An Event-Based Method of Construction of Cyberspace Models

Youjun Wang[1, a], Hongqi Zhang[1], Tianwei Che[2,b], Chuanfu Zhang[1], Yuntian Zhao[1] and Chao Yang[1]

[1]Zhengzhou Information Science and Technology Institute, Zhengzhou, Henan, 450000, China

[2]Beijing Jianyin Investment Technology Development Co.,Ltd, Xicheng District, Beijing, 100055, China

[a]daxia1wang@163.com, [b]chetianwei@bjcjitec.com

Keywords: Cyberspace; Event; Cyber Entity; Mapping

Abstract. Cyberspace has become an important domain the same as the land, sea, air and space. Many cyberspace models were proposed to explain such a high coupled complex domain, but lack of practical method of construction these models make them hard to function. This paper proposes an event based method of construction of cyberspace models. We formalize a cyber event as an attribute group by abstracting key elements of the event. Through entity-mapping and relation-mapping, we construct cyberspace models base on graph theory by representing cyber entities as vertexes and relations between entities as edges.

Introduction

Different form simple computer network, cyberspace is much more coupled and always support important national or military missions. Development of cyberspace model is a component of National Strategy for Trusted Identities in Cyberspace[1].

Current researches of cyberspace models have some consensuses:

1) Cyberspace models always consist multi layers. Army U.S.[2] divided cyberspace into five components in three layers. Jakobson et al.[3] also proposed a cyberspace framework containing assets, services and missions as concept. Barnett[4][5] viewed cyberspace from three layers: capability, assets and events.

2) Relations between cyber entities are very complex. Cyber relation is the foundation of information exchange and the precondition for cyberspace operations. Jakobson and Musman et al.[3][6] divided cyber relations as intra dependencies between entities from the same layer and inter dependencies between entities from different layers.

Cyberspace models depict cyberspace and they need a practical method to carry out their depictions. As no studies focused on this area, our work is offering such a method to fill this gap.

There are two train of thought for construction. One is recording a snapshot of cyberspace and the other is collecting the necessary data to analyze and construct cyberspace models. We adopt the later solution as the former solution is perfect but no feasible. In real cyber environment, cyberspace is a network of network[7]. Form the horizontal view, cyberspace consists many network such as telecommunications networks, computer systems, and embedded processors and controllers[1]. From the hierarchical view, it is coupled by many functional layers.

Definition of Cyber events

In practical life, an event indicates a thing that happens somewhere at some time. We need to redefine this concept in our work. A cyber event is an action that happens at some time in cyberspace and an event can affect or concern many entities (such as assets, service i.e.). Usually, cyber event data can be mined from an Intrusion Detection System (IDS) or the Supervisory Control And Data Acquisition (SCADA). Previous researches of cyber events aimed at casual relation modeling which was useful for system security state estimation or prediction. Our work considers less about concrete

action (interrupt action or remedy action i.e.) or its effects. To construct cyberspace models, we concern more about how to map cyber event data to cyber entities and their relations.

Definition: A cyber event concerns some cyber entities and we formalize these entities as its attributes.

Hypothesis 1: entities a cyber event concerns may be countless, we only concern about asset entities, service entities and mission entities.

Then we get the formalization of a cyber event:

$$I = \{ID, ID_g, \langle A \rangle, s, \langle M \rangle, t\} \quad (1)$$

Where,

ID : a serial number of a cyber event. ID is an unique identification of the cyber event.

ID_g : a group number indicating the event group a cyber event subjects to. We divide cyber events into different groups and each group has a group number ID_g .

$\langle A \rangle$: a collection of asset entities that a cyber event concerns. Here, $A = \{a_1, a_2, a_3, ...\}$, a_i indicates an asset entities.

s : a service that a cyber event concerns. We assume only one service is concerned in one cyber event. Here, $s \in S = \{s_1, s_2, s_3, ...\}$. A service can be File Transfer Service, E-mail service or Geographic Information Service i.e..

$\langle M \rangle$: a collection of missions that a cyber event concerns. Here, $M = \{m_1, m_2, m_3, ...\}$.

t : the time that a cyber event happens.

The Method of Construction of Cyberspace Models

Cyberspace is a complex domain concerning various entities. Relations between entities is also very complex. By graph theory, we map an entity as a vertex and relation between entities as an edge. Thus, graph of cyberspace models can be expressed as:

$$G = \langle V_a, V_s, V_m, R_a, R_s, R_m, R_{a-s}, R_{s-m} \rangle \quad (2)$$

Where,

V_a : a collection of asset vertexes.

V_s : a collection of service vertexes.

V_m : a collection of mission vertexes.

R_a : relations among asset vertexes.

R_s : relations among service vertexes.

R_m : relations among mission vertexes.

R_{a-s} : relations between asset vertexes and service vertexes.

R_{s-m} : relations between service vertexes and mission vertexes.

Suppose that we can collect enough cyber events, we now need to map cyber events into cyberspace models. Construction process include entity-mapping and relation-mapping.

Entity-mapping

Attributes of a cyber event represent different entities(assets, a service and missions). We sort entities from different attributes into different classes. For example, a cyber event ID_1, its ID value is 1 and derives from group2. We assume ID_1 concerns three asset-entities: a_1 , a_2 and a_3 , one service-entity: s_1, and two mission-entity: m_1 and m_2 . It happens at $t = 2s$. Formalization of ID_1 is $ID_1 = \{1, 2, \langle a_1, a_2, a_3 \rangle, s_1, \langle m_1, m_2 \rangle, 2\}$. Sort entities from different attributes as table 1.

When processing another cyber event, add entities into the Entity Pool the same way. There is no need to add the same entity into the Entity Pool when it already exists. After processing all the events, an Entity Pool is built, entities from different attributes are aggregated into relevant layers.

Table 1 Classification of Entities

Cyber Layer	Cyber Event Attribute	Entity Pool
Asset layer	$\langle A \rangle$	$a_1, a_2, a_3, ..$
Service layer	s	s_1
Mission layer	$\langle M \rangle$	m_1, m_2

Mapping entities into vertexes of cyberspace graph models:

$$V_a = \{a_1, a_2, a_3, ...\} \quad (3)$$

$$V_s = \{s_1, s_2, s_3, ...\} \quad (4)$$

$$V_m = \{m_1, m_2, m_3, ...\} \quad (5)$$

Entity-mapping is illustrated in Fig. 1:

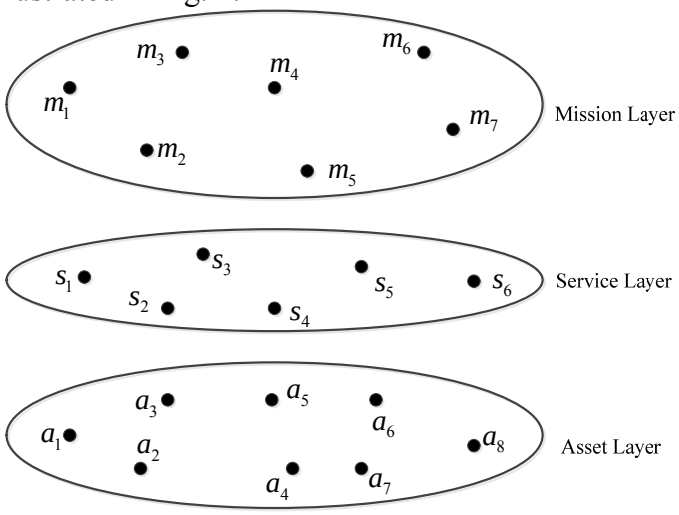

Fig 1 Entity-Mapping

Relation-mapping

Entities connect and interact with each other by relations. After mapping entities, we now consider how to construct relations between entities. We call relation of entities from the same layer homogeneous relation and relation of entities from different layers heterogeneous relation. We take the two relations separately.

1) Homogeneous Relation-mapping

Hypothesis 2: Homogeneous entities from the same cyber event are fully connected. Homogeneous entities from different cyber event but belong to the same event group are connected with a certain probability.

Take asset entities as an example. For cyber event $ID_1 = \{1, 2, \langle a_1, a_2, a_3 \rangle, s_1, \langle m_1, m_2 \rangle, 2\}$,asset entities (a_1 , a_2 and a_3) are fully connected. for cyber event $ID_2 = \{2, 2, \langle a_4, a_5, a_6, a_7 \rangle, s_2, \langle m_3, m_4, m_5 \rangle, 3\}$, entities (a_4 , a_5 , a_6 and a_7) are fully connected， illustrated as Fig. 2:

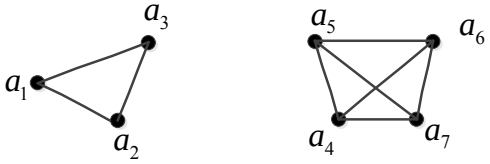

Fig 2 Relation-Mapping of Homogeneous Entities From One Cyber Event

As ID_1 and ID_2 have the same ID_g value, entities $\langle a_1, a_2, a_3 \rangle$ and $\langle a_4, a_5, a_6, a_7 \rangle$ are connected with a certain probability, illustrated as Fig. 3:

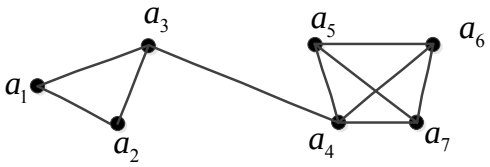

Fig 3 Relation-Mapping of Homogeneous Entities From The Same Cyber Event Group

Homogeneous entities form a sub graph. Take Fig. 3 as an example, an asset sub graph $G_a = \langle V_a, R_a \rangle$ can be described by matrix E_a in (6). Homogeneous entities of other layers will form similar sub graphs. In (6), if element $e_{a-ij} = 1$, asset a_i and asset a_j are connected.

$$E_a = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{6}$$

By the same process, we map relations of service entities and mission entities. Therefore, we can get the service sub graph $G_s = \langle V_s, R_s \rangle$ and the mission sub graph $G_m = \langle V_m, R_m \rangle$. Aggregating G_a, G_s and G_m together, homogeneous relation-mapping is illustrated as Fig. 4:

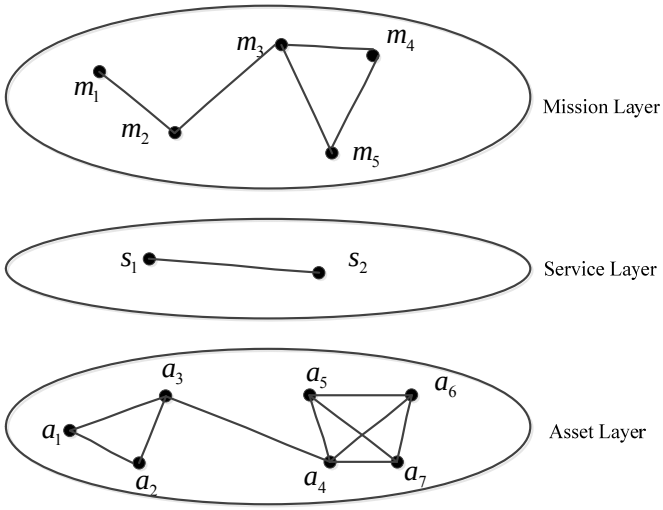

Fig 4 Homogeneous Relation-Mapping

2) Heterogeneous Relation-mapping

Hypothesis 3 : heterogeneous entities concerned in one cyber event are fully connected.

In cyberspace, asset entities support service entities and service entities further sustain mission entities. According to the H*ypothesis 3*, we map heterogeneous relations between heterogeneous entities. Take asset-service heterogeneous mapping as an example, the sub bipartite graph $G_{a-s} = \langle V_a, V_s, R_{a-s} \rangle$ can be described by matrix $E_{(a-s)}$ in (7) when there are two cyber events: ID_1 and ID_2. If element $e_{(a-s)ij} = 1$, asset a_j and service s_i are connected.

$$E_{(a-s)} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{7}$$

Service-mission sub bipartite graph $G_{s-m} = \langle V_s, V_m, R_{s-m} \rangle$ can be obtained in the same process. Combining G_{a-s} and G_{s-m}, heterogeneous relations between heterogeneous entities is illustrated in Fig. 5:

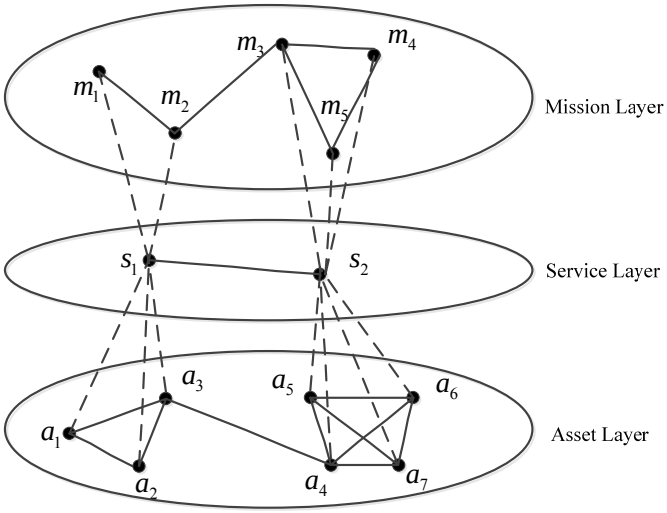

Fig 5 Heterogeneous relation-mapping

Conclusion and Future Work

We develop a framework to map cyber events into cyberspace models. Cyberspace models can be represented as a graph consisting various entities and their relations. How to picture such a graph is not a simple matter in that homogeneous entities and heterogeneous entities are connected by complex relations. This event based method proposes a novel way for practically build cyberspace models through entity-mapping and relation-mapping (include homogeneous relation-mapping and heterogeneous relation-mapping).

Building a real-time data collection system to extract relevant information (Event logs, IDS data or system alarms) is the next step of our work.

References

[1] The White House, 2011. "National Strategy for Trusted Identities in Cyberspace", April

[2] Army U S. Cyberspace Operations Concept Capability Plan 2016-2028[J]. US Army Capabilities Integration Center, 2010, 22.

[3] Jakobson G. Mission cyber security situation assessment using impact dependency graphs[C]//Information Fusion (FUSION), 2011 Proceedings of the 14th International Conference on. IEEE, 2011: 1-8.

[4] Barnett A, Smith S R, Whittington R P. Using Causal Models to Manage the Cyber Threat to C2 Agility: Working with the Benefit of Hindsight[R]. DEFENCE SCIENCE AND TECHNOLOGY LAB PORTON DOWN (UNITED KINGDOM), 2014.

[5] Barros Barreto M A, Costa P, Hieb M. 19th ICCRTS–C2 Agility: Lessons Learned from Research and Operations[J].

[6] Musman S, Temin A, Tanner M, et al. Evaluating the impact of cyber attacks on missions[C]//Proceedings of the 5th International Conference on Information Warfare and Security. 2010: 446-456.

[7] Halappanavar M, Choudhury S, Hogan E, et al. Towards a network-of-networks framework for cyber security[C]//Intelligence and Security Informatics (ISI), 2013 IEEE International Conference on. IEEE, 2013: 106-108.