J Ambient Intell Human Comput (2017) 8:1–8
DOI 10.1007/s12652-016-0417-9

EDITORIAL

Models and architectures for emergency management

I. Giordani[1,2] · **F. Archetti**[1,2]

Published online: 5 October 2016

1 Introduction

Securing our built and natural environment against natural disasters is one of the central elements of the functioning of any society. All sectors are to some extent impacted by disasters and concerned with related resilience and security issues. The general objective is to reduce the loss of human life, environmental, economic and material damage from natural and man-made disasters, including extreme weather events, crime and terrorism threats: the strategies rely on assessing risks, forecasting extreme events, communication and alerting and deploying resources (human, technological and financials) in different domains in optimal ways.

Communication and computing networks are not only critical infrastructures on their own, but underpin many other critical networks (e.g. energy, transport, health,…). This is particularly true during nature or man-made emergencies, where the malfunctioning or disruption of the communication channel or of an IT system can have a cascading effect on several other infrastructures or services.

The vulnerability of critical infrastructures, including the communication networks, stems, to a large extent, from the fact that ICT systems are deployed in an environment or for an application that it was not designed with resilience as primary concern. The deployment of ICT in new critical systems is exacerbating the problem by introducing new risks and vulnerabilities, in particular for a multisensory interconnected system.

Security monitoring of urban areas is one of the main requests from citizens around the world. This was evidenced by the past series of terrorist attacks against New York's World Trade Center in 2001, Madrid' s train system in 2004, London Underground in 2007, Moscow Metro in 2010 and Paris in 2015. These incidents have exposed vulnerabilities of urban environments against terrorist actions, which mainly stem from their diversity, heterogeneity and complexity.

The challenges of the urban environment are unique with particular and very specific issues. In order to cope with the complexity of operations in the urban environments, security and defense agencies have been increasingly turning in the last years to pervasive multi-sensory technologies for enhancing their ability to acquire, analyze and visualize events and situations. However, numerous challenges are associated with such technologies. The large-scale nature of both the geographically dispersed environment and the volume of the data, the multiple distributed heterogeneous components that need to be assembled spanning sensors, sensor processing, signal processing components often from multiple vendors, are some of the issues that need to be addressed. Moreover, we need to take in consideration that some activities need to be automated (i.e. video analysis since manual observation of multiple camera is not possible, anomaly detection ande high-level intelligent reasoning for event inference), as these are features without which the benefit of the system is limited.

✉ I. Giordani
giordani@milanoricerche.it; giordani@disco.unimib.it

F. Archetti
archetti@milanoricerche.it; archetti@disco.unimib.it

[1] Consorzio Milano Ricerche, Via Roberto Cozzi 53, 20125 Milan, Italy

[2] Department of Computer Science, Systems and Communication (DISCo), University of Milano-Bicocca, Viale Sarca 336, 20126 Milan, Italy

Recent advances in multi-sensor systems and data analytics enable the development of systems that can collect and process information from a wide variety of sources, including structured and unstructured data, but also real-time and non-real time data. Closely related to multi-sensor systems is the internet-of-things (IoT) paradigm (Petris et al. 2014), which enables the orchestration and coordination of a large number of physical and virtual internet-connected-objects towards human-centric services in a variety of security related applications.

This special issue stems from the final workshop of the FP7 project Proactive (PRedictive reasOning and multi-source fusion empowering AntiCipation of attacks and Terrorist actions In Urban EnVironmEnts) held in Milano during February 2015.

Since then terrorist attacks have spiked dramactically on European soil, both in terms of frequency and of human life loss making for an increasing awareness of the need of novel approaches to fight radicalization and terrorism.

The International NY Times (March 30, 2016) pointing out the scale up of recent attacks wrote "for years authorities have discounted small attacks as isolated random acts".

Quite to the contrary in the last months investigations have shown that terrorist cells, largely ISIS controlled, have been revvying up their machinery at least since early 2014 carrying out smaller attacks, while the devastating ones were in the making.

"It's a factory out there "an arrested terrorist is quoted in the same NYT issue as saying after the Bruxelles events.

Academia as well as government institutions have been aware quite a long time of this fact: terrorism thrives in some conditions; it may look like an "impromptu" individual act but requires instead a complex machinery to "produce" different kinds of terrors: shooting, kidnapping or bombing.

Security studies have time ago recognized the need to characterize the "modus operandi" of different groups and which conditions/events are more likely to trigger attacks.

A main objective of PROACTIVE was to show how patterns of strategic behaviour of different terrorist groups, identified analyzing large longitudinal data sets, can be linked to short term activity patterns identified analyzing feeds by "usual" surveillance technologies and that this fusion allows a better detection of terrorist threats.

This point is discussed in the paper by Sormani R. et al. "Criticality assessment of terrorism related events at different time scales" where it's shown how a Terrorist Reasoning Kernel (TRK) module based on statistical learning can provide a unified framework for near real-time reasoning and prediction of potential threat situations (e.g. terrorist actions). In this way patterns of strategic terroristic behaviors, identified analyzing large longitudinal data sets, can be linked to short term activity patterns identified analyzing feeds by "usual" surveillance technologies and that this fusion allows a better detection of terrorist threats. This time-layered framework processes information from a variety of sources including physical sensors (e.g. surveillance cameras) and "virtual" sensors (e.g. police officers, citizens) at different abstraction levels (e.g. sensor information, police inputs, external semantic crafted data sources).

This architecture simulates the three main expert user roles (i.e. operational, tactical and strategic user roles), as indicated in the intelligence analysis domain literature. The framework transforms all the sensors gathered data into symbolic events of interest following a generic scenario-agnostic semantics for terrorist attacks described in literature as terrorist indicators. Thru different reasoning and fusion techniques, the framework proactively detects threats and depicts the situation in near real-time.

Also the paper by Castelli et al. "Predicting Per Capita Violent Crimes in Urban Areas: an Artificial Intelligence Approach" is focalized on security studies in urban environment. It offers a genetic programming approach to crime prediction in urban areas, which is also of direct interest in estimating the radicalization level in critical urban environments.

Three papers of this special issue are about analytics of wireless sensor networks: the target application is environmental monitoring the proposed approach bear a direct relevance to anomaly detection and emergency management.

The paper by Altomare A. et al., "Mining frequent items and itemsets from distributed data streams for emergency detection and management", presents the design and the implementation of an architecture for the analysis of data streams in distributed environments.

The paper by Vella F. et al., "Analysis and visualization of meteorological emergencies" analysed the capability to sample and store meteorological information across a wide area which allows the possibility to analyze the historical evolution of data and extract events that are potentially bound to emergency and critical events. In this contribution, we detect the situation where a station show values that are sensibly different from the neighbour stations. We check the co-occurence of these events with emergency reported in web news. Result are encouraging and show how the statistical analysis can allow forecasting emergencies and reducing the impact of critical situations.

In the paper by Maniscalco U. et al., "A Virtual Layer of Measure Based on Soft Sensors", it is proposed a method to design and train a layer of soft sensors based on neural networks in order to constitute a virtual layer of measure in a wireless sensor network (WSN). Each soft sensor of the layer estimates esteems the missing values of some

hardware sensors by using the values obtained from some other sensors. In so doing, we perform a spatial forecasting. The correlation analysis for all parameter taken into account is used to define a cluster of real sensors used as sources of measure to esteem estimate missing values.

As regards specific technological aspects, two papers propose real time analytics of individual behavior based respectively on video feeds and smart phone accelerometer data.

In Varga D. et al., "Robust real-time pedestrian detection in surveillance videos" authors address the problem of analyzing pedestrians' behaviour in surveillance videos proposing a new feature extraction method based on Multi-scale Center symmetric Local Binary Pattern operator.

In Micucci D. et al., "Falls as anomalies? An experimental evaluation using smartphone accelerometer data" the authors evaluate the effectiveness of methods that detect falls as anomalies comparing traditional approaches with anomaly detectors. In particular, they experienced the kNN and the SVM methods using both the one-class and two-classes configurations comparing the results obtained with three different collections of accelerometer data, and four different data representations. Empirical results demonstrate that, in most of the cases, actual falls are not required to design an effective fall detector.

Users' requirements are critical in emergency management systems: emergency response teams, ERT (e.g. Protezione Civile), have experience in securing information networks and this competences can be applied to new types of networks such as smart grids linking communication, energy and transport networks.

During an emergency event, ERTs take time-sensitive decisions in order to help people, locate available resources, delivery assistance and disseminate relevant information. The timely acquisition of relevant geospatial data is crucial to plan and coordinate recovery actions in critical situations, especially when a disaster developes rapidly. The contents generated by the user and disseminated through social networks emerge as an additional source of data that could be integrated in decision support systems in order to help both government and citizens for managing critical situations.

As regards these aspects, in Fersini et al. "Earthquake Management: A Decision Support System Based On Natural Language Processing", the authors try to exploit user-generated contents to understand a critical event and its evolution over time taking advantages also from social social interactions among citizens/users which can be exploited as a dissemination gate to make people informed. The authors present a decision support system for earthquake management based on machine learning and natural language processing to effectively extract and organize knowledge from online social media data.

The results highlight the ability of the system to identify messages related to (real) earthquakes and critical tremors, emphasizing those posts provided by spontaneous users and containing any actionable knowledge about damages, magnitude, location and time references.

All these applications highlight the general agreement that data driven pattern analysis, based on statistical learning, will be one of the main technologies for the development of new systems. The management of emergency both natural (earthquakes, floods …) and man-made (terrorist attacks) offers some unique challenges. For example, contrary to the wealth of data in digital marketing, digital traces left by terror machinery are few and scattered; terrorism reinvents itself so it is difficult to match novel patterns into stored behavior.

2 Data models in urban security domain

In urban security monitoring there is awide variety of data at different time–space scales ans modern systems must fuse information coming from different types of sources.

Data fusion is the process of combing information from a number of different sources to provide a robust and complete description of an environment or process of interest (Azimirad and Haddadnia 2015). Data fusion is of special significance in any application where a large amount of data must be combined, fused and distilled to obtain information of appropriate quality and integrity on which decisions can be made.

A standard model for data fusion proposed by the US Department of Defense is the Joint Directors of Laboratories (JDL) data fusion model (Hall and Llinas 2001; Klein 2004). This model offers a multi-level functional model that describes how processing is organized in a military data fusion system and more generally, the JDL data fusion model is recognized as a de facto standard in data fusion issues (Foresti et al. 2015).

The JDL Model (Fig. 1) is a well-established reference model, which provides a sound basis for the identification of the major abstraction levels to be considered in the proposed solution approach. While levels 0–3 are directly involved in the real-time upstream information and processing flow from data sources to end users, JDL level 4, whose functionalities belong to medium and long term activities, is not directly involved in the real-time upstream information flows from sensing devices to end users.

Level 0 (Source pre-processing in JDL parlance) is in charge of processing raw data from individual sensors. Its activities include filtering and extraction of low-level features (Sabzevar 2015).

Level 1 (Object refinement) is in charge of translating perceptions into states of objects that model significant

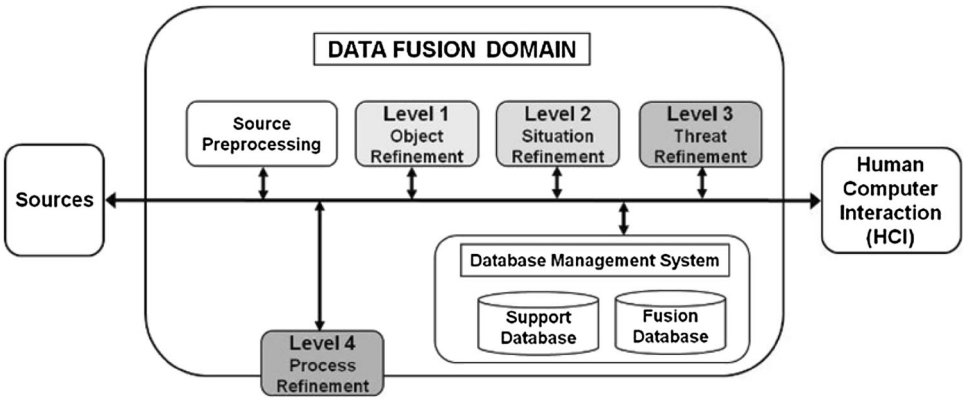

Fig. 1 JDL layers

domain entities (e.g., persons and cars) in a local context (Golestan et al. 2016).

Level 2 (Situation refinement) is in charge of fusing states of objects from Level 1 into higher level situations in the context of a micro-scenario (Pires et al. 2016). A micro-scenario models a target (e.g. a building, a metro station, a limited set of streets, etc.), which can be monitored by a set of information providers (i.e. devices and/or persons). Each micro-scenario defines a spatial reference system (e.g. the map of the building). A situation is the abstract representation of a set of observations of one or more objects, deriving from the temporal and positional fusion of the states of objects coming from Level 1 (for example, observations of a car from different cameras around a building is fused into a situations modelling the movement of the car in the reference space of the micro-scenario).

Level 3 (Threat refinement) is in charge of interpreting situations (in this work, threat detection) by assigning them threat levels which are presented to the final users (typically, through GUIs) (Sabzevar 2015).

Level 4 (Process refinement) (Pires et al. 2016) is a meta-layer, whose major role is to generate, train and tune the fusion models, which are exploited by lower layers of the system and, in particular, by the Level 3 (threat detection). Level 4 is not directly involved in the real-time upstream information flow from sensing devices to end users. L4 activities are not bound to strong real-time constraints.

The majority of urban surveillance systems, now operative, focus on situation awareness and common operation picture generation, and pay limited or even no attention to strategic consideration like the likelihood of new terrorist actions. This is a significant limitation given that the anticipation of terrorist actions could allow Law Enforcement Agencies (LEAs) to proactively deal with them thereby minimizing their adverse effects. The development of systems for predicting potential terrorist attacks hinges on devising appropriate reasoning and analytics techniques that could operate over information collected over many years from various sources (Sormani et al. 2016).

Early studies mainly due to the absence of data, took a conceptual and historical approach to the study of terrorism focused on the definition of terrorism, the myriad causes of terrorism, the tactics of the terrorists, and the identity of the primary terrorist groups and movements (Crenshaw 1981; Wilkinson 1986).

Moreover, scholars of the analytical approach, such as William Landes (Landes 1978), viewed terrorists as rational actors: if changes in terrorists' constraints, say through government policies, result in predictable behavioral responses by the terrorists, then terrorists are rational actors. Whether terrorists are rational, is widely debatable because they usually do not achieve their sought-after and stated objectives.

The collection of event data gave a further boost to the analytical approach. In his landmark study of skyjackings, Landes used US Federal Aviation Association (FAA) data on skyjackings to estimate the deterrent effects of US antiterrorism policies against skyjackings during 1961–1979.

After 2001 (9/11), there was an explosion of terrorism literature, both conceptual and analytical. Moreover for 9/11 opened a period of unprecedented investments by government and in turn companies into applications of advanced ICT into security and antiterrorism.

The starting point of the analysis concerns the study of the long-term behavioral patterns of terrorist groups, which can be "observed" by considering past attacks. This information has been gathered from various research groups, who have created and shared several historical data sets.

The Minorities at Risk Organizational Behavior (MAROB) (Victor et al. 2008) dataset is a subsidiary of the Minorities at Risk (MAR) Project. The project has identified 118 organizations representing the interests of all 22 ethno political groups in 16 countries of the Middle East and North Africa, operating between 1980 and 2004. While

The Global Terrorism Database—GTD-(START—National Consortium for the Study of Terrorism and Responses to Terrorism 2016) records both domestic and transnational terrorist incidents (LaFree and Dugan 2007). For GTD, this partition of domestic and transnational terrorist incidents was first accomplished by (Enders et al. 2011) for 1970–2007 and has been updated by them through 2014.

3 Models and algorithms

Hidden Markov Models (HMMs) have over the years taken center stage as the modelling tool for monitoring short term activities.

The basic motivation is twofold: firstly, carrying out a terrorist activity requires planning and preparations, following steps that form a pattern. This pattern of actions can be modeled using a Markov chain. Secondly, the terrorists leave detectable clues or "digital crumbs" about these actions which are not direct observations of the actions, but, rather, related to them, meaning that the states are hidden. For example, an observation of a purchase of chemicals could be indicative of intentions to produce a chemical weapon. However, a purchase of chemicals could very well be a benign event, which motivates inclusion of a model of observations that are unrelated to the HMMs.

Several papers show the power and flexibility of HMMs: (Schrodt 2000) uses "hidden Markov models" to measure similarities among international crises. The models are first estimated using the Behavioral Correlates of War data set of historical crises, then applied to an event data set covering political behavior in the contemporary.

Singh et al. (2004) develops a tool to detect and track terrorist activity. Authors follow two probabilistic approaches: HMMs and Bayesian networks (BNs). The HMMs detect the monitored terrorist activity and measure threat levels, whereas BNs combine the likelihoods from many different HMMs to evaluate the cumulative probability of terrorist activity.

The authors of (Coffman and Marcus 2004) present the methodology and results of a study that applies HMMs to time-varying social network analysis metric values, in order to classify the evolution of simulated social networks.

In this work (Weinstein et al. 2009), the authors describe an approach and some initial results on modeling, detection, and tracking of terrorist groups and their intents based on multimedia data. In particular it describes the development and application of a new Terror Attack Description Language (TADL), which is used as a basis for modeling and simulation of terrorist attacks.

In (Singh et al. 2009), the authors introduced feature-aided tracking combined with HMMs for analyzing asymmetric threats. The authors of (Andersson and Johansson 2010) propose a two-stage method based on on fusion of evidence from radar and optical sensors as well as automated identification system (AIS) signals. In the first stage, the sensors perform detection, tracking and classification locally. The high-level fusion is performed by HMMs. The reported results show that this approach is able to detect piracy operation at an early stage, i.e. close to the time, or possibly before, the attack has occurred.

Raghavan et al. (2013) develops a HMM framework to model the activity profile of terrorist groups. Key to this development is the hypothesis that the current activity of the group can be captured completely by certain states/attributes of the group, instead of the entire past history of the group. In the simplest example of the proposed framework, the group's activity is captured by a 2 state HMM with the states reflecting a low state of activity (Inactive) and a high state of activity (Active), respectively.

HMMs used in (Granstrom et al. 2015) for modeling asymmetric threats. The observations generated by such HMMs are generally cluttered with observations that are not related to the HMM. In this works the authors proposed a Bernoulli filter which processes cluttered observations and is capable of detecting if there is an HMM present, and if so, estimate the state of the HMM.

In the paper by (Sormani et al.) *Criticality assessment of terrorism related events at different time scales* HMMs are used for the threat detection activity, carried out by the defined "Micro-environments", a software component, based on HMMs, which interprets events coming from a limited zone in order to identify potential threats.

Shahir et al. (2015) is focused on the monitoring activity of critical infrastructures like sea lanes, ports, offshore structures (like oil and gas rigs). They consider such scenarios as probabilistic processes and analyze complex vessel trajectories using machine learning to model common patterns. Specifically, in this work the common patterns are represented through HMMs and such patterns are classified using Support Vector Machines.

4 Software tools and technologies

In Markov Models the transition to another state is triggered by an event, therefore one can see a direct corrispondence between HMMs and Event processing sytems.

One can see a direct correspondence to event processing systems. CEP engines are designed for implementing logic in the form of queries or rules over continuous data flows. Typically, they include a high-level declarative language for the logic definition with explicit support for temporal constructs. The need for CEP technology is rooted in various domains that require fast analysis of incoming

information. Since the role of MTR reasoning module in the TENSOR approach is to process numerous incoming events of different nature and update the sensitivity of the STR in near real-time, we believe that event-processing approaches fit requirements of the MTR module.

The last level, LTR, provides to MTR prediction levels with respect to different types of physical zones (e.g. squares, churches, government buildings, etc.). This feature is not provide by ASAM framework. In order to carry out this activity the LTR uses information generated by STR (i.e. detected events and threats notifications) and external data stored in the terrorist data sources aforementioned. In particular external data sources are used to build a clustering based prediction model, which is used by LTR in its activities.

In (Cugola and Margara 2012) the authors propose an abstract framework for event processing (information flow processing) systems that are able to manage multiple data stream sources and derive new information about the data stream through use of a set of processing rules. Two main types of existing information flow processing systems are defined: data stream management systems (DSMS) and complex event management systems (CEP). On one hand DSMS are rooted in classical data base management systems (DBMS) they deal with constantly updating data-streams and continuously execute queries as new data arrives. Similarly to DBMSs, they process incoming data through a sequence of transformations based on common SQL-like operators and continuously update the results. On the other hand CEP systems filter and combine incoming events of particular patterns from the external world to understand what high-level complex events have occurred and notify relevant actors or be reused as an input in the CEP solution.

As event patterns must specify complex relationships among input events entering the system they can rely on two types of languages for this (Etzion and Niblett 2010): stream-oriented style and rule-oriented style language. The stream-oriented (transforming) style is inspired by SQL and relational algebra [e.g. CQL (Arasu et al. 2006) from the STREAM project] and is used in DSMSs. The rule-oriented (detecting) style, commonly used in CEP systems, defines detecting rules by separately specifying the firing conditions (event patterns) and the actions to be taken when such conditions are satisfied (e.g. event-condition-action (ECA) rules (McCarthy and Dayal 1989).

Neither of the above mentioned language solutions can satisfy both the expressivity and effectiveness needs of CEP applications on their own. Hence, alternative CEP languages have been proposed that combine and extend operators from both language styles as in (Wu et al. 2006; Wang et al. 2009). Promising research directions consider using both background knowledge to reason about the events (e.g. ETALIS (Anicic et al. 2011) a logic-rules based CEP that uses contextual knowledge and defines semantic relations between events) and statistical knowledge to detect patterns of interest in event streams.

Even though a crucial feature in CEP systems is real-time processing in order to assure timely reaction, in a certain number of applications (e.g. terrorist threat, credit card fraud) the importance is on proactively preventing events before they occur and not only reacting after they happen. The value of the detected/predicted complex events decreases with time (terrorist threat notification in near real-time as opposed to a day after) as described in (Fülöp et al. 2012). The described setting satisfied the requirements of the thesis domain and its need to proactively detect and react to terrorist threats. Hence, to address this issue we jointly consider both CEP systems and predictive analytics approaches, in this way enabling processing online streams of events while inferring decisions based on past and current data concerning prediction of future events of interest. We accomplish this by learning predictions from both long-term and short-term historical data and integrating the mentioned predictive analytics approaches with real-time complex event processing, the mentioned combination is particularly useful in application where a certain level of uncertainty regarding complex events is allowed.

AI is in a period of a variety of unprecedented development and a variety of machine learning toolkits have been created to facilitate the learning process. Hadoop is well known and ubiquitous as a big data framework but there are a number of other open source options for machine learning that do not use it at all, which are getting "traction" in antiterrorism related applications (Arun and Jabasheela 2014) like: Massive Online Analytics (MOA), a WEKA-related project, which offers online stream analysis on a number of (WEKA) algorithms; Apache MADlib is a collection of SQL-based algorithms designed to run at scale within the database rather than porting data between multiple runtime environments.

Storm is used for processing data in real-time and was initially conceived to overcome deficiencies of other processors in collecting and analyzing social media streams. Storm does not ship with a Machine Learning library, but SAMOA, a platform for mining big data streams, currently has implementations for classification and clustering algorithms running on Storm.

Deep-learning technology is behind most of the recent breakthroughs in object recognition. The paper of (Kang and Choo 2016) introduces an emergency alert system based on the use of deep-learning technology with the main advantage of not requiring additional devices or infrastructure. They adapt a deep-learning-based real-time video analyzing module to immediately detect accidents and

natural disasters which can be quickly generalized to other specific applications.

5 System and customer requirements

Although research on automated information extraction from multimedia data has yielded significant progress, the development of automated tools for analyzing the results of information extraction and correlate them with specific events has been significantly slower. Moreover, some features of terrorist networks, such as low Signal to Noise Ratio (SNR) (in the sense of sparse relevant observations superimposed upon a large background of benign ones) and a wide geographic distribution operating in different socio economic conditions, make them difficult to observe.

Terrorist networks are often a string of small cells, and interconnection among cells are purposely weak and therefore very difficult to detect. While a terrorist cell has its own "modus operandi", in order to maintain a low profile, terrorist cells can move around geographically, alter their personnel and change their intended target.

A valuable solution could be a server-side middleware approach, running in a cloud-computing environment. The middleware layer collects data through gateways or sink nodes. They have less control over sensor network operations. The components in this layer are unable to control low-level operations such as routing though; they have more knowledge about the environment as they can analyze sensor data received through different sensors.

Todays' IoT systems rely on non-functional properties such as context awareness and semantic interoperability. Middleware systems can bundle those functionalities together to be reused in many applications (Wang et al. 2015). These new type of middleware systems have more control of low level operations of network such as network routing, energy consumption, etc. This layer is much closer to the hardware but it lacks the overall knowledge about the environment.

It is important that systems providing advanced capabilities for urban security and surveillance advance and integrate all above functionalities in order to handle multiple heterogeneous sensors suitable for the monitoring activity of urban environment. At the same time, these systems need to support JDL fusion level mandates by deploying various fusion techniques and algorithms (Hummel et al. 2012).

According to the classification proposed by The US Department of Defense in (Department of Defense 2010), three different type of users were identified: operational, tactical and strategic users. These users operate at three different levels as follows:

- The operational level refers to regional Intelligence services with more focus on the regional threat level. In this level local terrorist actions may increase the alert state at the regional level but still may not affect the National level.
- The tactical level refers to local Intelligence Units (e.g., intelligence units of local police). At this level the alert state changes with even small scale terror actions. The threat assessment is limited in time and space.
- The strategic level is a National Intelligence Service, where threat assessment covers the whole country. At the National level the alert state does not change instantly based on isolated small scale terrorist events. The threat assessment is broader in space and time.

It is important to note that, serious terror actions with political consequences at a local level may have serious impact to the National threat level based again on the "gravity" of the event. The level of gravity cannot be precisely defined and it is up to National Authorities and the higher political level to define the seriousness of a terror event based on National policies.

In a counter-terrorism applications, operational users have the aim to identify and notify tactical users about suspicious situations in a physical environment of limited size and complexity (i.e., a city zone) taking into account short histories of events provided by sensors (human or device). Tactical users need to analyze a medium term history (sensor data and threats notification) coming from different zones in order to infer the sensitivity/criticality (i.e. the alert levels) of the current situation in each monitored zone. Finally, strategic users work in order to predict the criticality of each monitored zone tacking into account historical data and external data sources.

References

Andersson M, Johansson R (2010) Multiple sensor fusion for effective abnormal behaviour detection in counter-piracy operations. In: Waterside Security Conference (WSS), 2010 International. IEEE, pp 1–7

Anicic D, Fodor P, Rudolph S, Stühmer R, Stojanovic N, Studer R (2011) Etalis: rule-based reasoning in event processing. In: Reasoning in event-based distributed systems. Studies in computational intelligence, vol 347. Springer, Berlin, pp 99–124

Arasu A, Babu S, Widom J (2006) The CQL continuous query language: semantic foundations and query execution. VLDB J Int J Very Large Data Bases 15(2):121–142

Arun K, Jabasheela L (2014) Big data: review, classification and analysis survey. Int J Innov Res Inf Secur (IJIRIS) 1(3):17–23

Azimirad E, Haddadnia J (2015) The comprehensive review on JDL model in data fusion networks: techniques and methods. Int J Comput Sci Inf Secur 13(1):53

Coffman TR, Marcus SE (2004) Dynamic classification of groups through social network analysis and hmms. In: 2004 IEEE Aerospace Conference Proceedings, vol. 5, pp 3197–3205

Crenshaw M (1981) The causes of terrorism. Comp Politics 13(4):379–399

Cugola G, Margara A (2012) Processing flows of information: from data stream to complex event processing. ACM Comput Surv (CSUR) 44(3):15

Department of Defense (2010) Joint Publication 1-02 Dictionary of Military and Associated Terms. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf **(Online)**

Enders W, Sandler T, Gaibulloev K (2011) Domestic versus transnational terrorism: data, decomposition, and dynamics. J Peace Res 48(3):319–337

Etzion O, Niblett P (2010) Event processing in action. Manning Publications Co, Greenwich

Foresti GL, Farinosi M, Vernier M (2015) Situational awareness in smart environments: socio-mobile and sensor data fusion for emergency response to disasters. J Ambient Intell Humaniz Comput 6(2):239–257

Fülöp LJ, Beszédes Á, Tóth G, Demeter H, Vidács L, Farkas L (2012) Predictive complex event processing: a conceptual framework for combining complex event processing and predictive analytics. In: Proceedings of the Fifth Balkan Conference in Informatics, ACM, pp 26–31

Golestan K, Soua R, Karray F, Kamel MS (2016) Situation awareness within the context of connected cars: a comprehensive review and recent trends. Inf Fusion 29:68–83

Granstrom K, Willett P, Bar-Shalom Y (2015) A Bernoulli filter approach to detection and estimation of hidden Markov models using cluttered observation sequences. In: IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2015, pp 3911–3915

Hall D, Llinas J (eds) (2001) Multisensor data fusion. CRC Press, Boca Raton

Hummel G, Russ M, Stütz P, Soldatos J, Rossi L, Knape T, Kompatsiaris I (2012) Intelligent multi sensor fusion system for advanced situation awareness in urban environments. In: Future security. Communications in computer and information science, vol 318. Springer, Berlin, pp 93–104

Kang B, Choo H (2016) A deep-learning-based emergency alert system. ICT Express. doi:10.1016/j.icte.2016.05.001 **(ISSN 2405-9595)**

Klein LA (2004) Sensor and data fusion: a tool for information assessment and decision making, vol 324. Spie Press, Bellingham

LaFree G, Dugan L (2007) Introducing the global terrorism database. Terror Polit Violence 19(2):181–204

Landes WM (1978) An economic study of US aircraft hijacking, 1961–1976. J Law Econ 21(1):1–31

McCarthy D, Dayal U (1989) The architecture of an active database management system. ACM Sigmod Record 18(2):215–224

Petris S, Georgoulis C, Soldatos J, Giordani I, Sormani R, Djordjevic D (2014) Predicting terroristic attacks in urban environments: an internet-of-things approach. Int J Secur Appl 8(4):195–218

Pires IM, Garcia NM, Pombo N, Flórez-Revuelta F (2016) From data acquisition to data fusion: a comprehensive review and a roadmap for the identification of activities of daily living using mobile devices. Sensors 16(2):184

Raghavan V, Galstyan A, Tartakovsky AG (2013) Hidden Markov models for the activity profile of terrorist groups. Ann Appl Stat 7(4):2402–2430

Sabzevar I (2015) A comprehensive review of the multi-sensor data fusion architectures. J Theor Appl Inf Technol 71(1):33–42

Schrodt PA (2000) Pattern recognition of international crises using hidden Markov models. Political complexity: Nonlinear models of politics, pp 296–328

Shahir HY, Glasser U, Shahir AY, Wehn H (2015) Maritime situation analysis framework: vessel interaction classification and anomaly detection. In: 2015 IEEE International Conference on Big Data (Big Data), IEEE, pp 1279–1289

Singh S, Allanach J, Tu H, Pattipati K, Willett P (2004) Stochastic modeling of a terrorist event via the ASAM system. In: 2004 IEEE International Conference on Systems, Man and Cybernetics, vol. 6, IEEE, pp 5673–5678

Singh S, Tu H, Donat W, Pattipati K, Willett P (2009) Anomaly detection via feature-aided tracking and hidden Markov models. IEEE Transact Sys Man Cybern Part A Sys Humans 39(1):144–159

Sormani R, Soldatos J, Vassilaras S, Tisato F, Giordani I (2016) A serious game empowering the prediction of potential terroristic actions. J Polic Intell Counter Terror 11(1):30–48

START—National Consortium for the Study of Terrorism and Responses to Terrorism (2016) Global terrorism database [Data file]. Retrieved from https://www.start.umd.edu/gtd

Victor A, Pate A, Wilkenfeld J (2008) Minorities at risk organizational behavior data and codebook version 9/2008 online. http://www.cidcm.umd.edu/mar/data.asp. Accessed July 2015

Wang F, Liu S, Liu P (2009) Complex RFID event processing. VLDB J Int J Very Large Data Bases 18(4):913–931

Wang M, Perera C, Jayaraman PP, Zhang M, Strazdins P, Ranjan R (2015) City data fusion: sensor data fusion in the internet of things. arXiv preprint arXiv:1506.09118

Weinstein C, Campbell W, Delaney B, O'Leary G (2009) Modeling and detection techniques for counter-terror social network analysis and intent recognition. In 2009 IEEE Aerospace conference, IEEE, pp 1–16

Wilkinson P (1986) Terrorism versus democracy the liberal state. Routledge: Taylor and Francis Group, New York, p 254 **(ISBN 0-415-38478-8)**

Wu E, Diao Y, Rizvi S (2006) High-performance complex event processing over streams. In Proceedings of the 2006 ACM SIGMOD international conference on Management of data, ACM, pp 407–418