<http://www.ijecs.in/index.php/ijecs/article/view/2091/1935>

**[0. Black Hole Attack]**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Black Hole Attack은 **network layer에 대한 공격**이다.   * Source node가 이웃한 노드에 Route Request (RREQ)를 전송하면 모든 node가 승인된 방법으로 작동하지만 **attacker node는 metric의 값이 가장 작아지는 루트를 답한다**. * 공격자는 직접적인 convention을 이용하여 **그것이 Source에서 Destination으로의 가장 제한적인 path를 경유한다고 광고**한다.   + 이것은 directing table을 확인할 필요 없이 **그 node에 대한 새롭고 빠른 path에서의 접근성을 증가**시킨다.   **<Black Hole 공격의 특징>**   |  |  | | --- | --- | | 1 | **Source node에 잘못된 directing data를 전송** | | 2 | **Destination node로 가야 하는 bundle을 차단하거나 drop시킴** | |

**[1. Literature review by Tao and Bharat]**

|  |
| --- |
| Tao and Bharat은 sign이 어떻게 서로 다르게 준비되는지, 그리고 **이러한 상황에서 Neural learning이 collective attack의 발견에 어떻게 도움을 줄 수 있는지**를 보여 주었다. |

**[2. Existing techniques]**

|  |  |
| --- | --- |
| Reputation Based System | 모든 노드는 **이웃한 노드들에 대해 reputation value를 확인하여 점수를 매긴다.**   * 이 점수를 통해 **normal node/deadly node인지를 결정**한다. * **단점:** node의 근본적인 특성 때문에 각 node의 **reputation value를 계산하는 것이 매우 어렵다.** |
| CORE | Node는 **서로 다른 노드를 모니터링하여 bundle을 forwarding**해 나간다.   * Sender node는 다른 node에 의존하며, 그 다른 node가 공격자이면 전송 경로가 수정된다. |
| Buddy System | Social structure에 의존하는데, 이것은 **한 노드가 다른 하나의 노드에 어떻게 의존하는지를 암시**한다.   * **장점:** 각 node가 **bundle을 forwarding하는지의 여부**에 관계없이 적용할 수 있다. * **단점:** 2개의 노드 간의 연결을 측정하는 것이 **결과적으로 node의 본질에 영향**을 준다. |
| **(NEXT PAGE)** | |

**[2. Existing techniques]**

|  |  |
| --- | --- |
| **(NEXT PAGE)** | |
| ERS (Event-based reputation system) | **현재 activity가 발생하는지의 여부**에 따른 Event-based reputation system   * **다른 이웃한 node에 의한 인식에 의해 결정**된다. * 확실성에 대한 association은 ERS의 이슈 때문에 모든 노드에서 무시된다. |

**[3. Conclusion and future work]**

|  |
| --- |
| Blackhole node가 없는 network을 만들기 위하여, **Blackhole attack을 하는 Blackhole node를 감지하는 새로운 방법이 제안되어야** 한다. |