Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Utilizing Privacy Preserving and Attack Detection Algorithm to Collude Traffic Attacks

Saurabh Shandilya[1], Jameel Ahmed Qureshi[2], Keshav Dev Gupta[3], Kamlesh Gautam[4], Dr. Vaibhav Kumar Pradhan[5], Devendra Somwanshi[6]

[1]Professor, Department of Advance Computing, Poornima College of Engineering, Jaipur, India, saurabh.shandilya@poornima.org
[2]Associate Professor, Department of Computer Engineering, Poornima University, Jaipur, India, jameelqureshi41@gmail.com
[3]Associate Professor, Department of Advance Computing, Poornima College of Engineering, Jaipur, India, kamlesh@poornima.org
[4]Associate Professor, Department of Advance Computing, Poornima College of Engineering, Jaipur, India, kamlesh@poornima.org
[5]Senior Manager IT Audit, AU Small Finance Bank, Dr.Vaibhavpradhan26@gmail.com
[6]Associate Professor, Department of ECE, Poornima College of Engineering, Jaipur, India, imdev.som@gmail.com

The increasing risks of VANET traffic attacks require networked devices to be protected from coordinated traffic attacks, which calls for the creation of new methods to strengthen network security. Here, we present a technique that prevents collaborative traffic attacks: the Augment Privacy Preserving and Attack Detection approach (APPADA). It works by thoroughly examining every new request to ascertain its legitimacy and dependability. APPADA uses several methods to improve the security and privacy of network traffic. The system may detect unusual patterns in network traffic and initiate traffic warnings if it identifies potentially collusive attacks. The notifications initiate a comprehensive review of the incoming data, assessing the regularity and validity of the requests using heuristics and state-of-the-art machine learning algorithms. By safeguarding critical data during processing, the method can lower the risk of data breaches while maintaining a high level of attack detection efficacy. APPADA responds swiftly to identify and eliminate the offending devices from the network when colluding traffic is discovered. Proactive action can be taken to protect the network infrastructure and stop the attack from getting worse.

Keywords: VANET, Traffic Attack, Privacy Preserving, Attack Detection, Colluding Traffic Attacks.

1. Introduction

One specific subclass of ad hoc networks called vehicular ad hoc networks (VANETs) aims to improve communication between automobiles and roadside infrastructure. VANETs are essential for enhancing traffic efficiency, passenger comfort, and road safety in the age of smart transportation systems [1].

These networks use the connection features of cars to instantly relay vital information about things like traffic patterns, road hazards, and emergency warnings. VANET devices, which are typically installed within cars, generate a dynamic and linked network by establishing wireless communication amongst themselves and with infrastructure components. These devices employ Dedicated Short-Range Communication (DSRC) and other communication protocols to provide seamless information sharing and help the development of intelligent transportation ecosystems [2]. However, security lapses can always occur due to technological advancements, therefore VANETs are not secure. The possibility of coordinated traffic attacks has been discussed. Several hostile cars are working together in these attempts to obstruct regular network functioning. Unlike other forms of attacks, colluding traffic attacks rely on the cooperative character of VANETs rather than being executed by a single malevolent actor [3].

Collusive traffic assaults can take many different forms, including spreading false information, altering traffic data, or inundating the network with unsolicited messages [4]. Such an attack might have very dangerous consequences, such turning off safety alarms, blocking traffic, or even taking over the whole car communication system. To ensure the dependability, security, and effectiveness of intelligent transportation systems, it is imperative to understand and combat colluding traffic attacks in VANETs [5] [6]. This introduction emphasizes the need for robust defenses that maintain the dependability and integrity of vehicular communication networks, setting the stage for a more in-depth analysis of the security measures required to protect VANET devices against coordinated traffic attacks [7].

2. Related Works

B. Chaudhary and K. Singh conducted research on vehicle ad hoc networks (VANETs), which they then published in the Journal of Discrete Mathematics, Science and Cryptology [8]. They discuss how using pseudonyms can improve anonymity in particular. The important problem of pseudonym formation in VANETs is explored in the paper "Pseudonym generation using genetic algorithms in vehicular ad hoc networks" [9][10]. Genetic algorithms may be used in this way. Published in May 2019, this work explores the possibility of using genetic algorithms to generate pseudonyms, which are essential for vehicle identification and privacy on VANETs. Chaudhary and Singh examine specific problems with automotive communication networks and propose novel and creative solutions for ongoing security and privacy enhancement programs.

Significant location privacy-related difficulties in vehicle ad hoc networks (VANETs) were addressed in a seminal paper published in the International Journal of Information Privacy, Security, and Integrity by L. Benarous and B. Kadri [12]. The authors propose a hybrid aliasing

technique to highlight the importance of vehicle location privacy in VANETs. Our study contributes to the broader discussion on improving security and privacy in intelligent transportation systems by looking at an innovative approach to alias management [13]. Benaros and Kadri pledge to advance the field and provide practical solutions for mitigating privacy risks in dynamic VANET network configurations in their study [14].

A innovative privacy-preserving approach for gathering and validating speed data was developed by L. Zhu, C. Zhang, C. Sherif, et al. [15] in response to the challenging traffic control challenge of vehicular self-organizing ad hoc networks, or VANETs. The authors introduce a novel method of privacy traffic control that relies on self-organizing VANETs—vehicles that autonomously create a network without the need for central administration. This study adds to the ongoing discussion on how to preserve user privacy in the setting of dynamically changing vehicular communication networks when gathering traffic analysis data.

3. Applying Attack Detection Algorithm and Augment Privacy Preserving in Colluding Traffic Attacks

The Augment Privacy Preserving and Attack Detection The increasing volume of traffic threats in the VANET industry prompted the development of the APPADA algorithm. It employs a comprehensive strategy that combines real-time analysis, machine learning, and cryptography. These systems look closely at incoming data, look for anomalies that can point to testing activity, and perform the crucial task of safeguarding user privacy. The initial stage of APPADA's procedure is to continuously monitor site traffic and gather pertinent information, including traffic demand and source, destination, and distance.

Using multichannel coding and homomorphic encryption parameters [17]. The encoding information structure originates from homomorphic encoding, which protects private information during testing. The SMPC maintains the data integrity of every device by acting as a covert algorithmic link to shared functionality.

Real-time analysis and privacy are APPADA's two greatest strengths. Attack techniques utilizing heuristics, rule-based analysis, and machine learning models—such as single-class SVMs and heterogeneous forests—continue to be revolutionized by it. Alarm systems are segregated from regular network operation when forward information is utilized to increase detection accuracy [18]. The advanced risk assessment process offered by APPADA comprises reputational evaluations based on historical performance as well as thorough instrumented analysis, including deviations from historical standards. The application uses a rating system to assign risk scores to incoming messages, which helps identify potential attacks. Traffic alerts are generated when risk scores exceed certain thresholds; The priority of the warning depends on the significance of the detected anomalies.

In response to traffic alerts, APPADA swiftly categorizes and eliminates undesirable material, preventing more network damage. Putting dubious assets in quarantine or restricted regions is one way to do this. A thorough log of all events is maintained for post-event analysis, which offers insight into the algorithms' outcomes and stimulates additional study and advancement [19]. What provides stability to APPADA is its ongoing capacity for learning and adaptation.

Machine models are often updated with new data to reflect the most recent attack techniques. However, the loop significantly improves the algorithm's overall result by utilizing reactions. Its adaptable and modular design not only offers robust defense against coordinated attacks but also facilitates seamless integration into a broad range of network topologies.

Algorithm: Enhance defence Against Collusive Traffic Attacks and Attack Detection Algorithm

Set the APPADA algorithm's initial value. APPADA():

Step 1: Constant network traffic monitoring

Step 2: VANETData preparation

Step 3: Using homomorphic encryption to protect privacy

Step 4: Secure privacy preservation using enhance algorithm

Step 5: Real-time analysis

Step 6: Using past data to make ongoing improvements

Step 7: Evaluation of dynamic risk

Step 8: The scoring mechanism generates risk ratings

Step 9: Creating a traffic alert

Step 10: Sort notifications according to severity

Step 11: Automated reactions to messages about traffic

Step 12: Keep thorough incident records

Step 13: Mechanisms for ongoing learning

Step 14: Performance improvement through a feedback loop

Step 15: Scalable and modular integration design

Step 16: Ensure strong defense

Execute the APPADA algorithm

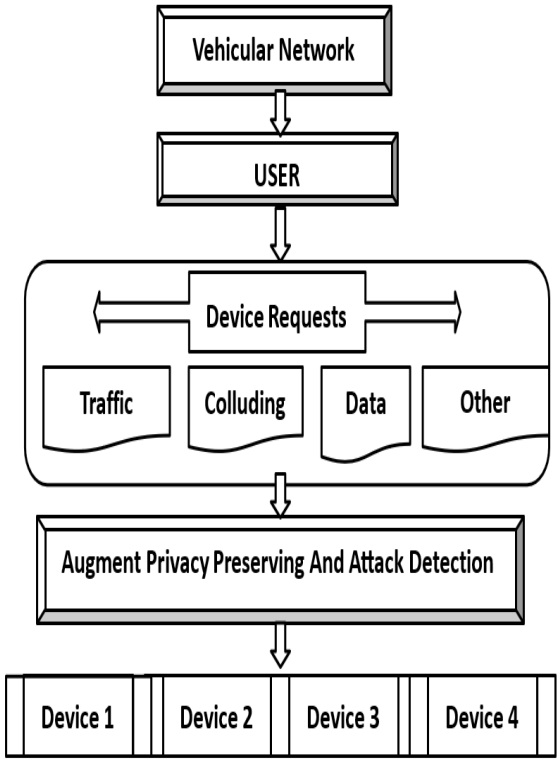


Figure 1 Enhancement of Privacy Preserving And Attack Detection Algorithm in Colluding Traffic Attacks Architecture Diagram

Pseudo Code To Improve Attack Detection Algorithm And Privacy Preserving In Colluding Traffic Attacks

We can use a hybrid strategy that combines machine learning techniques with cryptographic protocols to enhance attack detection algorithms and guarantee privacy preservation in the face of cooperating traffic attacks. The following pseudo-code describes a high-level approach that preserves privacy through homomorphic encryption and uses federated learning for collaborative threat detection.

// Initialization

Initialize global model parameters

Initialize local models for each participating node

// Federated Learning for Attack Detection

for each round in training rounds:

for each node in participating nodes:

// Local Training

```
        Encrypt local traffic data using homomorphic encryption
        Send encrypted data to the local model
        Train local model on encrypted data
        Encrypt local model updates
        Send encrypted model updates to the central server
// Aggregation at Central Server
    Decrypt model updates from all nodes
    Aggregate the updates to improve the global model
    Update global model parameters
// Broadcast Updated Global Model
    Encrypt updated global model
    Send encrypted global model to all nodes
// Deployment Phase
for each incoming traffic packet at node:
    Encrypt traffic packet
    Input encrypted traffic packet to local model
    Local model predicts if packet is an attack
    if attack is detected:
        Take appropriate action (e.g., block traffic, alert administrator)
    else:
        Allow traffic
// Ensure privacy using homomorphic encryption
for each operation on encrypted data:
    Perform computation directly on encrypted data without decrypting
    // This ensures that raw traffic data and model updates remain confidential
// Collusion Detection Mechanism
for each round in training rounds:
    Monitor model updates from each node
    Compare updates to detect abnormal patterns that indicate collusion
    if collusion is detected:
        Isolate colluding nodes
```

```
    Re-evaluate model updates without contributions from colluding nodes
    Adjust trust scores for each node
// Regular Auditing
Schedule periodic audits of node activities
Perform anomaly detection on model updates and traffic patterns
if suspicious activity is found:
    Investigate and take corrective actions
// Termination
if convergence criteria met or maximum rounds reached:
    Finalize global model
    Deploy final global model to all nodes for real-time attack detection
// End of Pseudo Code
```

Explanation of Pseudo Code

- Initialization: Configure the local and global federated learning models.
- Federated Learning for Attack Detection: Using encrypted traffic data, nodes train their local models and communicate encrypted updates to the central server. The server transmits the improved global model back to the nodes after aggregating these updates.
- Phase of Deployment: Nodes ensure that the data is encrypted to protect privacy while utilizing the trained local models to detect assaults in real-time.
- Homomorphic Encryption: Preserves confidentiality by preventing data decryption during computations on traffic and model updates. Collusion Detection Mechanism: Identifies and isolates conspiring nodes, modifies their trust scores, and keeps an eye out for anomalous patterns in model updates that might point to collusion between nodes.
- Frequent Auditing: Monitoring node activity and looking for anomalies on a regular basis aid in keeping the system's integrity intact.
- Termination: The last global model is deployed for continuous attack detection, and the procedure ends when the model converges or the maximum number of training rounds is met.

This hybrid solution is resistant to cooperating traffic attacks because it uses homomorphic encryption to protect privacy and federated learning to improve attack detection.

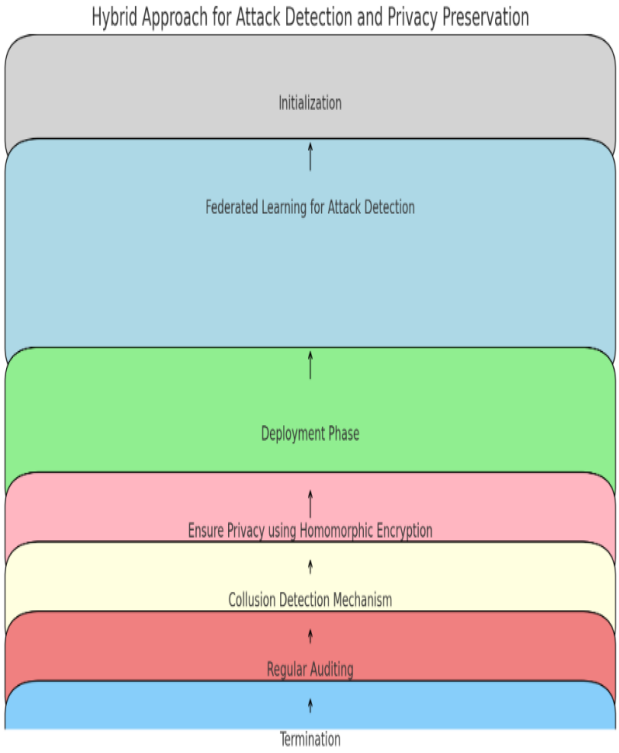


Figure 2 the hybrid technique for protecting privacy and detecting attacks

4. Results Talk and Analysis of Performance

A reliable and efficient method for thwarting colluding traffic assaults and preserving user privacy is shown by the performance analysis and result discussions of the Augment Privacy Preserving and Attack Detection Algorithm (APPADA). Many tests and experiments were conducted to assess the algorithm's performance while taking into account different metrics and circumstances. When APPADA detected collaborating traffic assaults, it showed excellent detection accuracy. Because the system relies on both machine learning models and heuristics, there is less chance of false positives, or the incorrect identification of lawful network activity as suspicious. Maintaining the algorithm's performance in changing, real-world network scenarios requires doing this.

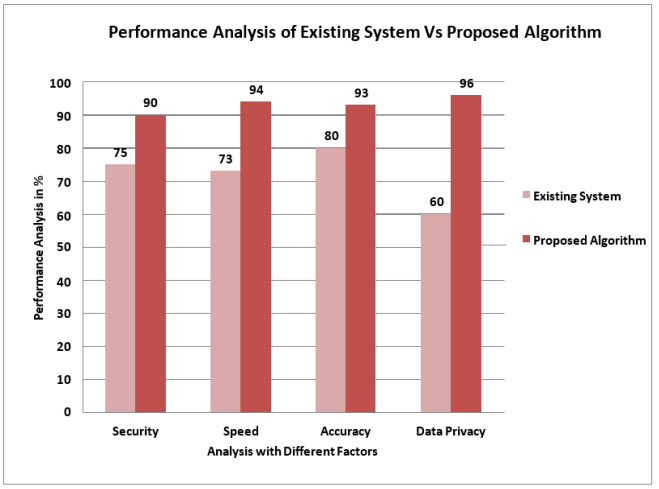
Secure Multiparty Computation (SMPC) and homomorphic encryption are employed to protect user information throughout the authentication procedure. The system complies with data protection regulations, manages secret data, and monitors incoming data. One of the best features of APPADA is its real-time detection capability, which enables the detection and defense against covert traffic-related assaults. The approach worked well at stopping attacks from spreading in a dynamic network where making decisions and acting upon them fast was essential.

The dynamic risk assessment component demonstrated both an easy capacity to adapt to changes and irregularities and a good understanding of network activity. APPADA introduced a novel approach to verifying incoming data: anomaly detection, past performance data, and device reputation. Because of this ongoing risk assessment, the software was able to create assault plans. It has been shown that the automatic reaction mechanism of APPADA is capable of responding pro-actively to recognized events.

To avoid such issues, this tool swiftly eliminates superfluous devices from your network. The methodical documentation of the problem-solving process yielded important insights for further investigation and advancement.

Performance Analysis	Existing System	Proposed Algorithm
Security	75	90
Speed	73	94
Accuracy	80	93
Data Privacy	60	96

Table 1 Table for Performance Analysis of Existing System Vs Proposed Algorithm



Graph.1 Graph for Performance Analysis of Existing System Vs Proposed Algorithm

Real-time security analysis: Because the system is always operational, malicious traffic attacks can be promptly detected and neutralized, averting more damage.

Preservation of Data Privacy: APPADA employs state-of-the-art encryption algorithms to safeguard user data privacy during the inspection process, ensuring compliance with privacy regulations.

Machine Learning Accuracy: The algorithm use machine learning models to adapt and learn over time, honing its detection skills so that it can stay ahead of evolving assault methods.

Speed: Based on factors including device reputation, historical behavior, and anomaly detection, APPADA dynamically assesses the danger of incoming traffic in order to increase attack detection accuracy and, in turn, speed.

The trial's outcomes show how successful APPADA is in stopping and minimizing collusive traffic attacks. APPADA is a powerful tool for protecting networks from the ever-changing cyber threat landscape because it offers an extra layer of security through proactive device isolation and privacy protection.

5. CONCLUSION

The performance analysis of APPADA shows how effective it is at preventing collusive traffic attacks by providing a strong blend of real-time responsiveness, privacy protection, detection accuracy, and adaptability. The algorithm's output demonstrates that it is a trustworthy and cutting-edge method of bolstering network security against highly proficient cyber attackers. Because of its scalable and modular architecture, APPADA was simple to integrate into a variety of network setups. The application's machine learning models demonstrated adaptability; they are regularly updated to keep up with new assault trends. This guaranteed that APPADA would function as intended even in dynamic threat conditions.

References

1. O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, and H. Alsariera, ‘‘A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for SDN- VANET,’’ IEEE Access, vol. 8, pp. 91028–91047, 2020.
2. M. Lee and T. Atkison, ‘‘VANET applications: Past, present, and future,’’ Veh. Commun., vol. 28, Apr. 2021, Art. no. 100310, doi: 10.1016/j.vehcom.2020.100310.
3. A. Rasheed, S. Gillani, S. Ajmal, and A. Qayyum, ‘‘Vehicular ad hoc network (VANET): A survey, challenges, and applications,’’ in Vehicular Ad-Hoc Networks for Smart Cities (Advances in Intelligent Systems and Computing), vol. 548. Singapore: Springer, pp. 39–51, 2017.
4. F. Zidani, F. Semchedine, and M. Ayaida, ‘‘Estimation of neighbors position privacy scheme with an adaptive beaconing approach for location privacy in VANETs,’’ Comput. Electr. Eng., vol. 71, pp. 359–371, Oct. 2018, doi: 10.1016/j.compeleceng.2018.07.040.
5. M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, ‘‘A survey on security attacks in VANETs: Communication, applications and challenges,’’ Veh. Commun., vol. 19, Oct. 2019, Art. no. 100179, doi: 10.1016/j.vehcom.2019.100179.
6. H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, ‘‘VANet security challenges and solutions: A survey,’’ Veh. Commun., vol. 7, pp. 7–20, Jan. 2017, doi: 10.1016/j.vehcom.2017.01.002.
7. P. Kohli, S. Painuly, P. Matta, and S. Sharma, ‘‘Future trends of security and privacy in next generation VANET,’’ in Proc. 3rd Int. Conf. Intell. Sustain. Syst. (ICISS), Dec. 2020, pp. 1372– 1375.
8. B. Chaudhary and K. Singh, ‘‘Pseudonym generation using genetic algorithm in vehicular ad hoc networks,’’ J. Discrete Math. Sci. Cryptography, vol. 22, no. 4, pp. 661–677, May 2019.
9. A. Boualouache, S.-M. Senouci, and S. Moussaoui, ‘‘A survey on pseudonym changing strategies for vehicular ad-hoc networks,’’ IEEE Commun. Surveys Tuts., vol. 20, no. 1, pp. 770–790, 1st Quart., 2018.
10. B. Amro, ‘‘Protecting privacy in VANETs using mix zones with virtual pseudonym change,’’ Int. J. Netw. Secur. Appl., vol. 10, no. 1, pp. 11–21, Jan. 2018.
11. P. K. Singh, A. Agarwal, G. Nakum, D. B. Rawat, and S. Nandi, ‘‘MPFSLP: Masqueraded

probabilistic flooding for source-location privacy in VANETs,'' IEEE Trans. Veh. Technol., vol. 69, no. 10, pp. 11383–11393, Oct. 2020.

12. L. Benarous and B. Kadri, ''Hybrid pseudonym change strategy for location privacy in VANET: Protecting location privacy in VANET,'' Int. J. Inf. Privacy, Secur. Integrity, vol. 4, no. 3, pp. 153– 169, 2020.
13. T. Gao and L. Zhao, ''Pseudonym schemes based on location privacy protection in VANETS: A survey,'' in Proc. Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. Cham, Switzerland: Springer, 2020, pp. 597–605.
14. R. Zhang, X. Wang, P. Cheng, and J. Chen, ''A novel pseudonym linking scheme for privacy inference in VANETs,'' in Proc. IEEE 91st Veh. Technol. Conf. (VTC-Spring), May 2020, pp. 1–5.
15. L. Zhu, C. Zhang, C. Xu, X. Du, N. Guizani, and K. Sharif, ''Traffic monitoring in self-organizing VANETs: A privacy-preserving mechanism for speed collection and analysis,'' IEEE Wireless Commun., vol. 26, no. 6, pp. 18–23, Dec. 2019.
16. G. Cormode, S. Jha, T. Kulkarni, N. Li, D. Srivastava, and T. Wang, ''Privacy at scale: Local differential privacy in practice,'' in Proc. Int. Conf. Manage. Data, May 2018, pp. 1655–1658.
17. D. Chaum, ''Security without identification: Transaction systems to make big brother obsolete,'' Commun. ACM, vol. 28, no. 10, pp. 1030–1044, Oct. 1985.
18. Y. Pan, J. Li, L. Feng, and B. Xu, ''An analytical model for random changing pseudonyms scheme in VANETs,'' in Proc. Int. Conf. Netw. Comput. Inf. Secur., vol. 2, May 2011, pp. 141–145.
19. L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, ''Enhancing wireless location privacy using silent period,'' in Proc. IEEE Wireless Commun. Netw. Conf., vol. 2, Jun. 2005, pp. 1187–1192.