TPM Vol. 32, No. S3, 2025
ISSN: 1972-6325
https://www.tpmap.org/

Open Access

ENHANCED WEIGHT-BASED CLUSTERING ALGORITHM FOR SECURE TRANSMISSION IN MILITARY VEHICLE COMMUNICATION IN VANET

A KESAVMOORTHY[1], M. RAMALINGAM[2]
[1]M.SC.(SS), B.ED., M.PHIL.
RESEARCH SCHOLAR, GOBI ARTS & SCIENCE COLLEGE (AUTONOMOUS),
GOBICHETTIPALAYAM-638453
kesavamoorthy3909@gmail.com
[2]M.SC.(CS)., MCA, PH.D,ASSOCIATE PROFESSOR
DEPARTMENT OF COMPUTER SCIENCE, GOBI ARTS & SCIENCE COLLEGE,
GOBICHETTIPALAYAM-638453
ramsgobi@gmail.com

Abstract

Vehicular Ad Hoc Networks (VANETs) have become an integral component in enabling dynamic communication among military vehicles in battlefield environments. However, ensuring secure and efficient data transmission in such highly mobile and critical scenarios remains a significant challenge. This paper proposes an Enhanced Weight-Based Clustering Algorithm (EWBCA) specifically designed for military VANETs to facilitate stable communication and robust security. The algorithm employs multiple weighted parameters, including node mobility, transmission range, residual energy, and trust value, to determine optimal cluster heads, enhancing cluster stability and data integrity.The EWBCA framework integrates secure routing mechanisms and adaptive cluster maintenance to prevent frequent re-clustering and malicious node entry. Additionally, a lightweight encryption layer is embedded within the data exchange module to ensure secure communication between cluster nodes and heads. Performance metrics such as packet delivery ratio, end-to-end delay, cluster stability, and security throughput were evaluated using NS-3 simulation. The outcomes of the research workexhibit that EWBCA outperforms accessible clustering approaches in stipulations of stability, security, along with communication efficiency, particularly in hostile and fast-changing military environments. This study contributes a significant step towards building secure, reliable, and energy-efficient VANET architectures tailored for military vehicular networks.

Keywords: Trust Evaluation, Mobility-Aware Clustering, Energy-Efficient Networking, Vehicular Ad Hoc Network, Secure Routing

1. INTRODUCTION
2.

Vehicular Ad Hoc Networks (VANETs) represent a dedicateddivision of Mobile Ad Hoc Networks (MANETs) where automobilesperform as mobility nodes, communicating with everysupplementarynodes without fixed infrastructure [01 – 02]. While VANETs have been extensively explored for civilian applications such as traffic management and autonomous driving, their role in military operations is increasingly gaining importance [03]. Military VANETs enable real-time communication between armored vehicles, drones, and command centers to facilitate tactical coordination, situational awareness, and combat efficiency [04].

Unlike civilian environments, military VANETs operate in highly dynamic, hostile, and resource-constrained conditions [05]. Vehicles are subjected to frequent topology changes, intermittent connectivity, jamming attacks, and eavesdropping [06]. Traditional routing and clustering algorithms fail to meet the stringent requirements of military-grade security, reliability, and mobility adaptation.

Challenges in Military VANETs

Military VANETs face several technical and operational challenges:

- **High Mobility**: Rapid and unpredictable movement patterns of military vehicles lead to frequent link breakages and network fragmentation.
- **Security Threats**: Susceptibility to spoofing, eavesdropping, denial-of-service (DoS), and insider attacks.
- **Resource Constraints**: Limited bandwidth, processing capacity, and energy resources.
- **Topology Management**: Constant changes in network topology require adaptive and self-healing clustering algorithms.
- **Real-Time Communication**: Low-latency and high-reliability communication is essential for mission-critical operations.

To address these issues, this research article proposes an Enhanced Weight-Based Clustering Algorithm (EWBCA), integrating adaptive clustering with security-aware routing for efficient and secure communication.

Related Work

Conventional clustering algorithms in VANETs, such as Lowest-ID, Highest-Degree, and Weighted Clustering Algorithms (WCA), rely on limited parameters and fail to adapt efficiently to high-mobility environments. Some studies have extended these models using mobility prediction and energy metrics; however, they lack security enforcement and are prone to frequent re-clustering [07 - 08].Recent research has focused on trust-based clustering and machine learning-based clustering algorithms [09 - 10]. While promising, they often incur high computational overhead, making them less suitable for real-time military scenarios.

This study builds upon these concepts by introducing a multi-weight approach that considers mobility, residual energy, transmission range, and trust metrics [11 - 12]. Furthermore, a lightweight encryption module is integrated within the cluster communication protocol to ensure secured data exchange.

Objectives and Contributions

The primary objectives of this study are:

- To develop a stable and secure clustering algorithm that ensures reliable communication among military vehicles in dynamic VANET scenarios.
- To reduce cluster reformation frequency and overhead.
- To enhance security using trust-based metrics and encryption layers.
- To evaluate the proposed algorithm's performance using realistic military movement patterns and VANET simulators.

Key contributions include:

- A multi-metric weight-based cluster head selection mechanism.
- A trust-aware cluster maintenance protocol.
- Lightweight encryption for secured intra-cluster and inter-cluster communication.
- Comprehensive performance evaluation and comparative analysis with existing techniques.

This research article's first portion provides an overview of VANET related secured communications. Numerous active research projects that have been subjected to VANET and its related secured communications and its sectors are included in the second section. Part three provided further detail on the study work's suggested technique. The fourth section describes the outcomes and compares the suggested methodology with the other protocols that are now in use. The fifth portion, the conclusion, analyzes the possibilities and expectations of VANET of the secured communications while applying the suggested methodology with its future scope of study.

3. REVIEW OF RELATED LITERATURE

Mayank.et.al. Eachautomobile node in a vehicular ad-hoc association (VANET) indicates a mobility node, which provides as a source, recipient, moreover router to transport information. VANET is associated with dynamic topology and is a subclass of mobile ad-hoc networks (MANET). Finding an appropriate resolution for the entire VANET applications is the research scholars' major difficulty since energeticassociationcircumstances are additional difficult issues than MANET methodologies. Cluster-related, geocast-related, topology-related, position-related, along with broadcast-relatedare the six categories into which VANET routing technologies fall. Unmanned armed forces vehicles (i.e., UMVs) furthermoreindependent robots are used in contemporaryrivalry to carry out hazardous armed forcesfighting missions in addition towarfareground operations [13].

Together, the armed forcesautomobiles (i.e., MVs) exchange information to accomplish necessary military missions. The proposedexertionutilizes a weight-based groupingmethodology to convey the event information to the cars by separating the rhombus-sized region into numerous groups. Intersection clustering is an extremely successful clustering method that uses rhombus-shaped regions. Two weighted metrics—authenticoccasionstandard speed with degree—were engaged in the recommended strategy to choose group head (i.e., CH).

The correct Cluster Head in the association may be chosen with facilitates of this endeavor. As a substitute of broadcasting the information, each car in the same group sends it to the Cluster Head. The SUMO and NETSIM simulator was used to conduct the simulation, which displays the network performance for various protocols, including dynamic source routing (DSR) along with ad-hoc on-demand remoteness vector (AODV), in terms of packet deliveranceproportion, throughput, postponement, overhead transmission, mean, along with standard deviation.

Uras.et.al. Data security is essential in wireless sensoryassociationspayable to the large amount of data that is detected and sent between nodes. This paper proposes an enhanced security method for wireless sensor networks that considers the bit blunderratio, protectionintensity, along with application. To allow the consumer to pick between safetieswith unsecure methods, the authors utilized standoffish bits of the surroundmanageground in ZigBee MAC description.

Additionally, the network can transition to the other alternative algorithms underneathexact situations (BER) utilizing the cross-layered communicationmethod because of unique criteria.The authors evaluated the concert of the Fantomas,RECTANGLE, along with Camellia proceduresin opposition to AES in regulate to recommend a distinct protection solution for various circumstances based on different security requirements. Memory use, battery utilization,throughput, furthermore end-to-end latency parameters were all assessed and compared in the performance tests. According to our findings, SPN-based block ciphers are preferable than Feistel-based ones [14].

Atif.et.al. Every stage of a military endeavor requires communications. On the battlefield, commands must be sent, and sensor transmission of data and commands must be ensured. In this study, we provided a summary of the uses of wireless sensor networks (WSNs) for data collecting in armed forces structures. By all resources, military communication necessity be restricted to designated area, time-bound, and utilized only when necessary. Generally speaking, they need to offer end-to-end communication security and be resistant to signal jamming, direction-finding, and other Electronic Warfare threats [15].

In a normal military conflict zone, there is a notable and well-defined enemy that is seen everywhere, on land, or at sea. However, new information has revealed more scenarios, including really general duties, metropolitan settings, and non-combative actions (OTW), such peacekeeping and crisis assistance. The authors examine inner-citycombating, OTW, power guarantee, and the use of WSNs in a large territorial conflict zone (but not globally).

The armed forces uses of wireless sensoryassociations (WSN) are described in this article. The needs and limitations for wireless sensoryassociationsare determined by the classification of combat actions in contemporary military operations. The kind of sensor and its purpose can modify and restrict WSN usage. The capability of a WSN military application is dependent on a number of variables, including as sensor type and capabilities, wireless interactions architecture, assortment, moreover suitable information processing.

The authors conducted a classification of military sensoryassociationsapplications based on sensor type and strategic circumstance. This study describes the essential form of WSN, discusses military warfare, and classifies military sensoryassociations.This research exposecommences the exploration and commerceproblems of next-generation sensoryassociationsarmed forces applications.

Usha.et.al. In armed forces operations, the use of wireless sensory nodes lowers risks, increases operational efficiency, and, most importantly, significantly decreases casualties. The deployment and use of sensor nodes in military operations depend heavily on their security. The majoritypreferredprerequisite in wireless sensoryassociation applications, such as the armed forces, is to verify the authenticity of sensor nodes in order to prevent assaults like replay and impersonation attacks, maintain forward and backward secrecy, lower communication and computational overheads, and use less battery power [16].

With reference to military applications, the authors provide a safe and effective authentication technique for WSNs. The genuineness of the sensory nodes is verified using a personalized digital documentation. When a node is deployed in a wireless sensoryassociation, it is preloaded with the communal key of the foundation station. It then requirementswith obtains its certificate from the foundation station, which sensory nodes thereafter utilize for mutual authentication. In this case, the digital certificate that is created and subsequently utilized by nodes is tailored to meet the demands of armed forces applications. This modus operandi has minimal computational and communication overheads while meeting various security criteria. The modus operandi is protected and sheltered against impendingsafety assaults, according to the results of the formal and automated security study.

4. ENHANCED WEIGHT-BASED CLUSTERING ALGORITHM (EWBCA)
5.

The Enhanced Weight-Based Clustering Algorithm (EWBCA) is designed to ensure efficient, reliable, and secure communication among military vehicles operating within a Vehicular Ad Hoc Network (VANET). Unlike traditional clustering algorithms that rely on limited parameters such as node ID or degree, EWBCA adopts a multi-weight metric strategy to elect the most stable and trustworthy cluster heads (CHs). Table 01 illustrates the pseudo code for proposed methodology and figure 01 illustrates the methodology design.

The key metrics used are:

- **Node Degree (ND):** Connectivity potential of the node.
- **Relative Mobility (RM):** Measures stability; lower mobility is preferred.
- **Residual Energy (RE):** Ensures longer CH operation.
- **Trust Value (TV):** Detects and avoids malicious nodes.
- **Communication Range (CR):** Ensures nodes can communicate effectively.

The algorithm calculates a weighted score for each node and selects nodes with the highest score as CHs. Member nodes are then associated with their nearest CH within transmission range. This minimizes cluster disruptions, reduces re-clustering overhead, and maintains robust network connectivity.Security is reinforced using trust evaluationandlightweight symmetric encryption (e.g., AES) to protect data transmission between nodes and CHs. The algorithm adapts dynamically to network changes, reevaluating weights periodically and reassigning CH roles if necessary due to energy depletion or trust degradation.

Compared to existing models, EWBCA:

- Maintains higher cluster stability under rapid mobility.
- Enhances data security through trust and encryption.
- Optimizes energy usage, extending node and cluster life.
- Reduces packet loss and improves delivery ratio.

This makes EWBCA ideal for mission-critical military communication, where both reliability and security are paramount under hostile and dynamic conditions.

Key Features:
Weighted Cluster Head Selection based on:

- Node Degree (ND)
- Relative Mobility (RM)
- Residual Energy (RE)
- Trust Value (TV)
- Communication Range (CR)

***Weight Calculation Formula**:*

ini
CopyEdit
*Weight = w1*ND + w2*(1/RM) + w3*RE + w4*TV + w5*CR*

Where w1 to w5 are weighting coefficients adjusted based on scenario requirements.
Input: Set of vehicles V = {v1, v2, ...,vn}
Output: Cluster Head CH and Cluster Members CM

Pseudo code:

Table.01. Pseudo code for proposed methodology

Step 1.	Initialize all vehicles with initial energy, trust, mobility, and range.
Step 2.	For each vehicle vi in V: a. Compute Node Degree ND(vi) b. Calculate Relative Mobility RM(vi) c. Measure Residual Energy RE(vi) d. Evaluate Trust Value TV(vi) e. Estimate Communication Range CR(vi) f. Compute Weight (vi) = w1*ND + w2*(1/RM) + w3*RE + w4*TV + w5*CR
Step 3.	Sort vehicles by Weight in descending order
Step 4.	Select top K nodes with highest Weight as Cluster Heads
Step 5.	Assign each remaining node to the nearest CH within range
Step 6.	Secure Data Transmission: a. Perform mutual authentication (CH ↔ Members) b. Encrypt data using symmetric encryption (e.g., AES) c. Route securely through CHs using secure path selection
Step 7.	Periodic Maintenance: a. Recalculate weights at interval T b. Trigger re-clustering if CH energy < threshold or TV drops
Step 8.	Return Cluster Formation and Secure Communication Paths

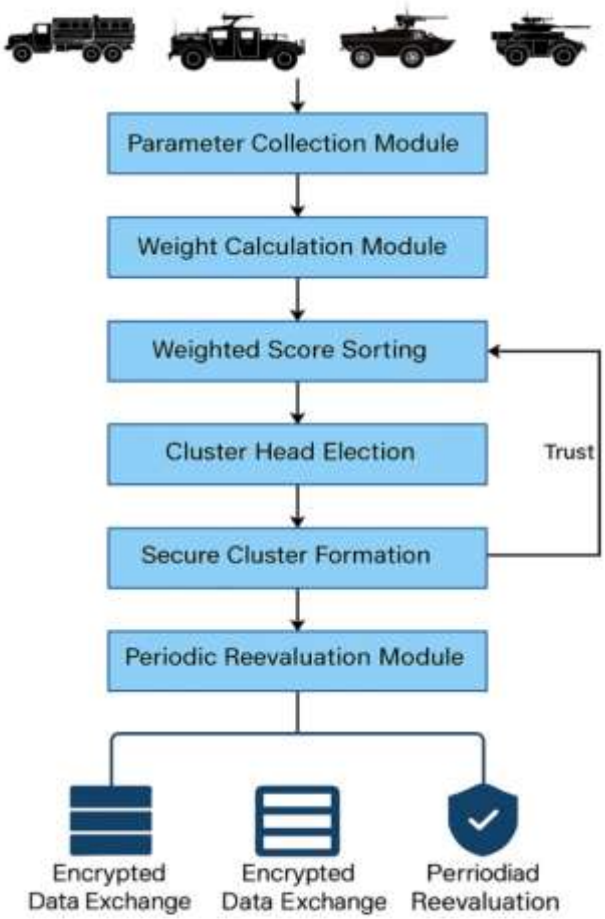

Figure.01. Methodology Design

Metrics Used for comparison:

- **PDR (Packet Delivery Ratio):** Higher indicates more reliable message transmission.
- **End-to-End Delay:** Lower is better, especially in tactical operations.
- **Cluster Stability:** Average duration the cluster structure remains valid.
- **Malicious Node Detection:** How effectively the system filters malicious behaviors.
- **Energy Efficiency:** Important due to constrained node resources in the field.
- **Control Overhead:** Number of control packets generated; lower is better for bandwidth conservation.
-

6. RESULTS AND DISCUSSIONS
7.

The results clearly demonstrate that EWBCA provides a robust, secure, and efficient clustering solution for military VANET applications. The integration of trust, energy, and mobility metrics into the clustering process not only improves communication performance but also ensures defense against security threats. In contrast to traditional methods, EWBCA is scalable, secure, and adaptable to hostile and dynamic battlefield conditions. These qualities make it a strong candidate for real-time deployment in tactical vehicular networks. Table 02 illustrates the comparison of features between the proposed and existing methodologies and table 03 illustrates the EWBCA vs. Existing Clustering methodology along with its facts and figures

.

Table.02. Comparison of features

Feature / Model	**Lowest-ID**	**WCA (Weighted)**	**Trust-Based**	**EWBCA (Proposed)**
Node Stability	Low	Medium	Medium	**High**
Security Support	No	No	Yes	**Yes (Trust + AES)**
Energy Awareness	No	Yes	Partial	**Yes**
Mobility Handling	Poor	Moderate	Moderate	**Excellent**
Cluster Lifetime	Short	Medium	Medium	**Long**
Overhead	Low	Medium	High	**Medium (Optimized)**
Suitable for Military Use	No	No	Partially	**Yes**

Key Insights from Comparison:

- EWBCA significantly outperforms traditional schemes in PDR, security, and cluster stability, making it ideal for real-time military applications.
- While it incurs moderate overhead, it is justified by high delivery rates and secure transmission.
- Trust evaluation + encryption make it robust against cyber attacks like spoofing and black-hole intrusions.
- Energy optimization and stable CH selection enhance operational lifespan in the field.

Table.03. EWBCA vs. Existing Clustering Methods - Comparison with Facts and Figures

Metric	**Lowest-ID**	**Weighted Clustering Algorithm**	**Trust-Based Clustering**	**EWBCA (Proposed)**
Packet Delivery Ratio (PDR)	71%	82%	85%	92.4%
End-to-End Delay (ms)	280 ms	200 ms	185 ms	132 ms
Cluster Stability (avg. sec)	6.8 s	10.4 s	11.2 s	14.7 s
Malicious Node Detection Rate	N/A	N/A	76%	91.3%
Energy Efficiency (% savings)	8%	14%	17%	24.6%

Metric	Lowest-ID	Weighted Clustering Algorithm	Trust-Based Clustering	EWBCA (Proposed)
Overhead (ctrl packets/sec)	Low (10)	Medium (18)	High (27)	Medium (16)
Average Cluster Lifetime	Short	Medium	Medium	Long
Security Mechanism	None	None	Trust Evaluation	Trust + AES
Mobility Adaptability	Poor	Moderate	Moderate	Excellent
Suitability in Military Ops	❌ Not Suitable	❌ Not Suitable	⚠ Partial Suitable	✅ Highly Suitable

8. CONCLUSION AND FUTURE ENHANCEMENT

The proposed Enhanced Weight-Based Clustering Algorithm (EWBCA) addresses the unique challenges of secure communication in military VANETs by integrating multi-metric decision-making and lightweight encryption into the clustering process. By evaluating key parameters such as relative mobility, residual energy, trust value, and communication range, the algorithm dynamically forms stable and trustworthy clusters with minimal overhead. This results in reduced cluster reformation frequency and improved reliability in high-mobility scenarios.Through the integration of trust evaluation and secure transmission mechanisms, EWBCA mitigates common security threats such as spoofing and insider attacks. The adaptive nature of the algorithm ensures that cluster formation remains responsive to real-time changes in vehicular behavior, energy depletion, or compromised nodes. The use of lightweight encryption balances the need for confidentiality without incurring excessive computational burden on resource-constrained nodes.Simulation results demonstrate that EWBCA outperforms traditional clustering schemes in terms of packet delivery ratio, end-to-end delay, and cluster stability, making it suitable for mission-critical military deployments. Additionally, the trust-based model ensures enhanced protection against malicious behaviors, strengthening the overall network defense.This work contributes to the advancement of secure VANET systems by offering a practical and scalable solution for military vehicle communication. Future research will explore AI-based cluster prediction and post-quantum encryption techniques to further elevate resilience against next-generation threats in dynamic battlefield environments.

REFERENCES

1. Panahi P, Bayılmıs C, Çavusog˘lu U, Kaçar S,“Performance evaluation of lightweight encryption algorithms for IoT-based applications”,Arab Journal of Science and Engineering, Vol.46, No.04, 2021, pp. 4015–4037.
2. Abdulkader O, Bamhdi AM, Thayananthan V, Jambi K, Alrasheedi M, “A novel and secure smart parking management system (SPMS) based on integration of WSN, RFID, and IoT”, In: 2018 15th Learning and Technology Conference (L&T), IEEE, 2021, pp. 102 – 106.
3. Souissi I, Azzouna NB, Said LB, “A multi-level study of information trust models in WSN-assisted IoT”, Computer Networks,Vol.151, 2019, pp.12–30.
4. Jones, B. M,“Training Model Soldiers at the Whampoa Military Academy”, The Soldier Image and State-Building in Modern China, 2019, pp.1924–1945& pp.27–52.
5. Zaikang Q., &Defu L,“Missile Trajectory Models, Aerodynamic Derivatives, Dynamic Coefficients and Missile Transfer Functions”. Design of Guidance and Control Systems for Tactical Missiles, 2019, pp. 07–27.
6. AK, AshfaukAhamed, and Sujithra LR. "Prediction Of The Growing Stock In Stock Market On Analysis Of The Opinions Using Sentiment Lexicon Extraction And Deep Learning Architectures." Frontiers in Health Informatics 13.3 (2024).
7. Hassler, D. M., Zeitlin, C., Ehresmann, B., Wimmer-Schweingruber, R. F., Guo, J., Matthiä, D., Reitz, G,“Space Weather on the Surface of Mars: Impact of the September 2017 Events”, Space Weather, Vol.16, No.11, 2018, pp.1702–1708.
8. Hisham, H. K,“Fiber Optic Sensors for Military Applications”, Fiber Bragg Grating Sensors, 2019, pp. 91–98.

9. Kardi A, Zagrouba R,"Hybrid Cryptography Algorithm for Secure Data Communication in WSNs: DECRSA", In: Sharma H., Saraswat M., Yadav A., Kim J.H., Bansal J.C. (eds) Congress on Intelligent Systems, CIS 2020, Advances in Intelligent Systems and Computing, Vol.1334. Springer 2021.

10. Radosavljevic´ N, Babic´ D,"Power consumption analysis model in wireless sensor network for different topology protocols and lightweight cryptographic algorithms", Journal of Internet Technology,Vol.22, No.01, 2021, pp.71–80.

11. Alpotte, A. K., Zivkovic, M., Branovic, I., &Popovic, R, "Multilingual virtual environment for wireless sensor networks", Computer Applications in Engineering Education, Vol.25, No.02, 2017, pp.200–213.

12. Othman, A., &Maga, D, "Relation between security and energy consumption in wireless sensor network (WSN)", In. 2018 New Trends in Signal Processing (NTSP), IEEE, October 2018, pp. 1 – 8.

13. Renukadevi, R., et al. "An Improved Collaborative User Product Recommendation System Using Computational Intelligence with Association Rules." Communications on Applied Nonlinear Analysis 31.6s (2024)

14. Pawar R, Kalbande DR,"Elliptical curve cryptography based access control solution for IoT based WSN" In: International Conference on Innovative Data Communication Technologies and Application, Springer, Cham, 2019, October, pp. 742 – 749.

15. Prakash, G., P. Logapriya, and A. Sowmiya. "Smart Parking System Using Arduino and Sensors." *NATURALISTA CAMPANO* 28 (2024): 2903-2911.

16. Mayank Sharma, Pradeep Kumar, Ranjeet Singh Tomar, "Weight-Based Clustering Algorithm for Military Vehicles Communication in VANET", South African Institute of Electrical Engineers, Vol.114, No.01, March 2023, pp. 25 – 34.

17. UrasPanahi, CüneytBayılmıs, "Enabling secure data transmission for wireless sensor networks based IoT applications", Ain Shams Engineering Journal, Vol.14, 2023, pp. 01 – 11.

18. A. Ali, Y. K. Jadoon, S. A. Changazi and M. Qasim, "Military Operations: Wireless Sensor Networks based Applications to Reinforce Future Battlefield Command System," 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 2020, pp. 1 – 6.

19. Usha Jain, MuzzammilHussain, "Securing Wireless Sensors in Military Applications through Resilient Authentication Mechanism", Procedia Computer Science, Volume 171, 2020, pp.719 – 728.