한국항행학회 논문지 제14권 제1호 2010년 2월

크로스 층에서의 MANET을 이용한 IDS

An IDS in MANET with Cross Layer Concept

김상언*, 한승조*

Sang-Eun Kim*, Seung-Jo Han*

요 약

침입 탐지는 인터넷 보안에 반드시 필요한 구성 요소이다. 발전하고 있는 추세에 뒤지지 않고 따라가기 위해 싱글 레이어 탐지 기술을 멀티 레이어 탐지 기술에 적용 할 수 있는 방법이 필요하다. 다른 타입의 서비스 거부 공격(DoS)은 인가된 사용자의 네트워크 접근을 방해하므로 서비스 거부 공격의 취약한 점을 찾아 피해를 최소화 하기위해 노력했다. 우리는 악의적인 노드를 발견하기 위한 새로운 크로스 레이어 침입 탐지 아키텍처를 제안한다. 프로토콜 스텍에서 서로 다른 레이어를 가로지를 수 있는 정보는 탐색의 정확성을 향상시키기 위하여 제안하였다. 제안한 프로토콜의 아키텍처를 강화하기 위해 데어터 마이닝을 사용하여 조합과 분배의 변칙적인 침입탐지 시스템을 사용했다. 제안하고 있는 구조의 시뮬레이션은 OPNET 시뮬레이터를 사용하여 결과 분석을 하였다.

Abstract

Intrusion detection forms a vital component of internet security. To keep pace with the growing trends, there is a critical need to replace single layer detection technology with multi layer detection. Different types of Denial of Service (DoS) attacks thwart authorized users from gaining access to the networks and we tried to detect as well as alleviate some of those attacks. We have proposed a novel cross layer intrusion detection architecture to discover the malicious nodes. The information available across different layers of protocol stack are exploited in order to improve the accuracy of detection. We have used cooperative and distributive anomaly intrusion detection with data mining technique to enhance the proposed architecture. The simulation of the proposed architecture is done in OPNET simulator and the results are analyzed.

Key words : IDS, Cross Layer, DoS

I. Introduction

A wireless ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure. Nodes within each other's radio range communicate directly via wireless links, while those that are out of range use other nodes as relays or routers. In this type of scenarios, a malicious or compromised node can deny network services by dropping packets or by launching DoS attacks which affect the availability of the nodes significantly thereby disrupting the whole network. [1].

* 조선대학교 정보통신공학과 (Dept. of Information and Communication Engineering, Chosun University)

· 제1저자 (First Author) : 김상언 · 교신저자 (Corresponding author) : 한승조

· 투고일자 : 2009년 12월 23일

· 심사(수정)일자 : 2009년 12월 24일 (수정일자 : 2010년 2월 5일)

· 게재일자 : 2010년 2월 28일

Nodes usually share the same physical media; they transmit and acquire signals at the same frequency band, and follow the same hopping sequence or spreading code. The data-link-layer manages the wireless link resources and coordinates medium access among neighboring nodes.

It is difficult to identify intrusions in the networks as nodes may fail to provide services due to genuine reasons such as network congestion, link failure or topology changes, thus causing high false positive. DoS attacks could be launched at multiple layers of the protocol suite [1]. By detecting abnormal be haviours at different layers and using information across layers, we can detect malicious nodes with increasing accuracy. The attacks may be either collision attack where an adversary node can induce a collision in the wireless channel by transmitting when another node in its range is already in transmission or a packet drop attack which occurs at the network layer when the adversary node randomly drops the control/data packets and results in denial of service to the destination node. It may also be misdirection attack that occurs when the adversary node forwards the data packet to the wrong destination node.

Ⅱ. Cross layer Techniques in IDS

Adaptive cross layer techniques have been used for increased reliability. The selection of correct combination of layers in the design of cross layer IDS is very critical to detect attacks targeted at or sourced from any layers rapidly. It is optimal to incorporate MAC layer in the cross layer design for MANET IDS as DoS attack is better detected at this layer. The routing protocol layer and MAC layer is chosen for detecting routing attacks in an efficient way. Data with be havioural information consisting of layer specific information are collected from multiple layers and forward it to data analysis module which is located in an optimal location [2]. This cross layer technique leads to an escalating detection rate in the number of malicious behaviour of nodes increasing the true positive and reducing false positives in the MANET. Sometimes legitimate nodes can be detected as malicious node due to lack of energy resource or congested buffer. So, in order to detect the malicious nodes more accurately, energy and congestion conditions information from different layers need to be analysed utilizing cross layer techniques [1].

2-1 Cross Layer Architecture

Our proposed architecture is shown in fig1. Each and every node participates in intrusion detection independently and locally as well as participates with neighbouring nodes collaboratively for broader investigation if the local detection data is insufficient. Each IDS module investigates independently and monitors user and system activities as well as communication activities within its radio range. Cross layers interactions are incorporated including Intrusion Detection System providing low false alarm rates. Hence, MAC and routing layers would have to collaborate with each other in order to evade points of congestion and redirect traffic and utilizing IDS to keep away from insertion of malicious nodes in the new routes. The physical layer collects various types of communication activities including remote access and logons, user activities, data traffics and attack traces. MAC contains information regarding congestion and interference. The detection mechanism for misbehaving nodes interacts with routing layer for the detection process as MAC layers also help in detection of certain routing attacks. MAC also interacts with the physical layer to determine the quality of suggested path [3]. By combining cross layer features, attacks between the layers inconsistency can be detected. Furthermore, these schemes provide a comprehensive detection mechanism for all layers i.e attacks originating from any layers can be detected with better detection accuracy.

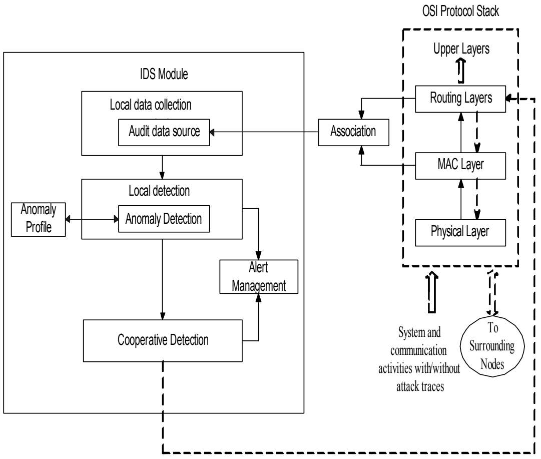


그림 1. 제안하는 구조
Fig. 1. Proposed Architecture

2-2 Association

Once association rules are extracted from multiple segments of a training data set, they are then aggregated into a rule set. The feature sets consist of control and data frames from MAC frames and control packets like Route Request, Route Reply and Route Error including data packets of IP packets from network layer. All the control packets are combined into one category as routing control packet and IP data packet as routing data packet. So, the payloads in MAC data frames contain either a routingCtrlPkt or routingDataPkt [4]. The characteristics are assorted based on dependency on time, traffic and other features and these features are correlated using a pre-defined correlation function [5]. An association rule is the form X→,c,s. Where X and Y are itemsets, and $X \cap Y = Ø$where s is the support and c is the confidence. Let D be database of traffic and the association rules have support and confidence greater than minimum support (minsup) and minimum confidence (minconf) respectively. The association rule is decomposed into itemsets and the rules. The itemsets with minimum supports are called frequent itemsets. In the Apriori algorithm, the contender itemsets to be counted in permission by using only the itemsets found frequently in the previous permission without considering the transactions in the database. The contender itemsets having k items can be generated by joining frequent itemsets having k-1 items, and removing those which contain any subset that is not frequent hence reducing the number of contender itemsets.

Ⅲ. IDS Module

The IDS module consists of four modules namely Local data collection, Local detection, Co-operative detection and alert management.

The local data collection module collects data streams of various information, traffic patterns and attack traces from network, MAC and physical layers via association module. The data streams can include system, user and mobile nodes' communication activities within the radio range. The audit data collects useful application data and system log files and monitors the events and computes time, traffic and other statistics and records the feature values.

The local detection module consists of anomaly detection engine. The local detection module analyzes the local data traces gathered by the local data collection module for evidence of anomalies. A normal anomaly profile is an aggregated rule set of multiple training data segments. New and updated detection rules across ad-hoc networks are obtained from anomaly profile. During testing process, normal and abnormal activities are processed and any deviations from the normal profiles are recorded. The anomaly detection distinguishes normalcy from anomalies as of the deviation data by comparing with the test data profiles with the expected normal profiles. If any detection rules deviate beyond a threshold interval and if it has a very high accuracy rate it can determine independently that the network is under attack and initiates the alert management.

When the support and confidence level is low or intrusion evidence is weak and inconclusive in the detecting node then it can make collaborative decision by gathering intelligence from its surrounding nodes via protected communication channel. The decision of cooperative detection is based on the majority of the voting of the received reports indicating an intrusion or anomaly. If the majority of the neighbouring nodes indicate that there is an anomaly then it concludes that the network is under attack.

The incoming traffics are analyzed by using a detector. If there are abnormal predictions than the normal predictions then it is regarded as "abnormal" and with adequate information an alarm is generated to inform than an intrusive activity is in the system. But we have to be careful about the false alarm rate. In order to reduce the false alarm rate we have to use the filters. Hence, repeated trials are needed before a good anomaly detection model is produced.

Ⅳ. Anomaly Detection mechanism

We try to detect the suspicious traffic in the network by identifying its behaviour from other normal traffic. The main objective is to collect set of useful features from the traffic to make the decision whether the sampled traffic is normal or abnormal. The process of anomaly detection comprises of two phases: training and testing. We try to build the basic framework for normal be haviourby collecting the noticeable characteristic from the audit data. We use the data mining technique for building Intrusion detection system to describe the anomaly detection mechanism.

In training phase, we have implemented fixed-width clustering algorithm as an approach to anomaly detection. It calculates how many points near each point in the feature space. In fixed width clustering technique, set of clusters are formed in which each cluster has fixed radius w also know as cluster width in the feature space [6]. The cluster width w is chosen as the maximum threshold radius of a cluster. For any pair of points x1 and x2, the distance between the two points "near" each other is less than or equal to w , $d(x1,x2) \leq w$ [7].

The fixed width algorithm is as follows:

```
Training samples ST = {si , i = 1,2······ NT }
where each sample has dimension d, si = <x1,·····, xd >

Initial set of clusters Ψ: = {}, the number of clusters C: =0

Normalizing ST,
For each training sample si Є ST
If C=0 then
Make new cluster ψ1 with centroid ψ1* from si
ψ1 :={ s1}, ψ1*: = si, Ψ: = {ψ1}, C= C+1
Else
Find the nearest cluster ψn to si
n :=argmink{Distance (si,ψ1*)}, where k=1······C
If distance to nearest cluster Distance (si, ψ1*) < w then
Add si to cluster ψn and update cluster centroid ψn*
        ψn:= { si } U ψn
Else
Make new cluster ψC+1 with centroid ψC+1* from si
ψC+1  := { si },
        ψC+1* := si ,
                Ψ: = {ψC+1} U Ψ,
                 C: = C+1
For each cluster ψk,
        Find the outermost point smax in cluster ψk
        smax  := argmini{Distance (si, ψk*)}, where si Є ψk
        Set width wk of cluster ψk
                wk :=  Distance (smax,ψk*)

Cluster Labeling:
        If |ψk |/NT < classification threshold τ then
Label ψk as anomalous
        Else
                Label ψk as normal.
```

The testing phase takes place by comparing each new traffic samples with the cluster set Ψ to determine the anonymity. The distance between a new traffic sample point s and each cluster centroid ψ1* is calculated. If the distance from the test point s to the centroid of its nearest cluster is less than cluster width parameter w, then the traffic sample shares the label as either normal or anomalous of its nearest cluster. If the distance from s to the nearest cluster is greater than w, then s lies in a sparse region of the feature space, and is labelled as anomalous.

Ⅴ. Simulation

The simulation is done in OPNET simulator in windows XP machine [8].The experimental set up consists of 12 similar wireless mobile nodes stations. All the nodes use AODV as a routing protocol within the area of 600m x 600m campus network. AODV protocol is a suitable approach for mobile networks due to low message overhead. The simulation is run for 320 seconds. The simulation statistic is shown in table 1.

표 1. 시뮬레이션 파라미터
Table 1. Simulation Parameter.

Statistics	Values
Scenario size	600mX600m
802.11b data rate	11 Mbps
Transmission Range	<250 meter
Power of each node	0.005 W
Simulation Time	320 seconds
No. of mobile nodes	12
Mobility	Random way point, random direction mobility

We have used custom application with a streaming multimedia of packet size 1024 which starts at around 20 sec. During simulation UDP data traffic is sent in bytes/sec by the source node to the destination node. We have used mobility configuration module for defining random way point and random direction mobility to the mobile nodes. In case of random way point mobility algorithm, the nodes choose a random position to move towards a new position with uniform distributed movement speed. The nodes wait there for certain time and again selects a new destination. Where as in case of random direction, nodes select a uniform direction and speed until it reaches the boarder of the scenario; wait there for certain time and select a uniform direction and speed. The mobility causes the network topology to be highly dynamic as a result the detectors should have up to date evidence to detect attacks with low false positive and negative rates.

The node model of our proposed IDS is shown in fig 3. The existing node model is modified at its IP layer and MAC layer for capturing the incoming and outgoing traffics for detecting intrusive activities as the IDS checks the payload of the traffics [9]. The added modules are packet capture, association and IDS specification. The packet capture model capture traffic from IP and MAC layer and filters out UDP packets and send them to association model.

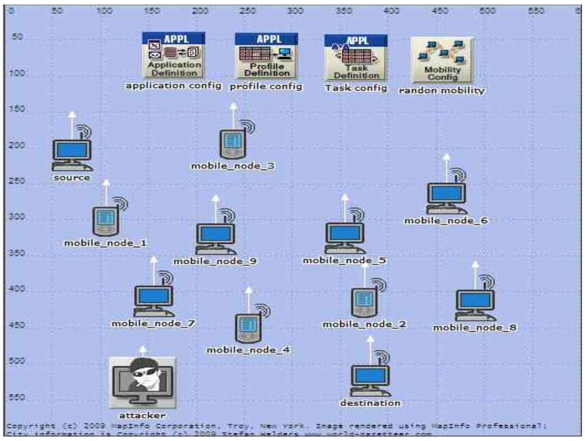
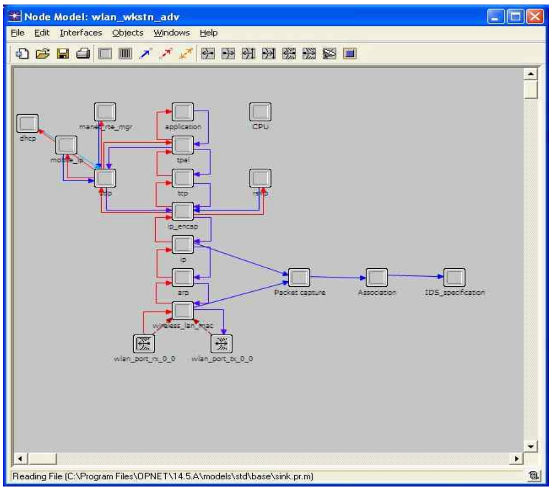


그림 2. 시뮬레이션 시나리오
Fig. 2. Simulation Scenario

The packet format and contents are checked by de-capsulating the payload and required UDP segments and port number are extracted from it. Then, the packet is send to association model where the common control packets and data packets from MAC and network layer are combined into one category as either routing control packets or routing data packets using correlated features. The packet is then sent to the IDS module for evaluating and verifying the Intrusion Detection. The IDS module consists of set of predefined detection rules and algorithms for detecting anomalous behaviour. The normal traffic behaviour is recorded as a profile in anomaly profile. When packets arrive in this module, a stream of interrupts is issued and the packet is processed for intrusion detection.



Reading File (C:\Program Files\OPNET\14.5.A\models\std\base\sink.pr.m)

그림 3. 노드 모델
Fig. 3. Node model

Ⅵ. Evaluation Results

We have used AODV routing protocol in 12 mobile nodes and implemented random mobility using mobility configuration. For evaluation purpose we mostly consider source, destination, attacker node and other nodes assists in routing of the packets and have their own purpose. In fig. 4 we can see the streaming multimedia UDP data traffic sent by the source to the destination node along with the anomalous traffic. The source node sends the data traffic at around 20 second which is almost a consistent UDP data traffic indicated by last line. The attacker starts to send the custom anomalous unidirectional traffic to the same destination node at around 180 seconds. This anomalous traffic consists of high request count and tries to flood the normal traffic at the destination node. The destination node receives the normal multimedia traffic from 20 seconds but at around 180 seconds it receives abnormal data traffic till the end of the simulation. These data traffic are collected by packet capture model and then sent to IDS specification where the data traffics are compared with the normal behaviour of the normal profile.

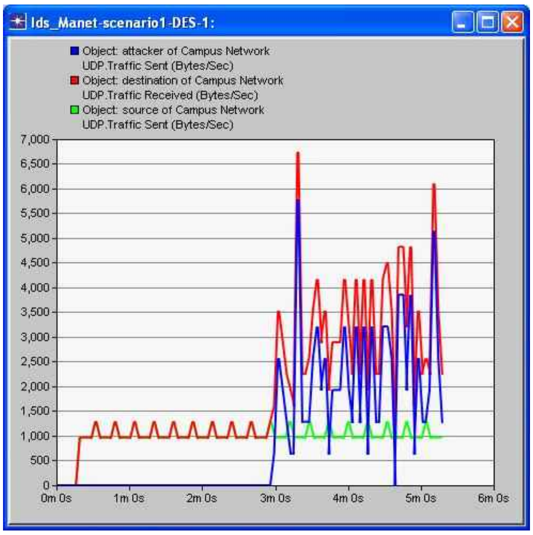


그림 4. 수신 노드의 UDP 트래픽 분석
Fig. 4. UDP traffic analysis in destination node

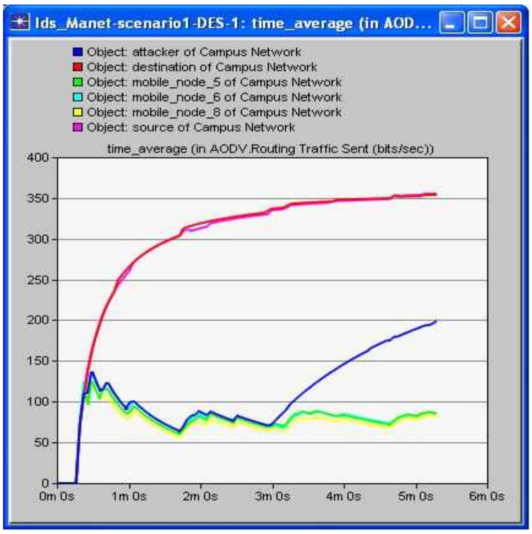


그림 5. AODV라우팅에서 전송하는 트레픽의 시간적 평균
Fig. 5. Time-average in AODV routing traffic sent

If any deviation is found from the normal behaviour then an anomaly is detected and an alarm is generated if the anomaly is of intrusive behaviour. In our case, an anomaly is detected and IDS treats this anomalous activity as an intrusive activity.

Fig. 5 shows the time-average in AODV routing traffic sent in bits/sec at source, attacker, destination and other mobile nodes. The source, destination and other intermediate nodes are in random way point mobility as assigned by the mobility configuration module. The transmission of data starts at 20 seconds. The time-average AODV routing traffic sent of source and destination is higher than other nodes because of continuous RREQ, RREP and Hello messages between the two nodes while transferring the UDP traffic. The traffic of other mobile nodes is due to RREQ and Hello messages. Also the attacker node starts to send anomalous traffic to the destination node at around 3 minute so there is sudden raise in the routing traffic as it is sending RREQ and RREP messages.

Ⅶ. Conclusion

Hence, we have implemented the proposed architecture and done the simulation and analyzed the result. Our proposed cross-layer based intrusion detection architecture is designed to detect DoS attacks at different layers of the protocol stack. Since, a single data detection module is presented which collects and analyze the data that are collected from data collection module, the data analysis overhead as well as the energy consumption is reduced. Also, cross layer detection confirms the misbehaviour caused by malicious node in the network, thus reducing the false positive rates and hence enhanced the accuracy in detecting attacks.

Future work will involve research into more robust and intelligent IDS system which includes further analysis of the simulation results of our proposed cross layer architecture with richer semantic information.

감사의 글

본 지식재산권은 지식경제부 및 정보통신산업진흥원의 지원을 받아 수행된 연구결과임

(09-기반, 산업원천기술개발사업)

This work was supported in part by MIKE & NIPA

참 고 문 헌

[1] Thamilarasu, G., et al. "A cross-layer based intrusion detection approach for wireless ad hoc networks", *Mobile Ad hoc and Sensor Systems Conference*, 2005. IEEE International Conference on 2005

[2] C. J. John Felix, A. Das, B.-C. Seet, and B.-S. Lee, "Cross Layer versus Single Layer Approaches for Intrusion Detection in MANET", *IEEE International Conference on Networks 2007 (ICON 2007)*, Nov 2007

[3] J. S. Baras and S. Radosavac, "Attacks and Defenses Utilizing Cross-Layer Interactions in MANET" , *Workshop on Cross-Layer Issues in theDesign of Tactical Mobile Ad Hoc Wireless Networks: Integration of Communication and Networking Functions to Support Optimal Information Management*, June 2–3, 2004, Naval Research Laboratory, Washington, DC

[4] Y. Liu, Y. Li, and H. Man, "Short paper: A distributed cross-layer intrusion detection system for ad hoc networks", *In Proc. IEEE/Create Net the First International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm 2005),* pages 418-420, September 2005

[5] C. J. John Felix, A. Das, B.-C. Seet, and B.-S. Lee, “CRADS: Integrated Cross Layer Approach for Detecting Routing Attacks in MANETs", *IEEE Wireless Communications and Networking Conference (WCNC), Las Vegas, CA, USA*, March 2008.

[6] C. Loo, M. Ng, C. Leckie and M. Palaniswami. Intrusion Detection for Routing attacks in Sensor Networks. In International Journal of Distributed Sensor Networks, october-December 2006,2(4): 313-332

[7] Eskin, E., Arnold, A., Prerau, M., Portnoy, L., Stolfo, S.: A geometric framework for unsupervised anomaly detection: detecting intrusions in unlabeled data. In: Applications of Data Mining in Computer Security. Kluwer (2002) and J. Oldmeadow, S. Ravinutala and C. Leckie, "Adaptive Clustering for Network Intrusion Detection."*In Proceedings of the Third International Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD 2004)*, May 2004, pp. 255-259

[8] OPNET modeler, http://www.opnet.com/

[9] T. Phit and K. Abe, "Protocol Specification-based Intrusion Detection System for VoIP," *Technical Report of IEICE*, 2008

김 상 언 (金 相 言)

2006년 : 조선대학교 전자공학과(학사)
2008년 : 조선대학교 정보통신공학과(공학석사)
1990년 : 성실데이타통신(주) 통신망 운영담당
1992년 : 케이디씨정보통신(주) 통신망 운영 담당
1993년 : (주)LG데이콤 입사 및 통신망 운용 담당
2008년 ~ 현재 : (주)LG데이콤 마케팅 업무 담당 (직급:과장(S급)) 재직중
관심분야 : 통신보안시스템, S/W 불법복제 방지시스템

한 승 조 (Seung-jo Han)

1980년 : 조선대학교 전자공학과(학사)
1982년 : 조선대학교 전자공학과(공학석사)
1994년 : 충북대학교 전자계산학과 (박사)
1986년 6월~1987년 3월 : 뉴올리언즈대학 객원교수
1995년 2월~1996년 1월 : 택사스대학 객원교수
2000년 12월~2002년 3월 : 버클리대학 객원교수
1998년 3월~현재 : 조선대학교 전자정보통신공학부 교수
관심분야 : 통신보안시스템설계, S/W 불법복제 방지시스템, ASIC