An Event-Based Method of Construction of Cyberspace Models

Youjun Wang¹, a, Hongqi Zhang¹, Tianwei Che², b, Chuanfu Zhang¹, Yuntian Zhao¹ and Chao Yang¹

¹Zhengzhou Information Science and Technology Institute, Zhengzhou, Henan, 450000, China
²Beijing Jianyin Investment Technology Development Co., Ltd, Xicheng District, Beijing, 100055, China

adaxia1wang@163.com, bchetianwei@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 Cyberspace¹.⁰

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. Barnett⁴⁵ 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.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 network⁷. Form the horizontal view, cyberspace consists many network such as telecommunications networks, computer systems, and embedded processors and controllers¹¹. 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:

\[ I = \{ID, ID_g, \{A\}, s, \{M\}, t\} \]  

(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**.
- **\{A\]**: a collection of asset entities that a cyber event concerns. Here, **A = \{a_1, a_2, a_3, \ldots\}**, \( a_i \) indicates an asset entities.
- **s**: a service that a cyber event concerns. We assume only one service is concerned in one cyber event. Here, \( s \in S = \{s_1, s_2, s_3, \ldots\} \). A service can be File Transfer Service, E-mail service or Geographic Information Service i.e.
- **\{M\]**: a collection of missions that a cyber event concerns. Here, \( M = \{m_1, m_2, m_3, \ldots\} \).
- **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:

\[ G = \{V_a, V_s, V_m, R_a, R_s, R_m, R_{a-s}, R_{s-m}\} \]  

(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_i**, its **ID** value is 1 and derives from group2. We assume **ID_i** concerns three asset-entities: \( a_1, a_2 \) and \( a_3 \), one service-entity: \( s_i \), and two mission-entity: \( m_1 \) and \( m_2 \). It happens at \( t = 2s \). Formalization of **ID_i** is \( ID_1 = \{1, 2, \{a_1, a_2, a_3\}, s_i, \{m_1, m_2\}, 2\} \). 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

<table>
<thead>
<tr>
<th>Cyber Layer</th>
<th>Cyber Event Attribute</th>
<th>Entity Pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset layer</td>
<td>$\langle A \rangle$</td>
<td>$a_1, a_2, a_3, \ldots$</td>
</tr>
<tr>
<td>Service layer</td>
<td>$s$</td>
<td>$s_1$</td>
</tr>
<tr>
<td>Mission layer</td>
<td>$\langle M \rangle$</td>
<td>$m_1, m_2, \ldots$</td>
</tr>
</tbody>
</table>

Mapping entities into vertexes of cyberspace graph models:

$$V_a = \{a_1, a_2, a_3, \ldots\}$$  \hspace{1cm} (3)

$$V_s = \{s_1, s_2, s_3, \ldots\}$$  \hspace{1cm} (4)

$$V_m = \{m_1, m_2, m_3, \ldots\}$$  \hspace{1cm} (5)

Entity-mapping is illustrated in Fig. 1:

![Entity-Mapping](image1)

**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:

![Relation-Mapping of Homogeneous Entities From One Cyber Event](image2)

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 $G_a = \{V_a, R_a\}$ can be described by matrix $E_a$ in (6). Homogeneous entities of other layers will form similar sub graphs. In (6), if element $e_{a-i,j} = 1$, asset $a_i$ and asset $a_j$ are connected.

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

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

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 Hypothesis 3, we map heterogeneous relations between heterogeneous entities. Take asset-service heterogeneous mapping as an example, the sub bipartite graph $G_{a-s} = \{V_a, V_s, R_{a-s}\}$ 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.

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

Service-mission sub bipartite graph $G_{s-m} = \{V_s, V_m, R_{s-m}\}$ 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:
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