



(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。 Int. Cl.	(45) 공고일자	2007년08월10일
H04L 12/26 (2006.01)	(11) 등록번호	10-0707101
H04L 12/22 (2006.01)	(24) 등록일자	2007년04월06일

(21) 출원번호	10-2006-0067160	(65) 공개번호
(22) 출원일자	2006년07월19일	(43) 공개일자
심사청구일자	2006년07월19일	

(73) 특허권자 이화여자대학교 산학협력단
서울 서대문구 대현동 11-1 이화여자대학교내

(72) 발명자 김미희
서울 서대문구 현저동 극동아파트 113-903

도인실
인천 계양구 용종동 초정마을 쌍용아파트 308-601

채기준
서울 성북구 돈암동 609-1 한신아파트 109-1801

(74) 대리인 김석현

(56) 선행기술조사문헌
KR1020070000728 A

심사관 : 김병균

이 발명을 지원한 국가연구개발사업

과제고유번호	C1090-0502-0004
부처명	정보통신연구진흥원
연구사업명	대학정보통신연구센터(ITRC) 육성 지원사업
연구과제명	차세대 인증 및 데이터 접근제어 기술
주관기관	성균관대학교
연구기간	2004년 8월 1일 ~ 2008년 7월 31일

전체 청구항 수 : 총 5 항

(54) 센서 및 이동 네트워크에서 유사 엔트로피를 이용하여플러딩 공격을 탐지하는 방법

(57) 요약

센서 및 이동 네트워크에서 유사 엔트로피를 이용하여 플러딩 공격을 탐지하는 방법을 개시한다. 본 발명은 센서 및 이동 네트워크에서 발생하는 플러딩 공격에 대한 위협으로부터 공격 패킷에 대한 빠른 탐지를 위해 작은 처리 능력의 단말 특성 및 이동성을 고려해 유사 엔트로피를 이용하여 빠른 탐지를 가능하게 하는 방법에 관한 것이다. 이를 위해 본 발명은 데이

터의 포워딩 및 집결이 되는 노드 즉 센서 네트워크에서는 aggregator노드, 클러스터 헤더노드 및 싱크노드 이동 네트워크에서는 이동라우터, 베이스스테이션, 기지국에서 수신된 트래픽을 이용해 유사 엔트로피를 계산하여 공격의 여부를 감시하고 탐지하는 것을 특징으로 한다. 또한, 노드의 이동성이 가정되는 이동 네트워크(이동 센서 네트워크 포함)에서는 탐지 성능을 높이기 위해 자신의 구역 내의 노드에서부터 송신된 트래픽뿐만 아니라 이웃 구역에서 발생된 트래픽을 합쳐 유사 엔트로피를 계산함으로써 이동 노드에 의한 공격 여부를 감시하고 탐지하는 것을 특징으로 한다.

대표도

도 1

특허청구의 범위

청구항 1.

센서 네트워크 및 이동 네트워크에서 플러딩 공격을 탐지하기 위한 탐지 방법에 있어서,

메시지의 집결 또는 포워딩 역할을 하는 탐지 노드에서는 기본 탐지와 겹침탐지를 수행하며,

상기 기본 탐지는

(a1) 자신의 구역의 노드에서 송신한 메시지 N 개에 대한 유사 엔트로피를 계산하는 단계;

(a2) 상기 유사 엔트로피를 계산하는 단계 이후에, 새로운 $\delta(1 \leq \delta \leq N)$ 개의 메시지 수신 시 이전에 수신된 $(N-\delta)$ 개의 메시지와 함께 새로운 유사 엔트로피를 계산하는 단계; 및

(a3) 연속적으로 계산된 상기 두 유사 엔트로피 값의 차를 기준에 정해 놓은 소정의 임계치와 비교하여 그 차이가 큰 경우 플러딩 공격으로 인식하여 이를 탐지하는 단계;를 포함하며,

상기 겹침 탐지는

(b1) 주기적으로 이웃 탐지 노드와 메시지에 대한 n_i 값을 교환하는 단계;

(b2) 이웃 구역과 통합된 구역에 대한 유사 엔트로피를 계산하는 단계; 및

(b3) 현재 계산된 유사 엔트로피의 값과 직전에 계산된 유사 엔트로피의 값의 차이를 기준에 정해 놓은 소정의 임계치와 비교하여 그 차이가 큰 경우 플러딩 공격으로 인식하여 이를 탐지하는 단계;를 포함하는 것을 특징으로 하는 유사 엔트로피를 이용하여 플러딩을 탐지하는 방법.

청구항 2.

제 1항에 있어서, 상기 기본 탐지 및 겹침 탐지는

각기 (a3), (b3)단계 이후 공격 상황이 탐지되면, 상위 또는 이웃 탐지 노드에게 해당 사실을 공지하고 상기 플러딩 공격에 대응하는 소정의 공격차단 기능을 수행하는 공격차단 단계;를 각기 더 포함하는 것을 특징으로 하는 유사 엔트로피를 이용하여 플러딩을 탐지하는 방법.

청구항 3.

제 1항에 있어서, 상기 유사 엔트로피를 계산하는 단계는

식
$$AppE = \alpha \cdot \sum_{k=2}^{20} \frac{1}{k(k-1)} \sum_{j=0}^k \binom{k}{j} \frac{\beta!}{(\beta+j)!} \cdot (-2)^{j/2} \sum_{i=1}^M \frac{(n_i+j)!}{n_i!}$$
 ($\alpha=0.5M, \beta=N+M-1$) 를 이용하고, 매 유사 엔트로피의 계산 시 메시지에 대한 n_i 값만이 변수로 적용되며, 곱셈만으로 이루어진 것;을 특징으로 하는 유사 엔트로피를 이용하여 플러딩 공격을 탐지하는 방법.

청구항 4.

제 3항에 있어서, 상기 유사 엔트로피의 계산 시 메시지를 M의 그룹으로 나누는 기준은

센서 네트워크인 경우,

센서의 지역, 센싱 데이터의 값 자체, 또는 센서들의 노드 아이디 등을 M개의 그룹으로 나누어 해당 그룹에서 발생한 메시지의 수를 n_i 로 구하여 유사 엔트로피의 값을 계산하며,

이동 네트워크인 경우,

이동 단말의 IP나 전화번호 등을 M개의 그룹으로 나누어 해당 그룹에서 발생한 메시지를 n_i 로 구하여 유사 엔트로피의 값을 계산하는 것;을 특징으로 하는 유사 엔트로피를 이용하여 플러딩 공격을 탐지하는 방법.

청구항 5.

제 1항에 있어서, 상기 소정의 임계치는

정상 트래픽에 대한 유사 엔트로피 값의 평균과 표준 편차를 이용하여 결정되는 것;을 특징으로 하는 유사 엔트로피를 이용하여 플러딩 공격을 탐지하는 방법.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 센서 네트워크나 이동 네트워크에서 단말의 작은 처리 능력과 이동성을 고려하여 적은 계산량으로 적은 트래픽 샘플을 가지고도 높은 탐지율을 제공하는 유사 엔트로피를 이용한 플러딩 공격 탐지 방법에 관한 것이다.

본 발명에서 포함하고 있는 네트워크는 단말의 이동이 가정되며, 네트워크 자체의 이동을 제공하는 NEMO 네트워크, Mobile IP 네트워크, 이동 통신 네트워크 및 이동 센서 네트워크 등 모든 이동 네트워크를 포함한다.

최근 인터넷 보안의 가장 큰 문제점으로 대두되고 있는 분산 서비스거부 공격의 대부분과 일부 웜바이러스(Worm Virus)가 다수의 공격 에이전트를 통해 짧은 시간 내에 많은 트래픽을 발생시키는 플러딩 공격의 양상을 보임으로 이에 대한 다양한 탐지 및 대응방안이 모색되고 있다.

그러나 이러한 플러딩 공격은 인터넷만의 문제가 아니라 최근 많은 관심을 받고 있는 센서 네트워크나 이동 네트워크에도 더욱 커다란 더욱 커다란 문제가 될 수 있다.

특히 센서 네트워크에서 플러딩 공격은 단순히 센서 데이터의 손실이나 센서 노드의 에너지 고갈과 같은 단순한 피해뿐만 아니라, 인간의 안전과 건강과 같은 실세계에 대한 피해를 입힐 수 있다. 또한 이미 이동 전화에 대한 플러딩 공격은 'SMS Flooder'라는 이름의 공격툴이 출현하여 현실 세계에 가시화되고 있다. 이 공격은 Microsoft Outlook 소프트웨어에 침투하여 많은 문자 메시지를 한 희생자(victim)의 이동전화로 전송하도록 한다. 이동 네트워크에서 플러딩 공격은 통신 두절이라는 피해뿐만 아니라, 사용량 기반의 요금체계가 적용된 경우에는 높은 경제적 손실로 인한 피해를 줄 수 있는 문제점이 있다.

한편, 유선 네트워크에서의 플러딩 공격에 대한 탐지 방법은 통계적 방법, 데이터 마이닝 기법 등 다양한 방법이 연구되었지만, 센서 네트워크나 이동 네트워크의 단말의 작은 처리 능력이나 이동성을 고려한 탐지 기법에 대한 연구는 아주 미비하다.

종래의 기술로서는 센서 네트워크에서 플러딩 공격을 탐지하기 위해 한 지역에서 발생한 메시지의 빈도 수가 일정 수보다 많아지면 공격으로 탐지하는 간단한 방법, 휴리스틱(Heuristic)하게 통신채널의 질이 일정 수준 이하로 떨어지면 해당 지역을 잼밍(Jamming)지역으로 정하고 다른 트래픽들이 이 지역을 우회할 수 있도록 특수한 메시지를 생성하여 공지하는 방법 등이 있었다.

여기에서, 종래 유선 네트워크에서 공격을 탐지하는 데이터 마이닝 기법 중 대표적인 방법으로, 수학적 1에 의한 엔트로피 계산에 의한 방법이 있는데, 이는 엔트로피 계산에 사용되는 샘플 메시지의 수가 작으면 낮은 탐지 성능을 보이는 단점이 있고, 또한 처리 능력이 작은 노드에서는 log 계산이 부담이 될 수 있는 문제점이 있다.

수학적 1

$$Entropy = - \sum_{i=1}^M r_i \log_2 r_i$$

- N : 엔트로피를 계산할 때 사용되는 샘플 메시지 수
- M : 메시지의 그룹 수
- n_i : N개의 메시지 중 각 그룹에 해당하는 메시지의 개수
- r_i : N개의 메시지 중 각 그룹에 해당하는 메시지의 확률

발명이 이루고자 하는 기술적 과제

본 발명은 상술한 바와 같은 종래의 문제점을 극복하기 위하여 창안된 것으로, 센서 네트워크 및 이동 네트워크에서 다수의 공격 에이전트를 통해 짧은 시간 내에 많은 트래픽을 발생하는 플러딩 공격에 대해 가능한 빠르게 탐지하도록 하며, 단말의 특성을 고려하여 적은 계산량을 요구하고 적은 트래픽 샘플로도 높은 탐지율과 공격 노드의 이동성에 대해서도 대응할 수 있는 유사 엔트로피를 이용한 플러딩 공격 탐지 방법을 제공함에 목적이 있다.

발명의 구성

상기 기술한 바와 같은 과제를 이루기 위하여 본 발명의 특징에 따르면, 센서 및 이동 네트워크에서 유사 엔트로피를 이용하여 플러딩 공격을 탐지하는 방법은 센서 네트워크 및 이동 네트워크에서 플러딩 공격을 탐지하기 위한 탐지 방법에 있어서, 메시지의 집결 또는 포워딩 역할을 하는 탐지 노드에서는 기본 탐지와 겹침탐지를 수행하며,

상기 기본 탐지는

(a1) 자신의 구역의 노드에서 송신한 메시지 N개에 대한 유사 엔트로피를 계산하는 단계; (a2) 상기 유사 엔트로피를 계산하는 단계 이후에, 새로운 $\delta(1 \leq \delta \leq N)$ 개의 메시지 수신 시 이전에 수신된 $(N-\delta)$ 개의 메시지와 함께 새로운 유사 엔트로피를 계산하는 단계; 및 (a3) 연속적으로 계산된 상기 두 유사 엔트로피 값의 차를 기준에 정해 놓은 소정의 임계치와 비교하여 그 차이가 큰 경우 플러딩 공격으로 인식하여 이를 탐지하는 단계;를 포함하며,

상기 겹침 탐지는

(b1) 주기적으로 이웃 탐지 노드와 메시지에 대한 n_i 값을 교환하는 단계; (b2) 이웃 구역과 통합된 구역에 대한 유사 엔트로피를 계산하는 단계; 및 (b3) 현재 계산된 유사 엔트로피의 값과 직전에 계산된 유사 엔트로피의 값의 차이를 기존에 정해 놓은 소정의 임계치와 비교하여 그 차이가 큰 경우 플러딩 공격으로 인식하여 이를 탐지하는 단계;를 포함하는 것이 특징이다.

여기에서, 상기 기본 탐지 및 겹침 탐지는 각기 (a3), (b3)단계 이후 공격상황이 탐지되면, 상위 또는 이웃 탐지 노드에게 해당 사실을 공지하고 상기 플러딩 공격에 대응하는 소정의 공격차단 기능을 수행하는 공격차단 단계;를 각기 더 포함하는 것이 특징이다.

한편, 상기 유사 엔트로피를 계산하는 단계는

$$AppE = \alpha \cdot \sum_{k=2}^{20} \frac{1}{k(k-1)} \sum_{j=0}^k \binom{k}{j} \frac{\beta!}{(\beta+j)!} \cdot (-2)^{j/2} \sum_{i=1}^M \frac{(n_i+j)!}{n_i!}$$

식 ($\alpha=0.5M, \beta=N+M-1$) 를 이용하고, 매 유사 엔트로피의 계산 시 메시지에 대한 n_i 값만이 변수로 적용되며, 곱셈만으로 이루어진 것이 특징이다.

여기에서, 상기 유사 엔트로피의 계산 시 메시지를 M의 그룹으로 나누는 기준은 센서 네트워크인 경우, 센서의 지역, 센싱 데이터의 값 자체, 또는 센서들의 노드 아이디 등을 M개의 그룹으로 나누어 해당 그룹에서 발생한 메시지의 수를 n_i 로 구하여 유사 엔트로피의 값을 계산하며,

이동 네트워크인 경우, 이동 단말의 IP나 전화번호 등을 M개의 그룹으로 나누어 해당 그룹에서 발생한 메시지를 n_i 로 구하여 유사 엔트로피의 값을 계산하는 것이 특징이다.

또한, 상기 소정의 임계치는 정상 트래픽에 대한 유사 엔트로피 값의 평균과 표준 편차를 이용하여 결정되는 것이 특징이다.

아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다. 또한, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

이제 본 발명의 실시예에 따른 센서 및 이동 네트워크에서 유사 엔트로피를 이용한 플러딩 공격 탐지 방법에 대하여 도면을 참고로 하여 상세하게 설명하는데 후술하는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 발명 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

도 1은 본 발명에 따른 탐지 수행에 대한 수행도 이고, 도 2 내지 도 3은 본 발명의 기본이 되는 센서 네트워크와 이동 네트워크의 예시도 이며, 도 4는 본 발명에 따른 이동 노드에 의한 공격에 대비하여 겹침 탐지를 수행하는 영역에 대한 구성도 이다.

먼저, 본 발명을 간단히 설명하자면, 기본 탐지(Basic Detection)와 겹침 탐지(Overlapped Detection)로 구성된 것을 특징으로 하며, 센서나 이동 노드의 작은 처리 능력이나 적은 저장 공간의 특성, 노드의 이동성 및 네트워크의 적은 트래픽 발생 가능성을 고려하여 기존의 엔트로피 방식보다 더 적은 트래픽 샘플을 가지고 적은 계산량으로 높은 탐지율을 제공할 수 있는 유사 엔트로피를 이용하여 한 지역에서의 기본 탐지 및 이웃 지역을 통합한 겹침(overlap) 탐지 방법을 제공함으로써 본 발명의 방법은 센서 네트워크 및 이동 네트워크에서 플러딩 공격에 대한 높은 탐지가 가능하게 하는 것이 특징이다.

한편, 수신된 메시지에 기반하여 탐지를 수행하는 노드는 데이터의 포워딩 및 집결이 되는 노드, 즉 센서 네트워크에서는 Aggregator 노드, 클러스터 헤드 노드 및 싱크 노드 등이며, 이동 네트워크에서는 이동라우터, 베이스스테이션 및 기지국 등이 있으며, 이하 이들 노드를 탐지 노드라 칭한다.

상기 탐지 노드에서는 자신이 관리하는 영역에 있는 노드에서 발생한 메시지 N개에 해당 메시지를 M개의 그룹으로 분류하여 수학식 2를 적용하여 유사엔트로피를 구하게 된다.

수학식 2

$$AppE = \alpha \cdot \sum_{k=2}^{20} \frac{1}{k(k-1)} \sum_{j=0}^k \binom{k}{j} \frac{\beta!}{(\beta+j)!} \cdot (-2)^{j/2} \sum_{i=1}^M \frac{(n_i+j)!}{n_i!}, \alpha=0.5M, \beta=N+M-1$$

- N : 유사 엔트로피를 계산할 때 사용되는 메시지 수

- M : 메시지의 그룹 수

- n_i : N개의 메시지 중 각 그룹에 해당하는 메시지의 개수

여기에서, 상기 메시지를 M개의 그룹으로 분류하는 기준은 네트워크의 메시지 특성에 따라 다양한 기준이 사용될 수 있는데, 센서 네트워크인 경우 센서들을 지역적으로 M개로 그룹핑을 하여 각 그룹에서 발생한 트래픽을 n_i 로 구하여 유사 엔트로피를 계산할 수도 있으며, 센싱 데이터의 값 자체를 또는 센서들의 노드 아이디를 M개의 그룹으로 나누어 해당 그룹에서 발생한 메시지의 수를 n_i 로 구하여 유사 엔트로피를 계산할 수도 있다.

마찬가지로 이동 네트워크인 경우에도 이동 단말의 IP나 전화번호를 M개의 그룹으로 나누어 해당 그룹에서 발생한 메시지를 n_i 로 구하여 유사 엔트로피 값을 계산할 수 있다.

그 외에도 정상 트래픽의 분포가 특정 분포를 나타낼 수 있도록 하는 다양한 기준이 사용될 수 있다.

또한, 탐지 속도를 높이기 위해서 상기 탐지 노드는 δ슬라이딩 윈도우(Sliding Window)를 사용할 수 있다. 즉 상기 탐지 노드는 도 1에서 도시한 바와 같이 N개의 메시지와 상기 N개의 메시지에 대한 유사 엔트로피 값(AppE)을 새로이 도착한 $\delta(1 \leq \delta \leq N)$ 개의 새로운 메시지를 가지고 새로이 유사 엔트로피 값(AppE')을 계산하고 이를 이전의 유사 엔트로피 값(AppE)과 비교하여 그 차이가 기준에 정한 소정의 임계치(Threshold)보다 크면 플러딩 공격으로 판정한다.

이때, 상기 소정의 임계치는 정상 트래픽을 가지고 계산된 유사 엔트로피의 평균과 표준 편차를 이용하여 결정하게 된다.

한편, 플러딩 공격으로 판정이 된 경우에는 상위 또는 이웃 탐지 노드에게 해당 사실을 공지하여 이후 미리 적절한 공격 차단을 수행할 수 있게 하며, 이때 이 δ값은 탐지 노드의 성능에 따라 결정되는데 즉 δ이 작으면 빠른 탐지가 가능한 대신에 노드가 탐지를 위해 더욱 자주 유사 엔트로피를 계산해야 하므로 노드 성능에 따라 결정되어야 바람직하다.

상기 설명한 바와 같이 본 발명에서 탐지 노드는 이러한 기본 탐지를 수행하게 된다. 또한, 상기 기본 탐지를 수행하면서 주기적으로 이웃지역의 탐지 노드와 n_i 값을 서로 교환하여, 수신된 n_i 값을 자신의 n_i 값과 합쳐 상기 수학식2에 적용하여 겹침(Overlap) 탐지를 수행한다. 이는 이동 노드에 의한 공격시 다른 지역으로의 이동에 의해 한 지역에 발생하는 트래픽이 줄어들음으로써 탐지 성능이 낮아질 수 있는 경우를 대비하여 본 발명에서는 유사 엔트로피의 계산 지역을 이웃 지역까지 합친 영역에서 주기적으로 유사 엔트로피에 의한 탐지를 수행하는 것이 특징이다.

이상에서 설명한 것을 다시 말하자면, 본 발명은 기본 탐지와 겹침 탐지로 구성되며, 상기 두 탐지 모두 탐지 노드에서 상기 도 1과 같이 연속적인 유사 엔트로피 계산의 값들을 미리 정해 놓은 임계치와 비교해 그 차이가 크면 플러딩 공격으로 탐지하게 된다. 이때, 각 유사 엔트로피 계산에 사용되는 메시지는 기본 탐지인 경우 자신의 관리영역에서 발생한 메시지이며, 겹침 탐지인 경우에는 이웃 관리 영역의 탐지 노드로부터 주기적으로 받은 n_i 값(이웃 관리영역의 노드에서 발생한 메시지에 대한 값)들은 합쳐 계산하게 된다.

또한, 탐지 노드의 성능에 따라 유사 엔트로피 값 계산 시 새로이 포함되는 메시지의 수인 δ 를 결정할 수 있다.

한편, 도 2를 설명하면, 상기 도 2는 1개의 SINK 노드(10), 4개의 Aggregator 노드(20) 및 16개의 센서 노드(30)로 구성된 계층적인 센서 네트워크의 예로, 도 2(b)에서는 도시한 바와 같이 상기 계층적인 센서 네트워크의 트래픽 관리의 논리적 표현을 도시하였다.

이러한 네트워크에서는 SINK 노드(10)와 Aggregator 노드(20)가 탐지 노드가 될 수 있고, 각 노드는 자신이 바로 서비스하는 센서 노드(30)들로부터의 메시지를 가지고 기본 탐지를 수행하게 된다. 예를 들어 A1은 s21과 s22로부터 수신된 메시지를 가지고 기본 탐지를 수행하게 된다.

또한, 도 3에서는 유선 네트워크에 연결된 1개의 액세스 라우터와 3개의 이동 라우터, 5개의 로컬 노드 및 1개의 이동 노드로 구성된 NEMO 네트워크의 간단한 예를 도시한 것으로, 이 네트워크에서는 액세스 라우터나 이동 라우터가 탐지 노드가 될 수 있고, 자신이 직접 서비스하는 로컬 노드 또는 이동 노드로부터 메시지를 가지고 기본 탐지를 수행한다.

예를 들어 MR1은 노드 3, 5로부터 메시지를 가지고 기본 탐지를 수행하게 되며, 또한, 기지국(베이스스테이션)과 다수의 이동 단말기로 구성된 Mobile IP 네트워크 또는 이동 통신 네트워크에서는 기지국 또는 베이스스테이션이 탐지 노드가 될 수 있다.

한편, 상기에서 설명한 기본 탐지와 함께 노드의 이동성이 가정되는 이동 네트워크에서는 주변 지역과 통합된 지역에서 발생한 메시지에 대해 겹침 탐지를 수행하게 되는, 이를 도 4에서 설명하기로 한다.

상기 도 4는 다양한 네트워크 구성에 있어서, 겹침 탐지 지역을 표시한 도면으로, 도 4(a)는 계층적인 네트워크에서는 다수의 이웃 구역의 탐지 로드(40)로부터 메시지에 대한 n_i 값을 주기적으로 전달받아 상기 수학식1을 통해 겹침 탐지를 수행하고 이웃 구역의 정보를 통합하여 받을 수 있는 경우에는, n_i 값의 상호 교환을 생략할 수 있다. 도면에 미설명 도면부호 (1), (2)는 이웃 구역이지만, 다른 구역으로부터 n_i 값이 통합되어 전달되므로 직접적으로 n_i 값을 전달할 필요 없는 구역을 나타낸다.

또한, 도 4(b)와 도 4(c)는 각각 6각, 4각 그리드 형태의 네트워크로 이웃 구역에서부터 메시지의 n_i 값을 전달받아 주기적인 겹침 탐지를 수행한다.

이때, 탐지 수행 시, 공격의 상황이 탐지되면 상위 또는 이웃 탐지 노드에게 해당 사실을 공지하여 이후 미리 적절한 공격 차단을 수행할 수 있게 한다.

도 5 내지 도 6은 본 발명에 따른 기본 탐지와 겹침 탐지를 수행하는 방법을 설명하기 위한 순서도이다.

한편, 상기 도 1내지 도 4에서 설명한 것처럼 본 발명에 따른 센서 및 이동 네트워크에서 유사 엔트로피를 이용하여 플러딩 공격을 탐지하는 방법은 메시지의 집결 또는 포워딩 역할을 하는 탐지 노드에서는 기본 탐지와 겹침 탐지를 수행하게 된다.

다시 말해, 본 발명에서 탐지 노드는 기본 탐지를 수행하면서 주기적으로 이웃지역의 탐지 노드와 n_i 값을 서로 교환하여 수신된 n_i 값을 자신의 n_i 값과 합쳐 수학식2에 적용하는 겹침 탐지를 병행하여 수행한다.

따라서, 본 발명에서는 상기 기본 탐지와 겹침 탐지를 수행하여 유사 엔트로피의 계산 지역을 이웃 지역까지 합친 영역에서 주기적으로 유사 엔트로피에 의한 탐지를 수행할 수 있는 것이 특징이다.

상기 기본 탐지와 같은 경우, 도 5에서 도시한 순서도에 따르면, 자신의 구역의 노드에서 송신한 다수의 메시지, 즉 메시지 N개에 대한 유사 엔트로피를 계산한다(s101). 이때, 사이 유사 엔트로피의 계산은 상기 수학식2인

$$AppE = \alpha \cdot \sum_{k=2}^{20} \frac{1}{k(k-1)} \sum_{j=0}^k \binom{k}{j} \frac{\beta!}{(\beta+j)!} \cdot (-2)^{j/2} \sum_{i=1}^M \frac{(n_i+j)!}{n_i!}$$

$\alpha=0.5M$, $\beta=N+M-1$ 을 이용하고, 매 유사 엔트로피 계산 시 메시지에 대한 n_i 값만이 변수로 적용하게 된다.

또한, 상기 유사 엔트로피의 계산은 간단한 곱셈만으로 이루어진다는 점이 특징이다.

한편, 상기 메시지 N개에 대한 유사 엔트로피를 계산한(s101) 후, 새로운 $\delta(1 \leq \delta \leq N)$ 개의 메시지를 수신하게 되는데, 이때, 이전에 수신된 $(N-\delta)$ 개의 메시지와 함께 상기 수학식2에 적용하여 새로이 또 다른 유사 엔트로피를 계산하게 된다(s102).

이후, 연속적으로 계산된 최신의 두 유사 엔트로피 값의 차를 기준에 정해 놓은 소정의 임계치와 비교하게 되는데, 상기 소정의 임계치는 정상 트래픽에 대한 유사 엔트로피 값의 평균과 표준 편차를 이용하여 결정된다.

또한, 상기 소정의 임계치와 비교하여 그 차이가 큰 경우 플러딩 공격으로 인식하여 플러딩 공격을 탐지하게 된다(s103).

이때, 상기 소정의 임계치와 비교하여 그 차이가 큰 경우 즉, 플러딩 공격이 탐지 시일 때(s104), 상위 또는 이웃 탐지 노드에게 해당 사실을 공지하여 이후 미리 적절한 공격 차단을 수행하며(s105), 플러딩 공격탐지가 아니라고 판단되면, 다시(s102)단계로 이동하게 되므로 본 발명에 따른 플러딩 공격 탐지는 실시간으로 이루어지게 된다.

한편, 도 6에서는 상기 기본 탐지와 함께 겹침 탐지를 수행하는 방법을 설명하기 위한 순서도로, 상기 도 5에서 설명한 기본 탐지와 병행하여 겹침 탐지를 수행하기 때문에 상기에서 설명한 기본 탐지 방법은 생략하기로 하고 겹침 탐지에 대해서만 설명하기로 한다.

상기 겹침 탐지의 경우에는 먼저, 기본 탐지 외에 주기적으로 이웃 탐지 노드와 메시지에 대한 n_i 값을 교환하고(s201). 이후, 이웃 구역과 통합된 구역에 대한 유사 엔트로피를 계산하게 된다(s202).

여기에서, 상기 유사 엔트로피를 계산할 때, 상기 기본 탐지와 마찬가지로 상기 수학식2를 적용하여 계산하게 되며, 상기 계산된 유사 엔트로피 값과 직전에 동일한 방법으로 계산된 유사 엔트로피 값의 차이를 기준에 정해 놓은 소정의 임계치와 비교하여 그 차이가 큰 경우에는 플러딩 공격으로 인식하게 되고, 플러딩 공격을 탐지하게 된다(s203). 즉, 겹침 탐지를 위한 최신의 연속된 두 유사 엔트로피 값의 차를 임계치와 비교하게 되고, 그 차이가 큰 경우를 플러딩 공격으로 판단하게 된다.

이때, 상기 연속된 두 유사 엔트로피 값이란 현재 계산된 유사 엔트로피의 값과 직전에 계산된 유사 엔트로피를 말한다.

또한, 플러딩 공격 탐지시(s104), 상위 또는 이웃 탐지 노드에게 해당 사실을 공지하여 이후 미리 적절한 공격 차단을 수행한다.

여기에서, 상기 공격 차단을 수행하는 방법은 당업자에게 있어서 다양한 방법을 행해질 수 있기 때문에 본 발명의 명세서에서는 생략하도록 한다.

한편, 플러딩 공격이 아니라고 판단시(s104)에는 다시 상위로 돌아가 재차 주기적으로 이웃 탐지 노드와 메시지에 대한 n_i 값을 교환하고(s201), 이웃 구역과 통합된 구역에 대한 유사 엔트로피를 계산하며(s202), 두 유사 엔트로피 값의 차를 임계치와 비교하여 플러딩 공격 탐지 판별을 하기 때문에 플러딩 공격 탐지를 실시간으로 실행하게 된다.

이상에서 살펴본 본 발명은 기재된 구체적인 실시예에 대해서만 상세히 설명되었으나 본 발명의 기술사상범위 내에서 다양한 변형 및 수정이 가능함은 당업자에게 있어서 명백한 것이며, 이러한 변형 및 수정이 첨부된 특허청구범위에 속함은 당연한 것이다.

발명의 효과

상기한 바와 같이, 본 발명에 따른 유사 엔트로피를 이용한 플러딩 공격 탐지 방법은 센서나 이동 단말의 처리 능력을 감안하여 적은 계산량을 통해 적은 메시지 샘플 수에도 높은 탐지율과 빠른 탐지 성능을 제공하며, 이동 노드에 의한 공격에서도 높은 탐지율을 제공함으로써 이에 따른 경제적 손실을 최소화 할 수 있는 효과가 발생한다.

도면의 간단한 설명

도 1은 본 발명에 따른 탐지 수행에 대한 수행도이다.

도 2 내지 도 3은 본 발명의 기본이 되는 센서 네트워크와 이동 네트워크의 예시도이다.

도 4는 본 발명에 따른 이동 노드에 의한 공격에 대비하여 검침 탐지를 수행하는 영역에 대한 구성도이다.

도 5 내지 도 6은 본 발명에 따른 기본 탐지와 검침 탐지를 수행하는 방법을 설명하기 위한 순서도이다.

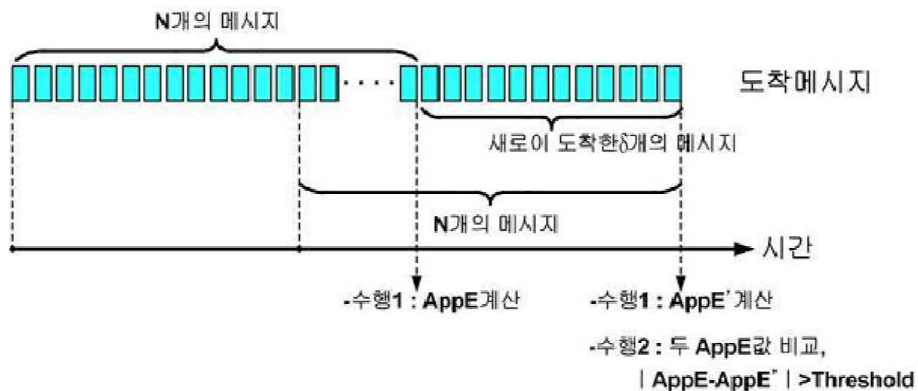
*** 도면의 주요부분에 대한 도면부호의 간단한 설명 ***

10 : SINK 노드 20 : Aggregator 노드

30 : Sensor 노드 40 : 탐지 노드

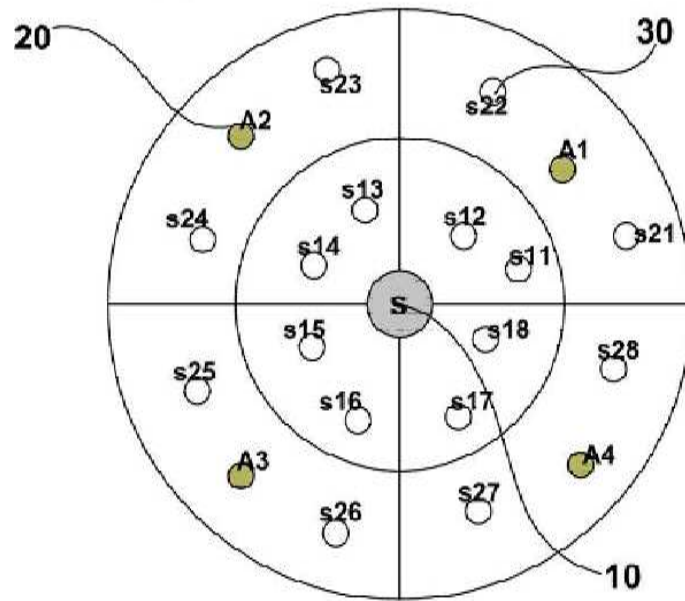
도면

도면1

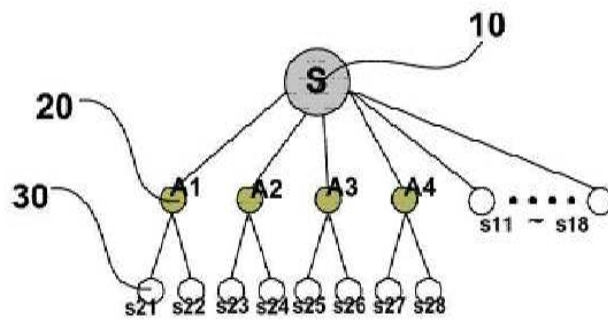


도면2

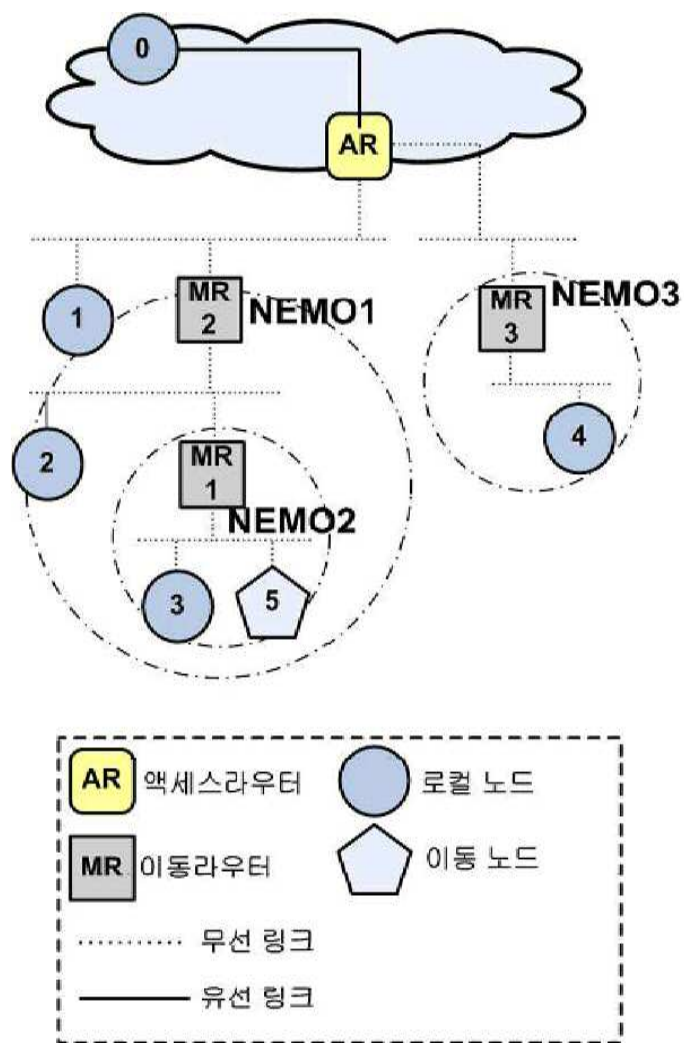
(a) 계층적인 센서 네트워크의 예



(b) 네트워크 (a)의 관리 측면도

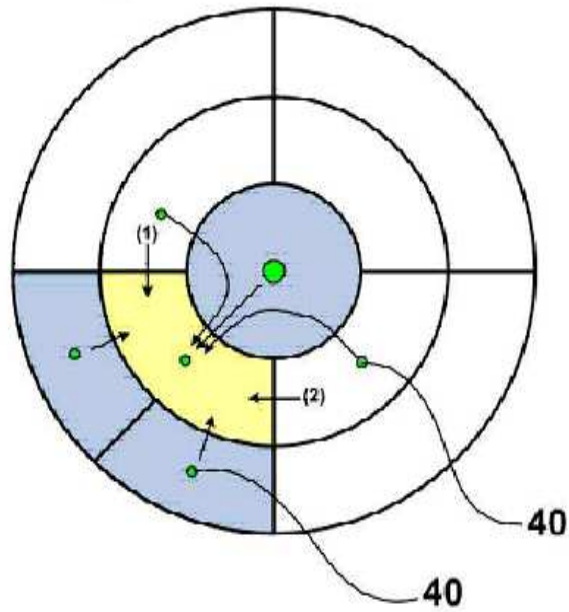


도면3

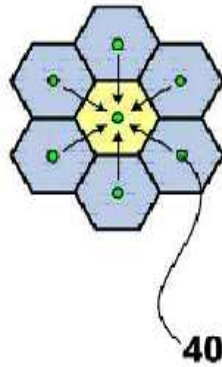


도면4

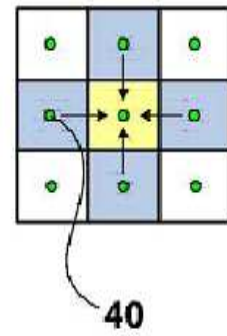
(a) 계층적인 네트워크



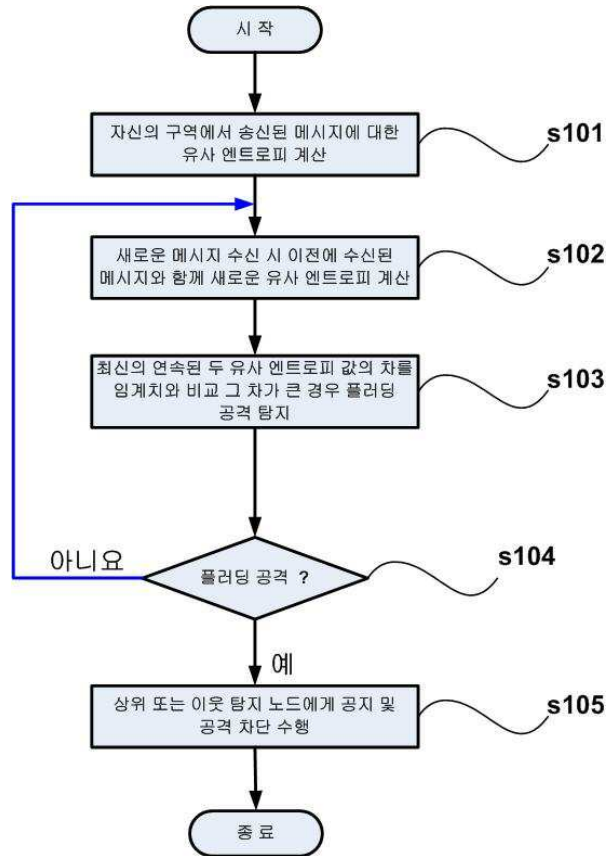
(b) 6각 그리드 형태(Hexagonal grid-based)의 네트워크



(c) 그리드 형태의 네트워크



도면5



도면6

