Supporting the Intelligence Analysis stages with Approximate Reasoning: Methods and Tools based on Granular Computing

Abstract

Le attuali minacce, come il terrorismo e il cyber-terrorismo, pongono nuove sfide alle comunità della sicurezza e della difesa. Appare cruciale la capacità di ragionare con diverse prospettive e di rilevare connessioni tra fatti, relazioni ed eventi. A tal fine, è utile un approccio meno procedurale e meno normato, in grado di fare leva sulle attuali tecnologie di intelligenza computazionale e artificiale per rilevare minacce e proteggere i sistemi fisici e cyber-fisici. Ciò solleva un forte interesse delle summenzionate comunità per la definizione e l'adozione di nuovi metodi e tecniche che, in una certa misura, siano tali da replicare, o almeno supportare, i processi cognitivi umani. Se consideriamo la "creatività" alla base di alcuni recenti attacchi, come quello del 11/09/2001, possiamo comprendere la necessità di ripensare la sicurezza in termini situazionali più che procedurali, e questo ha un'importante implicazione che aiuta a inquadrare il nostro problema e gli obiettivi di ricerca. Questa implicazione è un passaggio dall'essere consapevoli di ciò che dobbiamo prevenire (e delle relative norme e procedure a tal fine) all'acquisire maggiore consapevolezza di ciò che potrebbe accadere. Da qui emerge l'utilità di metodi e strumenti che supportano i decisori nella loro capacità di effettuare analisi di tipo speculativo che permettono di ipotizzare differenti scenari di minaccia, e ragionare sulle dinamiche di evoluzione di tali scenari. Questo è, sostanzialmente, l'obiettivo principale delle cosiddette attività di intelligence.

Il problema di ricerca affrontato in questi tre anni di studio è come migliorare la consapevolezza degli analisti e dei decisori nelle prime fasi di un'analisi di intelligence per prevenire attacchi intenzionali (terrorismo) e gli obiettivi specifici riguardano la definizione e validazione di metodi di reasoning approssimato basati sul Granular Computing (GrC) a tal fine. Nello specifico, sono stati definiti e validati metodi per:

- effettuare l'analisi ed assessment di ipotesi di attacco intenzionale, per attribuire tali ipotesi a gruppi terroristici;
- Partizionare in maniera sicura un target d'attacco per supportare i decisori nella definizione di strategie ed azioni per difendere il target in analisi;
- Analizzare l'evoluzione dell'attacco alla luce delle dipendenze tra componenti di un target, ed effettuare una stima della resilienza del target.

I risultati condividono una base metodologica comune che consiste dell'utilizzo di rough sets e loro estensioni, come fuzzy rough sets e dominance based rough sets, per l'analisi ed il processing dei dati, e di modelli di 3 way decisions per ridurre l'effort cognitivo dei decisori nella fase decisionale. I tre metodi definiti sono tesi a rinforzare i cicli di intelligence.

Il primo metodo combina teoria della probabilità, fuzzy e rough sets per analizzare differenti scenari di attacco ed attribuirli a gruppi terroristici noti. In primo luogo, permette di collezionare evidenze in termini di similarità di comportamento dei gruppi noti a partire da un data set storico di eventi terroristici. Ciò avviene grazie ad un algoritmo che combina classi di equivalenza e classi di equivalenza fuzzy per derivare matrici di similarità tra gruppi terroristici. A valle di questa fase di collezione delle evidenze, partendo da informazioni di intelligence su possibili schemi di attacco, tipi di arma e tipi di target, il metodo proposto utilizza due parametri che consentono la derivazione e l'analisi di una vasta gamma di ipotesi e la loro valutazione sulla base di diversi livelli di supporto di evidenze. Ciò avviene tramite l'utilizzo di operatori OWA con distribuzione di probabilità per aggregare le informazioni che provengono dalle sorgenti di intelligence, e l'uso di un modello di probabilistic three way decisions basato sui rough sets bayesiani per effettuare una tri-partizione dei gruppi terroristici in gruppi associabili alle ipotesi create (POS), non associabili (NEG) o per i quali non si può prendere decisione (BND). La valutazione dei risultati è stata effettuata su dati reali relativi a cinque anni (2012-2016) di attività terroristiche estratti dal Global Terrorism Database (GTD). Per considerare solo le informazioni che si presumono disponibili nelle fasi inziali di un'analisi di intelligence, abbiamo ridotto le feature descrittive del GTD da 135 a 3: strategia d'attacco, tipologia di target e tipologia di arma. Il metodo è stato valutato su tre casi rappresentativi di tre situazioni: 1) un pattern raro, 2) un pattern distintivo, 3) una

combinazione di pattern. I risultati sono stati valutati rispetto a metriche di errore quali Sensitività, Specificità e Balanced accuracy.

Il secondo metodo ha lo scopo di supportare i decision maker nell'analisi e nella protezione di target d'attacco (come infrastrutture a larga scala o aree urbane) identificando un'adeguata partizione dell'infrastruttura o dell'area in analisi. Il metodo funziona su un insieme molto limitato di informazioni relative alle vulnerabilità dei componenti e informazioni probabilistiche su come le vulnerabilità possono impattare su partizioni significative. Sulla base di tali informazioni, il metodo prevede la definizione di Threat Scenarios, triple che includono: attacchi, perdite attese, e probabilità di avere perdite il cui valore sia al massimo pari a quello atteso. I Threat Scenarios sono comparati sulla base del principio della dominanza stocastica usando un approccio basato sui Dominance Rough Sets, nello specifico Dominance-based Rough Set Approach under uncertainty. I risultati del caso studio, che si basa sull'ipotesi di un attacco terroristico, mostrano che il metodo fornisce soluzioni approssimate che permettono di ragionare a diversi livelli di granularità (come singolo attacco o gruppi di attacchi). Un misura per capire la bontà delle partizioni risultanti, sia nel complesso rispetto ai singoli attacchi, è stata definita contestualizzando misure di qualità tradizionalmente usate nelle partizioni 3 way.

Il terzo metodo fa leva su un approccio di modellazione granulare gerarchica per definire granuli informativi dell'attacco e delle sue evoluzioni alla luce delle dipendenze tra i componenti di un target. Le dipendenze, di varia natura (fisica, cibernetica, logica o geografica), sono modellate con strutture granulari. I granuli informativi dell'attacco sono usati per effettuare una stima della resilienza del target, sulla base di un modello di resilienza operazionale opportunamente adattato per operazioni tra intervalli. Il metodo ha come elemento di originalità l'integrazione sistemica del GrC per l'analisi di resilienza, ed è stato validato su un caso di studio modellato su una smart grid. Richiede, comunque, sviluppi futuri per contestualizzarlo meglio al dominio di questa tesi.

Supporting the Intelligence Analysis stages with Approximate Reasoning: Methods and Tools based on Granular Computing

Abstract

Current threats, such as terrorism and cyber-terrorism, pose new challenges to security and defence communities, and the ability to reason with different perspectives and detecting connections between facts, relationships and events becomes crucial to address these challenges. To this purpose, a less procedural and standardized approach is useful, able to leverage current computational and artificial intelligence technologies to detect threats and protect physical and cyber-physical systems. This raises a strong interest in defining and adopting new methods and techniques that, to a certain extent, are such as to replicate, or at least to support, human cognitive processes. If we consider the "creativity" behind some recent attacks, such as that one of 09/11/2001, we can understand the need to rethink security in situational rather than procedural terms, and this has an important implication that helps to frame the problem and research objectives of this thesis. This implication is a shift from being aware of what we need to prevent (and the related rules and procedures to that end) to gaining greater awareness of what might happen. From this consideration, it emerges the need of methods and tools that support decision makers in their ability to carry out analyses that allow to hypothesize different threat scenarios, and to reason about their evolutions. This is, essentially, the main objective of the so-called intelligence activities.

The research problem investigated in the Ph.D period is how to improve the awareness of analysts and decision makers in the early stages of an intelligence analysis to prevent intentional attacks, and the specific objectives concern the definition and validation of reasoning methods based on Granular Computing (GrC) for this purpose. Specifically, methods to:

- carry out analysis and assessment of hypotheses of intentional attacks, and to attribute these hypotheses to terrorist groups;
- Define security perimeters to protect a target of attack;
- Analyse evolutions of an attack, considering also the dependencies between components of a target, and estimate the resilience of a target.

The results share a common methodological basis consisting of the use of rough sets and their extensions, such as fuzzy probabilistic rough sets and dominance based rough sets, for data analysis and processing, and models of 3 way decisions to reduce the cognitive effort of decision makers in the decision-making phase. The three methods defined are intended to support the intelligence cycle stages.

The first method combines probability theory, fuzzy and rough sets to analyse different attack scenarios, such as high probability -low risk and low probability - high risk, and attribute the assumptions of attack to known groups. It starts from a minimum set of information, vague and preliminary, to derive hypotheses concerning attack events and evaluate them with respect to a body of evidence collected from historical data on terrorism events. The body of evidence is defined in terms of similarity of behaviour of known groups. This is constructed with an algorithm that combines equivalence classes and fuzzy equivalence classes to derive similarity matrices of terrorist groups behaviours. After the phase of evidence collection, the proposed method uses two parameters that allow the derivation and assessment of a wide range of hypotheses, starting from intelligence information on possible attack strategies, weapon types and target types. This happens through the use of Ordered Weighted Averaging (OWA) operators with probability distribution to aggregate information coming from intelligence sources, and the use of a probabilistic three way decisions model based on Bayesian rough sets to carry out a tri-partition of terrorist groups into groups that can be: associated to the created hypotheses (POS), not associated (NEG) or for which no decision can be made (BND). The evaluation of results has been carried out on real data relating to five years (2012-2016) of terrorist activities extracted from the Global Terrorism Database (GTD). To consider only information that is assumed to be available in the initial phases of an intelligence analysis, we have reduced the descriptive features of the GTD from 135 to 3: attack strategy, type of target and type of weapon. The method has been experimented on three representative cases: 1) a rare pattern, 2) a distinctive pattern, 3) a combination of

patterns. The results have been evaluated with respect to error metrics such as Sensitivity, Specificity and Balanced accuracy.

The second method aims at defining security perimeters to defend targets of attack. Based on the information previously derived, and including estimates of expected losses, Threat Scenarios are defined and analysed to increase the security level of the target. The method supports decision makers in the analysis and protection of targets (i.e., large-scale infrastructures or urban areas) by identifying an adequate partition of the infrastructure or area being analysed. The method works on a very limited set of information related to components vulnerabilities and probabilistic information on how vulnerabilities can impact on significant partitions. Based on this information, the method involves the definition of Threat Scenarios, triples that include: attacks, expected losses, and probability of having losses whose value is at most equal to the expected one. Threat Scenarios are compared based on the principle of stochastic dominance using an approach based on Dominance Rough Sets, specifically Dominance-based Rough Set Approach under uncertainty. The results of the case study, based on a hypothesis of a terrorist attack derived from GTD events, show that the method provides approximate solutions that allow reasoning at different levels of granularity (such as a single attack or groups of attacks). A measure to understand the goodness of resulting partitions, both overall and with respect to specific attacks, has been defined by contextualizing quality measures traditionally used in the 3 way partitions.

The third method is devoted to analyse the evolution of an attack, and evaluates the resilience of the target considering also the dependencies between components of the target. The method relies on a hierarchical granular modelling approach to define information granules of the attack. Dependencies, of various kinds (such as physical, cybernetic, logical or geographical), are modelled with granular structures. The attack informative granules are used to estimate the resilience of the target, based on an operational resilience model adapted for interval operations. The method has as its element of originality the systemic integration of the GrC for resilience analysis, and has been validated on a case study modelled on a smart grid. However, it requires further development in order to be better contextualized to the application sector of this thesis.