Event Detection Challenges, Methods, and Applications in Natural and Artificial Systems

The 14th International Command and Control Research and Technology Symposium

Washington, DC

June 15-17, 2009

LOCKHEED MARTIN

Mitchell C. Kerman
Principal Engineer
Lockheed Martin MS2
609-326-5156
mitchell.c.kerman@lmco.com

Agenda

- Introduction
  - Definition of a System
  - Classification of Systems
  - Definition of an Event
  - Event Detection
  - Sensor Employment
  - Static Threshold Event Detection
  - Research Goals
- Common Challenges in Event Detection
  - Situational Dependence
  - Criticality of Application
  - Numerous and Diverse Data Sources
  - Network Topology
  - Event Detection Algorithms
- Typical Event Detection Methods
  - Statistical Methods
  - Probabilistic Methods
  - Artificial Intelligence and Machine Learning Methods
  - Composite Methods
- Example Event Detection Applications
  - Network Monitoring
  - Health Monitoring and Management
  - Environmental Monitoring and Prediction
  - Safety and Security
  - Business Process Optimization
- Event Detection Modeling and Simulation
  - Requirements Development
  - Algorithm Testing
  - System Implementation
- Epilogue
- References

INTRODUCTION

Definition of a System

- System
  - "A combination of interacting elements organized to achieve one or more stated purposes" [INCOSE, 2006]
  - A collection of elements that, in combination, produce results generally not obtainable by the elements acting alone
    - Elements: Operators, hardware, software, firmware, information, policies, documents, techniques, facilities, services, and other support components
      - All items required to produce system-level results
    - System-level results: Qualities, properties, characteristics, functions, behaviors, and performance of the entire system

A system produces a desired behavior beyond the capacity of any individual system element or subgroup of system elements

Classification of Systems

- Main Category
  - Natural
    - May not have an apparent objective
    - System inputs and outputs can be interpreted as serving a purpose
  - Artificial (or Man-made)
    - Designed for a specific purpose
    - Achieved through the delivery of outputs or services
- Subcategory
  - Observable
    - System inputs and outputs may be directly perceived in real-time
  - Non-observable
    - Either or both the system inputs and outputs may not be directly observed
- Method of Analysis
  - Qualitative
    - Delivery of the outputs
  - Quantitative
    - Measurement and analysis of specific system performance and effectiveness metrics derived from the system outputs

Definition of an Event

- Event: A significant occurrence or large-scale activity that is unusual relative to normal patterns of behavior. May be associated with naturally occurring phenomena and manual system interactions.
  - Naturally occurring phenomena
    - e.g., Chemical and thermodynamic reactions and physical processes
  - Manual system interaction
    - e.g., An operator pushing a button
- An event results in the aberration of system parameters and output metrics
- Examples of events [Ihler, Hutchins, and Smyth, 2006]
  - A large meeting in an office building
  - A malicious attack on a Web server
  - A traffic accident on a freeway

Events are identified through a process known as "event detection"

Event Detection

- Observable systems
  - Direct observation of the system states
  - e.g., Looking outside to see if it is raining
- Non-observable systems
  - Sensors track the states of the parameters of interest
  - e.g., Using a thermometer to see if the outside temperature is below freezing

Sensor Employment

- Sensors
  - Organic (to the detection platform)
  - Local
  - Remote
  - Any combination of these
- Sensor outputs are inputs to event detection systems
- Regardless of the system, sensor-based event detection is among the most difficult and time-constrained of analysis problems
  - Requires excessive computational power
  - Consumes large amounts of storage space for voluminous data
- Example events detected using sensor-based event detection
  - A substantial change in sea level
  - An increase in background radiation level
  - The maneuver (or course change) of an anti-ship missile
  - An increase in pressure within a boiler (or heat exchanger)

Static Threshold Event Detection

- Various methods of sensor-based event detection exist
- Static threshold event detection is one of the simplest and most common
  - e.g., Automobile fuel level sensor
- Simple method, but typically less reliable than more advanced techniques
  - e.g., What if the automobile fuel level sensor fails?
  - Many systems employ multiple (or redundant) sensors to overcome the reliability issues associated with a single sensor
    - Add complexity to the event detection problem since multiple inputs must be evaluated in order to determine whether or not an event is transpiring

Research Goals

- Introduce the most common difficulties and challenges in event detection problems
- Describe the event detection methods most frequently employed
- Provide example event detection applications
- Explore the relationship between event detection and modeling and simulation

➢ This presentation incorporates the discoveries of and lessons learned by multiple researchers and authors over many combined years of experience in event detection theory and application

➢ This rather broad study has never been previously published within a single volume

COMMON CHALLENGES IN EVENT DETECTION

Situational Dependence

- Event detection problems are extremely situationally-dependent
- Several problems may be similar, but no two problems are ever exactly the same
  - Parameters, variables, and output metrics are selected based upon the specific event detection problem
  - Artifacts may or may not be applicable to other problems within the same domain, even for very closely-related problems

Approach in one domain may inspire alternative methods within other domains

Criticality of Application

- Problems often address the requirements of a critical application
- e.g., Monitoring critical assets, measuring indicators of imminent catastrophic machine failures, detecting breaches within security perimeters, and observing human vital signs
- Require high precision and extreme timelines
  - High precision: A high true positive (i.e., correct detection) rate and a low false positive (i.e., incorrect detection) rate
  - Extreme timeline: A very short period of time in which the event detection method is able to correctly identify events
    - May range from less than a second to several minutes in duration (application dependent)

Event detection method must operate in real-time and fast enough to address the criticality of the application so that the detection report is not too time-late for an action or reaction to occur

Numerous and Diverse Data Sources

- Any single event detection problem may consider a variety of diverse data sources with different data types and formats
  - Digital revolution exploded the number of data sources and amount of data readily available
  - Problem is compounded in assessing what data is actually relevant and approach must be capable of evaluating data from selected sources
    - Data must be aggregated, converted, or reformatted into a uniform structure that is independent of the data source
- Enormous volumes of data, often measuring in terabytes
  - Requires high-powered computing machinery and immense digital storage space
- Size of data set
  - Too little data can lead to missed detections or the development of an event detection solution which does not work in all cases
  - Too much data can lead to “analysis paralysis”
    - Detection problem is over-analyzed and never really solved
- Raw sensor data
  - Often plagued by inaccuracies and incompleteness
    - Inaccurate or missing position information
    - Delayed or out-of-order arrivals at receiving station
  - May exhibit cyclical, seasonal, and irregular trends
  - Often corrupted by a number of “burst” periods of atypical or unusual behavior

Network Topology

- Network: A system containing a number of transmitting and receiving sensor stations, or nodes, that are connected through cables, wires, or wireless communications medium
- Network topology considers the locations and connectivity of these sensors in relation to the entire sensor network over time
  - In remote and mobile sensor networks, the network topology changes continuously due to sensor mobility and sensor lifetime
- Care and maintenance of the sensor network
  - Motes, or remote sensor nodes within a wireless sensor network, require maintenance and reseeding due to movement outside of the intended observed area, power consumption, sensor failures, and finite sensor lifetimes
- Network throughput and capacity
  - Aggregated data
    - Increases network throughput and reduces data processing times, but can significantly reduce the chance of detection since data from unaffected areas can mask the event signature
    - Detection system takes longer to notice the slight change in the aggregated data
  - Localized, sensor-level data
    - Improves detection sensitivity, but processing time for larger volumes of data can affect timeliness of detection
- Other considerations
  - Event persistence: The number of positive sensor detections required (from the same sensor) in order to report the occurrence of an event
  - Event lifetime: The length of an event as determined by the event persistence algorithm in signaling the start and end of the event
  - Context fluttering: An event indication is activated and deactivated in close succession due to inaccurate sensor readings or network delays
    - Sensor hunting: Activation and deactivation in close succession due to errors in a single sensor

Event Detection Algorithms

- Three main requirements: Timeliness, a high true detection rate, and a low false alarm rate
- Timeliness
  - Implies immediate analysis of incoming data and immediate reporting of the results
  - Fast storage and analysis are critical
  - Detection algorithm must be efficient (i.e., fast and computationally cheap)
  - May give priority to some solution approaches over others
- Initialization, learning, and stabilization times
  - Time for the algorithm parameters to properly initialize, learn from the event-free environment, and then reach a stable state
  - Preliminary (learning) data for the algorithm must be known to be void of the events of interest
  - Detection system "learns" to detect the event based upon the event-free situation
  - Disadvantage
    - A "day zero" event: An event which is uncharacteristic of the normal events and has a never-seen-before signature
    - Detection algorithm has no means to detect a "day zero" event, as the algorithm is not actively "looking" for it
- "Roll-forward" approach
  - Each new data point is assessed for the indication of an event as it is added to the data set
  - Detection system should output an operational decision-making conclusion upon completion of the analysis
- Precision vs. Recall trade-off
  - Precision: The fraction of reported events that are actual (true) events
  - Recall: The fraction of all events that are reported correctly
  - In a pessimistic approach, the algorithm ignores large numbers of (potential) events due to the data uncertainty
    - Precision is high, but many actual events are missed, reducing the recall value
  - In the optimistic approach, events are reported even in the presence of uncertain data
    - Precision is lower since the errors in the input data result in false events, but the recall value is higher since fewer true events are missed
- Active adversary
  - Many event detection problems are exacerbated by the presence of an active adversary

TYPICAL EVENT DETECTION METHODS

Event Detection Methods

- No clear manner in which to characterize every event detection method
- Typical event detection methods may be classified into four rather broad categories
  - Statistical
  - Probabilistic
  - Artificial Intelligence and Machine Learning
  - Composite

Statistical Methods (1 of 2)

- Static threshold method
  - Simplest and most computationally straight-forward
  - Detections are reported when the monitored parameter exceeds a predetermined threshold value
  - Detection condition persists as long as the parameter value exceeds the threshold set point
  - Threshold values may be determined based upon historical parameter values, analogy to similar sensors and systems, engineering estimates, or parametric analysis
- Regression
  - A data modeling and analysis technique in which the dependent variable is modeled as a function of independent variables, constant parameters, and an error term
    - Error term represents the variation in the dependent variable that cannot be explained by the model
  - Linear regression
    - Models the relationship between the dependent and independent variables as a straight line
  - Polynomial regression
    - Models the relationship between the dependent and independent variables as a polynomial
  - LOESS regression
    - Locally weighted regression
    - Fits a regression surface to data by multivariate smoothing
      - Simple models are fit to local subsets of data
  - Quantile regression
    - Estimates models for any of the conditional quantiles by minimizing sums of absolute residuals
    - Provides a more complete statistical analysis of the stochastic relationships among random variables

Statistical Methods (2 of 2)

- Time series analysis
  - Time series: A sequence of successive data points typically separated by a uniform time interval
  - Three broad model classes
    - Autoregressive (AR)
    - Integrated (I)
    - Moving average (MA)
  - Composite models
    - Autoregressive moving average (ARMA)
    - Autoregressive integrated moving average (ARIMA)
- Kalman filter
  - An efficient recursive filter that estimates the state of a dynamic system from a series of incomplete and noisy measurements
- Model fitting interpolation
  - Interpolate values at intermediate points
  - e.g., use the bicubic technique to interpolate the value at a point as the weighted average of its nearest sixteen neighbor points
- Principal Component Analysis (PCA)
  - Also known as the Karhunen-Loève transform (KLT)
  - Uses singular value decomposition (SVD) to reduce high-dimensional datasets into datasets with lower dimensions that approximate the original data

Probabilistic Methods

- Techniques in which the probability of event occurrence and other related probabilities and parameters are computed and assessed rather than computing and testing statistics from a sample data set
- Time-varying Poisson process model
  - Adaptively separates unusual event plumes from normal activity
  - Accounts for anomalous events
  - Outperforms the static threshold-based event detection technique
- Distributed Gaussian Method (DGM)
  - Generates Gaussian curves centered on each node
  - Curves are normalized and summed to reduce the geometric effect of node placement
  - Maximum value is then easily located
- SensorGrid [Tham, 2006]
  - An architecture for integrating sensor networks with grid computing
  - Grid computing involves groups of heterogeneous computational servers connected via high-speed network connections
  - Real-time information is mined, extracted, correlated, and processed to facilitate "on-the-fly" decisions and actions
  - Architecture relies upon distributed data fusion, event detection, and classification via probabilistic algorithms

Artificial Intelligence and Machine Learning Methods

- Usually both computationally and informationally intensive
- Sensor sources are often sparsely distributed in time and space
  - Require advanced fusion algorithms to correlate the data from multiple sources
- Database operations
  - The most direct of these methods
  - Includes database queries and table joins
- Mote Fuzzy Validation and Fusion (Mote-FVF)
  - Developed for wireless sensors network
  - Can distinguish between sensor failures and abnormal environmental behaviors by using network redundancy to compensate for sensor reliability
  - Does not require or rely upon a mathematical model of the system
- Particle filtering
- Genetic algorithms
- Neural networks
- Intelligent agents

Composite Methods

- Those methods that combine techniques within a category or from two or more of the categories
- Bayesian Gaussian Process (BGP) models
  - Combine probabilistic and machine learning methods
  - Powerful non-parametric learning methods based on simple probabilistic models

EXAMPLE EVENT DETECTION APPLICATIONS

Network Monitoring

- Monitoring Internet connections and conducting Web access logging
  - Frequency of visits to websites
  - General geographic locations of website visitors
  - Internet usage by employees
  - Security of online systems
    - Website intrusion detection
    - Failed account access logging
- Traffic monitoring
  - Determine whether or not an intersection requires a traffic signal

Health Monitoring and Management

- Epidemic (or pandemic) detection and prevention
  - Center for Disease Control and Prevention (CDC) continuously monitors medical and public health information from physicians and hospitals across the country
  - Goals
    - Earliest possible detection of viruses and disease
    - Halt the spread by quarantining and treating the afflicted individuals
  - Afflictions of interest
    - Naturally occurring, such as the influenza virus
    - Bio-terrorist developed/released
- Early detection of disease within individual patients
  - Screening and monitoring programs
    - Diseases such as diabetes, hypertension, thyroid disease, tuberculosis, cancer, and coronary artery disease
    - Age to begin screening exams, the intervals between exams, and (possibly) the age to end screening exams
  - Diagnose and treat patients before they show any signs or symptoms (i.e., while in the pre-clinical state)
- Aerospace applications
  - Timely detection of local health anomalies has a great impact on the safety of the mission

Environmental Monitoring and Prediction

- Early warnings of impending natural disasters
  - Tornadoes
  - Hurricanes
  - Tsunamis
  - Earthquakes
  - Floods
  - Volcanic eruptions
- Contamination of natural resources
  - Potable water is continuously monitored by water utilities for purity and potential contaminants
    - Causes
      - Natural
      - Man-made (e.g., terrorist)

Safety and Security

- Physical intrusion detection
  - Home and corporate security alarm systems
- Fire safety
  - Fire, smoke, and carbon monoxide alarm systems
- Homeland security
  - Cargo security
    - Verify that the contents of cargo was not compromised during shipment
  - Threat detection and management
    - Detection, tracking, and interception of threat missiles is a quintessential military threat management example
    - Intrusion detection of enemy submarines within an operating area
- Prediction of 9-1-1 call volumes
  - Aids emergency service providers in service planning and recognition of anomalous calls

Business Process Optimization

- Manufacturers rely heavily upon event detection methods
  - Reduce overall maintenance costs
    - Manufacturing and condition-based maintenance
      - Identify machines or processes that are in need of repair or adjustment
  - Ensure compliance with requirements
    - Business process compliance
      - Food and drug manufacturing
        - » Strict regulatory requirements obligate companies to certify that products do not exceed specific environmental parameters during processing

EVENT DETECTION MODELING AND SIMULATION

Relationship between Event Detection and Modeling and Simulation

- Intimate relationship and indivisible link between Event Detection and Modeling and Simulation (M&S)
  - Requirements Development
  - Algorithm Testing
  - System Implementation

Requirements Development

- Use M&S at the forefront of the systems engineering process as a requirements development tool for an event detection system
- Requires a detailed study of the real-world system
  - Examine the parameters of interest
  - Understand the relationships between the system inputs and outputs
  - Gain deeper insight into the system interactions
- Through M&S, the systems engineer may determine what events can and need to be detected and what parameters must be monitored to detect these events
  - e.g., An engineer may determine that mechanical vibration and noise levels must be monitored as indications of an imminent machine failure

Algorithm Testing

- M&S provides a test bed for new event detection algorithms and faster than real-time studies
  - Event detection algorithms are implemented within an M&S framework more easily than within a real system
  - Simulation allows the implementations to be tested faster than in the real system
- Caveat: M&S must be of high enough fidelity to be validated (as similar enough to the actual operating environment of the fielded event detection system)

System Implementation

- M&S may be used within an event detection system implementation to abstract or simplify real-world data
- Andrade, Blunsden, and Fisher [2006] present an automatic technique for detecting abnormal events in crowds by abstracting the original data using M&S
  - Crowd behavior is typically difficult to predict or translate semantically
  - It is also difficult to track individuals in a crowd even when using state-of-the-art tracking algorithms
  - Characterize crowd behavior by observing the crowd optical flow and use unsupervised feature extraction to encode normal crowd behavior
  - Unsupervised feature extraction applies spectral clustering to find the optimal number of models to represent normal crowd motion patterns
  - Crowd motion models are Hidden Markov Models (HMMs) to cope with the variable number of motion samples that might be present within each observation window
  - Results of this technique clearly demonstrate its effectiveness in detecting crowd emergency situations

EPILOGUE

Summary

- This presentation merely scratched the surface of event detection challenges, methods, and applications
  - The domain of applicability of event detection and its associated methods is expansive and ever increasing
- Reliable event detection is a pervasive problem
  - Requires detailed problem analysis and innovative solutions to overcome a myriad of challenges
  - Fortunately, there is no lack of researchers willing to accept these challenges
- Event detection methods will continue to be an area of interest and much research now and into the future

REFERENCES

References

- Abadi D, Madden S, and Lindner W. 2005. “REED: Robust, Efficient Filtering and Event Detection in Sensor Networks.” *Proceedings of the 31st Very Large Databases (VLDB) Conference.* Retrieved March 14, 2008, from <http://db.lcs.mit.edu/madden/html/reed_cr4.pdf>.
- Andrade E, Blunsden S, Fisher R. 2006. “Modelling Crowd Scenes for Event Detection.” *Proceedings of the International Conference on Pattern Recognition*, 1, 175–178. Retrieved March 13, 2009, from <http://homepages.inf.ed.ac.uk/rbf/PAPERS/andrade-crowd.pdf>.
- Balazinska M. 2007. “Event Detection in Mobile Sensor Networks.” *National Science Foundation (NSF) Workshop on Data Management for Mobile Sensor Networks (MobiSensors) 2007*. Retrieved July 25, 2008, from <http://mobisensors.cs.pitt.edu/files/papers/balazinska.pdf>.
- Dash D, Margineantu D, and Wong WK. 2007. “Machine Learning Algorithms for Event Detection.” A Special Issue of the *Machine Learning Journal*. Springer. Retrieved March 14, 2008, from <http://www.pittsburgh.intel-research.net/~dhdash/mlj_eventdetection.html>.
- Favretto FO, Farias CRG, and Murta LO Jr. 2007. “A Decision Support System for Ischemic Event Detection.” *Computers in Cardiology*, 34, 213–216. Retrieved March 14, 2008, from <http://www.cinc.org/Proceedings/2007/pdf/0213.pdf>.
- Fienberg SE and Shmueli G. 2005. “Statistical Issues and Challenges associated with Rapid Detection of Bio-Terrorist Attacks.” *Statistics in Medicine*, 24, 513-529. Retrieved September 12, 2008, from <http://www.niss.org/dgii/TR/FienbergShmueli-SIM-2005.pdf>.
- Gupchup J, Burns R, Terzis A, and Szalay A. 2007. “Model-Based Event Detection in Wireless Sensor Networks.” *Proceedings of the Workshop on Data Sharing and Interoperability on the World-Wide Sensor Web (DSI)*. Retrieved September 11, 2008, from < http://lifeunderyourfeet.org/en/literature/download/paper/LUYF_JHU_CR.pdf>.
- Ihler A, Hutchins J, and Smyth P. 2006. “Adaptive Event Detection with Time-Varying Poisson Processes.” *The Twelfth International Conference on Knowledge Discovery and Data Mining (Association for Computing Machinery)*. Retrieved February 28, 2008, from < http://www.ics.uci.edu/~ihler/papers/kdd06.pdf>.
- International Council on Systems Engineering (INCOSE). 2006. *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities, Version 3*. San Diego, CA: International Council on Systems Engineering.
- Jasso H, Fountain T, Baru C, Hodgkiss W, Reich D, and Warner K. 2007. “Prediction of 9-1-1 Call Volumes for Emergency Event Detection.” *The Proceedings of the 8th Annual International Digital Government Research Conference.* Retrieved March 17, 2008, from < http://scirad.sdsc.edu/datatech/data911/data911_files/dg.o_2007_paper.pdf>.
- Kerman MC, Jiang W, Blumberg AF, and Buttrey SE. 2008. “A Comparison of Robust Metamodels for the Uncertainty Quantification of New York Harbor Oceanographic Data.” *Journal of Operational Oceanography*, 1(2), 3-13.
- Kerman MC, Jiang W, Blumberg AF, and Buttrey SE. 2009. “The Application of a Quantile Regression Metamodel for Salinity Event Detection Confirmation within New York Harbor Oceanographic Data.” *Forthcoming*.
- MSNBC News Service. 2008. “Crews fan out in Texas to search for Ike victims.” September 14, 2008. Retrieved October 18, 2008, from < http://www.msnbc.msn.com/id/26637482/>.
- NIST. 2008. *NIST/SEMATECH e-Handbook of Statistical Methods.* Retrieved October 18, 2008, from <http://www.itl.nist.gov/div898/handbook/index.htm>.
- Sauvageon J, Agogino AM, Mehr AF, and Tumer IY. 2006. “Comparison of Event Detection Methods for Centralized Sensor Networks.” *IEEE Sensors Applications Symposium 2006.*
- Schwiderski-Grosche S. 2008. “Context-Dependent Event Detection in Sensor Networks.” *The Second International Conference on Distributed Event-Based Systems (DEBS)*. Retrieved July 25, 2008, from <http://debs08.dis.uniroma1.it/pdf/fa-grosche-context.pdf>.
- Sykes AO. 1993. “An Introduction to Regression Analysis.” *Chicago Working Paper in Law & Economics*. University of Chicago Law School. Retrieved October 4, 2008, from <http://www.law.uchicago.edu/Lawecon/WkngPprs_01-25/20.Sykes.Regression.pdf>.
- Tavakoli A, Zhang J, and Son S. 2005. “Group-Based Event Detection in Undersea Sensor Networks.” *The Second International Workshop on Networked Sensing Systems*. Retrieved February 28, 2008, from <http://www.cs.virginia.edu/papers/GroupDetection_inss05.pdf>.
- Tham CK. 2006. “Sensor-Grid Computing and SensorGrid Architecture for Event Detection, Classification and Decision-Making.” *Sensor Network and Configuration: Fundamentals, Techniques, Platforms, and Experiments*. Springer-Verlag. Germany. Retrieved March 14, 2008, from < http://www.ece.nus.edu.sg/stfpage/eletck/sensorgrid/Springer%20CK%20Tham%20SensorGrid.pdf>.
- Trafalis TB, Ince H, and Richman MB. 2003. “Tornado Detection with Support Vector Machines.” *Lecture Notes in Computer Science*, 2660, 708.
- Welch G and Bishop G. 2006. “An Introduction to the Kalman Filter.” University of North Carolina at Chapel Hill, Chapel Hill, NC. TR 95-041. Retrieved October 4, 2008, from <http://www.cs.unc.edu/~welch/media/pdf/kalman_intro.pdf>.
- Wikipedia. “Regression analysis.” Retrieved October 4, 2008, from <http://en.wikipedia.org/wiki/Regression_analysis>.
- Zelen M. 2007. “The Early Detection of Disease – Statistical Challenges.” *Joint Statistical Meetings 2007*. Retrieved March 17, 2008, from < http://www.amstat.org/meetings/jsm/2007/webcasts/videos/JMS2007_FisherLecture/JSM2007_FisherLecture_files/fdeflt.htm>.