest.ContentName)
        if Content != null:
            RespondWithCachedContent(Content, ContentRequest.RequestingVehicle)
        else:
            BroadcastInterestPacket(ContentRequest.ContentName)
            ReceivedResponses = ReceiveContentResponses()
            TrustedResponses = FilterResponsesByTrust(ReceivedResponses, TrustThreshold)
            if Empty(TrustedResponses):
                RespondWithNoContentFound(ContentRequest.RequestingVehicle)
            else:
                AggregatedContent = AggregateResponses(TrustedResponses)
                StoreInLocalContentCache(AggregatedContent)
                RespondWithContent(AggregatedContent, ContentRequest.RequestingVehicle)
                UpdateTrustModel(VehicleTrustModel, ReceivedResponses)
                UpdateTrustScores(ReceivedResponses)
    ContinueTrustMonitoring()
end procedure
```

Algorithm 3 Trust-Based Content Dissemination

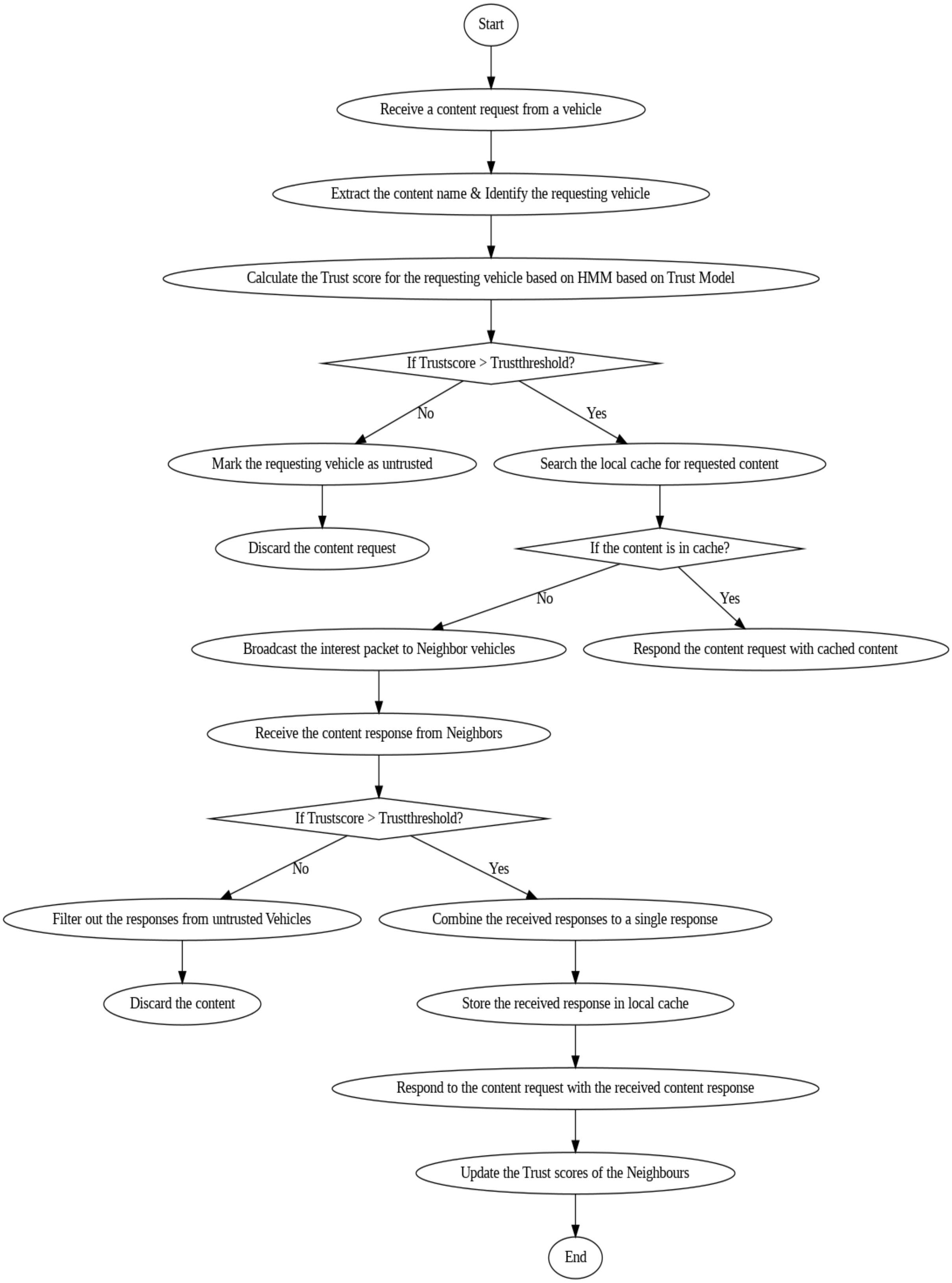
Start
Receive a content request from a vehicle
Extract the content name & Identify the requesting vehicle
Calculate the Trust score for the requesting vehicle based on HMM based on Trust Model
If Trustscore > Trustthreshold?
No
Yes
Mark the requesting vehicle as untrusted
Search the local cache for requested content
Discard the content request
If the content is in cache?
No
Yes
Broadcast the interest packet to Neighbor vehicles
Respond the content request with cached content
Receive the content response from Neighbors
If Trustscore > Trustthreshold?
No
Yes
Filter out the responses from untrusted Vehicles
Combine the received responses to a single response
Discard the content
Store the received response in local cache
Respond to the content request with the received content response
Update the Trust scores of the Neighbours
End

Figure 2 TAFRCD Process

4. PERFORMANCE EVALUATION

This section aims to determine the effectiveness of TAFRCD in mitigating trust-related issues and delivering reliable information in VANETs. This section presents a detailed analysis of the proposed work compared to existing solutions (NOTRINO and TROVE) across various metrics such as trust detection accuracy, content retrieval latency, network overhead, and dissemination efficiency.

4.1. Simulation Setup

The simulation was conducted using the Simulation of Urban Mobility (SUMO) framework with the Random Way Point Mobility model to replicate urban vehicular behavior. A synthetic dataset was created to evaluate TAFRCD across different security scenarios, incorporating various vehicle attributes and content-related factors (Table 4). Key scenarios such as content verification, tampering detection, and trust challenges were simulated alongside temporal factors like timestamps and duration.

Table 4 Simulation Parameter

Sl. No	Simulation Parameter	Values
1	Simulation duration	500
2	Interest Lifetime	4s
3	Vehicle Speed	40-80 Km/hr
4	Simulation run	50
5	Trust update interval	30s
6	Trust threshold	0.7
7	Communication range	150m
8	Traffic density	Moderate
9	Network Topology	Urban
10	Communication Protocol	NDN

4.2. Comparison with Existing Solutions

In [23] NOTRINO, a hybrid trust management scheme ensures trustworthy communication in the Internet of Vehicles (IoV). It combines direct trust (based on direct interactions between vehicles) and indirect trust (based on reputations reported by other vehicles). It aims to enhance road safety and reliability by providing comprehensive trust assessments to varying traffic conditions. The benefits include improved safety, better cyber-attack resistance, and reliable information sharing. However, challenges include the complexity of implementation, reliance on accurate data, potential latency issues, and privacy concerns. In [24] the author proposes a solution (TROVE) to ensure reliable information in vehicular ad hoc networks (VANETs) which enhance driving safety through information sharing. This model evaluates the trustworthiness of received messages by considering the context (time and location) and uses reinforcement learning to improve its trust evaluation strategy over time. It combines internal information from a vehicle's sensors with external information from other vehicles, using an entropy-based calculation method. It is designed to remain accurate, reliable, and resilient against false information. However, implementing this system is complex, relies on data accuracy, and raises privacy concerns.

4.3. Performance Metrics

4.3.1. Trust Accuracy Metrics

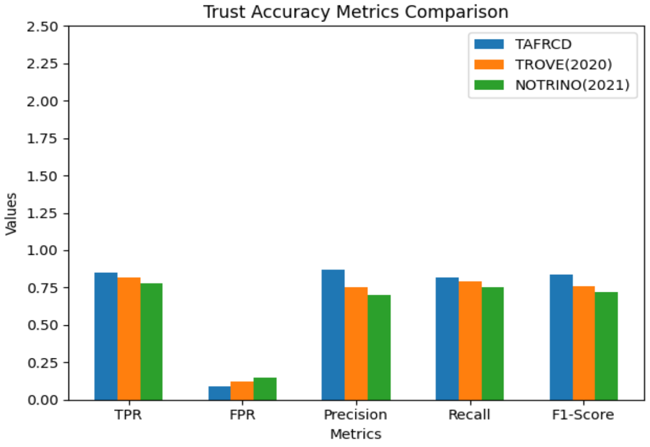

Figure 3 Trust Accuracy Metrics Comparison

Figure 3 demonstrates that TAFRCD consistently achieves higher true positive rates, precision, recall, and F1-score compared to NOTRINO and TROVE. This indicates TAFRCD's superior capability in correctly identifying trustworthy content and minimizing false positives. The enhanced accuracy is due to TAFRCD's integration of Named Data Networking (NDN) with the Hidden Markov Model (HMM), which improves the system’s ability to assess trustworthiness in real-time, thereby outperforming existing solutions.

4.3.2. Trust Detection Accuracy

Trust detection accuracy (equation 5) measures the system’s ability to accurately predict the trustworthiness of vehicular interactions. This is critical for ensuring reliable communication in VANETs.

$$Accuracy = \frac{Number\ of\ Correct\ Predictions}{Total\ Number\ of\ Predictions} \times 100 \qquad (5)$$

Upon analyzing the detection accuracy (Figure 4) of the three approaches—TAFRCD demonstrates higher accuracy rates across all tested scenarios, showcasing its robustness in correctly identifying and detecting relevant content. NOTRINO and TROVE exhibit competitive accuracy scores, albeit slightly lower than TAFRCD, indicating their capability to perform adequately in content detection tasks.

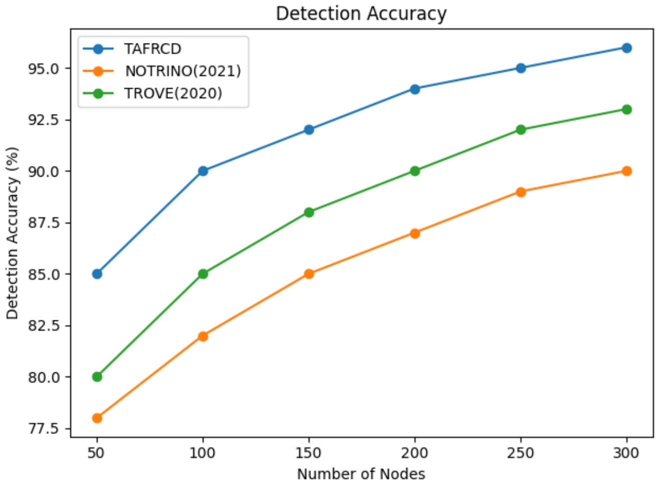

Figure 4 Detection Accuracy

4.3.3. Content Retrieval Latency

Content retrieval latency (equation 6) refers to the time taken to retrieve and deliver content from the source to the requester, which is vital for ensuring timely information dissemination in VANETs.

$$Content\ Retrieval\ Latency = Time\ of\ content\ Retrieval - Time\ of\ Content\ request \qquad (6)$$

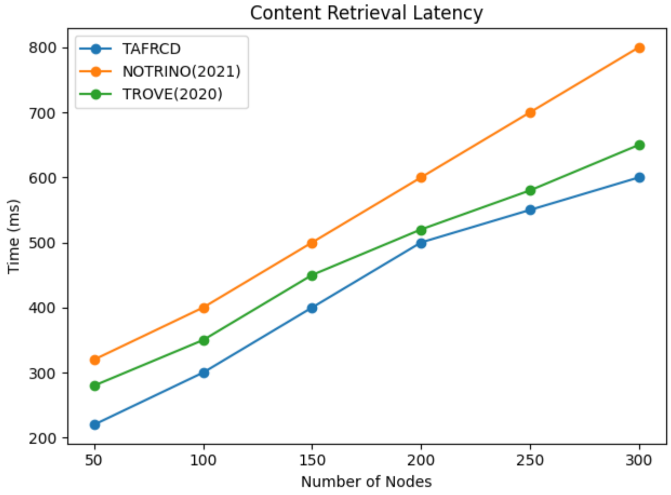

Figure 5 Content Retrieval Latency

Figure 5 shows that TAFRCD consistently exhibits the lowest content retrieval latency compared to NOTRINO and TROVE. The reduced latency can be attributed to TAFRCD’s use of NDN, which eliminates the need for centralized servers and allows content to be retrieved directly based on its name. This streamlined approach significantly enhances the speed of content retrieval, making TAFRCD more efficient than existing models.

TAFRCD's data routing is optimized through its content-centric approach, ensuring that content is retrieved from the nearest available source, further reducing latency.

4.3.4. Network Overhead

Network overhead measures the additional control messages exchanged among vehicles for trust establishment and trust-based content dissemination (equation 7). Lower overhead indicates a more efficient system.

$$Number\ of\ Control\ Packets = Total\ no\ of\ trust\ certificates + Total\ number\ of\ trust\ score\ update \qquad (7)$$

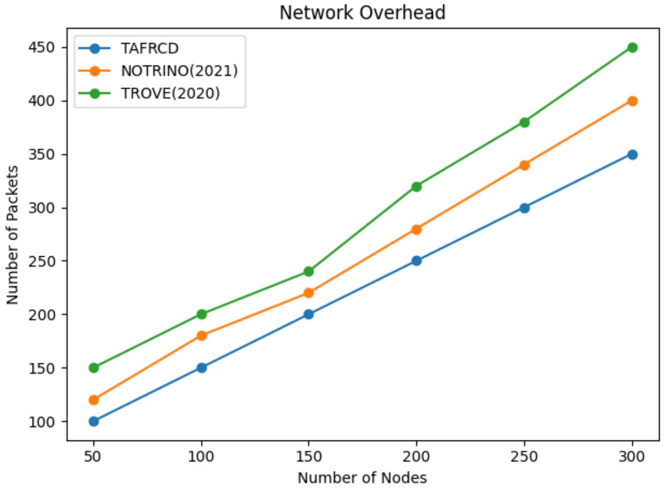

Figure 6 Network Overhead

As depicted in Figure 6, TAFRCD generates the lowest network overhead across all node counts compared to NOTRINO and TROVE. The efficiency in minimizing overhead is due to TAFRCD's optimized packet usage and streamlined trust establishment process, which reduces the number of control packets required for effective content dissemination.

The content-centric nature of NDN combined with TAFRCD’s optimized trust management results in lower network overhead, especially in larger and denser networks. This makes TAFRCD more scalable compared to other models.

4.3.5. Trust-Based Dissemination Efficiency

Trust-based dissemination efficiency is the percentage of trusted content successfully disseminated within the VANET, reflecting the system's ability to effectively distribute reliable information (equation 8).

$$\textbf{\textit{Trust based Dissemination Efficency}} = \frac{\textbf{\textit{Number of Trusted content disseminated}}}{\textbf{\textit{Total number of content}}} \times \mathbf{100} \quad (8)$$

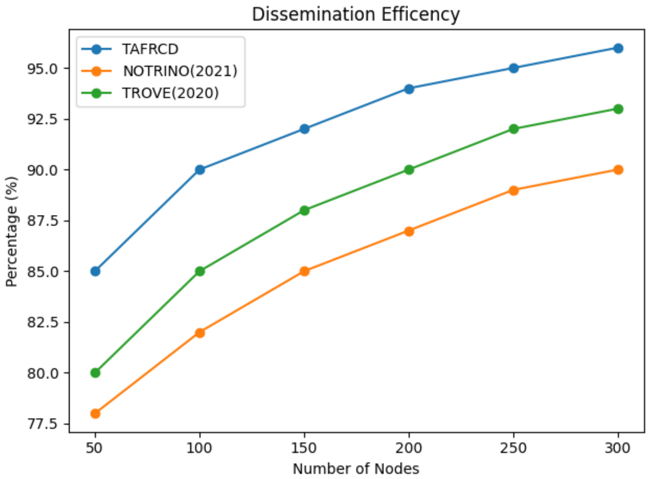

Figure 7 Dissemination Efficiency

Figure 7 illustrates that TAFRCD achieves the highest dissemination efficiency among the three models, followed by TROVE and NOTRINO. The superior dissemination efficiency is a result of TAFRCD's robust trust management mechanism, which ensures that only trustworthy content is propagated throughout the network, thus maximizing the reach and reliability of the disseminated information. The model's ability to adapt to different security scenarios and dynamically adjust trust levels ensures that the most reliable content is always prioritized, enhancing overall network efficiency.

4.3.6. Content Retrieval Latency by Varying Vehicle Speed

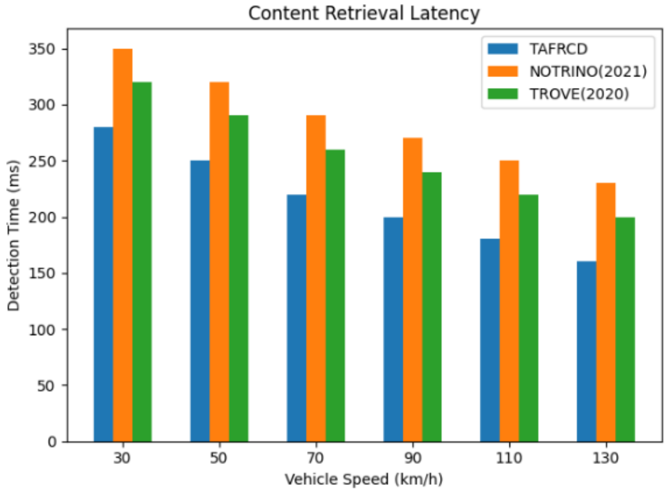

Figure 8 Content Retrieval Latency by Varying Vehicle Speed

Upon examining the content retrieval latency (Figure 8) across different vehicle speeds for the three approaches - TAFRCD consistently achieves the lowest retrieval latency times, indicating its efficiency in swiftly retrieving content across various speeds. TAFRCD consistently showcases quicker retrieval times, highlighting its ability to provide timely access to information.

4.3.7. Detection Accuracy Across Varying Speeds

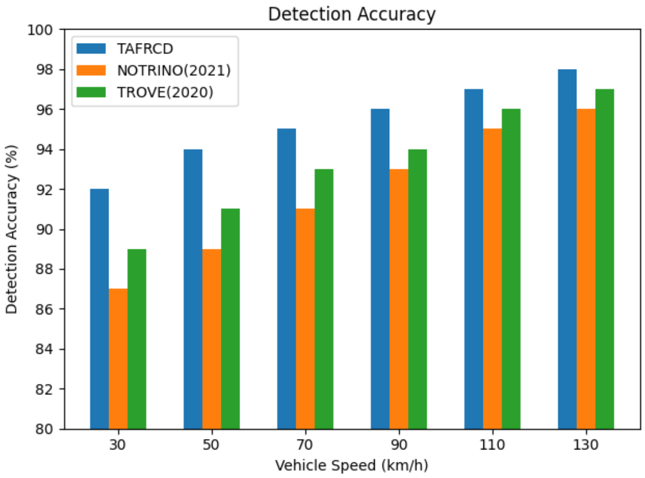

Figure 9 Detection Accuracy by Varying Vehicle Speed

(Figure 9) TAFRCD's trust assessment process remains consistent and accurate across different vehicle speeds due to the dynamic nature of the HMM. This ensures that trust levels are accurately maintained even as network conditions change rapidly. The reliance on content names rather than IP addresses ensures that the detection process is not impacted by the high mobility of vehicles, making TAFRCD more reliable in varying speed scenarios.

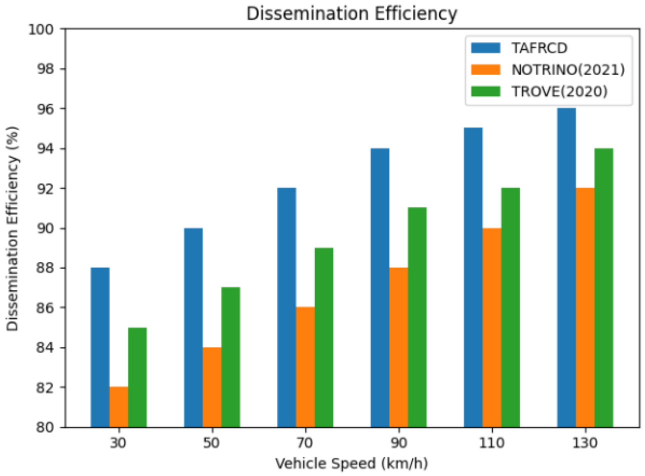

Figure 10 Dissemination Efficiency by Varying Vehicle Speed

The examination of dissemination efficiency across varying vehicle speeds (Figure 10) reveals that TAFRCD consistently achieves higher efficiency levels compared to NOTRINO and TROVE, indicating its ability to effectively disseminate content across different speeds. TAFRCD's content-centric model ensures that content is propagated efficiently across the network, regardless of the speed of the vehicles. This reduces delays and ensures that content reaches all relevant nodes quickly. The model's design inherently handles the challenges posed by high-speed mobility, ensuring that content dissemination remains efficient even in high-speed scenarios.

5. CONCLUSION

In this research work, we have proposed a novel method for securing trusted content dissemination in VANET based on Named data networking and the hidden Markov model. The integration of NDN and HMM improves the trustworthiness and authenticity of content dissemination in VANET by modeling the hidden states through a sequence of trust evaluation techniques. TAFRCD consists of four phases: trust modeling, trust establishment, trust-based content dissemination, and performance evaluation. In the trust modeling phase, a trust model is created using HMM to capture the dynamic trustworthiness of producers based on past interactions, reputation, and context. The trust establishment phase involves the implementation of a trust establishment algorithm to establish trustworthy communication, including the exchange of trust-related information and trust scores. The trust-based content dissemination phase combines the advantages of NDN and the trust model to prioritize content from various sources based on trust level and facilitate content caching and retrieval. Finally, the performance evaluation phase evaluates the performance of the proposed framework through extensive simulation using the SUMO framework and synthetic datasets, comparing it with existing trust management schemes. The performance evaluation results demonstrate the effectiveness and efficiency of the proposed framework. TAFRCD consistently outperforms existing approaches such as NOTRINO and TROVE in terms of trust accuracy, content retrieval latency, network overhead, and dissemination efficiency. By leveraging the advantages of NDN and utilizing HMM for trust modelling and evaluation, TAFRCD contributes to the advancement of intelligent transportation systems and enables a safer and more efficient vehicular environment. Future research can explore further optimizations of the proposed framework, as well as investigate its applicability in real-world VANET scenarios.

REFERENCES

[1] L. Zhang et al., "Named Data Networking (NDN) Project," 2010. [Online]. Available: http://named-data.net/techreports.html. [Accessed: Aug. 5, 2024].

[2] R. W. L. Coutinho, A. Boukerche, and A. A. F. Loureiro, "Design Guidelines for Information-Centric Connected and Autonomous Vehicles," IEEE Communications Magazine, vol. 56, no. 10, pp. 85–91, Oct. 2018, doi: 10.1109/MCOM.2018.1800134.

[3] R. Amici, M. Bonola, L. Bracciale, A. Rabuffi, P. Loreti, and G. Bianchi, "Performance assessment of an epidemic protocol in VANET using real traces," in Procedia Computer Science, Elsevier B.V., 2014, pp. 92–99. Doi: 10.1016/j.procs.2014.10.035.

[4] M. Chaqfeh, A. Lakas, and I. Jawhar, "A survey on data dissemination in vehicular ad hoc networks," Vehicular Communications, vol. 1, no. 4. Elsevier Inc., pp. 214–225, 2014. Doi: 10.1016/j.vehcom.2014.09.001.

[5] S. H. Ahmed, S. H. Bouk, and D. Kim, "RUFS: RobUst Forwarder Selection in Vehicular Content-Centric Networks," IEEE Communications Letters, vol. 19, no. 9, pp. 1616–1619, Sep. 2015, doi: 10.1109/LCOMM.2015.2451647.

[6] C. Bian, T. Zhao, X. Li, and W. Yan, "Boosting named data networking for efficient packet forwarding in urban VANET scenarios," in IEEE Workshop on Local and Metropolitan Area Networks, IEEE Computer Society, May 2015. Doi: 10.1109/LANMAN.2015.7114718.

[7] M. Amadeo, C. Campolo, and A. Molinaro, "CroWN: Content-Centric Networking in Vehicular Ad Hoc Networks", IEEE Communications Letters, doi: 10.1109/LCOMM.2012.12.120282.

[8] L. Liu, C. Chen, T. Qiu, M. Zhang, S. Li, and B. Zhou, "A data dissemination scheme based on clustering and probabilistic broadcasting in VANETs," Vehicular Communications, vol. 13, pp. 78–88, Jul. 2018, doi: 10.1016/j.vehcom.2018.05.002.

[9] S. Dahmane and P. Lorenz, "Weighted probabilistic next-hop forwarder decision-making in VANET environments," in 2016 IEEE Global Communications Conference, GLOBECOM 2016 – Proceedings, Institute of Electrical and Electronics Engineers Inc., 2016. doi: 10.1109/GLOCOM.2016.7842381.

[10] A. Mehmood, A. Khanan, A. H. H. M. Mohamed, S. Mahfooz, H. Song, and S. Abdullah, "ANTSC: An Intelligent Naïve Bayesian Probabilistic Estimation Practice for Traffic Flow to Form Stable Clustering in VANET," IEEE Access, vol. 6, pp. 4452–4461, Jul. 2017, doi: 10.1109/ACCESS.2017.2732727.

[11] R. Kumar and M. Dave, "A framework for handling local broadcast storm using probabilistic data aggregation in VANET," Wireless Personal Communications, vol. 72, no. 1, pp. 315–341, Sep. 2013, doi: 10.1007/s11277-013-1016-0.

[12] W. Huang, T. Song, Y. Yang, and Y. Zhang, "Cluster-Based Cooperative Caching With Mobility Prediction in Vehicular Named Data Networking," IEEE Access, vol. 7, pp. 23442–23458, 2019, doi: 10.1109/ACCESS.2019.2897747.

[13] N. Kumar and J. H. Lee, "Peer-to-peer cooperative caching for data dissemination in urban vehicular communications," IEEE Syst J, vol. 8, no. 4, pp. 1136–1144, Dec. 2014, doi: 10.1109/JSYST.2013.2285611.

[14] E. T. da Silva, A. L. D. Costa, and J. M. H. de Macedo, "On the realization of VANET using named data networking: On improvement of VANET using NDN-based routing, caching, and security," International Journal of Communication Systems, vol. 35, no. 18, Dec. 2022, doi: 10.1002/dac.5348.

[15] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)," Vehicular Communications, vol. 25. Elsevier Inc., Oct. 01, 2020. doi: 10.1016/j.vehcom.2020.100247.

[16] J. Wang, X. Jing, Z. Yan, Y. Fu, W. Pedrycz, and L. T. Yang, "A Survey on Trust Evaluation Based on Machine Learning," ACM Computer Survey, vol. 53, no. 5, Sep. 2020, doi: 10.1145/3408292.

[17] W. Ahmed, W. Di, and D. Mukathe, "Privacy-preserving blockchain-based authentication and trust management in VANETs," IET Networks, vol. 11, no. 3–4, pp. 89–111, May 2022, doi: 10.1049/ntw2.12036.

[18] I. A. Kapetanidou, C. A. Sarros, and V. Tsaoussidis, "Reputation-based trust approaches in Named Data Networking," Future Internet, vol. 11, no. 11. MDPI AG, Nov. 01, 2019. doi: 10.3390/fi11110241.

[19] B. Li, R. Liang, D. Zhu, W. Chen, and Q. Lin, "Blockchain-Based Trust Management Model for Location Privacy Preserving in VANET," IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 6, pp. 3765–3775, Jun. 2021, doi: 10.1109/TITS.2020.3035869.

[20] U. Jayasinghe, G. M. Lee, T. W. Um, and Q. Shi, "Machine Learning Based Trust Computational Model for IoT Services," IEEE Transactions on Sustainable Computing, vol. 4, no. 1, pp. 39–52, Jan. 2019, doi: 10.1109/TSUSC.2018.2839623.

[21] K. Sharshembiev, S. M. Yoo, and E. Elmahdi, "Protocol misbehaviour detection framework using machine learning classification in vehicular Ad Hoc networks," Wireless Networks, vol. 27, no. 3, pp. 2103–2118, Apr. 2021, doi: 10.1007/s11276-021-02565-7.

[22] S. Guleng, C. Wu, X. Chen, X. Wang, T. Yoshinaga, and Y. Ji, "Decentralized Trust Evaluation in Vehicular Internet of Things," IEEE Access, vol. 7, pp. 15980–15988, 2019, doi: 10.1109/ACCESS.2019.2893262.

[23] F. Ahmad, F. Kurugollu, C. A. Kerrache, S. Sezer, and L. Liu, "NOTRINO: A Novel Hybrid TRust Management Scheme for INternet-of-Vehicles," IEEE Transactions on Vehicular Technology, vol. 70, no. 9, pp. 9244–9257, Sep. 2021, doi: 10.1109/TVT.2021.3049189.

[24] J. Guo et al., "TROVE: A Context-Awareness Trust Model for VANETs Using Reinforcement Learning," IEEE Internet Things J, vol. 7, no. 7, pp. 6647–6662, Jul. 2020, doi: 10.1109/JIOT.2020.2975084.

Authors

Padmadevi S received B.E in Computer science and engineering (2004) from Madurai Kamaraj University, Tamil Nadu, India, and M.E in Computer science and Engineering (2007) from Anna University, Tamil Nadu, India. Currently, she is working as an Assistant Professor in the Department of Computer science and engineering, Velammal College of Engineering and Technology, Tamil Nadu. Her research interests include Wireless networks, Mobile Computing, Ad Hoc networks, and VANET. She has published research papers in national and international journals, conference proceedings as well as chapters of books.

Dr. Dhanalakshmi K completed her Ph.D. (Engg) in the area of image mining, from Anna University, Tamil Nadu, India. Currently, she is working as a Professor in the Department of Computer Science and Engineering, PSNA College of Engineering and Technology. Her research interests include Wireless networks, Data mining, Image Processing, Soft Computing, Medical image analysis, and prediction. She is the author of many research studies published in national and international journals as well as conference proceedings.

How to cite this article:

Padma Devi S, Dhanalakshmi K, "A Trust-Aware Framework for Reliable Content Dissemination in NDN-Based VANETs Using Hidden Markov Models", International Journal of Computer Networks and Applications (IJCNA), 11(4), PP: 527-539, 2024, DOI: 10.22247/ijcna/2024/34.