애드 혹 네트워크에서 최소 걸침 나무를 이용한 효과적인 침입 탐지 시스템 배치
An Efficient IDS Node Distribution Scheme Using Minimum Spanning Tree in Wireless Ad Hoc Networks

Sungchul Ha[a], Yeongjun Park[b], Sehun Kim[c]
[a,c]Department of Industrial Engineering, KAIST, 373-1,
Guseong-dong, Yuseong-gu, Daejon, 305-701, Korea
[b]Department of Computer Science, KAIST, 373-1,
Guseong-dong, Yuseong-gu, Daejon, 305-701, Korea
E-mail : scha@tmlab.kaist.ac.kr;pyj1111@kaist.ac.kr;shkim@kaist.ac.kr

ABSTRACT

Wireless Ad-hoc network communicate with other nodes using wireless interface. The wireless ad-hoc network don't have any infrastructure, then it has some problems to operating centralized intrusion detection system such as wired network. Accordingly each node install the agent to operate intrusion detection system in wireless ad-hoc network. However a node that installed an agent additionally consumes battery power and reduces lifetime. Therefore, need to install and manage the intrusion detection agent which considers both enhancing network lifetime and an efficient intrusion detection

In this paper, we propose an efficient IDS node distribution scheme using MST to minimize a number of IDS nodes and lifetime-enhancing of network.

1. INTRODUCTION

An Intrusion Detection System (IDS) is widely employed for security purpose to detects unwanted manipulations to network systems. Because illegal attackers can break whole networks, many network systems need intrusion detection systems. So some networks nominate some nodes to intrusion detection nodes [1]. But a node nominated as an IDS node to monitoring consumes additional resources such as batteries, time, and so on. Because it checks all packets within communication range and sends warning messages to its neighbor nodes. In wireless ad-hoc networks, resources such as power, bandwidth of nodes are limited, therefore wireless ad-hoc networks need an efficient IDS node distribution scheme to use resources efficiently and enhance network lifetime [2], [3].

2. RELATED WORKS

Wireless networks don't have a fixed, well-protected communication medium-instead, all communication is conducted in an open air environment. This makes it impossible to monitor network traffic at bottlenecks. Therefore, network monitoring in wireless ad-hoc networks is performed at every network node [1], [2].

Kachirski O. and Guha R [1], proposed a distributed intrusion detection system (DIDS) for wireless ad-hoc networks based on mobile agent technology. A distributed IDS allocates the overall packet-monitoring task to a small subset of nodes with the high connectivity.[1] However, the lifetime of whole network is possibly reduced since the work load is easily concentrated to the selected nodes. Therefore some IDS nodes on which most of work load concentrated suffer from a shortage in battery power.

This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Informaion Technology Research Center) support program supervised by the IITA(Institute of Information Technology Assessment) (IITA-2005-(C1090-0502-0020)).

Kim H., Kim D. and Kim S. [2], proposed a lifetime-enhancing monitoring node selection (LES) scheme of adaptively choosing a node, for intrusion detection, that has a maximum remaining battery power between adjacent mobile nodes. By dispersing the battery power consumption among the nodes with relatively high remaining battery power, LES scheme can enhance the network lifetime. In LES scheme, If a relative node has more battery power than IDS node, then the IDS node give its IDS node right to other node. However the IDS node is exchanged too much frequently, because IDS node exchanging happen when a node detects a relative node more battery power than it.

In wireless ad-hoc network, the lifetime of network is defined as the duration of time until the first node is dead, because of whole battery out [1], [2], [3]. The network lifetime is one of the most significant measures in ad hoc networks since a single node failure can partition the network into unconnected sub-networks and further communication services are interrupted between separate networks [2].

In this paper, we propose an efficient IDS node distribution scheme for intrusion detection. The scheme uses Minimum Spanning Tree to find appropriate to IDS Node location. The IDS nodes locate on Minimum Spanning Tree of whole networks. It guarantees that a IDS node is nearest node among relative nodes. It means we can choose transmission range and control power level which is appropriate reaching to a target node. By controling power level and using Minimum Spaning Tree, compare with DIDS and LES scheme, the proposed scheme nominate less nodes to intrusion detection and enhance network lifetime.

3. PROBLEM DEFINITION

We will concentrate our discussion on wireless ad-hoc networks. Wireless ad-hoc network is a collection of mobile nodes that establish a communication protocol dynamically. The nodes may join the network at any time and communicate with entire network via the neighboring nodes. There are no base stations, and each member of such a networks is responsible for accurate routing information, and takes part in routing decisions. We consider all nodes distributed in limited area and all nodes have limited resources. The properties of nodes are having limited battery power and transmission range and moving dynamically. So, we consider that the distribution of nodes is randomness in limited area. And we define power consumption of nodes. It occurs when a node basically sends a packet, receives a packet, overhears a packet and especially when a node operates intrusion detection service at an IDS node.

4. PROPOSED ALGORITHM

4.1 IDS Node Selection Using MST

In proposed algorithm, a mobile node within the shortest distance is found among the neighboring nodes and selected as a candidate of a bridge node to make Minimum Spanning Tree. Neighboring nodes of node i are nodes that can be reached by one-hop from node i. One hop of node i means that it is within maximum transmission range of node i. Let N^i be the set of neighboring nodes of node i including node i itself and D_i be the distance of node i. The candidate of bridge node i^* is searched for every node i such that

$$i^* = \arg\min_{j \in N^i} D_j \qquad (1)$$

At network starting, each node sends a control packet containing the value of distance to its neighbors. All nodes always know the value of distance of their neighbors. Based on a control packet, each node connects the first bridge with its nearest neighbor. We operate this process for all nodes. When each node complete first connection, each group, made by first connection, makes its second bridge within maximum transmission range. Before connecting second bridge, if a node have more than three bridges, then the node nominate IDS node. We finish this process when all nodes make complete Minimum Spanning Tree. As an example, we consider a connection graph of ten nodes given Fig. 1. and we can see complete Minimum Spanning Tree given Fig. 2.

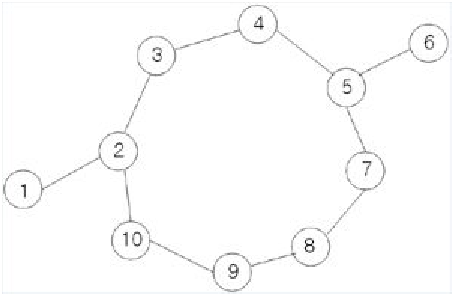

Fig. 1. Distributed nodes in wireless ad-hoc network

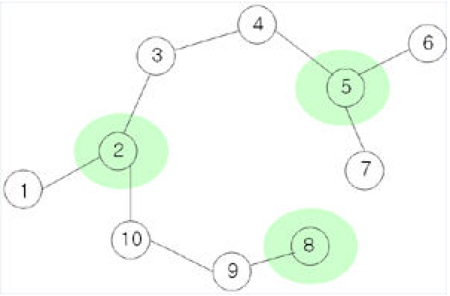

Fig. 2. IDS node selection.

Nodes selected to intrusion detect are highlighted in Fig. 2. We can see that three nodes out of ten nodes become network IDS node resulting in the entire network being monitored. The IDS node selection based on Minimum Spanning Tree consist of two steps.

Step 1)

Starting with checking a number of bridge of each node. If we find a node which has more than three bridges, then the node nominate IDS node.

Step 2)

Starting with checking IDS node distribution. At this time, we check entire network monitored by IDS nodes. If not, we check near the IDS node. To monitor entire networks, IDS nodes have to locate within 3-hop distance each other. If the ids node is not within 3-hops from other ids nodes, then we set up a ids node at 3-hop distance.

4.2 Control Transmission Power Level

After making Minimum Spanning Tree, we need to control transmission power level of each node. At section 4.1, we select some nodes based on Minimum Spaning tree to intrusion detection. It means the nearest node of most of nodes are IDS node. It is guaranteed by Minimum Spanning Tree. Now, we can control transmission power level of each node. Because the IDS node of each node locates closer than other nodes, so any sending packets of each node are monitored by IDS node. Very small portion of all nodes may don't have IDS node in its nearest area. In this case, we consider it is exceptional case. Because it is very tiny portion and no problem to the whole efficiency of proposed algorithm. The transmission power lever controling algorithm is following to Fig. 3.

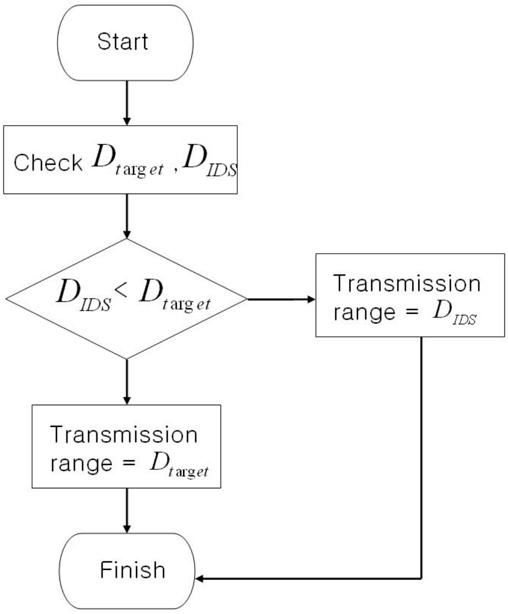
Start
Check D_{target} , D_{IDS}
$D_{IDS} < D_{target}$
Transmission range = D_{IDS}
Transmission range = D_{target}
Finish

Fig. 3. Transmission power level control Algorithm

As discussed above, the Minimum Spanning Tree guarantee that IDS node locate nearest area of most of nodes. Therefore, almost nodes decide a transmission range with D_{target}. Each node which decides a transmission range with D_{target} sends its packet to a target node, simultaneously IDS node checks the packet. An exceptional case, D_{IDS} is the transmission range of an exceptional node. If all nodes in wireless ad-hoc networks follow Fig. 3. algorithm, then they can send any packets under watching of IDS nodes and enhance network lifetime. Because all nodes can reduce their sending power.

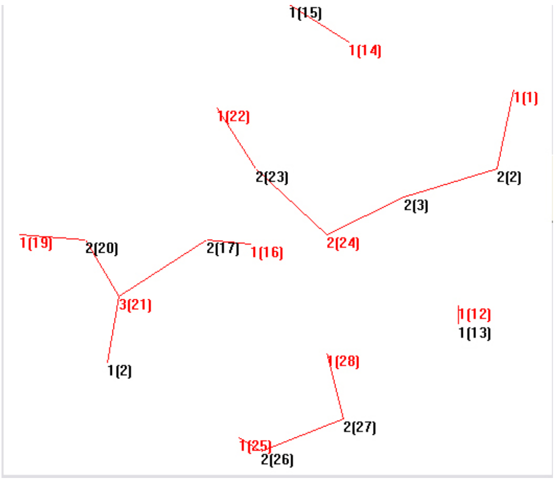

Fig. 4. IDS selection at 20 nodes

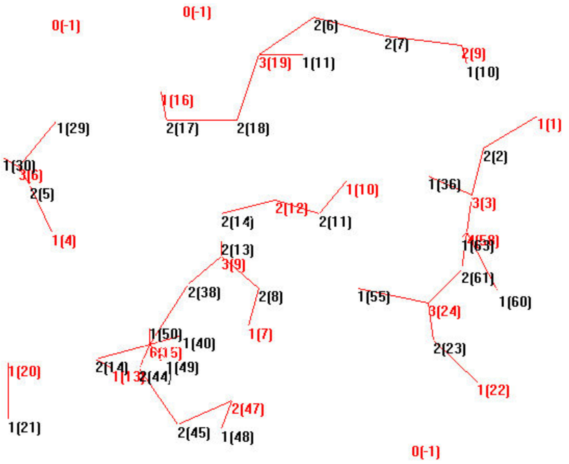

Fig. 5. IDS selection at 50 nodes

Figure	Fig. 4.	Fig. 5.
Max transmission range	20m	20m
A number of nodes	20	50
A number of IDS nodes	10	21
nodes and IDS nodes ratio	0.5	0.42

Table 1. Simulation condition and result

5. SIMULATION

In the simulation, we consider a wireless ad-hoc network. We assume low mobility condition because we concentrate our simulation on selecting of IDS nodes. For the purpose of comparison, we consider 20 & 50 nodes. The reason why we select this situation is to see the reducing rate of nodes to IDS nodes. The reducing rate of IDS nodes is very important. The fewer IDS nodes in network are, the better performance of network is, because the lifetime enhancing possibility and an efficiency of network increases.

The table 1. is conditions and result of IDS node selecting simulation and Fig. 4, Fig. 5 illustrate distribution of IDS node selection based on Minimum Spanning Tree. The red line means MST bridges and the red character means IDS nodes. The left integer of each node is a number of bridges and the right one is node number.

We can see the more nodes, the more IDS nodes. It is omit. But we can also find the more nodes, the smaller ratio of node and IDS nodes ratio. It means 50 nodes network is more excellent from the network efficient side than 20 nodes networks.

6. CONCLUSIONS and FUTURE WORK

In this paper, we propose an efficient IDS node distribution scheme using Minimum Spanning Tree in wireless ad-hoc networks. Using Minimum Spanning Tree guarantee that the IDS node locates near any nodes in wireless ad-hoc network. We can easily find strong point of proposed method. The first good point of proposed method is reducing the rate of nodes to IDS nodes. And the second good point of proposed method is enhancing network lifetime. Based on our method, wireless ad-hoc network selects easily and efficiently IDS nodes and can enhance lifetime.

In a future, we will simulate proposed algorithm which is focused on enhancing lifetime.

< Reference >

[1] Kachirski O. and Guha R., "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks", Proceeding of the international conference on system sciences, Hawaii, 2003. p.57-64

[2] Kim H., Kim D. and Kim S., "Lifetime-enhancing selection of monitoring nodes for intrusion detection in mobile ad hoc networks", International Journal of Electronics and Communications, (AEǛ) 60, 2006, p.248-250

[3] Chang J.H., Tassiulas L., "Maximum Lifetime Routing in Wireless Sensor Networks", IEEE/ACM Transactions on Networking, Vol. 12, No. 4, August 2004.

[4] Cardei M., Wu J., Yang S., "Topology Control in Ad Hoc Wireless Networks Using Cooperative Communication", IEEE Transaction on Mobile Computing, Vol. 5, No. 6, June 2006.

[5] Cardei M., Wu J., Yang S., "Topology Control in Ad Hoc Wireless Networks with Hitch-Hiking", Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on, 4-7 Oct. 2004, p.480-488

[6] Li N., Hou J.C., Sha L., "Design and Analysis of an MST-based Topology Control Algorithm", IEEE Transactions on Wireless Communications, Vol. 4, No. 3, May 2005.

[7] Gallager R.G., Humblet P.A., Spira P.M., "A distributed Algorithm for Minimum-Weight Spanning Trees", ACM Transactions on Programming Languages and Systems, Vol. 5, No. 1, January 1983, p.66-77