Challenges of distributed intelligent surveillance system with heterogenous information

Weiru Liu, Paul Miller, Jianbing Ma, Weiqi Yan
School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast,
Belfast BT7 1NN, UK

Abstract

CCTV and sensor based surveillance systems are part of our daily lives now in this modern society due to the advances in telecommunications technology and the demand for better security. These systems are traditionally used in forensic mode – finding evidence in video images when certain events detected or happened. In recent years, research and development on events detection in real time CCTV surveillance has attracted significant attention, in order to identify and prevent potential threats. In this paper, we discuss some challenging issues faced by the artificial intelligence research for such real-time distributed intelligent surveillance systems, where the detection and composition of threats and abnormal behaviors involve multiple sources (e.g., cameras) with heterogeneous information. These challenges include but are not limited to resolving conflicting conclusions provided by different sources; managing uncertainty associated with the conclusions from the sources and the reliability of the sources themselves; managing the heterogeneity of information provided; exploring the scalability and ontological issues presented in large surveillance networks, as well as evaluation criteria etc.

Introduction

CCTV-based surveillance is an inseparable part of our society now – everywhere we go we see CCTV cameras (e.g. (Bsia 2009; Security 2005; Abreu *et al.* 2000; Shu *et al.* 2005), etc). The role of such systems has shifted from purely passively recording information for forensics to proactively providing analytical information about potential threats/dangers in real-time fashion. This shift poses some dramatic challenges on how information collected in such a network shall be exchanged, correlated, reasoned with and ultimately be used to provide significantly valuable predictions for threats or actions that may lead to devastating consequences.

In this paper, we discuss challenges faced by intelligent surveillance systems from the view of the AI community. However, before diving into details of discussing potential challenges, let us first focus on the concept and scope of *events*, a key concept in surveillance and similar systems, such as sensor based smart homes, intrusion detection systems, etc.

Definitions of an event from different research fields are very diverse and tend to reflect the content of the designated application. For instance, in text topic detection and track, an event is something that happened somewhere at a certain time; in pattern recognition, an event is defined as a pattern that can be matched with a certain class of pattern types, and in signal processing, an event is triggered by a status change in the signal, etc (Yan & Miller 2008). In CCTV surveillance systems, an event shall at least consists of the following aspects. It can be either *instantaneous* (event duration is 0, i.e., takes place at a specific point of time) or it has a *duration*, it occurred during a period of time. For example, a bus-boarding pass scanned by an electronic-reader is instantaneous whilst an even of two people fighting usually has a duration. It is *atomic* (it happens or not). The atomic requirement of an event is closely related to how elementary (atomic) events are defined. For instance, a person boarding a bus can be an atomic event whilst a person boarding a bus and taking a seat is not. It is *interesting* to the particular application, meaning it is what we want to study and could be correlated with other events to form a scenario, e.g., usually we are interested in a young male boarding a bus with odd behavior rather than an old woman boarding a bus.

Equipped with this understanding of events that can be recognized from CCTV cameras or other sensors, we now look into challenges that are faced by intelligent surveillance systems possibly involving a huge number of cameros/sensors.

The first challenge is the *quality* of CCTV data. Images or audio recordings are not always perfect in such systems, objects of interest can be partially obscured; camera lenses maybe covered or damaged, the person (object) being recognized may have deliberately covered itself up. Even when these problems do not exist, there are other factors causing quality concerns, such as, poor illumination, sensor noise, particularly in poor lighting conditions and low resolution of the cameras. Furthermore, CCTV technology has now begun to be deployed on public transport systems such as buses and trains e.g., (Bsia 2009; Security 2005), which brings unique problems that are

not encountered in conventional CCTV deployments. Therefore, information recorded by such systems is strongly subject to noise and obscurity.

The second challenge is the *uncertainty* of recognized events from a source (e.g., a camera) due to the poor quality of data provided. Any events detected from such imperfect information are subject to uncertainty and many possible events can be generated from the same set of images, e.g, multiple explanations. For instance, it can be very difficult to judge if a person is a male or female if the person wearing a heavy coat entering a bus with its back deliberately leaning towards a camera. Therefore, adequate mechanisms shall be deployed to model such uncertainty and ignorance associated with the detected events (multiple explanations of events).

Along with this challenge comes the issue of *reliability* of sources. An example of this scenario is when an algorithm being applied to detect an event is not 100% accurate itself. So there is an issue about how the reliability (of the algorithm) should be integrated with the detected events (which are uncertain).

The third challenge is the *inconsistency or conflict* among multiple sources. A CCTV-based surveillance system could consist hundreds of cameras, such as in a medium-sized airport. The detection of events related to certain individuals come from different cameras when the individuals moving around at the airport or on a bus. Therefore, events detected from multiple cameras/sensors relating to the same object (person/people) must be combined to reduce uncertainty and inconsistency. A typical scenario is that from a camera with poor visibility a *male* is detected while from the audio recording it strongly indicates a *female*. So adequate methods must be applied to resolve this inconsistency.

The fourth challenge is the adequate *modelling* of events information. For real-time surveillance involving multiple sources, the representation of events is particularly important, since it influences fundamentally the ways to merging detected events from multiple sources and the uncertainty and inconsistency handling during the fusion process. Since events can be detected from various sources with different types of information, a formal event model defining all its elements (attributes) with clear semantics is fundamental not only to representing events themselves but also to making inferences subsequently. We shall also bear in mind that different knowledge representation mechanisms may be only suitable for certain kind of event scenarios. Therefore, selecting an adequate reasoning mechanism coupled with suitable events modelling is crucial for event-driven applications.

The fifth challenge is the *composition* of elemental events for inferring and predicting threats. A single event cannot reveal potential threats most of the time unless it is extremely significant. Most of the time. multiple atomic events together paint a picture of certain intentions by the objects (e.g., people) and then actions can be taken to prevent them. This is referred to as events composition. A common technique to event composition is to create a set of rules correlating atomic events for predicting other events. Therefore, obtaining these rules and validate them are important for drawing meaningful conclusions.

The sixth challenge is the *scalability* of the system. Imaging a real-time intelligent surveillance system with many hundreds of cameras across a large network, the scalability of its modelling and reasoning power is greatly challenged. What should be the manner that we revise/update rules for events composition if rules are used? Do we expect all the sources provide information/conclusion with the same set of vocabulary? How much change is needed if new types of equipment are brought into the system? Another issue in this challenge is the requirement of software suitable for developing event management and event reasoning systems.

The seventh challenge is building *ontologies* for surveillance systems. To realize the scalability of a large surveillance system, surveillance ontologies must be considered. An ontology is a specification of a conceptualization. That is, an ontology is a description of the concepts and relationships that can exist for an agent or a community of agents. If each camera/sensor/equipment is taken as an agent, then a surveillance ontology is needed, at least for events models, in order to allow information from multiple sources to be exchanged and merged. For example, *taking a seat* should be explained as equivalent to *sitting down* under the context of bus surveillance.

The eighth challenge is the *evaluation* of a surveillance system. For data mining or machine learning algorithms, there are now some standard data sets for validating and evaluating new algorithms and for comparing them with existing ones. For CCTV-based surveillance systems, each security concern is different, the objects being recognized and events being detected more application specific, is that possible to establish a repository containing some common surveillance scenarios? Who are the people providing these scenarios, and what are the evaluations criteria? Realistically, it is a very difficult task to evaluate a complete surveillance system from a situation awareness viewpoint, not from the point of individual video/image analysis algorithms.

It needs to be pointed out that there are equally challenging issues for video/image analysis, signal processing etc, from the vision/signal research perspective. However, in this short discussion paper, we only concentrate on the challenges for the AI community posed by such systems.

We now investigate these challenges to some detail in the following sections.

Quality, Uncertainty, Reliability

The first factor is the *quality* of the original data from a source, be it an image from a camera, a recording from

an audio equipment, or an alarm/signal from a sensor. For instance, a camera may have been tampered with or the illumination could be poor; the audio recording involves a heavy background noise etc. When the quality of original information to be analyzed is poor, any analysis result from such information will have a great degree of *uncertainty* and the result of analysis must reflect such uncertainty adequately.

For example, in the case of a person entering a bus doorway with its back facing the camera, the person may be classified as *male* with a certainty of 85% by a classification program. However, this does not imply that the person is *female* with a 15% certainty, rather, it is unknown. This imperfection in information means that we do not know how the remaining 15% shall be distributed except it could include any possibility, *male, female*.

In addition to the poor quality of information contributing to the uncertainty of an analysis result, the accuracy of a classification program is another factor to consider, that is the *reliability or accuracy* of the program used. Even if the quality of some original information is excellent, a classifier may still come with the wrong conclusion. Therefore, the reliability of a source (e.g., a classifier) shall be taken into account when accepting the result from such a program.

Now let us turn to the mechanisms that can be used to model and reason with the above mentioned aspects contributing to uncertainty of a conclusion. In the past two decades, many theories/mechanisms have been proposed to represent uncertain information, such as, the Dempster-Shafer theory of evidence (Dempster 1967; Shafer 1976), fuzzy sets theory (Zadeh 1978), and possibility theory (Zadeh 1978; Dubois & Prade 1988). The most common and popular choice is probability theory which is adequate when there is a statistical analysis to justify a probability distribution. For instance, if statistics show that 80% of people taking buses after 10pm are male, then $p(male) = 0.8, p(female) = 0.2$ and anyone boarding a bus after 10pm with probability 0.8 being a male, before we observing anything related to the person. However, not all the situations will give a satisfactory probability distribution and in some situations such distributions are impossible to get. For the above example about identifying a persons's gender from a video image, if we do not want to split the remaining 15% equally between *male* and *female* options, we cannot use probability theory. A natural choice for this type of uncertainty is the Dempster-Shafer (DS) theory of evidence, which is regarded as an extension of probability theory. DS theory provides us a freedom to assign a probability mass value to a subset instead to every individual element of a set.

Let Ω be a finite set containing exclusive and exhaustive answers to a question (that is, Ω contains all the possible values to answering a question and only one value is the correct answer at a specific time, such as *male, female* for the question *what is the gender of a person*). We call Ω the frame of discernment and we denote $\Omega = \{w_1, \ldots, w_n\}$. A mass function is a mapping $m : 2^\Omega \rightarrow [0, 1]$ such that $m(\emptyset) = 0$ and $\sum_{A \subseteq \Omega} m(A) = 1$. For instance, the information that *the person entering a doorway is a male with certainty 85%* is represented as $m(\{male\}) = 0.85$, $m(\{male, female\}) = 0.15$ if $\Omega = \{male, female\}$.

To deal with *reliability* issue, in (Lowrance, Garvey, & Strat 1986), the *Discount rate* was defined with which a mass function can be discounted in order to reflect the reliability of evidence. Let r $(0 \leq r \leq 1)$ be a discount rate and m be a mass function, then the discounted mass function m^r is defined as

$$m^r(A) = \begin{cases} (1-r)m(A) & A \subset \Omega \\ r + (1-r)m(\Omega) & A = \Omega \end{cases} \quad (1)$$

When $r = 0$ the source is absolutely reliable and when $r = 1$ the source is completely unreliable.

There are many other methods to consider the reliability of sources, such as weighted average operators, or something similar (e.g., (Cron & Dubuisson 1998; Elouedi, Mellouli, & Smets 2004; Rogova & Nimier 2004)). The idea in these methods is to use parameters or weights to reflect which sources are more reliable than other sources, so the more reliable ones have stronger influence over the final outcome.

Possibility theory has close relationships with both DS theory and fussy sets theory. Since for every possibility distribution defined in possibility theory, we can always derive a mass function, possibility theory can be regarded as a subset of DS theory from this perspective. This view is in no position to undermine other distinct characteristics possed by possibility theory, such as its ability to express agents beliefs and its exclusive set of merging operators. Fuzzy sets theory has found its applications most in control-related areas, where problem parameters are more of continues in nature, such as, a car's speed, a room's temperature etc. Since the nature of attributes associated with uncertainty in CCTV-based surveillance is more of discrete, we believe DS theory is a more suitable candidate for this application when probability theory cannot be applied.

Resolving Inconsistency and Conflict: Merging Based Approaches

In a large surveillance network, we are facing the task of considering information collected from hundred of cameras, sensors, and other equipments. Therefore, we need to develop approaches to combining information (or conclusions) from different sources (e.g., cameras) to determine what the real situation is. A possible scenario on a bus surveillance is that the visibility of a camera is poor, so the classification of a person being male or female is indeterministic, though it slightly in favor of the person being male. The analysis from an audio recording involving the conversation of the person indicates this person is more likely to be a female. Then, we have a contradiction/inconsistency to resolve.

When the analysis from each source is represented as a kind of evidence with uncertainty explicitly modelled

using numerical values, such as a mass function, DS theory offers a combine rule (Dempster's combination rule) to produce a single outcome by fusing multiple pieces of evidence.

Let $m_1(\cdot)$ and $m_2(\cdot)$ be two mass functions over Ω from two distinct sources. Combining $m_1(\cdot)$ and $m_2(\cdot)$ gives a new mass function $m(\cdot)$ as follows:

$$m(C) = (m_1 \oplus m_2)(C) = \frac{\sum_{A \cap B = C} m_1(A) m_2(B)}{1 - \sum_{A \cap B = \emptyset} m_1(A) m_2(B)} \quad (2)$$

However, when two mass functions are telling almost totally contradicting information, Dempster's rule cannot be applied as it will produce a counterintuitive result (Liu 2006).

On the other hand, when the analysis from a source is represented as *beliefs* using logic based mechanisms, the merging is taken as a process to produce a new belief base which is consistent. Many different merging operators have been proposed for this type of merging ((Konieczny & Pino-Pérez 1998; Qi, Liu, & Glass 2004), etc). However, when a source (actually the analysis result of its information) believes a person is male, whilst another believes the person is female, the merging of these two belief bases produces nothing (a tautology). That is, both the numerical and logic based approaches cannot deal with situations when there is a conflict among information provided from different sources.

One possible way to resolve this is to adapt the *revision* principle in the community of belief/epistemic revision research. The underlying assumption in belief revision is that the newest evidence is the most reliable one and any inconsistency existing in the original belief set in relation to this new evidence should be removed. When adapting this principle to resolving a conflict like discussed above – we cannot decide if the person is male or female, one technique is to examine the reliability of the source providing the conclusion. The more reliable source should overrule the less reliable one if a single conclusion must be reached. Let us look at an example. Assume that source A provides a belief set about a person as

$$\{\mathsf{male}, \mathsf{tall}, \mathsf{having\ a\ huge\ bag}, ..., \mathsf{blue\ coat}\},$$

a witness B who saw the person gives a belief set as

$$\{\mathsf{female}, \mathsf{tall}, \mathsf{having\ a\ huge\ bag}\},$$

then the revised belief set is as below if source B is thought to be more believable.

$$\{\mathsf{female}, \mathsf{tall}, \mathsf{having\ a\ hugebag}, \mathsf{blue\ coat}\}.$$

The consistent beliefs are reserved and the inconsistent part (male verdict from source A) is eliminated.

To realize information/knowledge fusion with possible adoption of revision techniques, both numerical based and logic based methods are essential to deal with different kind of information. So one challenge is the integrated implementation of such systems and another is the computational issues involved, since logic based systems are known to be computational expensive when certain reasoning capability is required.

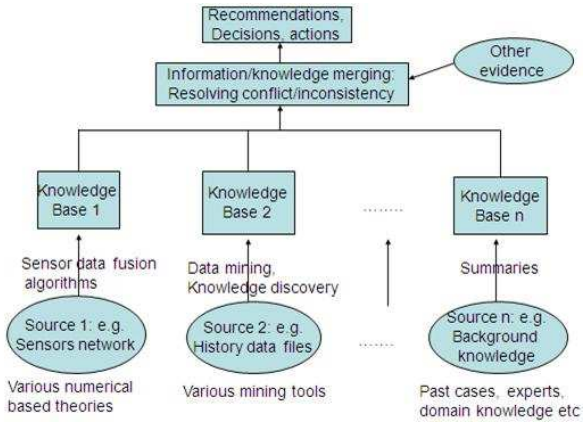

Figure 1: Fusion Architecture

Figure 1 shows a typical architecture of a fusin/merging framework where information is collected from multiple sources, with variety of format, can be uncertainty and inconsistent, and a final recommendation needs to be decided.

Events Modelling and Composition

Since events can be recognized from information provided by differen sources (e.g., video, audio, and speedometers) and this information is processed by different algorithms, there is a need to define an uniform event model that can accurately represent events from heterogeneous sources. Furthermore, for any application, domain knowledge is an essential part for reasoning. For example, recorded crime statistics can provide a likelihood of a criminal act occurring along bus routes at different times of the day. So we need to model such domain knowledge properly too.

Event model: As we mentioned in Introduction that events definitions are application specific. Also, in the literature, there are two types of events, one type contains *external events* (Adi & Etzion 2004) or *explicit events* (Wasserkrug, Gal, & Etzion 2005; 2008) and the other consists of *inferred events*. External events are events directly gathered from external sources (within the application) while inferred events are the results of the inference rules of an event model.

Intuitively, a concrete event definition is determined by the application domain which contains all the information of interest for the application.But there are some common attributes that every event shall possess, such as

1. $EType$: describing the type of an event, e.g., *Person Boarding Vehicle* abbreviated as PBV. Events of the same type have the same set of attributes.
2. $occurT$: the time interval (or point) that an event occurred.

3. sID: the ID of a source from which an event is detected.
4. *reliab*: the degree of reliability of a source.
5. *sig*: the degree of significance of an event.

Here the degree of significance of an event indicates the level of interest to further following the event. For example, in bus surveillance, an event that *a young man boards a bus at midnight* is more significant than that of an old woman. The degree of significance and reliability are usually estimated through domain knowledge.

Formally, we define an event e as a tuple

$$\mathsf{e} = (\mathsf{EType}, \mathsf{occurT}, \mathsf{sID}, \mathsf{reliab}, \mathsf{sig}, \mathsf{v_1}, \cdots, \mathsf{v_n})$$

where v_is are any additional attributes required to define event e based on the application. Attribute v_i can either have a single or a set of elements as its value, e.g., for attribute *gender*, its value can be *male*, or *female*, or *obscured*, or {*male, female*}. For any two events where they have the same event type, the same source ID and the same time of occurrence, these two events are from the set of possible events related to a single observation. For example,

$\mathsf{e_1} = (\mathsf{PBV},\ [\mathsf{20pm}, \mathsf{21pm}],\ 1,\ 0.8,\ 0.7,\ \mathsf{male}, \cdots)$
$\mathsf{e_2} = (\mathsf{PBV},\ [\mathsf{20pm}, \mathsf{21pm}],\ 1,\ 0.8,\ 0.7,\ \{\mathsf{male}, \mathsf{female}\}, \cdots)$

are two events with v_1 for *gender* (we have omitted other attributes for simplicity) when we cannot be sure if the person is male or female. So we preserve all these possible conclusions with some kind of uncertainty.

Probabilistic event models are proposed in (Wasserkrug, Gal, & Etzion 2005; 2008), while event models using Dempster-Shafer theory are proposed in (Ma *et al.* 2009) to describe possibly incomplete/uncertain surveillance data from multiple sources.

Event inference: A most common approach to event inference is to deploy a set of inference rules representing the relationships between events. An inference rule R can be defined as a tuple (EType, Condition, uncertainty) where EType is the event type of the inferred event, Condition is the set of conditions to infer the events, and Uncertainty is the assignment of any uncertainty values associated with the derivation of the event. We shall bear in mind that there could be multiple outcomes from a set of conditions, such as *threat* and *no threat* from similar behaviors etc.

However, once rules are created, unless they are constantly updated, a system using these rules would predict a relative stable set of events. To cope with the dynamics of a surveillance system, shall we consider a multi-agent based system where each agent could ideally evolve and learn from its environment overtime? This leads to the following discussion.

Scalability and Ontologies

Multi-agent based systems have been explored in the surveillance area by many researchers (e.g. (Vallejo *et al.* 2008; Abreu *et al.* 2000; Barber *et al.* 2004; Rossetti & Liu 2005; Chen, Cheng, & Palenc 2009), etc.). Developing a multi-agent system (MAS) is a challenging task, considering sophisticated agent interactions and uncertain environmental dynamics and domain requirements. The main premise in multi-agent systems is to model real world in terms of agents that exhibit intelligence, autonomy, and some degree of interaction with other agents and with its environment. Other characteristics of agents include, for example, reactivity, adaptability, pro-activity, and the ability to communicate and to behave socially. To achieve the scalability of a surveillance system, a multi-agent based system seems to be a choice for the future.

The development of such a system poses many challenges of its own, such as the requirement of proper selection of agent technologies where selection is based on adherence to the agent architecture structure and satisfaction of domain and installation requirements of a particular application. Since the main task here is not to develop novel agent technologies, rather is the proper application and adaption of existing agent technologies to CCTV-based surveillance, selecting a suitable agent system shell would greatly speed up the development of an applications system. However, in-depth understanding of agent systems, knowledge representation techniques, uncertainty and inconsistency management approaches, are all part of the development process. Therefore, an intelligent surveillance system over a large network requires its developers to master many aspects of research components within the broad area of artificial intelligence. This is in addition to signal, image, audio processing at the sensory level for providing elementary information for such a system.

As an essential part of a multi agent system, ontology development is a must in order to enable agents' communication. The questions we ask here in relation to the above discussions are: who are the people responsible for creating such ontologies, are there any existing ontologies by the surveillance research community, do we need to get a standardized ontology worldwide or shall we develop our own ontologies each time we want to build a surveillance system? There may be no easy answers to these questions at this stage. However, as more and more agent based surveillance systems are being developed and applied, these questions will need to be properly addressed by certain organizations similar to organizations overseeing the development of OWL, XML etc.

Evaluation Issues

An intelligent surveillance system is a complex artifact, especially if a multi-agent concept is adopted. When evaluating such a system, what aspects are we going to evaluate and how? Many individual elements of the the system, such as events detection, rules, fusion methods, agents communications are supposed to be evaluated already separately. When integrating everything together, we need to be able to pin down the exact problems that prevent us from obtaining the kind of

reasoning that we anticipate, if that occurs. How can we achieve this and more generally how can we compare different systems that claim to be able to deliver different things if they are only tested on their own case studies?

It seems some kind of repository collecting testing scenarios would be a way forward, like some standard datasets used in data mining and machine learning communities. However, unlike datatsets that are relatively easy to create while still maintaining data protection policies, surveillance scenarios may be harder to create and are more prone to privacy issues.

Conclusion

Real-time situation awareness surveillance poses more challenges than what we have discussed in this short position/discussion paper. What we have investigated here are closely related to our experience in developing intelligent surveillance systems in our research projects. We want to continue expending this list of challenges and discuss any related issues they bring during the next few years when we start working with industry on building such systems.

References

Abreu, B.; Botelho, L.; Cavallaro, A.; Douxchamps, D.; Ebrahimi, T.; Figueiredo, P.; Macq, B.; Mory, B.; Nunes, L.; Orri, J.; Trigueiros, M.; and Violante, A. 2000. Video-based multi-agent traffic surveillance system. In *Proc. IEEE Intelligent Vehicles Symposium*, Lecture Notes in Computer Science, 457–462. SPIE.

Adi, A., and Etzion, O. 2004. Amit - the situation manger. *VLDB J.* 13(2):177–203.

Barber, K.; Ahn, J.; Fullam, K.; Graser, T.; Gujral, N.; Han, D.; Lam, D.; McKay, R.; Park, J.; and Vanzin, M. 2004. Multi-agent system development: Design, runtime, and analysis. In *Proc. of AAAI*, 1006–1007.

Bsia. Florida school bus surveillance. In *http://www.bsia.co.uk/LY8VIM18989_action;displays tudy_sectorid;LYCQYL79312_caseid;NFLEN064798*.

Chen, B.; Cheng, H.; and Palenc, J. 2009. Integrating mobile agent technology with multi-agent systems for distributed traffic detection and management systems. *Transportation Research Part C: Emerging Technologies* 17(1):1–10.

Cron, G., and Dubuisson, B. 1998. A weighted fuzzy aggregation method. In *Fuzz-IEEE*, 675–680.

Dempster, A. P. 1967. Upper and lower probabilities induced by a multivalued mapping. *The Annals of Statistics* 28:325–339.

Dubois, D., and Prade, H. 1988. Representation and combination of uncertainty with belief functions and possibility measures. *Computational Intelligence* 4:244–264.

Elouedi, Z.; Mellouli, K.; and Smets, P. 2004. Assessing sensor reliability for multisensor data fusion within the transferable belief model. *IEEE Trans. on SMC-Part B* 34(1):782–787.

Konieczny, S., and Pino-Pérez, R. 1998. On the logic of merging. In Cohn, A. G.; Schubert, L.; and Shapiro, S. C., eds., *KR'98, Principles of Knowledge Representation and Reasoning*, 488–498. San Francisco, California: Morgan Kaufmann.

Liu, W. 2006. Analyzing the degree of conflict among belief functions. *Artificial Intelligence* 170:909–924.

Lowrance, J. D.; Garvey, T. D.; and Strat, T. M. 1986. A framework for evidential reasoning systems. In *Proc. of 5th AAAI*, 896–903.

Ma, J.; Liu, W.; Miller, P.; and Yan, W. 2009. Event composition with imperfect information for bus surveillance. In *Proc. of AVSS*.

Qi, G.; Liu, W.; and Glass, D. 2004. A split-combination method for merging inconsistent possibilistic knowledge bases. In *Proc. of KR*, 348–356.

Rogova, G., and Nimier, V. 2004. Reliability in information fusion: literature survey. In *Proc. of Information Fusion*, 1158–1165.

Rossetti, R., and Liu, R. 2005. *A Dynamic Network Simulation Model Based on Multi-Agent Systems*. 181–192.

Security, G. Glasgow transforms bus security with ip video surveillance. In *http://www.ipusergroup.com/doc-upload/Gardiner-Glasgowbuses.pdf*.

Shafer, G. 1976. *A Mathematical Theory of Evidence*. Princeton University Press.

Shu, C. F.; Hampapur, A.; Lu, M.; Brown, L.; Connell, J.; Senior, A.; and Tian, Y. 2005. Ibm smart surveillance system (s3): a open and extensible framework for event based surveillance. In *Proc. of IEEE Conference on AVSS*, 318–323.

Vallejo, D.; Albusac, J.; Gonzalez-Morcillo, C.; and Jimenez, L. 2008. A service-oriented multiagent architecture for cognitive surveillance. In *Proc. of the 12th international workshop on Cooperative Information Agents XII, CIA'08*, 101–115. Berlin, Heidelberg: Springer-Verlag.

Wasserkrug, S.; Gal, A.; and Etzion, O. 2005. A model for reasoning with uncertain rules in event composition. In *Proc. of UAI*, 599–608.

Wasserkrug, S.; Gal, A.; and Etzion, O. 2008. Inference of security hazards from event composition based on incomplete or uncertain information. *IEEE Transactions on Knowledge and Data Engineering* 20(8):1111–1114.

Yan, W., and Miller, P. 2008. Visual event computing: A survey.

Zadeh, L. 1978. Fuzzy sets as a basis for a theory of possibility. *Fuzzy Sets and Systems* 1:3–28.