

Robust Multi-Class Intrusion Detection Using Explainable Ensemble Intelligence for Heterogeneous UAV and Smart Manufacturing Networks

Dr. Rafi Pratama

Department of Artificial Intelligence,
Jakarta Institute of Technology, Jakarta, Indonesia

Dr. Siti Maharani

Department of Intelligent Computing, Bandung
Institute of Digital Engineering, Bandung, Indonesia

VOLUME 03 ISSUE 08 (2026)

Published Date: 27 August 2026 // Page no.: - 42-49

ABSTRACT

The convergence of unmanned aerial vehicle (UAV) systems, industrial Internet-of-Things infrastructures, cyber-physical manufacturing platforms, and heterogeneous communication networks has created an increasingly complex intrusion detection environment. Conventional intrusion detection approaches frequently struggle with heterogeneous traffic distributions, evolving attack behaviors, class imbalance, overlapping network structures, and the requirement for interpretable security decisions. This paper develops a robust conceptual framework for multi-class intrusion detection based on explainable ensemble intelligence, with particular emphasis on heterogeneous UAV and smart manufacturing networks. The proposed framework integrates multi-objective representation learning, structural network analysis, ensemble classification, adaptive feature selection, and explainable artificial intelligence to distinguish multiple categories of malicious and benign activity. Community-structure research provides a theoretical basis for identifying latent relationships among network entities, while multi-objective evolutionary clustering supports the discovery of complex and dynamically changing traffic patterns. The framework further incorporates structural consistency, graph embedding, k-core analysis, label propagation, and objective-function selection as complementary mechanisms for representing heterogeneous attack surfaces. Explainability is incorporated at both global and instance levels to improve analyst confidence and facilitate operational response. The resulting analytical framework indicates that combining structural intelligence with ensemble decision-making can improve robustness against heterogeneous and evolving attacks while reducing the opacity associated with conventional high-capacity classifiers. The study positions explainable ensemble intelligence as a practical direction for security monitoring across UAV-assisted and smart manufacturing environments, while identifying computational overhead, concept drift, data imbalance, and cross-domain generalization as important limitations requiring further empirical investigation.

Keywords: Intrusion Detection; Explainable Artificial Intelligence; Ensemble Intelligence; Multi-Class Classification; UAV Networks; Smart Manufacturing; Community Detection; Graph Learning; Cybersecurity; Heterogeneous Networks.

INTRODUCTION

The rapid integration of UAVs, industrial sensors, robotic systems, edge devices, programmable controllers, and interconnected manufacturing platforms has transformed network security from a relatively isolated information-technology problem into a multidimensional cyber-physical challenge. Heterogeneous networks contain devices with different communication protocols, computational capabilities, traffic characteristics, and security requirements. Consequently, an intrusion detection system (IDS) operating across such environments must recognize diverse attack categories while maintaining reliable discrimination between legitimate but unusual operational behavior and

genuinely malicious activity.

A fundamental difficulty is that heterogeneous network traffic cannot always be represented adequately through independent statistical features. Network entities interact through communication relationships, temporal dependencies, and structural patterns. Community-detection research demonstrates that meaningful groups can emerge from complex relational structures and that algorithmic choices influence how those groups are identified (Orman and Labatut, 2009). Similar observations arise in studies comparing community-detection strategies and their sensitivity to network characteristics (Wagenseller et al.,

2018). These principles are directly relevant to intrusion detection because malicious activities may manifest not only through abnormal packet-level attributes but also through changes in communication communities, influential nodes, connectivity patterns, and structural dependencies.

The problem becomes more challenging in UAV and smart manufacturing environments because the same infrastructure may simultaneously support autonomous control, telemetry, sensing, machine coordination, remote management, and data exchange. An intrusion detection model must therefore solve a multi-class problem rather than simply classify traffic as benign or malicious. It should distinguish different attack behaviors while remaining sufficiently robust when attack distributions change.

Recent work on advanced explainable ensemble models for multi-class intrusion detection in heterogeneous drone and industrial networks provides a closely aligned research direction, emphasizing the combination of ensemble intelligence and interpretability for heterogeneous security environments (Islam et al., 2026). The present framework extends this conceptual direction by emphasizing the structural properties of heterogeneous networks and integrating community-oriented analytical mechanisms with explainable ensemble classification.

The primary objective is to formulate a robust architecture in which heterogeneous network observations are transformed into structurally meaningful representations before being processed by complementary ensemble classifiers. A second objective is to integrate explainability so that security analysts can understand why particular traffic instances or network entities are classified as specific attack categories. A third objective is to examine how structural network intelligence can address weaknesses associated with isolated feature-based intrusion detection.

The significance of this approach lies in its attempt to bridge three traditionally separated perspectives: network structure, machine-learning classification, and security explainability. Community detection provides information about relationships; ensemble intelligence provides classification diversity; and explainability provides operational transparency. Their integration can create a more resilient IDS architecture for environments where false alarms, missed attacks, and unexplained automated decisions can all have significant operational consequences.

LITERATURE REVIEW

2.1 Community Structure as a Foundation for Network

Intelligence

Community detection provides a theoretical foundation for identifying groups of strongly related entities within complex networks. Orman and Labatut (2009) comparatively examined community-detection algorithms using artificial networks, demonstrating the importance of evaluating algorithms according to network characteristics rather than assuming that one technique is universally optimal. This observation is important for cybersecurity because UAV and manufacturing networks can exhibit substantially different topologies.

Yang et al. (2016) further investigated comparative community-detection performance using artificial networks, reinforcing the importance of structural evaluation. Their work suggests that community quality cannot be interpreted independently from the underlying network configuration. In an IDS, this implies that structural features extracted from communication graphs should be interpreted relative to the network's topology and operational context.

Peel (2010) addressed network-parameter estimation for selecting community-detection algorithms. The methodological implication is particularly valuable for heterogeneous intrusion detection: algorithm selection itself can become an adaptive component of the security pipeline. Rather than applying a single structural model to all traffic, an IDS can use measurable network properties to determine which representation or clustering strategy is most appropriate.

2.2 Multi-Objective and Evolutionary Network Analysis

Multi-objective optimization is relevant when network structure cannot be adequately represented through a single criterion. Shi et al. examined objective-function selection for multi-objective community detection, highlighting the importance of selecting objectives capable of representing competing structural properties (Shi et al., 2009). In intrusion detection, analogous conflicts may arise between detection sensitivity, structural consistency, computational efficiency, and false-positive control.

Orouskhani et al. (2021) proposed multi-objective evolutionary clustering for complex networks, demonstrating the value of evolutionary approaches for discovering multiple structural objectives. Su et al. (2021) extended the evolutionary perspective to large-scale complex networks through a parallel multi-objective evolutionary algorithm. These contributions are particularly relevant to large manufacturing infrastructures in which centralized exhaustive optimization can become computationally expensive.

Yin et al. (2021) investigated multi-objective evolutionary clustering for large-scale dynamic community detection. The dynamic dimension is highly relevant because industrial and

UAV networks are not static. Devices may join or leave, UAV communication patterns can change according to mission requirements, and production processes can generate periodic or event-driven traffic. A structurally adaptive IDS must therefore tolerate evolving network communities.

2.3 Structural Acceleration and Node-Level Intelligence

Peng et al. (2014) investigated the use of k-core subgraphs to accelerate community detection. K-core decomposition can identify densely connected portions of a network and can therefore support the prioritization of structurally important regions. Rajeswari and Bhavana (2023) combined k-core and random-walk algorithms for identifying influential spreaders in diverse networks. From an intrusion-detection perspective, influential or highly connected nodes may deserve additional monitoring because compromise of such nodes can potentially affect a larger portion of the network.

Xu et al. (2023) examined influence-based label propagation for overlapping communities. The notion of overlapping membership is particularly important in heterogeneous cyber-physical environments because an endpoint can simultaneously participate in multiple functional relationships. For example, an industrial gateway may communicate with control devices, cloud services, maintenance systems, and UAV platforms. A representation that assumes strictly separated communities may therefore lose meaningful information.

2.4 Graph Representation and Structural Consistency

Zhang et al. (2020) proposed a complex-network graph-embedding method based on shortest paths and multi-objective optimization for community detection. Graph embedding offers an alternative to manually designed structural indicators by transforming relational information into numerical representations suitable for machine-learning systems.

Wang et al. (2023) investigated dual structural consistency for community detection on social networks. The principle of preserving structural consistency is applicable beyond social networks because heterogeneous cybersecurity environments also contain relational dependencies that should remain meaningful after representation learning.

Traag (2015) examined faster unfolding of communities through improvements associated with the Louvain algorithm. Efficient community detection is important in IDS environments because security decisions may need to be produced continuously rather than through lengthy offline processing.

2.5 Explain ability and Security Intelligence

Sangaiah et al. (2023) investigated explainable AI in big-data intelligence for community detection in digital healthcare services. Although the application domain differs, the work supports an important theoretical principle: high-dimensional intelligent systems require interpretable mechanisms when their decisions affect operational processes.

For intrusion detection, explainability is not merely a presentation feature. It can support incident validation, analyst prioritization, false-positive investigation, and model auditing. Islam et al. (2026) specifically emphasize advanced explainable ensemble models for multi-class intrusion detection across heterogeneous drone and industrial networks. This provides a direct conceptual basis for combining ensemble decision-making with explanation mechanisms in the present framework.

Overall, the literature reveals a gap between structural network intelligence and operational multi-class intrusion detection. Community-detection research provides sophisticated tools for understanding relationships, while explainable machine learning provides decision transparency. However, a unified architecture that combines structural representations, multi-objective optimization, ensemble classification, and explainability for heterogeneous UAV and smart manufacturing environments remains insufficiently developed. The proposed framework addresses this integration gap.

METHODOLOGY

3.1 Proposed System Architecture

The proposed architecture consists of six conceptual stages: heterogeneous traffic acquisition, preprocessing and normalization, structural graph construction, multi-objective representation generation, explainable ensemble classification, and security interpretation.

Let the observed heterogeneous traffic be represented as

$$X=\{x_1,x_2,...,x_n\} \quad X=\{x_1,x_2,\ldots,x_n\}$$

where each x_i represents a network observation containing temporal, statistical, protocol, behavioral, and structural attributes. The corresponding class label is represented as $y_i \in \{0,1,...,K-1\}$ $y_i \in \{0,1,\ldots,K-1\}$, where class 0 represents legitimate traffic and the remaining classes correspond to distinct intrusion categories.

The first stage converts heterogeneous observations into a unified analytical representation. Normalization is required because packet-level measurements, connection durations, frequency statistics, and graph-derived features can exist on substantially different scales. Without normalization, high-magnitude variables may disproportionately influence

ensemble decisions.

3.2 Heterogeneous Network Graph Construction

The second stage constructs a graph $G=(V,E)$, where V represents network entities and E represents communication relationships. Nodes may correspond to UAVs, sensors, industrial controllers, gateways, edge devices, robotic systems, or servers.

An edge can be weighted according to communication frequency, duration, transferred volume, or interaction intensity. The resulting graph provides structural information unavailable from isolated traffic records.

Community structure is then identified using complementary mechanisms. Louvain-style optimization can provide computationally efficient structural partitioning (Traag, 2015), whereas multi-objective evolutionary approaches can capture competing structural criteria (Su et al., 2021; Yin et al., 2021). K-core analysis can identify structurally dense regions (Peng et al., 2014), while label propagation can capture overlapping relationships (Xu et al., 2023).

This combination is particularly useful in manufacturing environments. For example, a compromised industrial gateway may not exhibit extreme packet-level abnormalities, but it may suddenly establish relationships with an unusual collection of devices. Structural features can reveal this behavioral shift.

3.3 Multi-Objective Feature and Representation Intelligence

A central component of the framework is multi-objective representation optimization. Instead of maximizing a single detection criterion, the model considers several objectives:

$$F=\{f_{det},f_{struct},f_{comp},f_{exp}\}F=\{f_{det},f_{struct},f_{comp},f_{exp}\}$$

where f_{det} represents detection effectiveness, f_{struct} measures preservation of meaningful network relationships, f_{comp} represents computational efficiency, and f_{exp} reflects interpretability.

This formulation recognizes that maximizing accuracy alone may produce a model that is computationally expensive or difficult to interpret. Shi et al. (2009) demonstrate the importance of objective-function selection in multi-objective community analysis, while Orouskhani et al. (2021) and Yin et al. (2021) support evolutionary optimization for complex and dynamic network structures.

The representation can combine conventional traffic variables with structural indicators such as node degree, k-core index, community membership, shortest-path characteristics, neighborhood similarity, and embedding coordinates. Zhang et al. (2020) provides theoretical support for using shortest-path information and graph embedding in complex network analysis.

3.4 Ensemble Intelligence for Multi-Class Detection

The classification layer employs an ensemble of complementary learners rather than relying on a single model. Conceptually, the ensemble can be represented as

$$\hat{y}=\arg\max_c\sum_{m=1}^Mw_mP_m(y=c|x)\hat{y}=\arg\max_{\{c\}}\sum_{m=1}^Mw_mP_m(y=c|x)$$

where P_m is the class-probability output of the m -th classifier and w_m is its adaptive contribution.

The motivation for ensemble intelligence is that different classifiers may capture different aspects of heterogeneous attack behavior. One learner may perform strongly on statistical traffic patterns, another on nonlinear feature interactions, and another on graph-derived representations. Combining these perspectives can reduce dependence on one decision boundary.

The framework is explicitly multi-class. Instead of reducing all anomalies to a binary malicious/benign distinction, it produces class-specific predictions. This is important because different attacks may require different mitigation strategies. A flooding event, credential-related anomaly, reconnaissance pattern, or protocol manipulation event can have different operational consequences.

The explainable ensemble direction is consistent with Islam et al. (2026), whose work directly addresses explainable ensemble modeling for multi-class intrusion detection in heterogeneous drone and industrial networks.

3.5 Explain ability Layer

The explainability layer generates both global and local interpretations. Global explanations identify which features consistently influence classification across the dataset. Local explanations identify why a particular network observation received a particular class prediction.

For an observation x_i , the explanation vector can be represented as

$$E(x_i)=\{e_1,e_2,...,e_p\}E(x_i)=\{e_1,e_2,\ldots,e_p\}$$

where each e_j expresses the contribution of feature j to the final decision.

Structural explanations should also be considered. For

example, the system may report that an endpoint was classified as suspicious because of an unusual increase in communication degree, a change in community membership, or abnormal interaction with a high-connectivity core. This provides a richer interpretation than simply stating that a packet-level feature exceeded a threshold.

Explainability is particularly important in cyber-physical manufacturing because automated security decisions may interrupt production processes. Analysts need evidence before isolating a device or modifying operational configurations. Sangaiah et al. (2023) reinforces the importance of explainable intelligence when AI is applied to complex information environments.

3.6 Robustness Against Heterogeneity and Concept Drift

A robust IDS must account for concept drift. Network behavior during normal production may differ substantially from behavior during maintenance periods, UAV deployment, system upgrades, or emergency operation.

The framework therefore incorporates periodic structural reassessment. Community structures can be recalculated as the network evolves, while ensemble weights can be updated according to recent classification performance. Dynamic community research supports this adaptive orientation (Yin et al., 2021).

A hypothetical example illustrates the mechanism. Suppose a UAV fleet normally communicates with a manufacturing edge gateway during daytime operations. During a maintenance event, communication patterns expand to include diagnostic servers. A static IDS might interpret this new behavior as suspicious. A structurally adaptive IDS can recognize the temporary change in community structure and use contextual evidence before generating a high-confidence intrusion alert.

3.7 Evaluation Framework

A complete empirical implementation should evaluate the framework using accuracy, precision, recall, macro-F1, weighted-F1, false-positive rate, false-negative rate, inference latency, and explanation stability.

For class k , precision and recall can be expressed as

$$\text{Precision}_k = \frac{TP_k}{TP_k + FP_k} \quad \text{Precision}_k = \frac{TP_k}{TP_k + FP_k}$$

and

$$\text{Recall}_k = \frac{TP_k}{TP_k + FN_k} \quad \text{Recall}_k = \frac{TP_k}{TP_k + FN_k}.$$

Macro-F1 is particularly important for imbalanced multi-class datasets because it prevents dominant classes from masking poor minority-class performance.

The evaluation should also include ablation experiments. Removing graph features can determine the contribution of structural intelligence; removing explainability can quantify operational overhead; removing ensemble components can reveal the value of model diversity; and removing adaptive structural updates can evaluate resilience to changing network conditions.

RESULTS

Because the present study is formulated as a research framework rather than a report of a newly executed benchmark experiment, the findings are interpreted as analytical outcomes derived from the proposed architecture and the supplied literature rather than as fabricated numerical measurements.

The first principal finding is that structural information should complement conventional traffic-level features. Community relationships, k-core structure, shortest paths, and graph embeddings can expose behavioral information that may remain hidden when each network flow is analyzed independently. The comparative community-detection literature indicates that algorithm performance depends strongly on network characteristics (Orman and Labatut, 2009; Yang et al., 2016). Therefore, structural intelligence is most valuable when its extraction mechanism is adapted to the observed topology.

The second finding concerns multi-objective optimization. Large and dynamic heterogeneous networks cannot realistically be characterized through a single structural objective. Evolutionary clustering studies demonstrate the usefulness of simultaneously considering competing structural criteria (Orouskhani et al., 2021; Su et al., 2021; Yin et al., 2021). In the proposed IDS, this principle translates into balancing detection quality, structural fidelity, computational cost, and interpretability.

Third, ensemble classification is theoretically better aligned with heterogeneous attack surfaces than a monolithic decision mechanism. Different classifiers can capture different statistical and structural characteristics. The expected benefit is particularly important for multi-class detection because minority attack classes may occupy decision regions that are difficult for a single learner to model reliably.

Fourth, explainability has a functional security role rather than merely a user-interface role. A security analyst should be able to determine whether an alert originates from packet-level abnormalities, structural changes, or a combination of both. The explainable ensemble direction represented by Islam et al. (2026) supports this interpretation, while explainable network intelligence research further establishes

the relevance of transparent decision processes (Sangaiah et al., 2023).

Finally, the principal limitation identified by the framework is computational complexity. Graph construction, community optimization, evolutionary clustering, ensemble inference, and explanation generation can collectively increase latency. Traag (2015) demonstrates the importance of computationally efficient community detection, while large-scale evolutionary approaches highlight the need for scalable implementations. Consequently, deployment should use hierarchical processing in which inexpensive anomaly screening precedes computationally intensive structural analysis.

DISCUSSION

The proposed framework contributes theoretically by connecting structural network science with explainable ensemble intrusion detection. Conventional IDS design often treats traffic records as independent observations. Such a representation is insufficient when security behavior is strongly dependent on relationships among devices. Community-oriented research demonstrates that network structure contains meaningful information, while graph embedding and structural consistency approaches show how relational properties can be transformed into machine-learning representations (Zhang et al., 2020; Wang et al., 2023).

The framework also exposes a trade-off between structural sophistication and operational efficiency. Multi-objective evolutionary methods can produce richer representations, but they introduce optimization overhead. This tension is particularly important in UAV environments, where edge devices may have limited computational resources. Consequently, structural analysis should not necessarily be applied at maximum complexity to every observation. Adaptive selection based on network parameters, as suggested by Peel (2010), provides a rational basis for controlling this overhead.

Another important issue is overlapping network behavior. Xu et al. (2023) show the relevance of overlapping community analysis, while Rajeswari and Bhavana (2023) emphasize influential structures through k-core and random-walk analysis. In a smart factory, a gateway or edge node can legitimately belong to multiple functional communication groups. Treating such overlap as inherently anomalous would increase false positives. The proposed framework therefore interprets overlapping structure contextually rather than as an automatic attack indicator.

The practical implication is that explainability should operate at multiple levels. A global explanation can inform

administrators that structural connectivity, traffic periodicity, or protocol behavior are major determinants of the model. A local explanation can clarify why one UAV or industrial controller was classified as suspicious. Such information is valuable when an alert requires operational intervention.

However, the framework has important limitations. First, the supplied literature is primarily concerned with community detection, graph analysis, and explainable intelligence rather than a single unified benchmark covering every UAV and smart manufacturing attack class. Second, structural features can be vulnerable to adversarial manipulation if attackers deliberately alter communication patterns. Third, explanations may become unstable when the underlying ensemble contains highly correlated models or when the network changes rapidly. Fourth, cross-domain transfer remains challenging because a model optimized for UAV traffic may not automatically generalize to industrial control traffic.

These limitations suggest that future empirical research should investigate adaptive ensemble weighting, streaming graph learning, adversarially robust explanations, and lightweight edge deployment. Benchmark evaluation should also include cross-network testing, temporal validation, minority-class analysis, and explanation consistency. The research direction represented by Islam et al. (2026) is particularly relevant because it directly connects explainable ensemble modeling with heterogeneous drone and industrial intrusion detection.

CONCLUSION

This paper developed a robust conceptual framework for multi-class intrusion detection in heterogeneous UAV and smart manufacturing networks using explainable ensemble intelligence. The central proposition is that reliable security detection should integrate three complementary forms of intelligence: traffic-level behavioral information, network-level structural information, and transparent ensemble decision-making.

The literature indicates that community detection, multi-objective evolutionary clustering, k-core analysis, graph embedding, label propagation, and structural-consistency mechanisms can provide valuable representations of complex network behavior. Their integration with ensemble classification creates a pathway toward detecting multiple intrusion categories without treating network observations as isolated events.

The proposed methodology further establishes explainability as a core component of cybersecurity rather than an optional visualization mechanism. Local and global explanations can help analysts understand the behavioral and structural evidence supporting an alert, thereby improving trust and facilitating operational response.

Nevertheless, robustness cannot be equated with

classification accuracy alone. A practical IDS must also address computational cost, concept drift, class imbalance, overlapping network roles, explanation stability, and cross-domain generalization. Future research should therefore validate the framework experimentally using heterogeneous UAV and industrial datasets, investigate online graph adaptation, evaluate adversarial robustness, and quantify the relationship between explanation quality and analyst decision performance.

Overall, explainable ensemble intelligence combined with structural network analysis offers a theoretically grounded direction for next-generation intrusion detection. Its greatest potential lies not in replacing conventional security analytics but in integrating multiple complementary perspectives into a unified, interpretable, and adaptive security decision process.

REFERENCES

1. Orman, G.K. and Labatut, V. (2009) A comparison of community detection algorithms on artificial networks. In *Discovery Science: 12th International Conference, DS 2009, Porto, Portugal, October, 2009* 12 (pp. 242-256). Heidelberg (Berlin: Springer), 3–5.
2. Orouskhani, M., Shi, D. and Orouskhani, Y. (2021) Multi-objective evolutionary clustering with complex networks. *Expert Systems with Applications* 165(11391): 6.
3. Öztemiz, F. and Karçı, A. (2023) Ko: Modularity opti- mization in community detection. *Neural Computing and Applications* : 1–15.
4. Peel, L.. (2010) July). estimating network parameters for selecting community detection algorithms. In *13th International Conference on Information Fusion (IEEE)*: 1–8.
5. Peng, C., Kolda, T.G. and Pinar, A. (2014) Accelerating community detection by using k-core subgraphs. *arxiv. Preprint*, 1403.2226.
6. Rajeswari, S. and Bhavana, S.U.. (2023) August). In *Community Detection in Diverse Networks to Locate Influential Spreaders based on K-core and Random Walk Algorithms (In12th International Conference on Advanced Computing (ICoAC) . IEEE)*: 1–6.
7. Redekar, S.S. and Varma, S.L.. (2022) May). a survey on community detection methods and its application in biological network. In *International Conference on Applied Artificial Intelligence and Computing (ICAAIC) (IEEE)*: 1030–1037.
8. Sangaiah, A.K., Rezaei, S., Javadpour, A. and Zhang, W. (2023) Explainable ai in big data intelligence of community detection for digitalization e-healthcare services. *Applied Soft Computing* 136(11011): 9.
9. Shi, C., Yu, P.S., Cai, Y., Yan, Z. and Wu, B.. October). In *Proceedings, I. [ed.] On selection of objective functions in multi-objective community detection (of the 20th ACM international conference on Information and knowledge management)*: 2301–2304.
10. Song, Y., Zheng, Z., Shi, Y. and Wang, B. (2023) Glod: The local greedy expansion method for overlapping community detection in dynamic provenance networks. *Mathematics* 11(15): 3284.
11. Su, Y., Zhou, K., Zhang, X., Cheng, R. and Zheng, C. (2021) A parallel multi-objective evolutionary algorithm for community detection in large-scale complex networks. *Information Sciences* 576: 374–392.
12. Traag, V.A. (2015) Faster unfolding of communities: Speeding up the louvain algorithm. *Physical Review E* 92(3): 032801.
13. Wagenseller, P., Wang, F. and Wu, W. (2018) Size matters: A comparative analysis of community detection algorithms. *IEEE Transactions on Computational Social Systems* 5(4): 951–960.
14. Wang, Y., Cao, J., Bu, Z., Wu, J. and Wang, Y. (2023) Dual Structural Consistency Preserving Community Detection on Social Networks (*IEEE Transactions on Knowledge and Data Engineering*).
15. Xu, H., Ran, Y., Xing, J. and Tao, L. (2023) An influence-based label propagation algorithm for overlapping community detection. *Mathematics* 11(9): 2133.
16. Yang, J. and Leskovec, J.. August). Defining and evaluating network communities based on ground-truth : 1–8.
17. Yang, Z., Algesheimer, R. and Tessone, C.J. (2016) A comparative analysis of community detection algorithms on artificial networks. *Scientific reports* 6(1): 30750.
18. Yin, Y., Zhao, Y., Li, H. and Dong, X. (2021) Multi-objective evolutionary clustering for large-scale dynamic community detection. *Information Sciences* 549: 269–287.
19. Zachary, W.W. (1977) An information flow model for conflict and fission in small groups. *Journal of*

anthropological research 33(4): 452–473.

20. Zhang, W., Shang, R. and Jiao, L. (2020) Complex network graph embedding method based on shortest path and moea/d for community detection. *Applied Soft Computing* 97(10676): 4.
21. Islam, M.S., Ahmed, F., Ishtiaq, W. et al. Advanced explainable ensemble models for multi-class intrusion detection in heterogeneous drone and industrial networks. *J. Inf. Secur.* 2026, 14 (2026).
22. Ramamurthy, K., Gumber, S., Abdelfattah, W.M. et al. Human AI trust modeling in cognitive systems via ensemble learning and advanced feature engineering. *Discov Artif Intell* 6, 366 (2026). <https://doi.org/10.1007/s44163-026-01255-7>
23. Geo Philip, Paulson, Robotics-Enabled Sustainable Construction Management: A Socio-Technical Framework for Operational Efficiency, Digital Integration, and Sustainability Performance. Available at SSRN: <https://ssrn.com/abstract=6845167> or <http://dx.doi.org/10.2139/ssrn.6845167>