ICIC Express Letters
Volume **10**, Number **5**, May **2016**

ICIC International ©2016 ISSN 1881-803X
pp. 1053–1059

RESEARCH ON INTRUSION DETECTION FOR WMN BASED ON REGION-COVERAGE

Hongyu Yang and Xinyuan Wang

Department of Computer Science and Technology
Civil Aviation University of China
No. 2898, Jinbei Road, Dongli District, Tianjin 300300, P. R. China
yhyxlx@hotmail.com; xinyuan71522@163.com

Received October 2015; accepted January 2016

Abstract. *This paper proposed a Region-Coverage based Distributed Intrusion Detection method (RCDID) in order to solve the intrusion detection problem of Resource-limited Wireless Mesh Network (WMN). In RCDID, firstly, we divided Snort rule files into several detection modules by the dependency between rules and rule files to preprocessors, and split large rule files to ensure that the rules and essential preprocessing rules are divided into the same rule file. Then, all nodes must participate in intrusion detection for WMN, every node employs the Regional Coverage Optimization (RCO) algorithm to load detection modules, and it would have multi-monitoring nodes for the detection of each communication link, achieving the detection of the whole network traffic by detecting all communication links. Experimental results demonstrate that our method has a better adaptability and scalability in different scale networks, and it has higher memory utilization and intrusion detection rate, especially in large scale WMN.*

Keywords: Wireless Mesh Networks, Resource-limited, Intrusion Detection, Grouping rule files, Regional Coverage Optimization

1. Introduction.

Wireless Mesh Networks (WMN) is a new generation of wireless network technology which is combined by wireless LAN technology and mobile ad hoc grid technology [1], and has the characteristics of wide coverage, self-organization, cost-effective, high reliability, etc. WMN can provide Internet, Intranet networking services in no network infrastructure areas, and also serve as a backbone communication infrastructure among hosts and mobile clients. With the increasing application of WMN, WMN security issues have become increasingly prominent [1,2]. Intrusion Detection (ID) technology as an important means of network security, plays a very important role in the network security monitoring system. Because of lacking of superiority nodes which can detect network traffic (e.g., wired network gateway) and a strong restrictive about hardware resources (e.g., CPU and Memory), the traditional intrusion detection methods are no longer suitable for WMN [3].

The intrusion detection motheds of WLAN and Wireless Sensor Networks are not applicable to Resource-limited WMN [4,5]. Some researchers have proposed deploying Intrusion Detection System (IDS) in a few of key nodes [6,7], these methods require deploying a complete IDS modules in monitoring nodes, and because of limited hardware resources, only a few modules can be invoked, which results in a lower detection rate. In cooperative detection methods, grouping method [8] swaps neighbor nodes detecting information; hierarchical methods [9,10] aggregate different layers detecting information. These methods increase the detection rate, but reduce network performance and have a high detection latency due to the need to exchange a large amount of detecting information. A traffic paths based IDS solution was proposed for resource-limited WMN [3], however, the majority of real-world traffic paths of WMN applications are constantly changing, and it might not be feasible for them.

This paper proposes a Region-Coverage based Distributed Intrusion Detection method (RCDID). On the premise of no node (Mesh router or Access point) being overloaded, running an IDS instance for each node, the monitoring object is the communication links, the traffic on each communication link can be detected by multi-monitoring nodes, and the Intrusion Detection Rate (IDR) can be enhanced through optimizing distribution of detection modules on the nodes.

The remainder of this paper is organized as follows. In Section 2, basic principle of the region coverage model is introduced, and the modular grouping for Snort rule files is also given as a necessary background, and the RCO algorithm is also elaborated. Section 3 describes experimental results and analysis, and conclusions are drawn in the last section.

2. **Intrusion Detection Method Based on Region Coverage.**

The system model of RCDID conforms with the IEEE 802.11S WLAN Mesh standard [11].

2.1. **Detection system.**

In this paper, detection system employs open-source ID tool Snort. Firstly, the data acquisition mode of Snort was improved to detect single-hop and multi-hop attacks simultaneously. It is feasible to asynchronously get network data of local and upstream interfaces by running a single Snort instance and opening two Libpcap packet capture handles. Experimental results in Aruba AirMesh MSR1200 router showed the memory load of improved Snort increased by only 3% compared to the original.

2.1.1. *Modular rule files.*

Snort detection engine is based on thousands of detecting rules and preprocessors. It can reduce the complexity of Snort rules by decreasing the amount of rule files and independent preprocessor. Experiments showed that the modular rule files can reduce the dependence on the preprocessors and save memory overhead.

2.1.2. *The composition of modular grouping.*

We parsed each detection rule by the keywords which represent rules dependency [12], according to the dependency of rules and rule files to preprocessors, splitting large rule files to ensure that the rules and essential preprocessing rules are divided into the same rule file. Snort preprocessor is implemented by plugins, and plugins can be written based on actual needs, therefore, Snort has good scalability.

In this paper, we describe the set of all detection modules by $M = \{m_k | m_k \text{ is a set of detection rules}\}$, where K is the size of $|M|$. The set of preprocessors is represented by $C = \{c_r | c_r \text{ is a group of preprocessors}\}$, where R is the size of $|C|$. We divided the rule files into 6 modules and 12 modules respectively, and grouped Snort preprocessors based on the dependency of rule files to preprocessors and their functionality. Here, we did not enumerate the grouping detail due to the limited space of this paper.

According to experimental results in Aruba AirMesh MSR1200, the memory load of each detection module and preprocessor are shown in Table 1 and Table 2 respectively.

Table 1. 6-module memory load

Modular	ID	Memory load	ID	Memory load	ID	Memory load
6 modules	m_1	13.32%	m_3	13.04%	m_5	14.66%
	m_2	14.66%	m_4	17.33%	m_6	17.33%

Table 2. Preprocessors' memory load

Grouping	ID	Memory load
3 Groups	c_1	15.2%
	c_2	1.3%
	c_3	1.1%

It is noted that we assume each module requires all three groups of preprocessors when the corresponding rule files are invoked. Every module requires the preprocessor c_1, and also requires preprocessor c_2 or c_3. Therefore, the extra overhead on every node is at most 1.3%.

2.2. **Region-coverage solution.** It needs to obtain maximum Link Coverage Rate (LC-R), so the nodes which cover the communication link should load maximum detection modules.

2.2.1. *Basic concepts.* In a given network, it can be regarded as an undirected graph $G = \{V, E\}$, where V is the set of network nodes (Mesh routers or Access points), and E is the set of backbone communication links. We assign n represents the amount of nodes, and q represents the amount of communication links. Then, $V = \{v_1, v_2, \ldots, v_n\}$, $E = \{e_1, e_2, \ldots, e_q\}$.

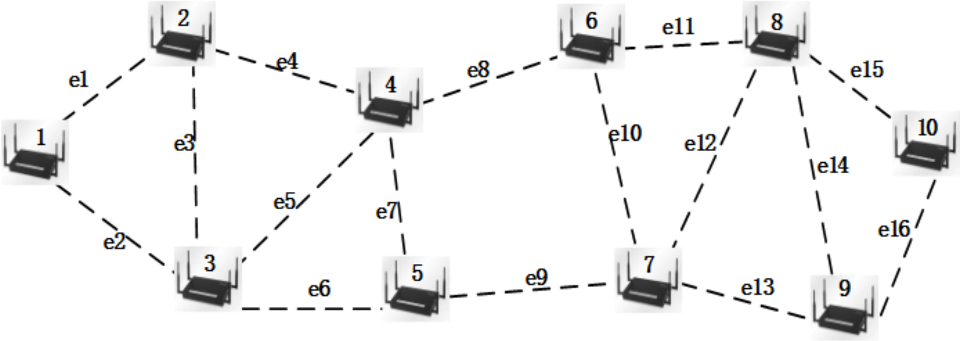


Figure 1. Network sample

In order to acquire the distribution information of detection modules on links, we take Figure 1 as an example to define some concepts as follows.

Definition 2.1. *The mapping matrix between links and nodes, is represented by $D_{q\times n}$ where $d_{ij} = 1$ means that node v_j can detect link e_i. It should be noted that if a link e_i connect to the node v_j directly, or the node v_j connect with the two nodes which link e_i is directly connected, the node v_j can monitor link e_i.*

Definition 2.2. *The distribution matrix of detection modules on nodes, is represented by $S_{n\times k}$ where $s_{jk} = 1$ means that node v_j has loaded the detection module m_k.*

Definition 2.3. *The distribution matrix of detection modules on the links, is represented by $L_{q\times K} = D_{q\times n} \cdot S_{n\times K}$, where $l_{ik} = 1$ means that the link e_i can be detected by detection module m_k.*

For a given communication link e_i,

$$LCR_i = |M_i|/|M| \tag{1}$$

where M_i is the set of modules which can detect the link e_i.

2.2.2. *Problem formulation.* RCDID requires loading maximum detection modules on nodes without overload, so we need to calculate the total memory load of nodes.

We denote the memory load of detection module m_k and preprocessor c_r by w_k^m and w_r^c respectively (see Tables 1 and 2). The basic memory load (without preprocessor or rule actived) is represented by vector $B = [b_1, b_2, \ldots, b_n]$. The memory threshold (maximum allowable memory load) is represented by vector $T = [t_1, t_2, \ldots, t_n]$, and it is usually set by network administrator.

Definition 2.4. *The total memory load of node v_i,*

$$W_i = b_i + \sum_{m_k \in M_i} w_k^m + \sum_{c_r \in C_i} w_r^c \tag{2}$$

if $W_i > t_i$, the detection modules on node v_i will be disabled.

RCDID needs to obtain maximum LCR, and T is memory load constraint, therefore, this optimization problem can be formulated as a non-linear programming problem as follows:

$$\textbf{MAX} \quad 1/q \left(\boldsymbol{E}^T \cdot L(D \cdot S) \cdot E \right) \tag{3}$$

$$\textbf{S.T} \quad \boldsymbol{W}^T \leq \boldsymbol{T}^T \tag{4}$$

where Function (3) is average link coverage rate; Function (4) is a constraint of memory load on every node, where the vector W represents total memory load of all nodes.

2.3. **Regional Coverage Optimization algorithm.** We adopt a distributed solution and propose a Regional Coverage Optimization (RCO) algorithm – nodes can locally decide which detection modules they should run.

In RCO, we assign the region which a monitoring node can cover as an optimized region, every node randomly selects non-repeat detection modules according to its memory threshold, and then optimizes the distribution of detection modules in the same region by the broadcast about the information of loading detection modules on the smaller number neighbor nodes. The set of maximum executable detection modules on node, represented by U. RCO Problem is designed as RCO Algorithm. The communication overhead and delay can be neglected due to that the broadcast among nodes is only once and exchange information is very little.

RCO Algorithm

```
Initialization($M, W^m, W^c, b, t$)
while $M! = $ null do
    $m_k = \text{Random}(M)$
    $l = w_k^m + W^c + b$
    if $l \leq t$ then
        $U = U + m_k$
        $M = M - \{m_k\}$
        $t = t - w_k^m$
    end if
end while
Return $U$
```

3. Experiment and Simulation.

3.1. **Experimental verification.** In order to validate the feasibility of RCDID, we built a Mesh network environment shown in Figure 2, and we deployed the improved Snort in MSR 1200. Attacker Clients was installed to run IDS Informer, and attack data is defined by each detection module rules. We launched different types of attacks from Attacker Clients to the Clients in the same Mesh Router and other Clients which connect to other Mesh Routers. The alerts generated by the Response Server proved that our proposed solution is feasible for WMN.

Because of restrict experiment conditions, we evaluated the performance of RCDID in different scale networks by Matlab and compared with the methods in literature [3,6]. The basic memory load of nodes was 32% which is acquired from verification experiment.

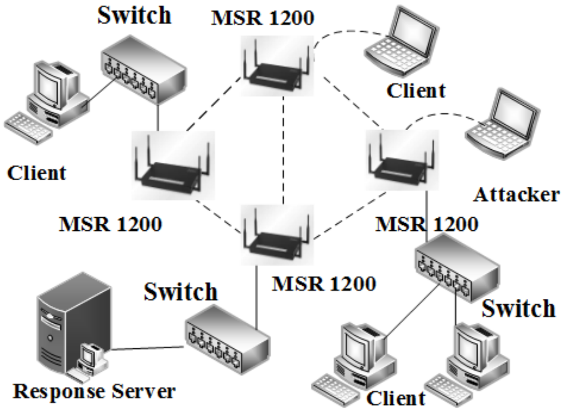


Figure 2. LAN experimental environment

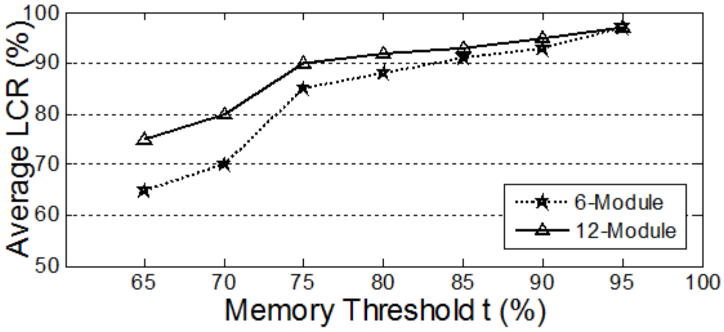


Figure 3. Average Link Coverage Rate

3.2. **Average Link Coverage Rate.** We randomly created 50 networks composed by 10 nodes, and Figure 3 shows the average LCR for 6-module and 12-module configuration.

As shown in Figure 3, we can see that the LCR of 12-module is a little higher than 6-module, when the memory threshold is lower. It indicates that 12-module is more suitable for smaller memory hardware condition. Experimental results indicate that the LCR of RCDID can be more than 90%, when memory threshold reaches 80%.

3.3. **Intrusion Detection Rate and memory utilization.** We created a network composed by 10 nodes and simulated 100 single-hop attacks and 20 multi-hop attacks (randomly chose from 2 to 6 hops). We respectively measured the Intrusion Detection Rates and memory utilizations for EEMON [7], PRIDE [3] and RCDID.

According to the theory of RCDID, the variation trend of LCR represents the variation trend of IDR. Through the analysis of the variation trend of LCR in Figure 3, the LCR increases obviously when the memory threshold is from 65% up to 75%; the LCR increases steadily when the memory threshold is from 75% up to 90%; the LCR basically reaches the peak value when the memory threshold is over 90%. Thus, we chose the Intrusion Detection Rates and memory consumption when the memory threshold is 70%, 80% and 90% respectively as the evaluation criteria and uniformly employed 6-module configuration to evaluate the three methods. Experimental comparison results are shown in Tables 3, 4 and 5.

Table 3. Memory threshold being 70%

Method	Single-hop IDR	Multi-hop IDR	Memory utilization
EEMON	10%	43%	33%
PRIDE	15%	67%	62%
RCDID	31%	93%	65%

Table 4. Memory threshold being 80%

Method	Single-hop IDR	Multi-hop IDR	Memory utilization
EEMON	12%	51%	35%
PRIDE	34%	83%	73%
RCDID	43%	95%	76%

Table 5. Memory threshold being 90%

Method	Single-hop IDR	Multi-hop IDR	Memory utilization
EEMON	16%	69%	38%
PRIDE	37%	87%	69%
RCDID	56%	97%	83%

We can conclude from above experimental results as follows:

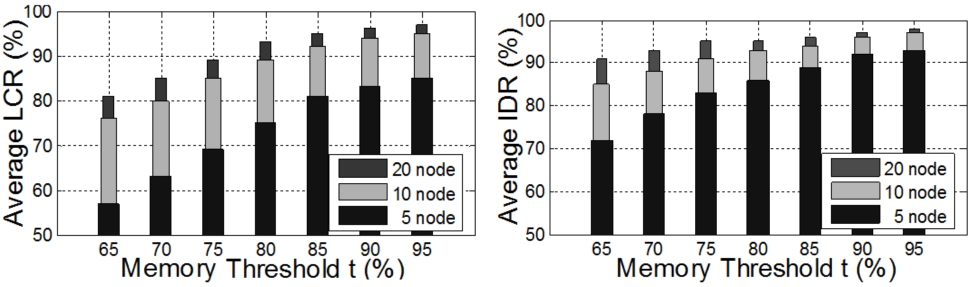
(1) EEMON deploys the same detection modules only on few nodes, and thus, it has a very low average IDR of Single-hop attacks and a lower average memory utilization; with memory threshold increasing, the average IDR of Multi-hop attacks can reach 70%.

(2) PRIDE deploys different detection modules only on the nodes which are along the traffic paths, and the average IDR of Single-hop attacks and average memory utilization are higher than EEMON, because the amount of its monitoring nodes is more than that in EEMON; with traffic path length increasing, the average IDR of Multi-hop attacks can reach 90%. However, the IDR maybe very low due to the network topology and traffic paths may change frequently in practical WMN.

(3) RCDID deploys detection modules on all nodes, and both average IDR and average memory utilization are higher than another two methods. The average IDR of Multi-hop attacks is very high due to that every link can be detected by multi-monitoring nodes.

3.4. **Impact of network density.** The performance of 10 and 20 nodes networks are measured by the above experiments, and in order to validate the impact on different network density, we additionally created a network model composed by 5 nodes. According to the theory of RCDID, network density does not affect the IDR of Single-hop attacks which is based on the local traffic, and therefore, we only consider the Multi-hop attacks. Experimental comparison results are shown in Figures 4(a) and 4(b).

The experimental results show that (1) in the same conditions, the larger network density is, the higher Link Coverage Rates are, and the higher Intrusion Detection Rates are; (2) the average IDR is over 90% when network density is more than 10 nodes and memory threshold is over 75%; (3) RCDID has a better adaptability in large scale networks.



(a)

(b)

Figure 4. The effect of network density: (a) average LCR; (b) average IDR

4. **Conclusions.** This paper proposed a Region-Coverage based Detection method for Resource-limited WMN. It is very appropriate for the large scale WMN which network topology and traffic paths change frequently. When the memory threshold exceeds 90%, there may cause a load imbalance problem due to that detection modules are selected randomly. Thus, improving the method of selecting detection modules for monitoring nodes will be our future work.

Acknowledgement. This work is partially supported by the National Natural Science Foundation of China (NSFC). We would like to thank NSFC and people for their supports.

REFERENCES

[1] Y. Liu, Q. Q. Ruan and Y. He, A survey on security of wireless mesh networks, *Information Security and Communications Privacy*, vol.36, no.1, pp.96-98, 2010.

[2] Z. Y. Xiang and Y. L. Chen, A survey on security technologies in wireless mesh network, *Information & Communications*, vol.28, no.7, pp.97-98, 2014.

[3] A. Hassanzadeh, Z. Xu, R. Stoleru et al., PRIDE: Practical intrusion detection in resource constrained wireless mesh networks, *Proc. of the 15th ICICS*, Beijing, China, vol.8233, pp.213-228, 2013.

[4] A. Chhetri, H. Nguyen, G. Scalosub et al., On quality of monitoring for multi-channel wireless infrastructure networks, *Proc. of the 11th ACM MobiHoc*, New York, United States, pp.111-120, 2010.

[5] M. Valero, S. S. Jung, A. S. Uluagac et al., Di-Sec: A distributed security framework for heterogeneous wireless sensor networks, *IEEE Conference on Computer Communications*, pp.585-593, 2012.

[6] D. Shin, S. Bagchi and C. Wang, Distributed online channel assignment toward optimal monitoring in multi-channel wireless networks, *IEEE Conference on Computer Communications*, pp.2626-2630, 2012.

[7] A. Hassanzadeh, R. Stoleru and B. Shihada, Energy efficient monitoring for intrusion detection in battery-powered wireless mesh networks, *Proc. of the 10th International Conference on Ad Hoc Networks and Wireless*, Paderborn, Germany, vol.6811, pp.44-57, 2011.

[8] A. Morais and A. Cavalli, A distributed and collaborative intrusion detection architecture for wireless mesh networks, *Mobile Networks and Applications-Springer*, vol.19, no.1, pp.101-120, 2014.

[9] D. Liu and G. Cao, Distributed monitoring and aggregation in wireless sensor networks, *IEEE Conference on Computer Communications*, pp.1-9, 2010.

[10] L. Niu, Y. B. Guo and W. Liu, Flow-based cross-layer anomaly detection method in wireless mesh networks, *Computer Engineering*, vol.38, no.22, pp.88-91, 2012.

[11] G. R. Hiertz, D. Denteneer, S. Max et al., IEEE802.11s: The WLAN mesh standard, *IEEE Conference on Wireless Communications*, vol.17, no.1, pp.104-111, 2010.

[12] W. C. Hao, *Study on Grouping and Mapping Algorithm of Snort Rules*, Bachelor Thesis, Xi'an University of Science and Technology, Xi'an, China, 2014.