Concept Mapping: Renewing Learning and Thinking
Proc. of the Eighth Int. Conference on Concept Mapping
Medellín, Colombia 2018

REPRESENTING CONCEPTUALIZED DYNAMIC NETWORK KNOWLEDGE FOR CYBER-SITUATIONAL AWARENESS

Leslie F. Sikos[1], Dean Philp[2], Markus Stumptner[1], Wolfgang Mayer[1], Catherine Howard[2] & Shaun Voigt[2]
[1]University of South Australia, Australia
[2] Defence Science and Technology Group, Australia

Abstract. The formal representation of domain knowledge for communication networks, including computer and IoT networks, provides a way to overcome the syntactic and semantic interoperability issues of data integration. The concepts of expert knowledge and real-world network entities can be captured in ontologies at different levels of abstraction, and their properties described using restrictions that utilize mathematical logic. The dynamic nature of these concepts can be efficiently captured using provenance-aware statements, which can be used for querying and inferencing, thereby providing automated support for cyber-situational awareness. The visualization of these network concepts can help analysts understand network topology and traffic flow. Options to visualize network knowledge include, but are not limited to, conceptual graphs, concept maps, RDF graphs, named graphs, hypergraphs, and property graphs, the last three of which correspond to the dominant graph data models. Different representations, however, have different benefits and drawbacks, such as concept maps provide simple representations with no technical knowledge required, while RDF graphs have global identifiers for network entities and namespace prefixes for all terms, but require some familiarity with knowledge engineering to interpret. By using concept maps, network concepts and entities can be represented intuitively, allowing people at various levels of technical expertise to collaborate in network analysis. Concept maps can represent both one-way and two-way relationships between network concepts and individuals, allowing the categorization of concepts and relationships, and can capture temporal relationships as well. While conceptual maps are inherently informal, they can also represent precise machine-interpretable statements that utilize OWL ontology terms (by applying a set of conventions). The graphical representation of network knowledge can integrate network knowledge from diverse sources, such as open data, routing messages, and network device configuration files. A concept map of network knowledge can not only represent networking concepts, such as autonomous systems, routers, servers, and workstations, but may also indicate direct/indirect connection between network devices, inconsistencies in routing, suspicious traffic flow, and misconfigurations. Illustrating complex relationships and documenting network knowledge at different levels of abstraction may require other visualization options, such as conceptual graphs and RDF graphs, especially when specific elements have to be represented or implicit knowledge captured, more structure is needed, network entities have to be defined using a global web identifier, or the relationships between concepts need to be described precisely with mathematical logic. Because RDF graphs may be simplified to concept maps to make it easier to comprehend network topology while preserving most of the semantics of the more comprehensive representation, it is possible to exploit the benefits of both representations simultaneously to find related concepts and connected entities, and facilitate network knowledge discovery.

***Keywords**:* concept map, RDF graph, hypergraph, cybersecurity, cyber-knowledge