An Efficient Intrusion Detection System (IDS) Node Selection for Congested Systems in Wireless Mesh Networks

최재운, 김기성, 김세헌
KAIST 산업공학과 통신시스템 및 인터넷 보안 연구실
E-mail : juchoi, kskim, shkim@tmlab.kaist.ac.kr

Abstract

We propose a IDS node selection scheme for intrusion detection in wireless mesh networks. The proposed scheme considers network survivability and energy consumption. To utilize wireless resources efficiently, we apply a set covering problem (SCP) to IDS nodes selection problem. Our proposed scheme also considers congested networks.

1. Introduction

An Intrusion Detection System (IDS) for wireless networks is widely employed for security purpose to detect illegal intrusions. As illegal attackers can damage the network and gain important information of users in the network, many wireless networks use an intrusion detection system. If all nodes in the network implement intrusion detection processing, resource consumption of the whole network is high and some nodes may suffer from battery exhaustion. And a node acted as an IDS node consumes additional resources, because it overhears and analyses all packets within monitoring range. Since wireless network resources such as battery and bandwidth are limited, an efficient monitoring node selection scheme utilizing these resources efficiently is needed in wireless networks.

In this paper, we apply an IDS node selection scheme to a wireless mesh network (WMN). WMN is a promising wireless technology that supply wired infrastructure (Internet Gateway, IGW) with wireless backbone (Mesh Router, MR) to mobile users. Users who have wireless mobile device can always access WMNs by connecting to MRs. Thus in WMN, the users will be always on-line anywhere anytime [1]. In WMN, every MR transmits their information to the IGW. Therefore, the IGW is able to collect information about remaining battery and connectivity of each MR node. In this paper, we propose an efficient IDS placement in WMNs using collected information by the IGW.

Existing IDS node selection schemes only consider either network lifetime or battery consumption of the whole network. However, we suggest an efficient monitoring node selection method considering both enhancement of network lifetime and reduction of total battery consumption. To guarantee enough network lifetime and reduce the battery consumption of the whole network, we apply a set covering problem (SCP) to monitoring node distribution problem. Compared with existing schemes, the proposed scheme has balanced performance about network lifetime and battery consumption of whole network. Furthermore, we consider congestion of

"This research was supported by the Ministry of Knowledge Economy, Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement)" (IITA-2008-C1090-0801-0016)

monitoring load in a buffer of IDS node. When an overflow of packets occurs in a queue of monitoring node, the IDS can't monitor all packets and the battery consumption of monitoring node is very high due to excessive monitoring tasks. Therefore, it is important to consider congestion of monitoring tasks. In congested system, our proposed scheme has superior performance than other existing scheme.

2. Related works

There are two researches to select monitoring nodes for intrusion detection before, distributed IDS and lifetime-enhancing monitoring node selection. Kachirshi and Guha proposed a distributed IDS (DIDS) for wireless ad hoc networks which allocates intrusion detection tasks to nodes with high connectivity [2]. However, lifetime of whole network is reduced since the monitoring load is easily concentrated to the IDS nodes which have high connectivity. Consequently, IDS nodes suffer from battery depletion. A lifetime-enhancing monitoring node selection (LES) is proposed to enhance the network lifetime [3]. LES scheme selects IDS nodes which have a maximum remaining battery among neighbor nodes. Comparing to DIDS scheme, LES scheme enhances the network lifetime which is defined as the duration of time until the first node runs out of battery. Although LES scheme is able to enhance the network lifetime, the energy consumption of the whole network is relatively high as LES needs many IDS nodes in the network. Therefore, LES is not the best algorithm in terms of total energy consumption.

As mentioned above, although, the network lifetime of LES is longer than DIDS, the total energy consumption of LES is higher than DIDS. In other words, LES has the advantage of network lifetime enhancing and a strong point of DIDS is reducing the battery consumption of the whole network. However, both the network lifetime and the total energy consumption are meaningful performance measures. Therefore, to utilize wireless resources efficiently, we consider those two measures.

Our work also differs from others by considering congestion of monitoring tasks. When packets arrived at IDS node, they are buffered in the queue of an IDS node to be monitored. Network congestion occurs when a link or node is carrying so much data that its quality of service deteriorates. When congestion occurs in a node due to high packet arrival rates, the IDS cannot afford to monitor the all arrival packets and the buffer overflow happens. So the IDS becomes ineffective and deteriorated. Hence, it is desirable to assign IDS node to the network properly so that prevent the denial of IDS service due to the overflow.

In this paper, we propose a new IDS node selection scheme in WMN which guarantees the adequate network lifetime and reduces the energy consumption of the whole network, considering the monitoring task congestion as well as the network life time.

3. Formulation

In this section, we propose an IDS nodes selection scheme based on three requirements. First, to monitor all nodes in the network, every node should be in the monitoring coverage of IDS. Second, to enhance the network lifetime and reducethe battery consumption of whole network, we want to minimize the overall cost of monitoring tasks by the IDS nodes. Third, to prevent the congestion of monitored packets, we design the IDS nodes placement scheme considering congested systems. For satisfying the first and second requirements, we apply a set covering problem (SCP) to the IDS nodes selection scheme.

The SCP is a classical question in computer science and complexity theory. The SCP selects a minimum number of sets that contain all elements and additionally minimizes the cost of the sets. Therefore, the SCP guarantees that every element is

covered by at least one server at minimal total cost. To cover all nodes by minimal IDS nodes and guarantee the adequate network lifetime, we propose a formulation using the SCP. The formulation of the IDS node placement scheme using the SCP is as follows;

$$\begin{aligned} \min \quad & \sum_{j=1}^{n} c_j x_j \\ s.t \quad & \sum_{j=1}^{n} a_{ij} x_j \geq 1 \quad \forall i \in N \\ & x_j \in \{0,1\} \quad \forall j \in N \end{aligned} \quad . \quad (1)$$

Formulation (1) is a typical SCP formulation. Binary variable x_j is one if node j is IDS node, and zero otherwise. Like figure 1, binary variable a_{ij} is one if node j is in the transmission range of node i, and zero otherwise. In the typical SCP,

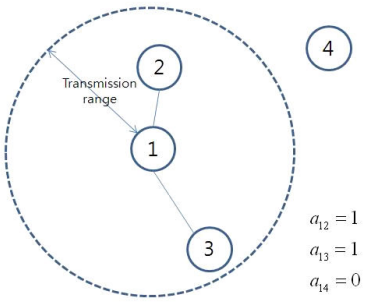

Fig. 1. Transmission range of node

c_j is the cost which is needed to select server j. In this problem, one of our objectives is enhancement of the network lifetime. To prevent selecting IDS node with low remaining battery, we define c_j as the reciprocal of node j's remaining battery. We define the set N as the set of all nodes in the network.

In formulation (1), objective function considers the lifetime of each node and minimizes the number of monitoring nodes. As we consider the amount of remaining battery in the objective function, our formulation guarantees sufficient network lifetime. Moreover, reduction of the total energy consumption is possible using our objective function because objective function of SCP minimizes the number of IDS nodes. In formulation (1), constraint states that every node should be monitored by at least one leader node. Therefore, formulation (1) satisfies the first and second requirements. We now discuss a constraint which considers congested systems.

An implicit assumption in traditional SCP is that each node in the coverage of a server always receives satisfied service. However, when a server suffers from congestion by excessive demand, some users are not able to receive satisfied service in the real situation. Especially, if an IDS node suffers from congestion of monitored packets, intrusion detection efficiency is reduced and battery consumption of the IDS node is high. Therefore, considering congested systems is important. To prevent congestions, any packet should not stand in waiting line in the buffer of IDS nodes for a time longer than a given time-limit [4]. The constraint which considers congestion is as follows;

$$P[\,\textit{waiting time at IDS node } j \leq \tau\,] \geq \alpha \quad \forall j \quad . \quad (2)$$

Constraint (2) makes the total time spent by a packet at the IDS node shorter than equal to τ with probability of at least α. The variables τ and α are predefined time and probability. In order to express constraint (2) as a numerical formula, we use the queuing theory [4]. In this paper, we make an assumption that an arrival rate from node i to j appears according to a poisson process with intensity f_{ij}. Also, we assume an exponentially distributed monitoring service time, with an average

rate of μ_j. This is a reasonable assumption, since some people tested real IDS systems, and IDS systems behave as M/M/1 Systems. As we assume a M/M/1 queuing system, we are able to use the well known results for a M/M/1 queuing system for each IDS and its allocated nodes [4]. Rewriting constraint (2) as a numerical formula, we get

$$\sum_{i=1}^{n} f_{ij}\, a_{ij} x_j \le \mu_j + \frac{1}{\tau}\ln(1-\alpha) \quad \forall j \in N \quad . \tag{3}$$

Adding constraint (3) to formulation (1), we finally get our proposed formulation as follows;

$$\begin{aligned} \min \quad & \sum_{j=1}^{n} c_j x_j \\ s.t \quad & \sum_{j=1}^{n} a_{ij} x_j \ge 1 \quad \forall i \in N \\ & \sum_{i=1}^{n} f_{ij}\, a_{ij} x_j \le D_j \\ & where,\ D_j = \mu_j + \frac{1}{\tau}\ln(1-\alpha) \quad \forall j \in N \\ & x_j \in \{0,1\} \quad \forall j \in N \end{aligned} \quad . \tag{4}$$

4. Future Works

In this paper, we proposed an IDS node selection scheme for intrusion detection in wireless mesh networks. To enhance the network lifetime and reduce the battery consumption of whole network, we apply the SCP considering congested systems to select monitoring node. LES only considers enhancement of network lifetime and DIDS only considers minimization of total energy consumption. However, we consider both network lifetime and energy consumption of whole network using SCP. Especially, we consider congested systems using the queuing theory.

In future works, we should simulate our proposed algorithm. As proposed algorithm is so complicated, the reduction of calculation time is required. To reduce calculation time, we should apply heuristic algorithms to proposed scheme.

5. Reference

[1] Ian F. Akyildiz, Cudong Wang, Weilin Wang, Wireless mesh networks : a survey., Computer Networks., vol. 47, No. 4, 2005, p. 445-487.

[2] 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

[3] 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, (AEU) 60, 2006, p.248-250.

[4] Marianov, V. and Serra, D., Probabilistic Maximal Covering Location-Allocation Models for Congested Systems, Journal of Regional Science 38, 1998, p.401-424