Features of the Assessment of Malicious Activity in Smart City Infrastructure Based on Information Granulation and Fuzzy Granular Calculations

Annamurad Klychev
dept. Artificial intelligence and cybersecurity
Oguz han engineering and technology
university of Turkmenistan
Ashgabat, Turkmenistan
annamyrat.gylyjov@etut.edu.tm

Isgender Tagangylyjov
dept. Artificial intelligence and cybersecurity
Oguz han engineering and technology
university of Turkmenistan
Ashgabat, Turkmenistan
i.tagangylyjov@etut.edu.tm

***Abstract*—The pervasive integration of digital infrastructures within urban environments, while increasing smart city operational efficiencies, has concomitantly engendered intricate security vulnerabilities. Conventional cybersecurity paradigms, predicated on deterministic models, frequently prove inadequate in addressing the dynamic and epistemically uncertain nature of cyber threats. This research introduces a novel methodological framework, leveraging ontology-driven information granulation and knowledge graph-enhanced fuzzy granular computations, to facilitate semantic assessment and mitigation of malicious activities. By transforming raw security telemetry into semantically enriched granules, contextual knowledge extraction is enabled, enhancing inferential efficacy. A case study, employing semantic intrusion detection systems (SIDS) within a simulated 'Smart City', elucidates the potential of the framework for proactive, knowledge-driven threat detection and semantic response strategies.**

***Keywords*—Semantic Technologies, Smart City Infrastructures, Information Granulation, Fuzzy Granular Computations, Cybersecurity, Intrusion Detection Systems, Internet of Things (IoT) Security, Adaptive Machine Learning**

I. Introduction

The inherent complexity of smart city environments, characterized by dynamic topologies and a multitude of interacting components, renders traditional cybersecurity paradigms increasingly inadequate. To address this exigency, emergent computational methodologies, particularly those leveraging semantic technologies, such as information granulation and fuzzy granular computations, have garnered scholarly attention. Information granulation, a construct originating from the seminal work of Zadeh (1965), entails the decomposition of raw, high-dimensional data into semantically enriched granules, facilitating knowledge extraction and representation. This approach aligns with human cognitive processes by prioritizing approximate reasoning and knowledge-based inference over precise numerical representation, enhancing data interpretability and semantic interoperability. Recent investigations (e.g., Livi & Sadeghian, 2014) have demonstrated the efficacy of granular computing in managing ontological uncertainty and reducing computational complexity. Complementarily, fuzzy granular computations, when integrated with semantic reasoning, accommodate the inherent ambiguity and partial truths pervasive in real-world datasets. Unlike conventional crisp classifications, semantic fuzzy logic assigns degrees of membership to data elements within multiple granules, informed by domain ontologies, furnishing a nuanced framework for knowledge-driven uncertainty modeling. This is particularly significant within the domain of cybersecurity, where the delimitation between normative and anomalous behavior requires contextual semantic understanding. By using semantic inference systems and knowledge graphs, it becomes feasible to derive context-aware risk assessments that more accurately reflect the probabilistic nature of cyber threats. The synergistic integration of these semantic methodologies with machine learning (ML) techniques further augments the capacity of semantic intrusion detection systems (SIDS) to discern and respond to novel and sophisticated attack vectors. ML models, such as semantic neural networks, excel in the identification of intricate, knowledge-driven relationships within extensive datasets and have demonstrated considerable promise in enhancing the fidelity of threat detection. When amalgamated with semantically enriched information granulation and fuzzy granular computations, these models constitute a robust, adaptive framework that not only optimizes detection performance but also expedites real-time, knowledge-based decision-making.

This paper introduces an integrated semantic frame-

work that synergistically amalgamates these advanced computational techniques to address the cybersecurity challenges inherent in smart urban infrastructures. The subsequent sections provide a detailed exposition of the methodological components, encompassing semantic data acquisition, ontology-driven information granulation, knowledge graph-based fuzzy granular analysis, and semantic inference-based decision-making protocols, as well as a comprehensive case study illustrating the practical instantiation of the proposed approach. Through this research, we endeavor to contribute to the development of more resilient and adaptive semantic cybersecurity systems capable of mitigating the evolving threat landscape in smart urban environments

II. Background and Related Work

The rapid evolution of smart city infrastructures has precipitated a surge in the complexity of cybersecurity challenges. As urban environments integrate an ever-growing array of interconnected devices and systems, conventional security paradigms are increasingly inadequate for addressing the dynamic, heterogeneous, and semantically ambiguous nature of urban data. In this milieu, semantic technologies—when combined with advanced computational methodologies such as information granulation and fuzzy granular computations—offer a compelling framework for managing uncertainty and high dimensionality.

A. Information Granulation

Information granulation involves decomposing complex datasets into smaller, semantically coherent subunits known as granules. These granules encapsulate clusters of data points that share intrinsic attributes, thereby facilitating a reduction in computational complexity and enhancing interpretability. The theoretical foundation of this approach can be traced to Zadeh's seminal work on fuzzy sets (1965), which established a formal paradigm for representing imprecise information. This cognitive strategy, which mirrors the human tendency to process information in approximate, non-exact categories, has been pivotal in refining semantic data analysis. Recent empirical studies, including those by Livi and Sadeghian (2014), demonstrate that the application of granular computing principles can substantially improve the efficiency of data analysis in systems characterized by semantic ambiguity and uncertainty.

B. Fuzzy Granular Calculations

Building upon the principles of information granulation, fuzzy granular computations integrate fuzzy logic to more effectively manage imprecision within semantic granules. Unlike traditional crisp partitioning techniques, fuzzy granular methods allow data elements to exhibit varying degrees of membership across multiple granules. This approach enables the derivation of fuzzy measures that more accurately encapsulate underlying uncertainties. In this framework, each granule is delineated not by strict boundaries but through a membership function that quantifies the degree of affiliation of each data point. Such nuanced representations are crucial in decision support systems and pattern recognition tasks, where the inherent ambiguity of real-world data necessitates a flexible and semantically enriched computational model. In cybersecurity applications, for instance, the integration of fuzzy granular computations facilitates sophisticated reasoning over heterogeneous data sources, thereby enhancing the detection of complex, semantic cyber threats.

C. Applications in Smart City Infrastructures

Smart city environments generate vast and heterogeneous data streams from IoT devices, sensors, and control systems, posing unique analytical challenges. The integration of semantic technologies with information granulation and fuzzy granular computations creates a robust framework for synthesizing disparate datasets into actionable intelligence. By semantically enriching data granules and employing fuzzy logic to elucidate interrelationships, advanced security systems can more effectively identify anomalous patterns indicative of malicious activities. This methodological synergy is particularly valuable in scenarios where data uncertainty and the need for real-time decision-making converge, underpinning the development of adaptive, semantically aware cybersecurity infrastructures.

III. Methodology

This section articulates the proposed semantic methodology designed for the assessment and mitigation of malicious activity within smart city infrastructures, utilizing ontology-driven information granulation and knowledge fuzzy granular computations. The methodology comprises four integral phases: data collection, information granulation, fuzzy granular analysis, and semantic inference-based decision-making. Each phase is meticulously formulated to address the inherent complexities arising from the dynamic and heterogeneous semantic landscape of smart city environments.

A. Data Collection

The initial phase involves the systematic collection of security-related data from diverse sources within the smart city ecosystem. These sources encompass network traffic logs, sensor readings, device status reports, and user activity records. Given the vast and varied nature of this data, it is imperative to employ robust data aggregation mechanisms that ensure the integrity, accuracy, and timeliness of the collected information.

Table I provides an overview of the various sources from which data is aggregated in a smart city, highlighting the diversity and complexity of the data landscape.

Table I
Data Collection Sources in Smart City Infrastructure

Source	Data type	Example Devices	Description
Network traffic logs	Structured, time-series	Routers, gateways, switches	Logs capturing data packets exchanged among IoT devices
Sensor readings	Numerical, continuous	Temperature sensors, air quality monitors	Real-time measurement of environmental and operational parameters
Device status reports	Structured, categorical	Smart meters, surveillance cameras	Periodic reports on device health and performance
User activity records	Structured, textual	Mobile applications, online portals	Records of interactions through smart applications

B. Information Granulation

This process is pivotal in reducing computational complexity and enhancing the interpretability of the data. The granulation process can be executed through various methodologies, including:

Clustering Algorithms: Techniques such as K-means, hierarchical clustering, or density-based clustering are employed to group data points exhibiting similar characteristics. These algorithms operate by minimizing intra-cluster variance while maximizing inter-cluster differences, thereby forming distinct granules that encapsulate specific patterns or behaviors within the data.

Discretization Methods: Continuous variables are transformed into discrete categories through methods like equal-width binning or entropy-based discretization. This transformation facilitates the handling of continuous data by converting it into categorical granules, which are more amenable to analysis within the granular computing framework.

Rough Set Theory: This approach deals with the vagueness and ambiguity inherent in data by approximating uncertain concepts through lower and upper approximations, effectively creating granules that represent the boundary regions of these concepts.

The selection of an appropriate granulation technique is contingent upon the specific characteristics of the dataset and the nature of the security threats under consideration. The primary objective is to construct granules that encapsulate meaningful patterns, thereby facilitating more efficient and insightful analysis.

Table II summarizes the various techniques used for information granulation, discussing their respective benefits and challenges of managing complex and uncertain data.

Table II
Data Collection Sources in Smart City Infrastructure

Technique	Advantages	Limitations	Description
Clustering algorithms	Simplifies high-dimensional data; enhances pattern recognition	Sensitive to initialization and parameter tuning	Grouping data into clusters based on similarity metric (e.g., K-means, hierarchical clustering)
Discretization methods	Reduces computational complexity; improves interpretability	May oversimplify and lose subtle data variations	Converting continuous variables into discrete categories (e.g., equal-width binning)
Rough set theory	Effective with incomplete data; reduces uncertainty	Computationally intensive; less intuitive	Approximating data with lower and upper bounds to manage vagueness
Fuzzy granular method	Captures uncertainty effectively; offers flexible classification	Requires careful design of membership functions	Utilizing fuzzy logic to assign degrees of membership to date granules

C. Fuzzy Granular Analysis

Following the formation of information granules, the next phase involves the application of fuzzy granular analysis to assess the behavior of these granules under conditions of uncertainty. This analysis is conducted through the following steps:

Fuzzy Membership Function Design: For each granule, a membership function is defined to quantify the degree to which individual data points belong to the granule. These functions assign membership values ranging between 0 and 1, thereby accommodating the inherent fuzziness and partial truth present in real-world data.

Fuzzy Rule Base Construction: A comprehensive set of fuzzy rules is formulated to capture the relationships and interactions among different granules. These rules take the form of "IF-THEN" statements, where the antecedent specifies a condition based on the membership values of certain granules, and the consequent delineates the corresponding action or inference.

Fuzzy Inference Mechanism: Utilizing the constructed rule base, a fuzzy inference system is employed to evaluate the current state of the system. This mechanism integrates the membership values and applies the fuzzy rules to derive conclusions or predictions regarding potential security threats.

Defuzzification Process: The outcomes of the fuzzy

inference are typically in the form of fuzzy sets. To facilitate actionable decision-making, these fuzzy results are transformed into crisp values through defuzzification techniques, such as the centroid method or the maximum membership principle. This fuzzy granular analysis enables the system to effectively manage uncertainty and imprecision, thereby enhancing its capability to detect subtle and sophisticated malicious activities that may elude traditional binary classification approaches.

D. Semantic Inference-Based Decision-Making

The final component of the methodology encompasses the decision-making process, wherein the insights garnered from the fuzzy granular analysis are utilized to inform and execute appropriate security measures. This process involves:

Threat Level Assessment: The defuzzified outputs are interpreted to ascertain the severity and immediacy of identified threats. This assessment facilitates the prioritization of response actions based on the potential impact and urgency of the threats.

Response Strategy Formulation: Tailored response strategies are devised corresponding to the assessed threat levels. These strategies may encompass actions such as alert generation, automated system reconfigurations.

Iterative Semantic Feedback and Knowledge Refinement: To ensure adaptability and resilience, a feedback mechanism is established, where in the outcomes of implemented security measures are monitored and analyzed. This feedback enables the system to learn from past incidents, refine its fuzzy rule base, and adjust its granulation parameters, thereby perpetually enhancing its efficacy in threat detection and mitigation.

By integrating these components into a cohesive framework, the proposed methodology offers a robust and adaptive approach to cybersecurity within smart city infrastructures. It effectively addresses the challenges posed by data heterogeneity, volume, and uncertainty, thereby perpetually enhancing its efficacy in knowledge-driven threat detection and semantic mitigation.

IV. Intrusion Detection in Smart Cities

This study explores a machine learning-enhanced IDS framework underpinned by "semantic technologies", which enable contextualized threat analysis through ontological modeling and knowledge representation. Smart cities rely on IoT networks to optimize critical services—traffic control, energy distribution, and public safety—yet their interconnectivity exposes vulnerabilities to attacks like DoS, DDoS, Sybil, and DNS exploits. Conventional security mechanisms, constrained by static rule-based methodologies, struggle to interpret heterogeneous data streams or infer relationships between network entities. Semantic technologies address this gap by formalizing domain-specific taxonomies (e.g., device roles, attack patterns) and enabling reasoning over contextualized data. By enriching machine learning models with semantic metadata, IDS achieve enhanced interpretability and adaptive threat detection, aligning anomalous behaviors with predefined ontologies. This synergy ensures real-time, intelligence-driven mitigation of sophisticated cyber threats in IoT-dependent urban ecosystems.

A. Methodology

The IDS framework employed in this study integrates machine learning algorithms to enhance detection capabilities. The methodology encompasses the following stages: *Data Collection:* Network traffic data is gathered from various IoT devices within the smart city infrastructure. This dataset includes normal operational data and records of known attack patterns.

Feature Extraction: Relevant features are extracted from the collected data to serve as inputs for machine learning models. These features may include packet size, frequency, source and destination IP addresses, and protocol types.

Model Training: Machine learning classifiers, such as Artificial Neural Networks (ANN), Support Vector Machines (SVM), and Deep Neural Networks (DNN), are trained using the extracted features to distinguish between normal and malicious traffic patterns. *Detection and Response:* The trained models are deployed within the IDS to monitor real-time network traffic. Upon detection of anomalies indicative of potential intrusions, predefined response mechanisms are activated to mitigate the identified threats.

Table III presents the comparative performance metrics of various machine learning classifiers used in the IDS, emphasizing the trade-offs between detection accuracy and computational resources.

B. Results and Discussion

The implementation of the machine learning-based semantic intrusion detection system (SIDS) demonstrated significant advances in discerning diverse cyber threats within the smart city IoT knowledge graph. In particular, the system achieved an elevated accuracy in identifying DoS / DoS attacks, with lower false positive rates compared to traditional signature-based SIDS. The adaptive capacity of semantic neural networks enabled the system to recognize novel, semantically contextualized attack patterns, thereby fortifying the overall semantic security posture of the smart city knowledge infrastructure. However, computational overhead and energy consumption challenges were observed, particularly in resource-constrained semantic IoT endpoints.

The integration of ontology-driven information granulation, knowledge graph-enhanced fuzzy granular computations, and semantic machine learning within our

Table III
Data Collection Sources in Smart City Infrastructure

Classifier	Accuracy (%)	False positive rate (%)	False negative rate (%)	Computational overhead	Notes
Artificial Neural Network (ANN)	97	2.5	2.0	Moderate	High adaptability; requires extensive training
Support Vector Machine (SVM)	94	3.5	3.0	High	Effective in high dimensional feature spaces
Deep Neural Network (DNN)	98	2.0	1.5	High	Superior detection performance; resource-intensive
Random Forest	95	3.0	2.5	Low to moderate	Robust against overfitting; faster training times

SIDS framework provides a multi-faceted, knowledge-centric approach to addressing the inherent cybersecurity challenges of smart city infrastructures. Findings from our experimental evaluations and case study underscore several critical dimensions warranting in-depth semantic analysis.

The application of ontology-driven information granulation significantly attenuates the complexity of voluminous and semantically heterogeneous IoT data. By decomposing raw security telemetry into semantically coherent granules, aligned with domain ontologies, the framework not only reduces computational overhead but also enhances the semantic interpretability of underlying knowledge patterns. This aligns with theoretical insights from granular computing, which emphasize the cognitive advantage of processing knowledge in clustered semantic forms (Zadeh, 1965; Livi & Sadeghian, 2014). However, the efficacy of this approach is contingent upon the optimal instantiation of ontological granulation parameters.

The incorporation of knowledge graph-enhanced fuzzy granular computations has been instrumental in managing the pervasive epistemological uncertainty associated with cyber threat indicators within smart city knowledge domains. Semantic fuzzy logic enables the representation of security events as continuous membership functions, informed by knowledge graph relationships, thereby allowing the system to capture nuanced semantic anomalies overlooked by conventional binary models. This semantic fuzzy approach enhances the robustness of threat evaluation by providing graded, knowledge-driven risk assessments, facilitating nuanced semantic decision-making. However, the formulation of an effective, ontology-driven fuzzy rule base presents a significant challenge. The system's sensitivity to the selection of membership functions and rule thresholds necessitates iterative semantic calibration and expert ontological intervention.

Furthermore, the deployment of semantic neural networks has demonstrated considerable promise in classifying network behaviors with high semantic accuracy. The adaptive nature of these models allows the SIDS to learn complex, knowledge-driven patterns of both normative and malicious traffic, improving its ability to detect novel, semantically contextualized attack vectors. However, the integration of semantic machine learning introduces additional computational demands, particularly in resource-constrained semantic IoT environments. The observed trade-offs between detection performance and computational efficiency underscore the need for further ontological optimization, potentially through distributed knowledge processing or lightweight semantic model architectures.

In synthesizing these components, our framework represents a holistic, knowledge-driven departure from traditional signature-based SIDS. The synergistic application of ontology-driven granular computing, semantic fuzzy logic, and semantic machine learning enhances detection accuracy and provides a flexible, knowledge-adaptive platform. The continuous semantic feedback mechanism augments its ontological resilience, enabling real-time parameter tuning and knowledge graph refinement.

Despite these advancements, limitations warrant attention. The reliance on synthetic, semantically annotated datasets may limit external validity. Real-world deployments will encounter more heterogeneous, unpredictable, and knowledge-rich data streams, necessitating extensive field testing and iterative ontological refinement. Moreover, the balance between computational resource allocation and detection efficacy remains a critical constraint, particularly as smart city knowledge infrastructures scale.

This study elucidates the potential of integrating advanced semantic techniques to enhance cybersecurity in smart city knowledge domains. By addressing semantic heterogeneity, epistemological uncertainty, and computational constraints, our framework lays the groundwork for resilient and adaptive SIDS. A review of academic literature and case studies on advanced SIDS in smart cities underscored the importance of managing knowledge uncertainty and computational complexity through semantic granular and fuzzy methodologies (e.g., Livi & Sadeghian, 2014; Kozik et al., 2019). These insights informed the in-depth semantic discussion presented.

V. Conclusion

In summary, this study has significantly advanced the discourse on cybersecurity for smart city infrastructures by proposing an integrated framework that

synergistically combines information granulation, fuzzy granular computations, and machine learning techniques within a semantic technologies context. The framework addresses the inherent challenges of dynamic, heterogeneous, and high-dimensional urban data by leveraging semantic enrichment to transform raw data into coherent, meaning-laden granules. This transformation not only reduces computational complexity but also enhances interpretability through semantic annotations and ontological mappings, thereby enabling more robust anomaly detection.

The accompanying tables encapsulate critical facets of the research: Table 1 delineates the diverse data sources essential for smart city security analytics; Table 2 provides a comparative evaluation of semantic-based information granulation techniques; and Table 3 offers insights into the performance of machine learning classifiers for intrusion detection within semantically enriched environments. Collectively, these empirical findings underpin the methodological framework and substantiate its efficacy.

Moreover, the incorporation of fuzzy granular computations has empowered the framework to manage uncertainty more effectively, offering a nuanced, graded assessment of cyber threats—a notable improvement over traditional binary classification approaches in complex IoT ecosystems. The integration of adaptive machine learning models, particularly artificial neural networks, has demonstrated considerable potential in capturing intricate patterns and novel attack vectors, thereby bolstering the overall accuracy and responsiveness of the intrusion detection system.

Despite these promising contributions, the study acknowledges several limitations. The reliance on synthetic datasets for initial training and evaluation may constrain the external validity of the findings, and the computational demands of the integrated approach pose challenges for deployment in resource-constrained IoT environments.

In conclusion, by harnessing the capabilities of semantic technologies, the proposed framework represents a substantive step toward developing more resilient and adaptive cybersecurity solutions for smart cities. Future research should focus on refining granulation parameters, automating the fuzzy rule base, and further integrating semantic ontologies and knowledge graphs to accommodate emerging threats in evolving urban infrastructures. Such endeavors will be critical to ensuring the sustained security and operational integrity of smart city ecosystems in an increasingly interconnected digital landscape.

References

[1] Livi L., & Sadeghian, A., Data granulation by the principles of uncertainty. arXiv preprint arXiv:1407.7138. 2014.

[2] Kozik R., Pawlicki M., Choraś, M., & Pedrycz, W., Practical employment of granular computing to complex application layer cyberattack detection. Complexity, 2019, Article ID 5826737.

[3] Zadeh, L. A., Fuzzy sets. Information and Control, 8(3), Publisher: Elsevier, 1965. pp.338–353.

[4] Jain, A. K., Murty, M. N., & Flynn, P. J., Data clustering: A review. ACM Computing Surveys, 31(3), Publisher: ACM, 1999, pp.264–323.

[5] Ahmed, M., Mahmood, A. N., & Hu, J., A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, Publisher: Elsevier, 2016, pp. 19–31.

[6] Lyon, J., Intrusion detection: A survey. Computer Networks, 34(4), Publisher: Elsevier, 2001, pp. 579–595.

[7] Cocchia, A., Smart and digital city: A systematic literature review. In Smart City, Publisher: Springer, 2014, pp. 13–43.

[8] Zadeh, L. A., Fuzzy logic = computing with words. IEEE Transactions on Fuzzy Systems, 4(2), Publisher: IEEE, 1996, pp. 103–111.

[9] Pedrycz, W., & Kurgan, L., Advances in Granular Computing. IEEE Intelligent Systems, 22(6), 2007, pp. 76–81.

[10] Bargiela, A., & Polishchuk, V., Granular Computing for Knowledge Discovery. Journal of Intelligent Information Systems, 23(1), 2004, 15–35.

ОСОБЕННОСТИ ОЦЕНКИ ВРЕДОНОСНОЙ АКТИВНОСТИ В ИНФРАСТРУКТУРЕ УМНОГО ГОРОДА НА ОСНОВЕ ГРАНУЛЯЦИИ ИНФОРМАЦИИ И НЕЧЕТКО-ГРАНУЛЯРНЫХ ВЫЧИСЛЕНИЙ

Клычев А., Тагангылыжов И.

Повсеместная интеграция цифровых инфраструктур в городскую среду, одновременно повышая эффективность работы умных городов, одновременно порождает сложные уязвимости в системе безопасности. Традиционные парадигмы кибербезопасности, основанные на детерминированных моделях, часто оказываются неадекватными при решении динамической и эпистемически неопределенной природы киберугроз. Это исследование представляет новую методологическую структуру, использующую грануляцию информации на основе онтологии и нечеткие гранулярные вычисления, улучшенные графом знаний, для облегчения семантической оценки и смягчения последствий вредоносных действий. Преобразуя необработанные телеметрические данные безопасности в семантически обогащенные гранулы, становится возможным извлечение контекстуальных знаний, что повышает эффективность выводов. Тематическое исследование, в котором используются семантические системы обнаружения вторжений (SIDS) в моделируемом «умном городе», раскрывает потенциал этой структуры для проактивного, основанного на знаниях обнаружения угроз и стратегий семантического реагирования.

Received 21.03.2025