

Modeling Adversarial Activity (MAA)

Carey Schwartz
DARPA/I2O

Proposers Day

September 27, 2016





MAA program goal

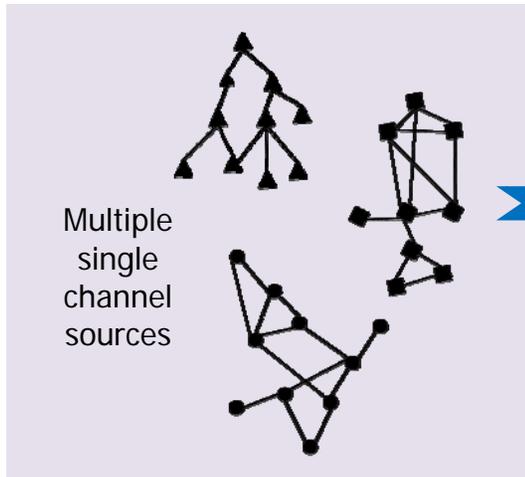
Goal: Develop mathematical techniques that integrate and analyze heterogeneous data sources to enable high confidence indications and warnings of Weapon of Mass Terrorism (WMT) activities

Hypothesis: Adversaries will leave a trail of observable transactions while they attempt to build or buy a WMT that MAA techniques will be able to detect



MAA vision

Observe transaction data



Multiple single channel sources

● ▲ ■ = Transactions associated with multiple channels

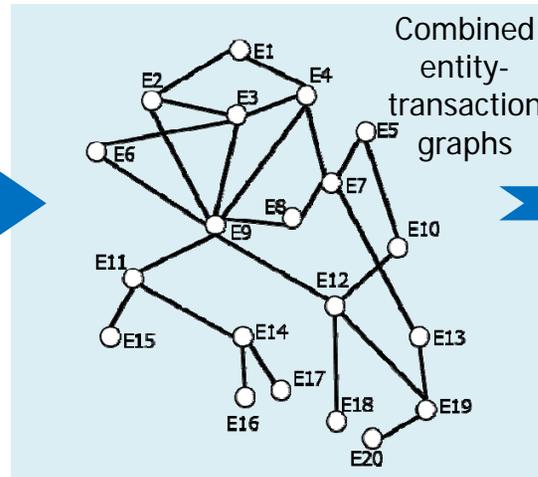
Challenges:

- Real world transaction data has PII & classification issues
- WMT activities may not be present in the data

Approach:

- Create realistic synthetic data for research with benign background activities
- Control presence or absence of WMT-related activities

Merge into graphs



Combined entity-transaction graphs

○ = ● ▲ ■ = Integrated view of all transactions

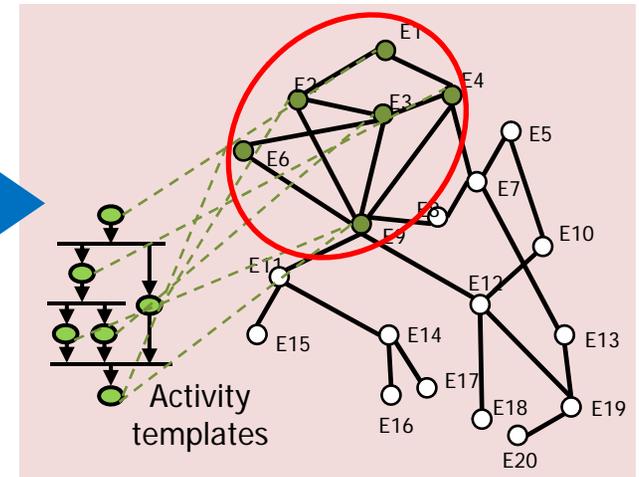
Challenges:

- Entities and transactions are often not correctly identified
- Product is a set of noisy, incomplete, mischaracterized, and mislabeled data

Approach:

- Create structure-based merge methods that can exploit relationships in graph topologies

Detect activity



Activity templates

Challenge:

- Adversaries' malicious activities are actively buried in benign background transactions

Approach:

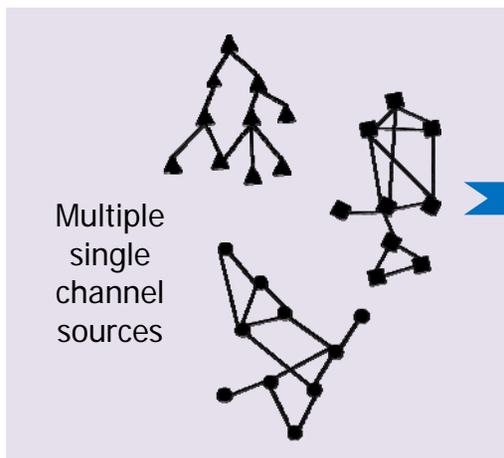
- Advance state of the art in sub-graph detection and graph isomorphism to improve graph matching



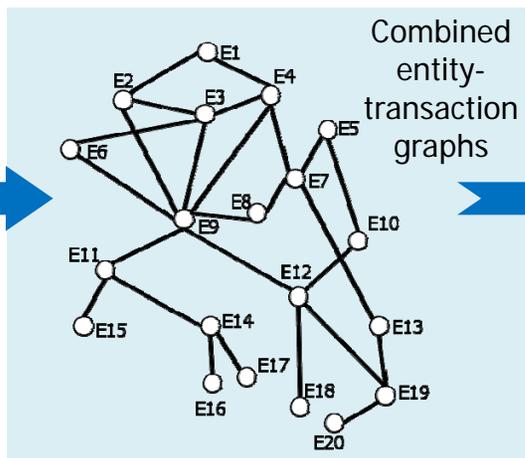
MAA acquisition strategy: Two phases

Phase 1: Mathematical underpinning

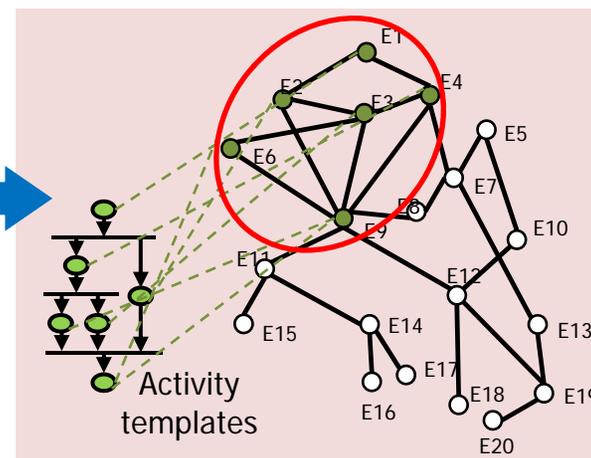
TA 1 Synthetic data creation



TA 2 Graph merging



TA 3 Activity detection



TA 4 Adaptive activity recognition

- Identify activities that resemble but are not exactly as specified by templates
- Reason over events and activity models generating hypothesis, data requests, and alternative explanations of observations

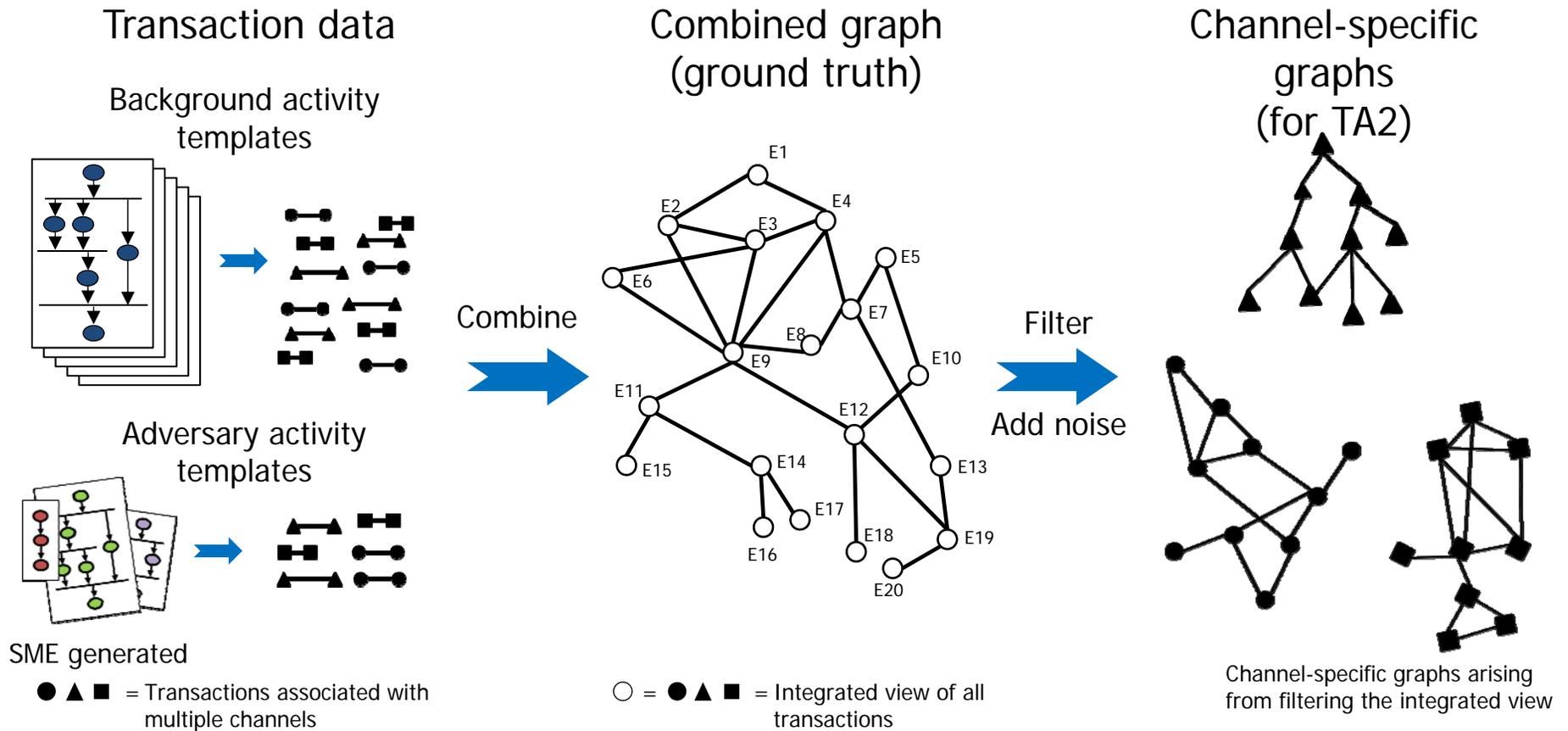
TA 5 System engineering and evaluation

- Build integrated MAA system and execute on synthetic transaction data
- Provide feedback to TA 1-4 based on performance
- Generate Receiver Operating Characteristic
- Conduct sensitivity analysis including value of data, quality of data, and instantiation of algorithms

Phase 2: System development (separate BAA)



TA1 Synthetic data creation



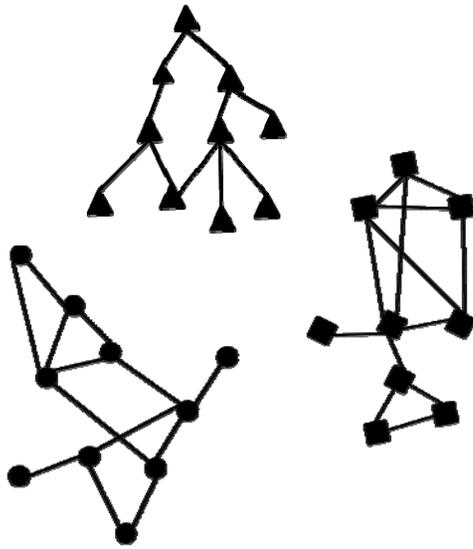
Challenges:

- Modeling the background and foreground at sufficient realism
- Scale of data sets and number of channels
- Embedding without trivializing detection



TA2 Graph merging

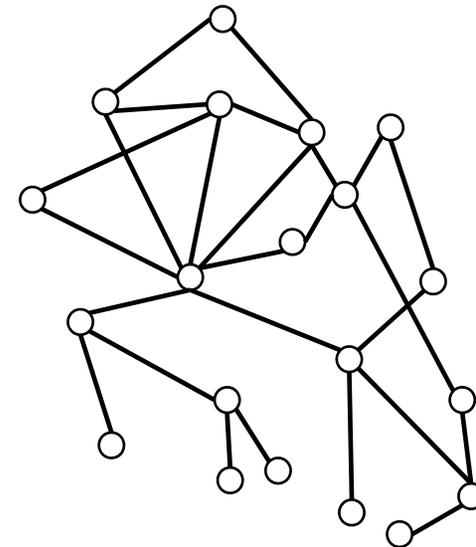
Channel-specific graphs
(from TA1)



Merge



Merged graph
(for TA3)

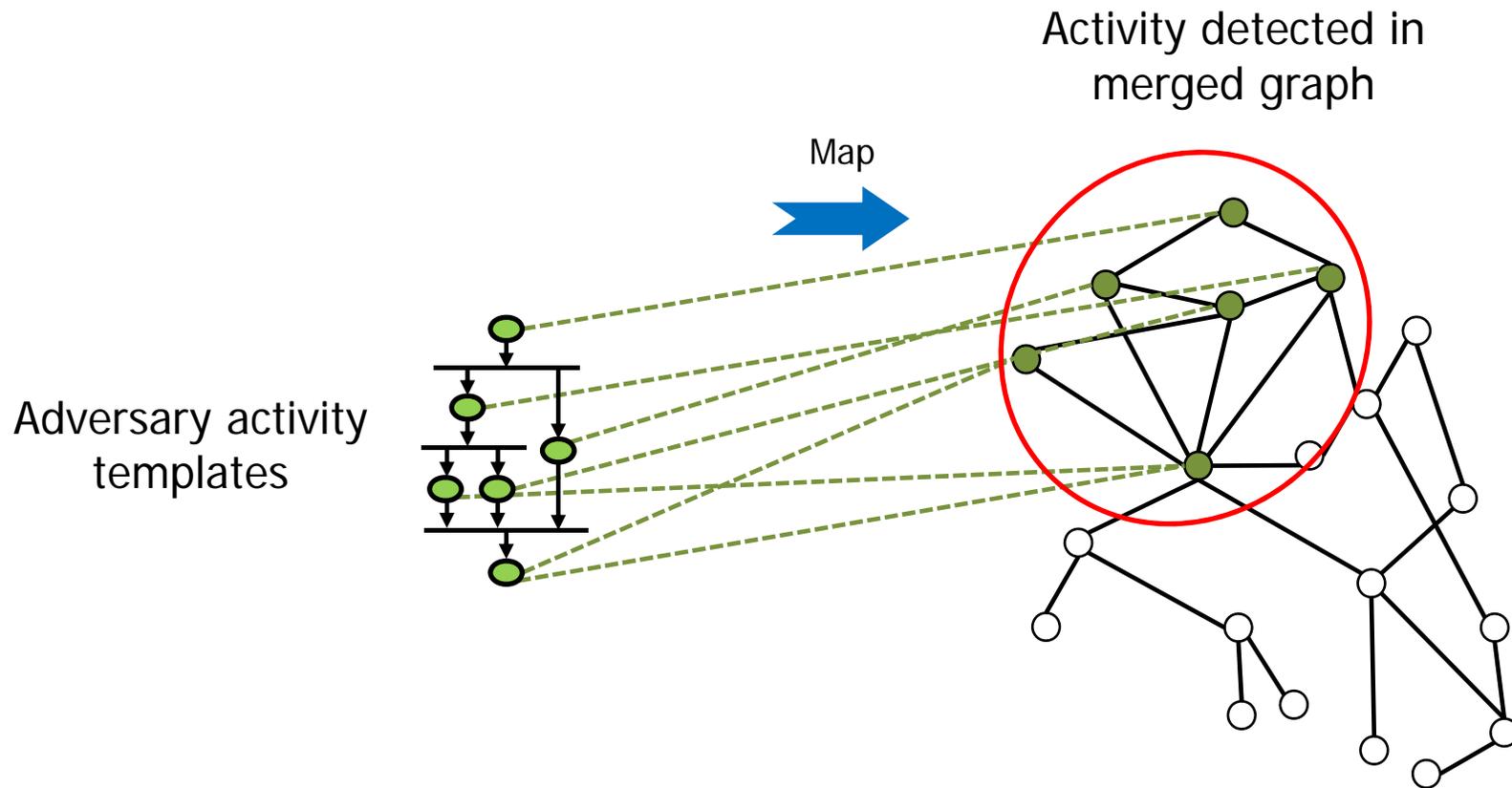


Challenges:

- Structural graph merging had been considered intractable
- Application of graph structure and topology to enhance feature matching



TA3 Activity detection



Challenges:

- Adaptation of adversary activity templates
- Requires application of sub-graph detection, graph isomorphism, community, clique detection in graphs, multi-commodity flow and temporal sequences in activity graphs



MAA Program Evaluation Schedule

MAA Program Schedule																
Task Area	FY17				FY18				FY19				FY20			
	Q1	Q2	Q3	Q4												
TA 1 Synthetic data creation		▲		▲		▲		▲		▲		▲		▲		▲
TAs 2 Graph merging			▲			▲		▲		▲		▲		▲		▲
TA3 Activity detection			▲			▲		▲		▲		▲		▲		▲
PI meetings	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘

Key ▲ Data or code drop and assessment
✘ PI Meetings



Teaming

- For performers seeking to team with others, we have created a MAA Teaming site:

<https://www.schafertmd.com/darpa/i2o/maa/teaming/>

- Account creation is required to participate
 - Immediate access will be granted to post your teaming information to the site
 - You can also browse or search the information of others
- You may also access the site through the MAA Proposers' Day meeting registration website
 - Use the "Teaming" link on the site navigation menu.

TEAMING IS NOT REQUIRED



www.darpa.mil