

A Semantic Wiki Alerting Environment Incorporating Credibility and Reliability Evaluation

Brian Ulicny^a, Christopher J. Matheus^a, Mieczyslaw M. Kokar^{a,b}
^a*VISTology, Inc.*; ^b*Northeastern University*

Abstract. In this paper, we describe a system that semantically annotates streams of reports about transnational criminal gangs in order to automatically produce models of the gangs' membership and activities in the form of a semantic wiki. A gang ontology and semantic inferencing are used to annotate the reports and supplement entity and relationship annotations based on the local document context. Reports in the datastream are annotated for reliability and credibility in the proof-of-concept system.

Keywords: media monitoring; semantic analysis; entity/relation extraction; event tracking; gangs; reliability; credibility

1 Introduction

In this paper, we describe a prototype we are developing that we call the Semantic Wiki Alerting Environment (SWAE). SWAE ingests streams of open-source news media and social media and automatically constructs a model of transnational criminal street gangs, including their membership and their activities. The system automatically provides updates and alerts to significant changes in that model in the form of emails, text alerts and semantic wiki pages. The system relies heavily on ontology-based semantic annotation [1].

In today's intelligence and battlespace environment, large amounts of data from many sources must be effectively analyzed in a timely manner in order to provide an accurate and up-to-date understanding of current and potential threats. Key to understanding these threats is the identification and characterization of the various entities that they involve. These include the relevant individuals, groups, locations and events along with their corresponding interrelationships.

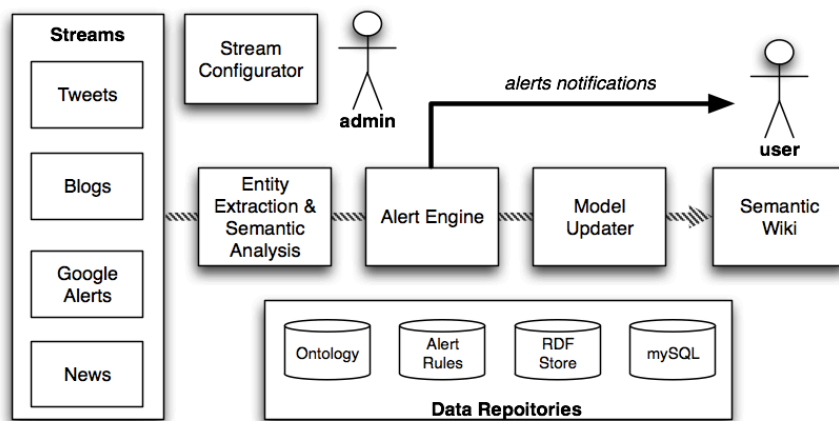
A wiki is a Web-based environment in which users can easily edit the text and layout of documents using a simplified, non-HTML syntax. Wikipedia is the most familiar example: a world-wide encyclopedia that any user can edit. Change-tracking by author and automatic hyperlinking are important aspects of wiki functionality. A semantic wiki is a wiki in which users can not only easily insert hyperlinks between documents, but in which semantic annotations of documents can be easily edited by users. In a semantic wiki, semantic web triples are encoded directly in the text. The subject of the triple is the topic of the page itself; predicate and object are then encoded as attribute::value pairs in the text. Thus, the markup `[[population::3,396,990]]` on a page for *Berlin*, asserts that Berlin has a population of that size. One can further represent that the *population* predicate is of Type::Number, to enable proper sorting and comparison. These triples can be used within semantic queries and to populate visualizations such as maps, timelines, and graphs automatically. We use the Semantic MediaWiki platform, an extension of the MediaWiki platform that underlies Wikipedia.

In their current state, semantic wikis are relatively primitive and require significant human effort in order to annotate the wiki's contents with semantic markup consistently [5]. However, in this project we have customized a semantic wiki to automatically pre-process incoming data from multiple sources, extracting relevant semantic information (explicit metadata and implicit relationships) and rendering it in a form readily consumable, and editable, by human analysts through the wiki interface. We also implement user definable alerting capabilities to permit automated notification regarding significant new events or critical changes in the composite representations of key entities such as dangerous individuals or groups. Ontology-based alerting capabilities of this sort necessitate the use of a formal inference engine, ideally one that is rule based to facilitate and simplify user customization.

2 System Overview

The high level design of SWAE is depicted in Figure 1. Data flows into the system from the left in the form of data streams (e.g. Tweets (Twitter updates), Blogs, news, alerts (standing news queries)). These reports are processed by the entity and relation extraction and semantic analysis algorithms. The annotated results are placed into the data repository and trigger the invocation of the alert engine, which is based on the SPARQL query engine available in the Open Sesame RDF data store. The results are used to inform the user of significant items and to update the semantic model maintained in the semantic wiki for subsequent access and further analysis by users. Semantic wiki pages are created automatically from the RDF produced during semantic analysis and entity extraction.

Figure 1. SWAE Data Flow



For development purposes, we have chosen to monitor data about the activities of transnational gangs as the focus of our investigation. There are many parallels between countering organized gang activity and counterinsurgency. Reports about gang activities are readily available from open sources and do not require translation.

We monitor several RSS feeds and periodically download and process new items in order to update the system. In addition we track news media outlets and law

enforcement press releases that we obtain via the news aggregator service Topix.net. Social media platforms such as Twitter (twitter.com), and Flickr (photo sharing) contain many reports by both self-professed gang associates and those chronicling their activity; these data streams, however, are quite noisy. Twitter status updates mentioning gang names contain a mix of chatter about the gang, unrelated uses of the term and links to news articles. Photo sharing sites such as Flickr (flickr.com) contain many depictions of gang graffiti, which can often be mapped to specific times and locations; several groups on Flickr are dedicated to documenting gang graffiti.

Our goal is to monitor these social media and open-source media streams in order to trigger alerts such as:

- A 10% increase in gang G's weekly incidents of type I in location L
- First occurrence of incident I by G in L in past year
- A 10% increase in attacks of G1 on G2
- New member of gang G
- A 10% increase in G membership in L since T
- New leader L of G
- A 20% increase in communications between members of G in past 24 hours
- Social media report of gang activity not correlated with media report
- Graffiti by or about gang G .

3 Ontology

In the Street Gang ontology (Figure 2) there are four primary top-level classes: Organization, Person, Incident and Information. The ontology defines numerous types of Incidents but distinguishes between CriminalIncidents and non-criminal incidents, the former of which is used to infer members of the Criminal class. There are also several types of Information corresponding to the source data that SWAE processes. There are two secondary classes - IncidentRate and Source. IncidentRate is intended to be used to record information about the *count* of incidents of a certain *incidentType* that are carried out by an Organization in a given period of time; these elements were added as it became clear from our sample rules that such constructs but be necessary to support many of them. There is also a Source class that was created to permit the author of a piece of Information to be either an Organization or a Person.

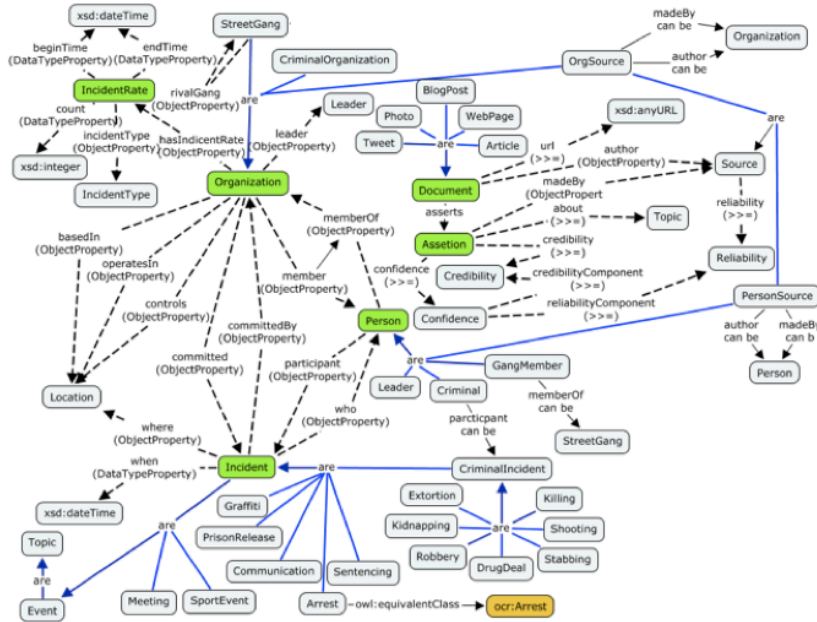
4 System Components

Feeds for data sources are periodically re-queried in order to obtain the latest reports from both media outlets (which are analogous to analyzed intelligence reports) and social media reports such as Tweets and Flickr photos (which, if not citing media outlets, are analogous to source material that has not yet been subject to intelligence analysis). Feeds in non-RDF compliant formats are converted to RDF automatically. These source feeds provide useful metadata about the reports. Links from the RSS feeds are automatically extracted and are then processed using the OpenCalais API¹ to extract basic level objects and relations based on their local context in the text.

In the following extract, OpenCalais's output detects the presence of an arrest relationship in the string

¹ OpenCalais Web Service API. <http://www.opencalais.com/calaisAPI>

Figure 2 Gang Ontology



...The arrest follows the May 28 arrest in Santa Cruz of [X], another [Gang Y] member...

The RDF output of Open Calais encodes the detection of an instance of the Arrest relation as follows: an entity of type InstanceInfo is created with URI ".../Instance/40". This InstanceInfo is about (oc:subject) URI. Note that this InstanceInfo doesn't by itself provide explicit information about who was arrested, when or where. (The 'oc' prefix denotes an OpenCalais namespace.)

```

<rdf:Description rdf:about="http://d.opencalais.com/dochash-1/6d3695ba-2142-3679-b8db-5e206844c924/Instance/40">
  <oc:detection>  <![CDATA[

in a news release.



<p> The arrest follows ]the May 28 arrest in Santa Cruz of [X] [, another [Gang Y], or [VariantName V], member]]></b:detection>
  <oc:docId rdf:resource="http://d.opencalais.com/dochash-1/6d3695ba-2142-3679-b8db-5e206844c924"/>
  <oc:exact>the May 28 arrest in Santa Cruz of [X]</b:exact>
  <oc:length>55</b:length>
  <oc:offset>1071</b:offset>
  <!--this incident URI is what the InstanceInfo is about-->
  <oc:subject rdf:resource="http://d.opencalais.com/genericHasher-1/f6e310ea-f54a-3aee-bc99-7293eea20f44"/>
  <rdf:type
  rdf:resource="http://s.opencalais.com/1/type/sys/InstanceInfo"/>
</rdf:Description>


```

This further part of the OpenCalais output says that the indicated incident is of `rdf:type oc:Arrest`. It also specifies that the `oc:person` of the Arrest incident is specified by the URI indicated. It also indicates the date string (“May 28”) and normalized date (2010-05-28) of the incident. Note that this RDF snippet about the incident URI (i.e. all the information about this incident in RDF form) doesn’t specify, in particular, where the Arrest took place. None of the elements below that are associated with the Arrest incident are guaranteed to be present in the OpenCalais output depicting an incident of `rdf:type Arrest`.

```
<!-- The same Incident URI identified in the InstanceInfo RDF-->
<rdf:Description rdf:about="http://d.opencalais.com/genericHasher-
1/f6e310ea-f54a-3aee-bc99-7293eea20f44">
  <rdf:type
rdf:resource="http://s.opencalais.com/1/type/em/r/Arrest"/>
  <c:person rdf:resource="http://d.opencalais.com/pershash-
1/1b1289ef-845f-31a9-a640-b6724dbe61e1"/>
  <c:date>2010-05-28</c:date>
  <c:datestring>May 28</c:datestring> </rdf:Description>
```

5 Semantic Analysis

OpenCalais’ processing is very sophisticated, but because it does not always specify what we need it to specify for our alert processing, we need to do semantic analysis of the RDF graph and the original text in order to both augment and correct the RDF that has been output. OpenCalais’ recognizes entities and relationships based on their local context only; we often need to use global- or document-level inferencing to determine other relationships and entities.

We use the VISTology-developed inference engine, BaseVISor², to modify and augment the RDF produced by OpenCalais, and save the modified RDF. BaseVISor is VISTology’s forward-chaining inference and rule engine that infers facts from an RDF/OWL store based on an ontology (using OWL 2 RL) as well as user-specified rules that can involve procedural attachments for things like computing the distance between two latitude/longitude pairs. BaseVISor has been optimized to process triples very efficiently.

This semantic processing by BaseVISor results in a number of augmentations to the data. First, the OpenCalais RDF output lacks datatypes on elements, so these must be supplied for integers, dates and other datatypes used in OpenCalais output. Second, we use BaseVISor rules to correct systematic misidentifications that OpenCalais makes. For example, OpenCalais always identifies one particular gang name as a Person, not as a variant name for a specific gang. These revision rules are necessary because end users cannot customize OpenCalais with a custom vocabulary at present. Third, we employ BaseVISor rules to make rule-based inferences about the text in order to supplement OpenCalais’s event representations. As noted above, while OpenCalais identifies Arrest-type incidents in texts, it does not always identify the *who*, *what*, *where*, and *when* attributes of these events presumably because they can’t be determined by the local context. We use BaseVISor rules to infer times and locations for the surrounding event based on the entire text. For example, if no

² VISTology BaseVISor Inference Engine. <http://vistology.com/basevisor/basevisor.html>

location is specified for an event in the OpenCalais RDF output, to a first approximation, we specify the closest instance of a City in the text as the location of the Arrest. Similarly, if no date for an arrest is specified, then we take the date of the report itself as the arrest date, and so on.

We also use BaseVISor to insert RDF triples for instances of types of things not identified by OpenCalais, such as the names of gangs, and to associate persons with gangs based on the OpenCalais RDF. For example, if OpenCalais specifies that there is a *joining* relationship, and the subject of the joining is a certain person, and the object of the joining event is “the ABC prison gang”, then based on the presence of the term “ABC” in the object, we assert an association between the person and the ABC gang.

BaseVISor is also used to infer relations that are implicit from the data and the ontology as explicit triples. For instance, if the ontology says that “ABC” is a Gang, then if John is a member of the ABC gang, he is a gang member. A triple encoding this fact will be inferred and imported into the RDF store. All of the triples that can be inferred by means of these semantic analysis rules and the combination of the RDF output and the OWL ontology, using OWL 2 RL, are inserted into the global fact base.

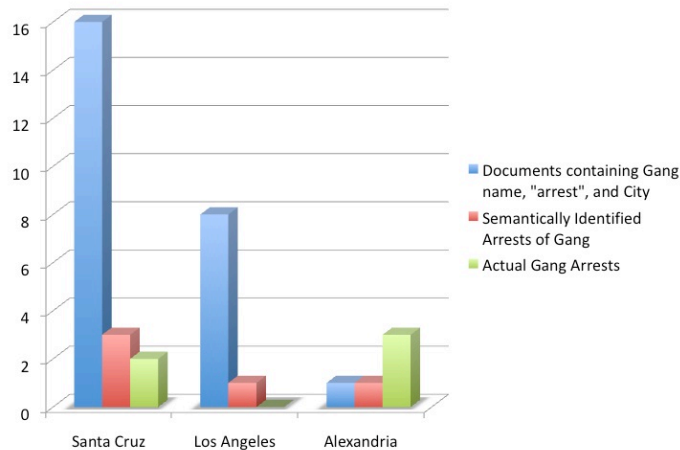
Finally, based on the OpenCalais RDF graph, we make API calls to other data sources in order to augment the RDF data store with the necessary data for querying. Although OpenCalais sometimes provides resolved geolocations for spatial entities like cities, it does not always do so. For instance, OpenCalais may identify “Santa Cruz” as being an instance of `rdf:type City`, but it does not always specify that this mention of a City actually refers to “Santa Cruz, California” with the corresponding latitude and longitude. Because OpenCalais cannot be forced to make a guess for every instance of City, we invoke the Geonames.org API in order to determine the latitude and longitude of the city based on document source metadata, from the feed.

After this, the data gathered and processed by the extraction component is imported into an OpenSesame RDF store and queried via SPARQL in order to update the model of the gang organization: its members, incident rates, event times and locations, and so on. The RDF data that has been input into the data store is periodically queried to provide semantic alerts, which are sent as email messages or text messages. Additionally, SPARQL queries are used to create and update topical pages in the Semantic MediaWiki reflecting our current knowledge of a gang.

6 Example and Discussion

In Figure 3, we contrast the approach outlined with more traditional keyword-based approaches to alerting and event tracking. The blue column shows the number of news stories containing a specified gang name, the name of the indicated city, and “arrest” over a two-week period in June, 2010. There were 16 documents corresponding to Santa Cruz, eight to Los Angeles, and one to Alexandria. Based on document counts alone, then, one would suppose that there were far more arrests in California than in Virginia during that period. However, the red column shows that automated semantic analysis identifies three arrests in Santa Cruz and one each in Los Angeles and Alexandria, VA. These are much closer to the actual figures (two in Santa Cruz; zero in Los Angeles; three in Alexandria, VA).

Figure 3 Event Counts: Keywords vs Semantic Analysis



The result of the semantic processing shows promise in that the total number of arrests identified per city is much closer to the actual result than one would infer from the document counts. Three arrestees out of four are correctly identified out of eighteen news articles (precision = 75%), and four out of six total arrestees in the corpus are identified (recall = 66%).

7 Information Evaluation

NATO STANAG (Standard Agreement) 2022 “Intelligence Reports” states that where possible, “an evaluation of each separate item of information included in an intelligence report, and not merely the report as a whole” should be made. It presents an alpha-numeric rating of “confidence” in a piece of information (compare [9]) which combines an assessment of the reliability of the source of the information and an assessment of the credibility of a piece of information “when examined in the light of existing knowledge”.³ The alphabetic Reliability scale ranges from A (Completely Reliable) to E (Unreliable) and F (Reliability Cannot Be Judged). A similar numeric information credibility scale ranges from 1 (Confirmed by Other Sources) to 5 (Improbable) and 6 (Credibility Cannot Be Judged).

As a first approximation, we have implemented some crude, initial rules for reliability and credibility. For example, if a source is from Topix (a news source) we mark it B (Usually Reliable). We could potentially mark reports from official government sources, such as FBI press releases, even higher. If a source is from Twitter or Flickr, we mark it 6 (Reliability Cannot Be Confirmed).

³ North Atlantic Treaty Organization (NATO) STANAG (Standardization Agreement) 2022 (Edition 8) Annex. Essentially the same matrix is presented as doctrine in Appendix B “Source and Information Reliability Matrix” of US Army FM-2-22.3 “Human Intelligence Collector Operations” (2006), although STANAG 2022 is not explicitly cited.

For credibility, if two reports identify the arrest/trial/conviction/killing of the same person, we mark each such report as 1 (Confirmed By Other Sources). STANAG 2022 does not prioritize coherence with the earliest reports; rather, it says that the largest set of internally consistent reports on a subject is more likely to be true, unless there is contrary evidence. It is a military truism that “the first report is always wrong” [6], so a bias towards coherence with the first report on a subject should be avoided. Further research is need to determine the degree to which two reports must be similar in order to count as independent confirmation of one another.

8 Conclusion and Future Work

We have described a proof-of-concept system for automatically creating and updating a model of a group (here, a criminal gang) in the form of a semantic wiki. We incorporate into this model a preliminary implementation of the STANAG 2022 metrics for source reliability and information credibility. Initial work on this system presented interesting design decisions that we outlined here, along with plans for future work. Our work differs from other available systems in that it attempts to create and maintain a usable model of a group and its activities automatically by creating semantic wiki pages that represent the current state of knowledge of the group. Significant changes in this model are sent as email or text alerts to concerned parties. By normalizing references to entities, relations and events across documents, the system provides a solution to the problem of data redundancy in reports. In ongoing work, we plan to investigate the incorporation of social-network metrics of centrality as proxies for estimating source reliability [7], and to incorporate social-network measures of source independence into our credibility calculation.

Acknowledgments. This material is based upon work supported by the United States Navy under SBIR Award No. N00014-10-M-0088.

References

1. W3C OWL Working Group. http://www.w3.org/2007/OWL/wiki/OWL_Working_Group
2. Model Driven Architecture and Ontology Development, by Dragan Gasevic, Dragan Djuric and Vladan Devedzic, Springer publisher, 2006.
3. Wikipedia entry for Wiki. <http://en.wikipedia.org/wiki/Wiki>
4. Semantic Web Technologies – Tends and Research in Ontology-based Systems, by John Davies, R. Studer and P. Warren, Wiley publisher, October 2007.
5. J. Bao. The Unbearable Lightness of Wiking – A Study of SMW Usability. Presentation. Spring 2010 SMW (Semantic MediaWiki Conference). MIT. http://www.slideshare.net/baojie_iowa/2010-0522-smwcon
6. LTG (Ret) Ricardo S. Sanchez, Military Reporters and Editors Luncheon Address. 12 Oct 2007. http://www.militaryreporters.org/sanchez_101207.html
7. Ulicny, B., Matheus, C., Kokar, M., *Metrics for Monitoring a Social-Political Blogosphere: A Malaysian Case Study*. IEEE Internet Computing, Special Issue on Social Computing in the Blogosphere. March/April 2010.
8. Semantic MediaWiki. <http://semantic-mediawiki.org>
9. Schum, D., Tecuci, G., Boicu, M., Marcu, D., Substance-Blind Classification of Evidence for Intelligence Analysis, in Proceedings of “Ontology for the Intelligence Community,” George Mason University, Fairfax, Virginia. October 2009.