International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Soft Topology for Cyber Threat Intelligence: A Knowledge Graph Perspective

R. Deepa[1], K. Amutha [2], M. Kiruthika[3],
R. Vijaya Chandra[4], A. P. Saravanan[5]
[1]Assistant Professor, Department of Mathematics,
Excel Engineering College, Namakkal, INDIA
e-mail: deepssengo@gmail.com
[2]Associate Professor, Department of Mathematics,
Meenakshi Sundararajan Engg College, Chennai, INDIA
e-mail: amutha_palanivel@@yahoo.com
[3]Assistant Professor, Department of Mathematics,
Suguna College of Arts and Science, Coimbatore, INDIA
e-mail: scaskiruthika@gmail.com
[4]Professor of Mathematics,
Nandha College of Technology, Erode, INDIA
e-mail: risrchandra@gmail.com
[5]Assistant Professor, Department of Mathematics,
Erode Sengunthar Engineering College, Perundurai, INDIA
e-mail: spsaravanan08@gmail.com

Abstract

Cyber threat intelligence (CTI) increasingly relies on knowledge graphs (KGs) to represent entities, relationships, and context across vulnerabilities, exploits, actors, and mitigations. Real-world CTI is, however, uncertain and parameter-dependent: intelligence feeds vary in confidence, temporal validity, and applicability. In this paper we introduce a *soft-topological* framework for cybersecurity knowledge graphs (ST-CKG). Our framework integrates soft set theory and soft topology with KG representations to model parameterized uncertainty and dynamic relationships. We define soft-open subgraphs, soft-closure and boundary operators, soft-connected components, and soft-continuous mappings to formalize KG evolution and risk propagation. A prototype implementation built from public CTI sources demonstrates the framework's utility in identifying robust threat clusters and emerging vulnerabilities. We discuss applications in threat prioritization, risk assessment, and cyber situational awareness, and outline directions for future research.

1 Introduction

Knowledge graphs have become central in modeling cyber threat intelligence: they encode entities (CVE identifiers, software products, threat actors), relationships (exploits, targets, mitigations), and contextual metadata (confidence, timestamps, sources). Despite progress in automated KG construction and graph-based analytics, a fundamental challenge remains: CTI is inherently uncertain and context-dependent. Data items and relations may be valid only under certain conditions (e.g., threat confidence levels, temporal windows, or attacker capabilities). Conventional graph and KG representations lack a lightweight, principled way to represent such *parameter-dependent* uncertainty.

Soft set theory (Molodtsov, 1999) offers a parameterized set-theoretic model for uncertainty; soft topology extends these ideas to topological operators such as opens, closures, and continuity in a

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

parameter-aware manner. We propose a novel integration: *Soft Topology for Cyber Threat Intelligence* (ST-CKG). The central idea is to treat KG entities and relations as elements of soft sets indexed by security-relevant parameters (e.g., threat confidence, time windows, attacker sophistication). Soft-topological operators then enable analysis of parameter-specific subgraphs, boundary nodes, and connectivity patterns.

This manuscript presents: (1) formal definitions for ST-CKG, (2) algorithms for computing soft-topological operators on KGs, (3) a prototype case study using public CTI sources, and (4) discussion of applications and limitations.

2 Related Work

Cybersecurity Knowledge Graphs. Recent surveys summarize methods for building CTI KGs, including NLP-based extraction, ontology design, and reasoning methods [2, **?**]. These approaches emphasize schema and embedding techniques but do not address parameterized uncertainty in a topological manner.

Soft Sets and Soft Topology. Soft set theory and its topological variants have been developed to model parameterized uncertainty and soft-open/closed operators [1, 5]. Applications appear in decision-making, image analysis, and graph-theoretic models (soft graphs, fuzzy-soft graphs) but rarely in cybersecurity.

Soft Graph Models. There are several works on soft graphs and neutrosophic soft graphs that combine soft set ideas with graph theory [3, 4]. These provide a basis for soft-topological constructs on graphs.

3 Preliminaries

We briefly recall soft set and soft topology notions used throughout.

3.1 Soft Sets

Let U be a universe (here, KG entities), and let P be a set of parameters (e.g., threat confidence levels, time windows). A *soft set* over U with parameters P is a pair (F, A) where $A \subseteq P$ and $F : A \to \mathcal{P}(U)$ assigns to each parameter a subset of U. Intuitively, $F(p)$ denotes elements relevant under parameter p.

3.2 Soft Topology

A *soft topology* on (U, P) is a collection of soft sets satisfying: (i) the null soft set and the whole soft set belong to , (ii) arbitrary soft unions of members of are in , and (iii) finite soft intersections of members of are in . Soft-open, soft-closed, soft-interior, and soft-closure are defined analogously to classical topology but per-parameter.

3.3 Cybersecurity Knowledge Graphs

A CTI knowledge graph is a directed labeled graph $G = (V, E)$ with metadata functions assigning attributes such as confidence scores and timestamps to nodes and edges. We treat V as the universe U for soft-set constructions; edges also admit parameterized soft assignments.

4 Soft-Topological Framework for CKGs

4.1 Parameter Design

Choose a parameter set P relevant to the cybersecurity domain. Example parameters include:

- Threat confidence: {low, medium, high}
- Temporal windows: {last-6m, 6m–12m, older}

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- Attacker sophistication: $\{\text{script-kiddie}, \text{organized}, \text{APT}\}$
- CVSS severity buckets: $\{\text{low}, \text{medium}, \text{high}, \text{critical}\}$

4.2 Soft Sets on Vertices and Edges

For each $p \in P$, define a vertex-soft-set $F_V(p) \subseteq V$ (entities relevant under p) and an edge-soft-set $F_E(p) \subseteq E$ (relations valid under p). These assignments may be obtained from KG metadata: e.g., edges with confidence ≥ 0.8 belong to $F_E(\text{high})$.

4.3 Soft-Open Subgraphs

Given a soft set (F_V, A), the soft-open subgraphs for parameter $p \in A$ are the induced subgraphs $G[F_V(p)]$ using edges from $F_E(p)$. A family of such induced subgraphs over parameters captures KG views under varying contexts.

4.4 Soft Closure and Boundary

Define the soft-closure of a vertex set $S \subseteq V$ under parameter p by:

$$\text{cl}_p(S) = S \cup \{v \in V : \exists u \in S \text{ s.t. } (u, v) \in F_E(p)\}. \tag{1}$$

The soft-interior $\text{int}_p(S)$ is the complement of the soft-closure of the complement. The soft-boundary $\partial_p(S) = \text{cl}_p(S) \setminus \text{int}_p(S)$ identifies vertices that lie on the fringe under parameter p.

4.5 Soft-Connected Components and Paths

For each $p \in P$, connectivity is classical graph connectivity restricted to edges in $F_E(p)$. The family of p-connected components across parameters yields a parameterized connectivity profile for subgraphs.

4.6 Soft-Continuous Mappings for KG Updates

A KG update or a mapping $f : G \to G'$ is called *soft-continuous* if for every soft-open subgraph U' of G' the preimage $f^{-1}(U')$ is soft-open in G. This models stable transformations of CTI under parameterized uncertainty.

5 Algorithms

We outline algorithms to compute core soft-topological operators on practical KGs.

5.1 Building Soft Sets from Metadata

Inputs: KG $G = (V, E)$ with metadata (confidence, time), parameter definitions P, thresholding rules.

1. For each $p \in P$, compute $F_V(p) = \{v : \text{ meta}(v) \text{ satisfies } p\}$.
2. For each $p \in P$, compute $F_E(p) = \{e = (u, v) : \text{ meta}(e) \text{ satisfies } p\}$.

5.2 Computing soft-closure

Algorithm: for each p, perform one-step neighborhood expansion on S restricted to $F_E(p)$. This is $O(|E_p|)$ per parameter using adjacency lists.

5.3 Soft-connected components

For each p, run BFS/DFS restricted to $F_E(p)$. Complexity linear in the size of the parameter-specific subgraph.

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

6 Case Study

We implemented a prototype ST-CKG pipeline using public CTI sources: CVE/NVD and MITRE ATTCK.

6.1 Data ingestion and KG creation

We extract CVE nodes, software nodes, and exploit relations. Edges were annotated with timestamps and source confidence (derived from feed reliability). Parameters chosen: $P = \{\text{high-conf}, \text{med-conf}, \text{recent}\}$.

6.2 Analyses performed

- Soft-connectedness under *high-conf* to identify robust exploit chains.
- Soft-boundary computation for sets of critical CVEs to identify vulnerable fringe nodes.
- Simulation of KG update (ingestion of a new feed) modeled as a soft-continuous mapping to observe stability of clusters.

6.3 Key findings

Preliminary results show: (i) certain actor-CVE clusters persist across parameters (robust threats); (ii) many CVEs appear only in low-confidence or older parameters (emerging or noisy signals); (iii) boundary CVEs highlight candidates for prioritization.

7 Applications

- **Threat Prioritization**: patch or monitor soft-boundary CVEs that bridge clusters under high-confidence parameters.
- **Risk Propagation**: soft-connected paths under increased attacker capability parameters show potential cascading risks.
- **Analyst Dashboards**: parameter toggles to visualize soft-open subgraphs for situational awareness.

8 Discussion

We discuss theoretical and practical trade-offs: parameter design and thresholding require domain expertise; soft-set assignment may use heuristics or ML; scalability can be achieved by parallel parameter processing. The framework complements probabilistic and embedding-based KG methods by offering explicit parameterized set-theoretic structure.

9 Conclusion and Future Work

This paper introduced ST-CKG, a soft-topological framework for cybersecurity knowledge graphs. Future work includes automated parameter learning, integration with probabilistic soft logic, development of soft-topological invariants (soft Betti numbers), and UX studies for analyst adoption.

10 Elaborate Explanation of Soft Connectedness in Threat Communities

Soft-connectedness plays a crucial role in analyzing the structural integrity of threat communities in cybersecurity knowledge graphs (KGs). A threat community is a group of entities—such as malware families, vulnerabilities, exploits, IP addresses, and command-and-control (C2) servers—that collectively represent an adversarial ecosystem. The relationships among these nodes include shared infrastructure, attack similarity, behavioral overlap, or co-occurring exploit usage.

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Soft topology enhances the classical notion of connectedness by incorporating uncertainty, partial information, and parameter-driven semantics. In cybersecurity contexts, parameters may represent behavior classes, severity ratings, attack stages, or observable threat attributes.

10.1 Soft-Connectedness and Its Importance

In a soft-topological threat space (U, T), a subset $C \subseteq U$ representing a threat community is said to be soft-connected if it cannot be partitioned into two disjoint soft-open sets. This means that no combination of uncertainty parameters can separate the community into independent components.

This property is essential because real-world threat intelligence frequently contains incomplete or conflicting data. For example, malware families may exhibit overlapping behaviors across campaigns, and APT (Advanced Persistent Threat) groups may reuse infrastructure in inconsistent patterns.

10.2 Interpretation Through Cyber Threat Intelligence

Let C be a cluster of malicious entities in a knowledge graph. Under parameter sets representing attributes such as attack stage, behavior category, or severity level, a soft-open set contains nodes that share a consistent attribute profile. If every soft-open set describing the threat properties overlaps with others, then C cannot be split by any parameter configuration and is considered soft-connected.

This means that the threats form a cohesive operational unit, even if described under uncertain or partially known conditions.

10.3 Example: Threat Behavior Overlap

Consider a KG that contains nodes representing malware families (MalwareA, MalwareB), exploits (ExploitX, ExploitY), and C2 servers (C2Server1). Suppose the following parameter-driven soft-open sets are defined:

- Execution behavior: contains MalwareA, MalwareB, ExploitX
- Persistence behavior: contains MalwareA, MalwareB
- Delivery behavior: contains MalwareA, ExploitY

Since each of these soft-open sets overlaps significantly, no parameter can partition the community into fully disjoint soft-open subsets. Therefore, the threat community represented by these nodes is soft-connected.

10.4 Implications for Cybersecurity

Soft-connectedness helps analysts validate whether nodes in a KG genuinely represent a unified threat ecosystem. Its applications include:

- Identifying cohesive threat clusters despite uncertainty
- Tracing multi-stage attacks through evolving parameter sets
- Modeling APT campaigns exhibiting inconsistent patterns
- Supporting robust classification of threat entities

This provides a mathematically grounded approach for interpreting incomplete or evolving threat intelligence within complex cyber ecosystems.

11 Additional Theoretical Foundations

[Soft-Topological Threat Neighborhood Theorem] Let (U, E) be a soft set universe representing cyber entities and attributes. If T is a soft topology on (U, E), then for any threat entity $t \in U$, the soft neighborhood system $N_T(t)$ forms a directed subgraph of the cybersecurity knowledge graph.

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Given a soft-open set $(F, A) \in T$ containing t, all related entities in $F(a)$ for $a \in A$ represent attribute-consistent neighbors. Since KG edges encode attribute or relational consistency, all nodes in the soft-open set maintain directed reachability, forming a directed subgraph.

[Soft Closure of Threat Propagation] For a threat node t, the soft closure $\text{cl}_T(\{t\})$ captures all nodes reachable under uncertain propagation paths in the KG.

Soft closure includes all nodes belonging to every soft-closed set containing t. Since propagation involves uncertain paths (malware spread, privilege escalation), soft-closed sets represent maximal containment sets under parameters. Their intersection yields all reachable uncertain nodes.

[Soft Boundary of Vulnerability Zones] Let V be a set of vulnerability nodes. The soft boundary $\partial_T(V)$ represents entities with partial or conflicting vulnerability attributes.

Boundary is defined as $\text{cl}_T(V) - \text{int}_T(V)$. Nodes that are uncertain members of vulnerability zones appear only in the closure but not in the interior, capturing partial overlap in KG attribute consistency.

[Soft Connectedness in Threat Communities] If $C \subseteq U$ is a threat community, then C is soft-connected iff it cannot be partitioned into two disjoint soft-open subgraphs.

Directly from soft-connectedness definition: if such a partition existed, there would be two disjoint soft-open sets covering C, contradicting the semantic continuity of threat relationships in KG.

[Continuity of Threat Evolution Mapping] Let $f : (U, T) \to (U', T')$ represent a mapping between soft-topological threat spaces. If f preserves soft-open sets, then it preserves evolving attack signatures in both KGs.

If f is soft-continuous, then $f^{-1}(G, B) \in T$ for every $(G, B) \in T'$. Thus evolving threat signatures mapped into (U', T') can be traced back to consistent soft-open threat sets in (U, T).

References

[1] D. Molodtsov, *Soft set theory—first results*, Computers & Mathematics with Applications, 1999.

[2] Survey on Cybersecurity Knowledge Graphs, Knowledge and Information Systems, 2023.

[3] M. Akram, S. Shahzadi, *Neutrosophic Soft Graphs*, 2016.

[4] R. K. Thumbakara et al., *Soft Graphs*, 2014.

[5] Generating Soft Topologies via Soft Set Operators, MDPI Symmetry, 2022.

Received: August 10, 2025