Dynamic, Covert Network Simulation

Patrick O'Neil
oneil.patrick@geoeye.com

GeoEye Analytics

April 5, 2012

GeoEye Analytics

Motivation

Problems

- There is a lack of open source covert network data.
- Any data on covert networks is almost certainly incomplete.
- Data we do have corresponds to one specific network with unique evolution.

Motivation

Problems

- There is a lack of open source covert network data.
- Any data on covert networks is almost certainly incomplete.
- Data we do have corresponds to one specific network with unique evolution.

Solution

- Generating data with DCNS allows us to test network analysis algorithms on a wide variety of networks, for which we know the ground truth.

Motivation

Problems

- There is a lack of open source covert network data.
- Any data on covert networks is almost certainly incomplete.
- Data we do have corresponds to one specific network with unique evolution.

Solution

- Generating data with DCNS allows us to test network analysis algorithms on a wide variety of networks, for which we know the ground truth.

Objective: Generate a dynamic network which grows and evolves in response to internal characteristics as well as external intervention.

Model Overview: Nodes and Edges

- In this simulation, nodes are given the ability to communicate and work with other nodes to accomplish randomly generated objectives.

Model Overview: Nodes and Edges

- In this simulation, nodes are given the ability to communicate and work with other nodes to accomplish randomly generated objectives.
- Nodes operate in a covert manner and from this local behavior, a globally secretive network is simulated.

Model Overview: Nodes and Edges

- In this simulation, nodes are given the ability to communicate and work with other nodes to accomplish randomly generated objectives.
- Nodes operate in a covert manner and from this local behavior, a globally secretive network is simulated.
- To begin, an undirected network structure, $G(V, E)$, forms the foundation upon which the network will build.

Model Overview: Nodes and Edges

- In this simulation, nodes are given the ability to communicate and work with other nodes to accomplish randomly generated objectives.
- Nodes operate in a covert manner and from this local behavior, a globally secretive network is simulated.
- To begin, an undirected network structure, $G(V, E)$, forms the foundation upon which the network will build.
- The network nodes, V, are *leaders* and *subordinates*

GeoEye Analytics

Model Overview: Nodes and Edges

- In this simulation, nodes are given the ability to communicate and work with other nodes to accomplish randomly generated objectives.
- Nodes operate in a covert manner and from this local behavior, a globally secretive network is simulated.
- To begin, an undirected network structure, $G(V, E)$, forms the foundation upon which the network will build.
- The network nodes, V, are *leaders* and *subordinates*
- The network edges, E, are weighted edges which reflect when two nodes have the ability to communicate and work together. Large edge weights indicate the connected members work well together.

GeoEye Analytics

Model Overview: Operations

Tasks

Tasks involve one leader and a subset of that leader's subordinates. These nodes work together to recruit new members to the network and collect resources. At the end of the task, the members travel to a "target location".

Model Overview: Operations

Tasks

Tasks involve one leader and a subset of that leader's subordinates. These nodes work together to recruit new members to the network and collect resources. At the end of the task, the members travel to a "target location".

Cooperative Tasks (co-Ops)

Cooperative tasks involve up to three leaders and a subset of those leaders' subordinates. co-Ops are designed to mimic the activities of real terror cells leading up to attacks that have occured in the past. In this presentation, the co-Op discussed is based upon the 2002 terror attacks in Mombasa, Kenya.

GeoEye Analytics

Member Attributes: Overview

Members of the network are assigned a set of attributes and roles that define their behavior within the network.

Member Attributes: Overview

Members of the network are assigned a set of attributes and roles that define their behavior within the network.

Attributes

- **Leadership**: A node may be a leader or a subordinate. Leaders can organize cells and begin operations while subordinates are members of cells and participate in the operations.
- **Roles**: Determines the node's available actions.
- **Chance of Discovery**: How exposed the member is to external intervention (capture, kill).
- **Radical**: Indicates the devotion of the member to the network. Used for promotion/demotion.

Member Attributes: Roles

Member roles were selected from the JJATT dataset. There are two ways for a node to obtain a role, it can enter the network with the role or it can be given the role during the simulation.

Member Attributes: Roles

Member roles were selected from the JJATT dataset. There are two ways for a node to obtain a role, it can enter the network with the role or it can be given the role during the simulation.

Available Upon Recruitment	
Sympathizer	Does not do much to help the network
Logistician	Needed for successful task completion
Bomb Maker	Needed for successful task completion
Bomber	Needed for successful task completion
Foot Soldier	Needed for successful task completion
Financier	Collects resources needed for tasks
Weapons	Collects resources needed for tasks
Acquired	
Trainer	Gives nodes new roles
Recruiter	Recruits new members for tasks

GeoEye Analytics

Member Attributes: Chance of Discovery

A member's chance of discovery $x_d \in [0, 1]$ (CoD) indicates how exposed it is to external intervention. A threshold value λ may be set so that any node x with $x_d > \lambda$ is captured or killed.

Member Attributes: Chance of Discovery

A member's chance of discovery $x_d \in [0,1]$ (CoD) indicates how exposed it is to external intervention. A threshold value λ may be set so that any node x with $x_d > \lambda$ is captured or killed.

CoD Influences

- **Neighbors:** As captured nodes may yield information about other nodes, when a node x is captured or killed, the *CoD* of all x's neighbors increases by the parameter ρ (i.e. $\forall y \in N_x, y_d(t+1) = y_d(t) + \rho$).
- **Location:** At any time, a member may be located in one of three types of locations: hostile (increases x_d), neutral, and friendly (decreases x_d).
- **Secrecy:** Each member is assigned a secrecy score, x_s. Every round, x_s is subtracted from x_d (i.e. $x_d(t+1) = x_d(t) - x_s$). This reflects the fact that some nodes are harder to track than others.

GeoEye Analytics

Member Attributes: Radical

A member's Radical score, $x_r \in [0, 1]$, indicates how committed it is to the success of the network.

Member Attributes: Radical

A member's Radical score, $x_r \in [0, 1]$, indicates how committed it is to the success of the network.

Radical

- High Score: Results in promotion after which the node can begin operations.
- Low Score: Demotion and eventually the node abandons the network.

GeoEye Analytics

Member Attributes: Radical

A member's Radical score, $x_r \in [0,1]$, indicates how committed it is to the success of the network.

Radical

- High Score: Results in promotion after which the node can begin operations.
- Low Score: Demotion and eventually the node abandons the network.

Radical Influences

- Increases when engaged in an operation
- Receives a bonus for successful completion
- Decreases when not involved in an operation

Network Attributes

Network Security

Network Security, $NS(c_m, k_m)$, is dependent upon the number of members captured/killed, $c_m, k_m \in \mathbb{N}$ in the past $m \in \mathbb{N}$ rounds. Higher NS values result in lower connectivity rates.

Network Attributes

Network Security

Network Security, $NS(c_m, k_m)$, is dependent upon the number of members captured/killed, $c_m, k_m \in \mathbb{N}$ in the past $m \in \mathbb{N}$ rounds. Higher NS values result in lower connectivity rates.

Operation Generation Rate

The probability of a new operation being generated, $P_O(c_m, k_m, r_c, r_k)$, depends on the number of members captured/killed in the past m rounds and the reaction to members being captured or killed, $r_c, r_k \in [-1, 1]$. For example, if $r_c < 0$, then the network will generate fewer operations in response to members being captured.

Node Update Process: Updating Attributes

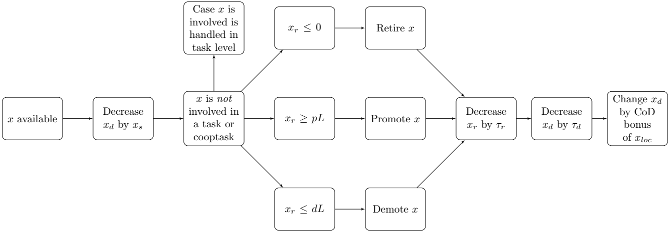


Figure: Node Update Process

Nodes are updated each round in the above process. When a node is involved in an operation, their attributes are updated in the operation update process. Thus, nodes can only be promoted/demoted when they are *not* involved in operations.

Node Update Process: Updating Connections

- Connections reflect when two nodes can communicate with each other.

Node Update Process: Updating Connections

- Connections reflect when two nodes can communicate with each other.
- If nodes i and j are connected, then $e_{ij} \in E$. The strength of this connection is given by $w : E \to [-1, 1]$. When an edge, e_{ij}, is first created, $w(e_{ij}) = 0.1$.

GeoEye Analytics

Node Update Process: Updating Connections

- Connections reflect when two nodes can communicate with each other.
- If nodes i and j are connected, then $e_{ij} \in E$. The strength of this connection is given by $w : E \to [-1, 1]$. When an edge, e_{ij}, is first created, $w(e_{ij}) = 0.1$.
- For all remaining time,

$$w_{t+1}(e_{ij}) = w_t(e_{ij}) + qO_c + sL_c,$$

where $q = 1$ when i, j are involved in the same operation (0 otherwise), $s = 1$ when i, j are in the same location (0 otherwise), and $O_c, L_c \in [0, 0.1]$.

GeoEye Analytics

Node Update Process: Updating Connections

- Connections reflect when two nodes can communicate with each other.
- If nodes i and j are connected, then $e_{ij} \in E$. The strength of this connection is given by $w : E \to [-1, 1]$. When an edge, e_{ij}, is first created, $w(e_{ij}) = 0.1$.
- For all remaining time,

$$w_{t+1}(e_{ij}) = w_t(e_{ij}) + qO_c + sL_c,$$

  where $q = 1$ when i, j are involved in the same operation (0 otherwise), $s = 1$ when i, j are in the same location (0 otherwise), and $O_c, L_c \in [0, 0.1]$.
- Connection rates are determined by C_n (mutual neighbor), C_t (same task), C_c (same co-Op). These rates are modified based on NS.

GeoEye Analytics

Node Update Process: Updating Connections

- Connections reflect when two nodes can communicate with each other.
- If nodes i and j are connected, then $e_{ij} \in E$. The strength of this connection is given by $w : E \to [-1, 1]$. When an edge, e_{ij}, is first created, $w(e_{ij}) = 0.1$.
- For all remaining time,

$$w_{t+1}(e_{ij}) = w_t(e_{ij}) + qO_c + sL_c,$$

where $q = 1$ when i, j are involved in the same operation (0 otherwise), $s = 1$ when i, j are in the same location (0 otherwise), and $O_c, L_c \in [0, 0.1]$.

- Connection rates are determined by C_n (mutual neighbor), C_t (same task), C_c (same co-Op). These rates are modified based on NS.
- When a node x is captured/killed, the neighbors of this node may disconnect from x.

GeoEye Analytics

Operations: Tasks

- Tasks consist of one leader and a number of subordinates working to accomplish a goal.

Operations: Tasks

- Tasks consist of one leader and a number of subordinates working to accomplish a goal.
- When a task is generated it is given the following attributes,

Operations: Tasks

- Tasks consist of one leader and a number of subordinates working to accomplish a goal.
- When a task is generated it is given the following attributes,
    - T_{rec}: the required number of members to successfully complete the task.

Operations: Tasks

- Tasks consist of one leader and a number of subordinates working to accomplish a goal.
- When a task is generated it is given the following attributes,
  - T_{rec}: the required number of members to successfully complete the task.
  - T_{res}: the required number of resources to successfully complete the task.

Operations: Tasks

- Tasks consist of one leader and a number of subordinates working to accomplish a goal.
- When a task is generated it is given the following attributes,
  - T_{rec}: the required number of members to successfully complete the task.
  - T_{res}: the required number of resources to successfully complete the task.
  - $T_{\Delta t}$: the amount of time until the task ends. This value is subject to $T_{\Delta t} \geq \max(T_{rec}, T_{res}) + opTime$ where $opTime$ is the duration of the operational stage of a task.

GeoEye Analytics

Operations: Tasks

- Tasks consist of one leader and a number of subordinates working to accomplish a goal.
- When a task is generated it is given the following attributes,
  - T_{rec}: the required number of members to successfully complete the task.
  - T_{res}: the required number of resources to successfully complete the task.
  - $T_{\Delta t}$: the amount of time until the task ends. This value is subject to $T_{\Delta t} \geq \max(T_{rec}, T_{res}) + opTime$ where $opTime$ is the duration of the operational stage of a task.
  - T_d: the amount each member's CoD increases each round.

Operations: Tasks

- Tasks consist of one leader and a number of subordinates working to accomplish a goal.
- When a task is generated it is given the following attributes,
  - T_{rec}: the required number of members to successfully complete the task.
  - T_{res}: the required number of resources to successfully complete the task.
  - $T_{\Delta t}$: the amount of time until the task ends. This value is subject to $T_{\Delta t} \geq \max(T_{rec}, T_{res}) + opTime$ where $opTime$ is the duration of the operational stage of a task.
  - T_d: the amount each member's CoD increases each round.
  - T_r: the amount each member's radical increases each round.

GeoEye Analytics

Operations: Tasks

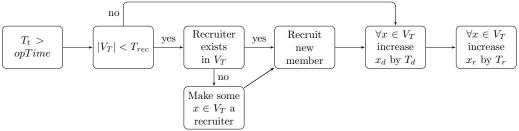


Figure: Preparation Stage

Operations: Tasks

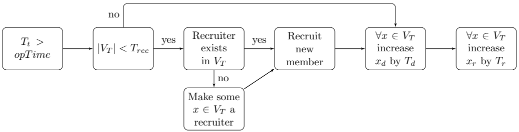


Figure: Preparation Stage

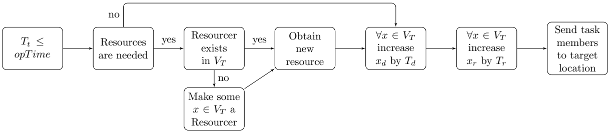


Figure: Operational Stage

Operations: Tasks

End of Task

- For a task to qualify for success, it must have met the recruitment and resource requirements.
- The probability of success is determined by a utility function $U(T)$.
- The utility function used in this simulation averages the edge weights of all involved members using weights of 0 when an edge does not exist.
- Since edge weights grow over time and inexperienced members would have low edge weights, $U(T)$ indirectly captures the experience of the members involved.
- If the task is successful, all of the task members receive bonuses to their edge weights.

Operations: Cooperative Tasks (co-Ops)

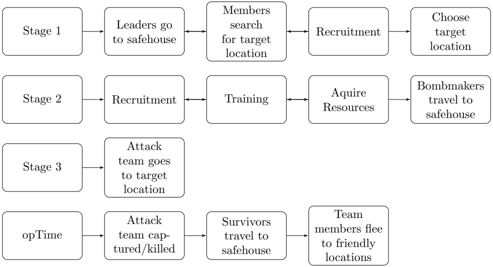


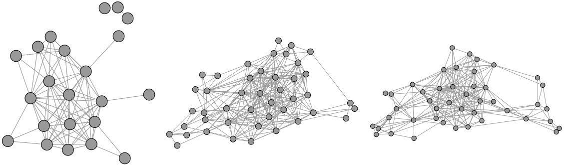
Figure: Mombasa co-Op Attack Sequence

- co-Ops are similar to tasks except they have up to three leaders and the behavior of those involved is more specific.

Results

Although the primary advantage to using DCNS is the ability to generate a wide range of networks, accurately recreating a real, historical network more readily demonstrates the tunability of DCNS. We begin with Jemaah Islamiyah's (JI) network structure in 1995 and simulate the network up to 2005.

Network	Nodes	Edges	Leaders	Avg Degree	Density	Avg Path Length
Real Start	22	83	14	7.55	0.36	1.60
DCNS Sim	44	236	15	10.72	0.25	2.02
Real Finish	45	233	14	10.36	0.24	2.07



(a) JI Start (b) DCNS Sim (c) JI Finish

Conclusion

- DCNS can be tuned to generate a wide variety of dynamic networks.

Conclusion

- DCNS can be tuned to generate a wide variety of dynamic networks.
- The simulator reacts to external intervention and acts in a cover manner.

GeoEye Analytics

Conclusion

- DCNS can be tuned to generate a wide variety of dynamic networks.
- The simulator reacts to external intervention and acts in a cover manner.
- Realistic networks can be generated using the correct parameters.

Conclusion

- DCNS can be tuned to generate a wide variety of dynamic networks.
- The simulator reacts to external intervention and acts in a cover manner.
- Realistic networks can be generated using the correct parameters.
- Networks with dynamics we have not yet encountered can be investigated and network analysis algorithms can be tested on these networks.

Conclusion

- DCNS can be tuned to generate a wide variety of dynamic networks.
- The simulator reacts to external intervention and acts in a cover manner.
- Realistic networks can be generated using the correct parameters.
- Networks with dynamics we have not yet encountered can be investigated and network analysis algorithms can be tested on these networks.
- DCNS allows a researcher to determine the sensitivity of their algorithms to the input networks they test upon.

GeoEye Analytics

Conclusion

Questions?