R. Roman, J. Lopez, and J. Zhou, "Aplicación de Sistemas de Detección de Intrusiones en Redes de Sensores", *Simposio sobre Computación Ubicua e Inteligencia Ambiental (UCAmI05)*, pp. 113-120, 2005.
NICS Lab. Publications: `https://www.nics.uma.es/publications`

Aplicación de Sistemas de Detección de Intrusiones en Redes de Sensores

Rodrigo Roman, Javier López
E.T.S. Ingenieria Informatica
Universidad de Málaga, 29071
Málaga, España
roman@lcc.uma.es, jlm@lcc.uma.es

Jianying Zhou
Institute for Infocomm Research
21 Heng Mui Keng Terrace
Singapore 119613
jyzhou@i2r.a-star.edu.sg

Resumen

Los sistemas de detección de intrusiones (IDS) son una herramienta imprescindible de seguridad a la hora de proteger una red. Recientemente se han investigado y desarrollado arquitecturas de IDS para redes inalámbricas, en concreto para redes "Ad Hoc". No obstante, no existe un trabajo previo que desarrolle una arquitectura de IDS para una red de sensores. En este artículo, analizamos porque los sistemas IDS de redes "Ad Hoc" no pueden aplicarse a redes de sensores, e introducimos una arquitectura de IDS para redes de sensores que incorpora una nueva técnica para vigilar las comunicaciones de la red en ciertos escenarios.

1. Introduction

La seguridad es uno de los aspectos más importantes en el diseño de cualquier arquitectura de red. Las redes deben protegerse ante cualquier ataque, detectarlo, y reaccionar ante él si esto es posible. La detección de ataques se suele llevar a cabo utilizando los denominados sistemas de detección de intrusiones (IDS).

Una intrusión puede definirse como el conjunto de acciones que pueden conducir a un acceso o alteración no autorizado del sistema. La tarea de un sistema IDS es la de verificar las redes y los sistemas pertenecientes a la red, detectando posibles intrusiones, y alertar a los usuarios si existe algún problema [1].

Ha sido recientemente cuando los sistemas IDS han sido aplicados a redes inalámbricas, o más concretamente a redes "Ad Hoc". Toda red inalámbrica es mucho más vulnerable ante cualquier tipo de ataque, puesto que no existe un único punto de entrada en la red, cualquier información puede ser interceptada por un sistema que se encuentre dentro del rango de la red inalámbrica, y cualquiera de los nodos puede ser reprogramado para actuar como adversario.

Sin embargo, no existe un trabajo previo que aplique un sistema IDS a una red de sensores [2]. El propósito de este artículo es por lo tanto analizar porque los sistemas IDS existentes en redes "Ad Hoc" no pueden aplicarse a redes de sensores, y desarrollar una arquitectura de IDS para este tipo de redes. Esta arquitectura utiliza una nueva técnica para vigilar las comunicaciones de la red, denominada "Watchdogs" espontáneos.

El resto del artículo se organiza de la siguiente forma: La sección 2 muestra tanto las diferencias entre las redes de sensores y "Ad Hoc" como el porque no pueden aplicarse las soluciones IDS de redes "Ad Hoc" a redes de sensores. La sección 3 presenta la arquitectura de IDS para redes de sensores, junto a la técnica de los "Watchdogs" espontáneos, y la sección 4 concluye el artículo.

2. IDS en Redes Inalámbricas

2.1. Redes de Sensores y Redes "Ad Hoc"

Una red inalámbrica esta compuesta por una colección de nodos capaces de establecer

un canal de comunicación inalámbrico con los demás miembros de la red, sin contar en la mayoría de los casos con una infraestructura previa.

Debido a la naturaleza inalámbrica de las comunicaciones, no existe un punto único de acceso a este tipo de redes. Cualquiera que se encuentre dentro del rango de transmisión de un nodo puede enviar o recibir información. Además, todos los nodos deberían ser capaces de autoconfigurarse para poder crear la infraestructura necesaria para ciertas operaciones, como el enrutado. Finalmente, la mayoría de las operaciones de la red se deben llevar a cabo de forma distribuida.

Tanto las redes de sensores como las redes "Ad Hoc" pueden clasificarse como redes inalámbricas. No obstante, existen ciertas diferencias entre ambas.

- En una red "Ad Hoc", cada nodo suele estar manejado por un usuario humano. Por otro lado, los nodos de una red de sensores actúan de forma independiente, enviando las lecturas de sus sensores a un usuario humano situado en un sistema denominado estación base.

- Los nodos pertenecientes a redes "Ad Hoc" son mucho mas potentes y de mayor capacidad que los nodos pertenecientes a las redes de sensores[1].

- El objetivo de una red de sensores es muy específico: medir la información física (temperatura, sonido) del entorno circundante. Esto implica que tanto sus componentes como los protocolos empleados suelen ser muy especializados.

- En una red de sensores existe una mayor densidad de nodos, pero al mismo tiempo hay una mayor posibilidad de que un nodo desaparezca de la red por diversas causas (problemas de batería, baja seguridad física,...)

[1] Un sensor suele tener un microprocesador de 8Mhz, con una memoria RAM de 128Kb y una capacidad de almacenamiento masivo de 512Kb.

2.2. Estado del Arte y Análisis

Dado que las redes inalámbricas son muy vulnerables ante cualquier tipo de ataque, sea éste externo a la red o procedente de un nodo interno, es necesario proporcionar mecanismos de seguridad eficientes para prevenir, detectar y reaccionar ante cualquier intrusión. Los sistemas IDS son los encargados de realizar las tareas de detección.

Debido a las características específicas de las redes inalámbricas, se hace necesario utilizar una arquitectura descentralizada en los sistemas IDS, en la que un grupo de nodos recogería la información producida por la red y la analizaría en busca de posibles intrusos utilizando un sistema software denominado agente [2]. Además, esos nodos deberían ser capaces de comenzar un proceso de colaboración para contrastar sus informaciones locales con los demás agentes y ser más eficientes.

Esta arquitectura descentralizada es la que se utiliza actualmente en las redes "Ad Hoc", donde cada uno de los nodos existentes en la red participa dentro de las tareas de búsqueda [3, 4]. La colaboración entre estos nodos puede ser estática, intercambiando únicamente información de auditoría, o dinámica, en la que agentes software migran de un nodo a otro para analizar la información de una forma más profunda [5, 6].

Sin embargo, las arquitecturas de IDS utilizadas en redes "Ad Hoc " no pueden emplearse tal cual en redes de sensores. La densidad de las redes de sensores es alta, y sus nodos están más restringidos en cuanto a recursos. Como resultado, no es posible ni óptimo que todos los nodos contengan un agente que analice tanto la información interna como externa a él. Además, las alertas deberían enviarse a la estación base puesto que ningún usuario humano controla directamente los nodos, y los protocolos empleados en la detección de intrusiones deberían estar especializados para el funcionamiento de la red de sensores.

Existen soluciones parciales que permiten a un nodo de una red de sensores comprobar la

[2] Un agente IDS puede ser inteligente o no, dependiendo de su capacidad de aprender y reaccionar ante los estímulos.

seguridad de la red y que podrían formar parte de un sistema IDS si éste existiese, sea comprobando si un grupo de nodos esta vivo [7], Analizando las fluctuaciones en las medidas [8], comprobando la integridad de la memoria de instrucciones [9], o vigilando las comunicaciones de los demás nodos [10].

3. Arquitectura de IDS para Redes de Sensores

Debido a las limitaciones impuestas por la infraestructura de una red de sensores, como los bajos recursos computacionales y la limitación de batería de sus nodos, es necesario planear de forma cuidadosa como distribuir los agentes dentro de la red de sensores, que tareas deben realizar, y que información pueden contener. Nuestra arquitectura divide a los agentes en dos partes: agentes locales y agentes globales.

- *Agentes Locales*: Controlan la información local al nodo, es decir, tanto los paquetes recibidos y enviados por él como la información manejada internamente.
- *Agentes Globales*: Controlan la información externa al nodo, es decir, vigilan las comunicaciones de sus vecinos y actúan como watchdogs [10].

Ambos agentes, locales y globales, deben existir dentro de cada uno de los nodos de la red, integrados con el sistema operativo para optimizar el consumo de energía y tiempo de ejecución. No obstante, solo una parte de los nodos tendrá activo a su agente global en un instante determinado del tiempo. De esta forma, podremos cubrir el intercambio de mensajes de la red sin malgastar los recursos de sus nodos.

La información que los agentes deben almacenar, se divide en información de auditoría e información sobre el entorno. La información de auditoría guarda las alertas que el nodo ha ido descubriendo. Al estar compartida por los agentes globales y locales, es posible que ambos pueden intercambiar información. Además, pueden utilizarse técnicas de otros sistemas IDS "Ad Hoc" [3, 5] para que agentes existentes en distintos nodos puedan intercambiar información.

La información sobre el entorno consiste en la lista de vecinos de cada uno de los nodos existentes en el vecindario del agente. Esta lista puede existir "a priori", o generarse después de la creación de la red (como en el intercambio de claves en LEAP [11]). Toda información (tanto de auditoría como de entorno) debe optimizarse para ocupar la menor memoria posible (en el caso de la lista de vecinos, puede utilizarse un filtro de Bloom [12] para reducir el tamaño de la lista en un 75 %).

Una vez que un agente descubre una posible brecha en la seguridad de la red, debe crear y enviar una alerta al usuario, y la única manera de acceder a él es a través de la estación base. Por lo tanto, todas las alertas deberían enviarse hacia ésta. El mecanismo para enviar las alertas depende de la infraestructura de la red de sensores, pero debe asegurar que todas las alertas alcancen su destino de forma segura (utilizando mecanismos como, por ejemplo, μTesla [13]).

3.1. Agentes Locales

La tarea de los agentes locales es la de descubrir cualquier tipo de amenaza que pueda afectar el comportamiento normal de un nodo, analizando únicamente las fuentes locales de información. Estas son el estado actual del nodo, los paquetes recibidos y enviados por el nodo, las medidas realizadas en el entorno, y la información disponible acerca de sus vecinos.

¿Que clase de amenazas pueden ser detectadas por el agente local?. Primero, los ataques cometidos contra la integridad física o lógica de los nodos puede ser detectada si los nodos son capaces de comprobar si están siendo manipulados o no. La integridad de las medidas de un nodo puede ser comprobada utilizando técnicas de detección de anomalías. Finalmente, el agente local puede manejar otros aspectos relacionados con los nodos vecinos, la duplicación o repetición de mensajes, y la disponibilidad de la red.

Cualquier nodo perteneciente a una red de sensores puede ser accedido físicamente, por lo

que sería relativamente sencillo atacar tanto a la integridad física como a la integridad lógica del nodo. Respecto a la integridad lógica, un adversario debe incluir su propio código dentro de un nodo para poder manejarlo como le convenga. En la mayoría de los casos los nodos son capaces de detectar cuando son reprogramados, y deben enviar una alarma antes de permitir la ejecución de código ajeno a su programación original.

Respecto a la integridad lógica, un nodo puede ser destruido utilizando medios mecánicos (p. ej. machacándolo) o mediante métodos más específicos (p. ej. sumergiéndolo en agua). En cualquier caso, si un nodo es capaz de detectar un fallo hardware, debería enviar una alarma inmediatamente si es capaz de hacerlo.

Las medidas realizadas por los nodos del medio ambiente circundante son también vulnerables. De todas formas, todos esas lecturas provienen del mundo real, y o están limitadas o siguen una serie de patrones. Por ejemplo, la temperatura de una oficina no puede subir varios grados en unos pocos segundos - a menos que alguien este tratando de modificar las medidas o exista un incendio. O un nodo estático no puede moverse - al menos que alguien esté tratando de llevárselo. Por lo tanto, se pueden utilizar técnicas de detección de anomalías para controlar las medidas realizadas por el nodo.

El agente local también controla los paquetes que están directamente dirigidos hacia el nodo. Dado que el formato y el significado de los paquetes depende de los protocolos utilizados por la red, los agentes locales deben estar preparados para analizar las situaciones anormales (p. ej. repetición de los mensajes de control) que ocurran en ellos. Esta arquitectura de IDS trata de ser lo más genérica posible, por lo que estos sistemas de análisis no se encuentran desarrollados en este artículo.

No obstante, existen aspectos que son independientes de los protocolos utilizados por la red, y que pueden desarrollarse aquí: la incorporación de un nuevo nodo a la red, y la ocupación del canal de comunicaciones. En ciertos escenarios donde pocos nodos son incluidos dentro de la red una vez que ésta haya sido distribuida en su entorno, es posible lanzar una alarma por cada nuevo nodo que entre en la red, utilizando para ello la lista de vecinos que cada nodo contiene. Respecto a la ocupación del canal, si un nodo trata de enviar un paquete varias veces sin conseguirlo, puede utilizar técnicas de análisis que comprueben si esta situación es anormal.

3.2. Agentes Globales

Como se ha expuesto anteriormente, los agentes globales están encargados de analizar los paquetes que sus vecinos inmediatos envían o reciben, actuando asimismo como "Watchdogs" [10]. Esto les permite comprobar, entre otras cosas, si un nodo ha modificado o eliminado un paquete mientras éste estaba siendo encaminado hacia su destino.

Estos análisis son, sin embargo, una operación costosa en términos de energía y tiempo de cálculo, ya que todos los paquetes pertenecientes a la vecindad del agente global deben ser escuchados y procesados. Idealmente, solo un subgrupo de los nodos que cubriera toda el área de la red de sensores debería activar a sus agentes globales al mismo tiempo.

La forma en la que los agentes globales se configuran para activarse o desactivarse depende de la infraestructura de la red de sensores. Existen dos infraestructuras básicas que especifican tanto la forma en la que los nodos encaminan la información hacia su destino como la forma en la que los nodos están agrupados: Jerárquica, y Plana.

En la infraestructura *jerárquica*, los sensores se agrupan en grupos denominados "clusters", donde uno de sus miembros ("cluster head") se encarga de recibir las medidas de su grupo y de reenviarlas a la estación base cooperando con otros "cluster heads". En la infraestructura *plana*, los nodos no están agrupados, y todos los miembros de la red ayudan en el encaminamiento de la información hacia su destino.

En las infraestructuras jerárquicas, los agentes globales están activados en cada uno de los "cluster heads", ya que en la mayoría de los casos la combinación de todos los "cluster heads" permite cubrir todo el intercambio de información de la red. Esta configuración permite

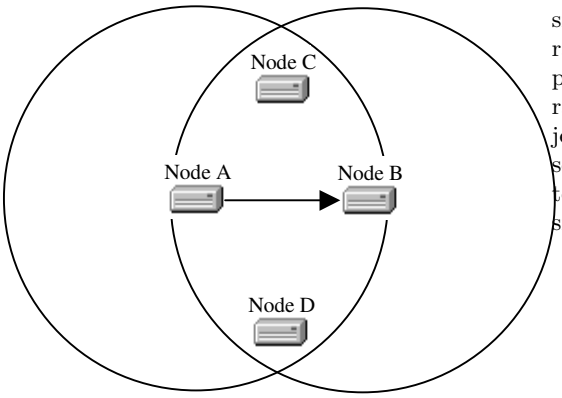

Figura 1: Posibles "Watchdogs" espontáneos

preservar la energía del sistema, puesto que los "cluster heads" o tienen una reserva mayor de energía que los demás nodos o se rotan periódicamente [14, 15].

La activación de los agentes globales es más difícil de manejar en las infraestructuras planas, ya que no es posible, a priori, saber que conjunto de nodos es capaz de cubrir todos los mensajes enviados en la red. Una posible solución sería utilizar técnicas de agrupamiento únicamente para el sistema IDS, donde periódicamente se eligieran "cluster heads" con el único propósito de activar sus agentes globales.

Esta solución añade tanto un nuevo punto de ataque como complejidad a la red, debido a la creación y el mantenimiento de grupos que buscan alcanzar una cobertura máxima, y a los mensajes de negociación necesarios para crear los grupos. No obstante, existe una solución distribuida alternativa que puede ser aplicada a infraestructuras planas sin tener que organizarlas en grupos, denominada *"Watchdogs" espontáneos*.

3.3. "Watchdogs" Espontáneos

Nuestra técnica de los "Watchdogs" espontáneos se basa en la siguiente premisa: por cada uno de los paquetes que circulan por la red, existe un grupo de nodos capaces de recibir tanto ese paquete como su reenvío a cargo del siguiente nodo, como puede verse en la figura 1. Por lo tanto, todos esos nodos tienen la posibilidad de activar sus agentes globales para analizar ambos paquetes. El principal objetivo de nuestra técnica es la de activar un solo agente global por cada uno de los paquetes enviados en la red, y el proceso es como sigue:

- Cada uno de los nodos que se encuentre activo recibirá todos los paquetes enviados dentro de su vecindario, debido a la naturaleza de las comunicaciones inalámbricas.
- El nodo comprobará si el paquete va dirigido a él. Si éste no es el caso, el paquete no será descartado inmediatamente, sino que el nodo verificará si tanto el origen como el destino del paquete están en su vecindario.
- Si lo anterior es cierto, el nodo puede ser un "watchdog" espontáneo. Seguidamente, comprobará cuantos nodos pueden encontrarse en su misma situación. No habrá intercambio de mensajes en este proceso, por lo que el tráfico de la red no se incrementará.
- Si el número de nodos que cumplen los requisitos son n, un nodo se seleccionará a sí mismo como "watchdog" espontáneo con una probabilidad de $\frac{1}{n}$. Este proceso es semejante al siguiente juego: n personas con un dado de m caras cada una, siendo $n = m$, intentando obtener un 1 en su tirada para activar a su agente global.

Dado que todos los nodos almacenan una lista con los vecinos de cada uno de los nodos de su vecindario, es posible calcular cuantos nodos pueden activar sus agentes globales interseccionando el conjunto de vecinos del origen del paquete con el conjunto de vecinos del destino del paquete. En la figura 1, por ejemplo, el nodo A quiere enviar un paquete al nodo B, mientras C y D se encuentran en el vecindario. Tanto C como D interseccionarán el conjunto de vecinos de A ($\{B, C, D\}$) y B ($\{A, C, D\}$), y el resultado será $\{C, D\}$, es

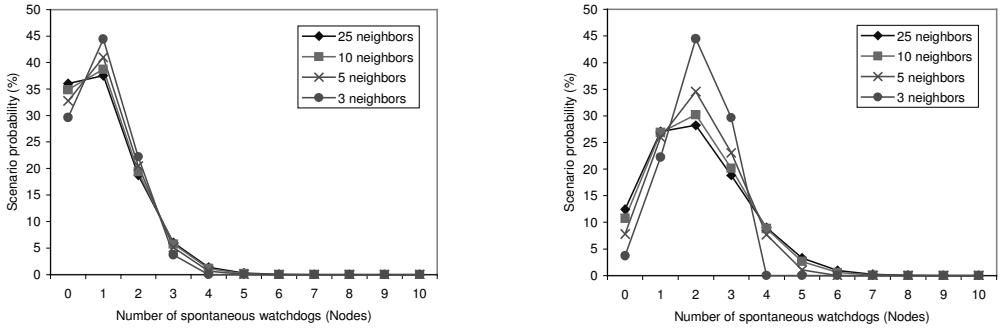

Figura 2: Número de "Watchdogs" espontáneos, con (a) probabilidad normal, (b) doble probabilidad

decir, dos vecinos. Por lo tanto, ambos nodos tienen una probabilidad de $\frac{1}{2}$ de activar sus agentes globales.

Pudiera parecer que esta técnica incrementa el consumo de energía de los nodos hasta niveles prohibitivos, puesto que todos los nodos deben recibir y analizar los paquetes enviados por sus vecinos para decidir si deben ser "Watchdogs" espontáneos. No obstante, esto ocurre así por defecto en las redes de sensores, ya que los nodos no son capaces de saber si un paquete está dirigido a ellos sin antes recibir todo el paquete y comprobar la dirección del destinatario [16]. La única carga impuesta por nuestra técnica a un nodo consiste en calcular el número de vecinos que pueden activar su agente global, y comprobar si él debe serlo.

Sin embargo, nuestra técnica no asegura que únicamente un nodo activará su agente global por cada uno de los paquetes existentes en la red. La explicación de este problema yace en la independencia del comportamiento de los nodos. Dado que un nodo no comunica su decisión a los demás, más de dos nodos (o incluso ninguno) pueden activar sus agentes globales.

La probabilidad de que α nodos activen sus agentes globales al mismo tiempo esta dada por la siguiente ecuación:

$$f(\alpha, n, m) = \frac{PR_n^{n-\alpha,\alpha} \cdot (m-1)^{n-\alpha}}{VR_{m,n}} \qquad (1)$$

donde $PR_n^{n-\alpha,\alpha}$ es la fórmula de la permutación con elementos repetidos, $VR_{m,n}$ es la fórmula de las variaciones con repetición, n es el número de nodos que podrían activar su agente global (el número de nodos que "van a tirar un dado"), y m es el número de nodos que van a influenciar en la probabilidad de activar los agentes globales, normalmente igual a n (el número de "caras en cada dado").

La figura 2a se dibuja utilizando (1) donde $n = m = \{3, 5, 10, 25\}$ y $\alpha = [0.,10]$. Como ejemplo, si dos nodos tienen $n = 3$ vecinos comunes, la probabilidad de tener 0, 1, 2, o 3 de ellos como "Watchdogs" espontáneos es 0.296, 0.444, 0.222 y 0.038, respectivamente.

Como puede observarse en la figura 2a, la probabilidad de que un paquete quede sin supervisar se encuentra entre 0.29 y 0.36. Por lo tanto, en nuestra técnica, uno de cada tres paquetes no será analizado. Además, la mayoría de los paquetes serán analizados por uno o dos nodos independientemente de la densidad del vecindario. Por lo tanto, el consumo de energía será menor en redes con una alta densidad.

Todos estos resultados se basan en la siguiente suposición: todos los nodos tienen la misma probabilidad de activar su agente global. Es por lo tanto posible modificar el comportamiento de los nodos incrementando esa probabilidad, y por lo tanto disminuyendo el número de caras del "dado" (m en (1)). Los resultados de un experimento donde cada nodo dobla su probabilidad de convertirse en un "Watchdog" espontáneo ($m = \frac{n}{2}$) se muestran en la figura 2b. La probabilidad de que un paquete quede sin supervisar se encuentra sola-

mente entre 0.03 y 0.12, pero el número de nodos que analizan el mismo paquete se incrementa en el orden de uno.

Por lo tanto, es posible disminuir el número de paquetes que no están supervisados incrementando la probabilidad de que un nodo se elija a sí mismo como "Watchdog" espontáneo, a costa de incrementar el número de agentes globales activados por paquete. Mantener el equilibrio entre la seguridad y la utilización de energía es una decisión que los diseñadores de la red de sensores deben tener en cuenta.

4. Conclusión

En este artículo, se han estudiado las soluciones existentes de IDS para redes inalámbricas, analizando las razones por las que un sistema de IDS para redes "Ad Hoc" no puede aplicarse a una red de sensores. También se ha propuesto una arquitectura de IDS para redes de sensores estáticas, y se ha introducido una nueva técnica, los "Watchdogs" espontáneos, en la que los nodos de la red son capaces de elegir de forma independiente si desean monitorizar las comunicaciones de la red.

Como trabajo futuro, esta arquitectura será simulada encima de una infraestructura de red de sensores específica, para así poder analizar los patrones de consumo de energía. Existen otros factores que deben ser investigados más a fondo, como la actualización de la lista de vecinos en el caso de que los nodos empiecen a fallar, o el cálculo del número de nodos que pueden activar sus agentes globales cuando la lista anterior no existe. El área de la detección de intrusiones en redes de sensores es un área abierta, llena de problemas interesantes como el desarrollo de un sistema IDS que pueda manejar nodos móviles.

Referencias

[1] R. Bace. *Intrusion Detection*. MacMillan Technical Publishing, 2000.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, y E. Cayirci. *Wireless Sensor Networks: A Survey*. Computer Networks, 38(4), Marzo 2002.

[3] Y. Zhang, W. Lee. *Intrusion Detection Techniques for Mobile Wireless Networks*. ACM/Kluwer Wireless Networks Journal, 9(5):545-556, Septiembre 2003.

[4] J. Kong, H. Luo, K. Xu, D. L. Gu, M. Gerla, S. Lu. *Adaptive Security for Multi-Layer Ad-Hoc Networks*. Special Issue of Wireless Communications and Mobile Computing, 2002.

[5] P. Albers, O. Camp, J. Percher, B. Jouga, L. Me, R. Puttini. *Security in Ad Hoc Networks: A General Intrusion Detection Architecture Enhancing Trust Based Approaches*. 1st International Workshop on Wireless Information Systems (WIS'02), Abril 2002.

[6] C. Karlof, D. Wagner. *Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures*. 1st IEEE International Workshop on Sensor Network Protocols and Applications, Mayo 2003.

[7] C. Hsin, M. Liu. *A Distributed Monitoring Mechanism for Wireless Sensor Networks*. 2002 ACM Workshop on Wireless Security (WiSe'02), Septiembre 2002.

[8] S. S. Doumit, D. P. Agrawal. *Self-Organized Criticaly & Stochastic Learning Based Intrusion Detection System for Wireless Sensor Networks*. Military Communications Conference '03 (MILCOM 2003), Octubre 2003.

[9] A. Seshandri, A. Perrig, L. Van Doorn, P. Khosla. *SWATT: SoftWare-based ATTestation for Embedded Devices*. 2004 IEEE Symposium on Security and Privacy, Mayo 2004.

[10] S. Marti, T. Giuli, K. Lai, M. Baker. *Mitigating Routing Misbehavior in Mobile Ad Hoc Networks*. ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'00), Agosto 2000.

[11] S. Zhu, S. Setia, S. Jajodia. *LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks.* 10th ACM Conference on Computer and Communications Security (CCS '03), Washington D.C., Octubre 2003.

[12] B. Bloom. *Space/time Trade-offs in Hash Coding with Allowable Errors.* Communications of the ACM, 13 (7). 422-426.

[13] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar. *SPINS: Security Protocols for Sensor Networks.* Proceedings of 7th Annual International Conference on Mobile Computing and Networks (MOBICOM 2001), Julio 2001.

[14] EYES European Research Project, IST-2001-34734. http://eyes.eu.org.

[15] O. Younis, S. Fahmy. *Distributed Clustering in Ad-Hoc Sensor Networks: A Hybrid, Energy-Efficient Approach.* IEEE Infocom'04, Marzo 2004.

[16] MICA2 Radio Stack for TinyOS. http://www.tinyos.net/tinyos-1.x/doc/mica2radio /CC1000.html

A. Demostración de la Ecuación (1)

El principal objetivo de (1) es conocer la probabilidad de que α nodos activen sus agentes globales al mismo tiempo en un vecindario de n posibles "Watchdogs" espontáneos, cuando la decisión de un nodo no puede influenciar en la de otros. Este problema puede abstraerse como lo siguiente:

> *Tenemos n jugadores (nodos) en una mesa, y cada jugador tiene un dado con m caras (donde m suele ser igual a n). Queremos conocer la probabilidad de que α jugadores obtengan un "1" (es decir, activen sus agentes globales) cuando todos los jugadores hayan tirando una vez su dado.*

En este nuevo problema, queremos resolver lo siguiente:

$$f(\alpha, n, m) = \frac{f'(\alpha, n, m)}{f''(\alpha, n, m)} \tag{2}$$

donde $f'(\alpha, n, m)$ son todos los casos donde se tiran n dados de m caras, y α y solo α dados tienen un resultado de 1; $f''(\alpha, n, m)$ son todos los casos donde se tiran n dados de m caras.

Si un jugador tira un dado, el resultado puede estar dentro de uno de estos conjuntos: {1} o {2..m}. El número de posibles casos donde α y solo α dados están en el conjunto {1} es el número de permutaciones con repetición (ya que cada dado es independiente y diferente de los demás) de n elementos (dados) donde el valor de que α elementos caigan en el conjunto {1} y $n-\alpha$ elementos caigan en el conjunto {2..m} es de

$$PR_n^{n-\alpha,\alpha} = \frac{n!}{n-\alpha! \cdot \alpha!} \tag{3}$$

Como ejemplo, si tenemos $n = 2$ dados con $m = 3$ caras, el número de casos donde uno y solo un dado ($\alpha = 1$) cae en el conjunto {1} es igual a 2, ({(1,[2..3]), ([2..3],1)}). Por cada uno de los casos del ejemplo anterior, tenemos $n - \alpha$ dados que han caído en el conjunto {2..m} de $m - 1$ elementos. Es por lo tanto posible saber $f'(\alpha, n, m)$, si multiplicamos (3) por $(m-1)^{n-\alpha}$:

$$f'(\alpha, n, m) = PR_n^{n-\alpha,\alpha} \cdot (m-1)^{n-\alpha} \tag{4}$$

ya que $(m-1)^{n-\alpha}$ son las variaciones ordenadas con repetición de $m-1$ elementos tomados de $n-\alpha$ en $n-\alpha$. En el ejemplo anterior ($n = 2$, $m = 3$, $\alpha = 1$), el número de casos donde uno y solo un dado tiene un resultado de 1 son $2 \cdot 2 = 4$, i.e., {(1,2), (1,3), (2,1), (3,1)}.

Finalmente, $f''(\alpha, n, m)$, o todos los casos en los que se tiran n dados de m caras, es las variaciones con repetición de m elementos tomados de n en n:

$$f''(\alpha, n, m) = VR_{m,n} = m^n \tag{5}$$

Concluimos que (1) y (2) son iguales, y ambos resuelven el mismo problema.