A SEMANTIC WIKI ALERTING ENVIRONMENT INCORPORATING CREDIBILITY AND RELIABILITY EVALUATION

STIDS 2010
Brian Ulicny, Chris Matheus
Mieczyslaw M. (Mitch) Kokar
aVIStology, Inc.
a,bNortheastern University
What Are We Trying to Do?

- Provide an up-to-date understanding of current and potential threat by identifying and characterizing the entities involved.
- These include the individuals, groups, locations, activities and events associated with the threat and their interrelationships.
- The threat we are modeling is transnational street gangs operating in the US.
- The current state of the threat is modeled by means of an automatically updated Semantic Wiki representing the state of the group.
- Alerts are automatically sent to relevant parties when the state of the threat changes in significant ways.
HOW ARE GROUPS TRACKED TODAY?

- Civilian/Open Source Technology:
  - Alerts:
    - Google News Alerts,
    - Twitter monitors,
    - Cayuga Event Processing (Cornell), RSS/Atom Feeds
  - Manual (Semantic) Wikis:
    - MediaWiki (Wikipedia);
    - Semantic MediaWiki

- Military Technology:
  - Alerts:
    - CIDNE, Military Chat
  - Wiki(-like):
    - Intellipedia, TiGR
CONTRAST WITH EXISTING SYSTEM

Query identifies documents that contain “elvis” and “born” and a location. Answers literally all over the map. Consensus answer not obvious from location clusters. Documents are recent news articles.
WHAT IS NEW IN OUR APPROACH?

- Automatic population of Semantic Wiki
  - Using Entity Extraction and Formal Reasoning
- Cross-document alert generation based on semantic knowledge base
- Generation of alerts based on dynamically updated model of group (not just watchlist)
  - E.g. Alert me if there is a 10% increase in arrests of gang members in a specific city, week over week.
- Information Evaluation (per STANAG 2022)
- A successful implementation will allow analysts to interact with a dynamically updated model and receive alerts when significant changes occur.
ANTICIPATED BENEFITS

- Timeliness of alerts to increase operator’s productivity
- Automatic analysis of large quantities of data (much redundant) to improve operator’s awareness
- Semantically normalized information (entities/relations/events) to improve quality of operator’s decisions, relevance reasoning
- Focused, customizable filtering/monitoring to make the approach useful for various types of operations
- Evaluation of information for reliability/credibility to provide higher operator’s trust in the system
- Visual interactive information exploration (maps, timelines/tracks, charts) to provide system usability
Semantic Wiki Alerting Environment (SWAE) Overview
PROBLEM DOMAIN: STREET GANGS

Street gangs are analogous to terrorist organizations
loose organizations with hierarchical membership
uniformed military
narcotics operations are often used for funding
the threat is organized in dispersed cells
the local population must often be won over to provide information against the threat

Wealth of dynamic, online information for various sources (Twitter, MySpace, news sources, etc.)

Mara Salvatrucha (MS-13):
Started in El Salvador in the 1980s
US: >15K members, >115 “cliques”, 33+ states
Foreign: Canada, Guatemala, Honduras, Mexico and El Salvador
Makes money through extortion and...
SWAE Phase I Prototype

SWAE Phase I Prototype
DATA SOURCES

RSS Feeds
- RSS 2.0 & Atom -> RDF

Data Sources
- Topix.net
- Twitter
- Flickr
- MySpace
- Google

Maniac Latin Disciples
A monk stands guard over the entrance to Wildside...Atjag & Washerare Maniacs (Gang graffiti)
<?xml version="1.0" encoding="utf-8"?>

<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
         xmlns:dc="http://purl.org/dc/elements/1.1/"
         xmlns:content="http://purl.org/rss/1.0/modules/content/
         xmlns:r="http://backend.userland.com/rss2"
         xmlns="http://purl.org/rss/1.0/">

  <channel rdf:about="http://www.topix.com/search/article?q=%22ms-13%22+OR+%22mara salvatrucha%22"
          rdf:about="http://www.topix.com/search/article?q=%22ms-13%22+OR+%22mara salvatrucha%22">
    <dc:title>Search for "ms-13" OR "mara salvatrucha"
          News continually updated from thousands of sources across the web</dc:title>
    <dc:description>News continually updated from thousands of sources across the web</dc:description>
    <items>
      <rdf:Seq>
      </rdf:Seq>
    </items>
  </channel>
</rdf:RDF>
ENTITY/RELATION EXTRACTION

- Information to extract from text:
  - Information source
  - URLs of cited information
  - Locations of events (where)
  - Times of events (when)
  - Types of events (what)
  - Participants in events (who)

- Extraction Software used:
  - OpenCalais
  - BaseVISor (RDF matching, Regex)
  - (UIMA)
The arrest follows the May 28 arrest in Santa Cruz of [X] [, another [Gang Y], or [VariantName V], member]]>
ENTITY/RELATION EXTRACTION

- OpenCalais, Geonames plus BaseVISor
- Leverages OpenCalais’ free web service
  - Results returned as RDF based on OpenCalais ontologies
  - Ontologies not specific to street gangs
  - Results not always correct or complete so requires additional analytic processing
  - Only based on local contexts (not document wide)
SEMANTIC ANALYSIS
**BaseVISor Semantic Analysis**

- Augments OpenCalais output
  - Adds data types to RDF
  - Corrects misidentifications (Mara Salvatrucha not a person)
  - Time and location inferencing based on Global Document Context
    - Provide who, what, when, where for ALL events of interest
    - Infer specific geolocation (lat/long) using Geonames and Global Document context. (San Francisco source, “Santa Cruz” -> Santa Cruz, CA)

- Ontological Reasoning
  - Insert initial facts AND inferred facts into RDF data store
  - Based on Gang Ontology and rules
  - E.g. If John is a member of Latin Disciples and Latin Disciples is a gang, then John is a GangMember (Ontology)
  - If John joined MS-13 (i.e. there is a joining and John is the Agent and MS-13 is the Theme/Object), and MS-13 is a gang, then John is a GangMember (Rule)
**RDF Data Store**

- Add RDF results stored in time-dependent context with an RDF Data Store
- Currently using OpenSesame
  - Free, open source Sesame-based RDF Store from openRDF.org
  - Implements a query language very close to SPARQL 1.0
  - Java based API integrates well with BaseVISor
SPARQL MODEL UPDATES AND ALERTS

"Arrests, Count"

SPARQL_ARRESTS_COUNT = PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> SELECT DISTINCT ?r ?n ?d

"Recent MS-13 Trial, Count"

The email contains the following information:

**Subject:** Daily MS-13 Summary Report

**Date:** Mon, 2 Aug 2010 14:50:42 -0400 (EDT)

**From:** ms13watcher@vistology.com

**To:** osimakoff@vistology.com

**Recently identified MS-13 members:**
- James Viadero
- Hector Retana
- Edel Hernandez-Martinez

**Recent MS-13 Arrests:**

**Recent MS-13 Convictions:**
- Alejandro Umana, date: 2010-06-29, locname: Cincinnati, age: 25, gender: M, charges: December 2007 murders of two brothers, url: [http://www.topix.com/rss/search/article.xml?q=%22ms-13%22%20%22mara%20salvatrucha%22&x=0&y=0](http://www.topix.com/rss/search/article.xml?q=%22ms-13%22%20%22mara%20salvatrucha%22&x=0&y=0)
Semantic MediaWiki

- **Semantic MediaWiki (SMW)** is an extension of [MediaWiki](http://www.mediawiki.org) – the wiki application best known for powering Wikipedia – that helps to search, organise, tag, browse, evaluate, and share wiki content.
- While traditional wikis contain only text which computers can neither understand nor evaluate,
- SMW adds *semantic annotations* that allow a wiki to function as a collaborative database.
- In-line triples. Subject is page topic. [Predicate:Object]
- Semantic MediaWiki was first released in 2005, and currently has over ten developers, and is in use on hundreds of sites.
- In addition, a large number of related extensions have been created that extend the ability to edit, display and browse through the data stored by SMW.
SMW Page Generation: GeoSpatial Overlay
SMW PAGE GENERATION: INDIVIDUAL

Ingmar Guandique

**Age(s)**: 27

**Alternate Name(s)**: Ingmar Guandique

**Name(s)**: Ingmar Guandique

**Gender**: Male

**Category**: Gang Members

**Facts about Ingmar Guandique**

- **AlternateName**: Ingmar Guandique
- **B:age**: 27
- **B:gender**: Male
- **B:name**: Ingmar Guandique
SWAE Benefit Example

Documents containing "MS-13", "arrest", and City
- Semantically Identified MS-13 Arrests
- Actual MS-13 Arrests
### NATO STANAG 2022 (JC3IEDM, US Army HUMINT)

<table>
<thead>
<tr>
<th>Reliability (Source)</th>
<th>Credibility (Reported Information)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A: Completely reliable.</strong> It refers to a tried and trusted source which can be depended upon with confidence.</td>
<td>1: <strong>Confirmed by Other Sources.</strong> It can be stated with certainty that the reported information originates from another source than the already existing information on the same subject. (JC3IEDM: 3 Independent Sources)</td>
</tr>
<tr>
<td><strong>B: Usually reliable.</strong> It refers to a source which has been successfully used in the past but for which there is still some element of doubt in particular cases.</td>
<td>2: ** Probably True.** The independence of the source of any item of information cannot be guaranteed, but from the quantity and quality of previous reports, its likelihood is nevertheless regarded as sufficiently established. (JC3IEDM: 2 Independent Sources)</td>
</tr>
<tr>
<td><strong>C: Fairly reliable.</strong> It refers to a source which has occasionally been used in the past and upon which some degree of confidence can be based.</td>
<td>3: <strong>Possibly True.</strong> Despite there being insufficient confirmation to establish any higher degree of likelihood, a freshly reported item of information that does not conflict with previously reported behaviour pattern of target. (1 ...)</td>
</tr>
<tr>
<td><strong>D: Not usually reliable.</strong> It refers to a source which has been used in the past but has proved more often than not unreliable. (JC3IEDM: The probability of producing erroneous information is high (&gt;30%).)</td>
<td>4: <strong>Doubtful.</strong> An item of information which tends to conflict with the previously reported or established behaviour pattern of an intelligence target.</td>
</tr>
<tr>
<td><strong>E: Unreliable.</strong> It refers to a source which has been used in the past and has proved unworthy of any confidence.</td>
<td>5: <strong>Improbable.</strong> An item of information that positively contradicts previously reported information or conflicts with the established behaviour pattern of an intelligence target in a marked degree.</td>
</tr>
<tr>
<td><strong>F: Reliability cannot be judged.</strong> It refers to a source which has not been used in the past</td>
<td>6: <strong>Truth of information cannot be judged.</strong></td>
</tr>
</tbody>
</table>
STANAG 2022 Extension to Ontology
BaseVISor Evaluation Reasoning

BaseVISor performs “information evaluation” based on NATO STANAG 2022 credibility/reliability metrics

Same event; different sources ➔ Credibility ↑

Same who; what; when; different where ➔ Credibility ↓

Social Media; no Mainstream source ➔ Reliability Cannot Be Judged

Mainstream (US) media ➔ Usually Reliable

Dec 10, 2008 ... Rod Blagojevich, a Democrat, was arrested Tuesday on federal corruption charges. Illinois Gov. Rod Blagojevich returned to work Wednesday, ... (CNN)

Oct 22, 2010 ... A twice-elected Democrat, Blagojevich, 53, was arrested in December 2008 on charges that he tried to link official actions by his office to ... (Bloomberg.com)

Jan 29, 2009 ... Mr. Blagojevich, who was arrested Dec. 9 on corruption charges, (NYTimes)

Dec 11, 2008... Blagojevich, who was arrested Tuesday on corruption charges. ... (ChicagoDefender.com)

<no date> ...Illinois Governor Rod Blagojevich (D) was arrested today on corruption charges. The (WhoPlaysIn.com)

Who: Rod Blagojevich owl:sameAs Blagojevich sameAs Illinois Governor Rod Blajojevich (D)

When: Today owl:sameAs Dec. 9 owl:sameAs Tuesday

Where: Location?

What: Arrested...on federal corruption charges owl:sameAs arrested ... on charges that he tried to link owl:sameAs corruption charges
SWAE Phase I Conclusions

- Implemented an automated SWAE process that:
  - Collects and assembles large amounts of streaming data
  - Uses semantic web technologies to provide understanding of content, including classifications and relationships/links
  - Automatically generates alerts about critical events in real time
  - Distributes alerts to users (currently via email, but easy to extend)
  - Allows user to specify alert conditions and to view the collected data within the SMW
  - Keeps/updates models of situation and detects when data deviates from in model
  - Represents assembled information in Semantic Wiki pages for distributed collaborative assessment

- Leveraged and integrated existing algorithms and software
  - OpenCalais, Geonames, SMW, SPARQL, BaseVISor

- BaseVISor-like reasoning on RDF/OWL graphs and ontology is critical to the approach
FUTURE RESEARCH

- Alert Language and Engine
- Semantic Wikis
- RDF Data Stores
- Data Sources
- Improved Extraction Algorithms
- Enhanced Alerting and Customization
- Reliability/Credibility/Uncertainty Reasoning
  - Can SNA metrics be used as indicators of Reliability?
  - How to infer source independence (e.g. on Twitter)?
  - How to maintain source track record?
- Evaluation and Stress Testing
Questions?