

## A Novel Cross Layer Intrusion Detection System in MANET

Rakesh Shrestha, Kyong-Heon Han, Dong-You Choi, Seung-Jo Han\*

Department of Information & Communication Engg.

Chosun University

Gwangju, South Korea

rakez\_shre@hotmail.com, newromeo12@naver.com, dychoi, sjbhan}@chosun.ac.kr

\*Corresponding Author

**Abstract**— Intrusion detection System 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. In this paper, we have proposed a novel cross layer intrusion detection architecture to discover the malicious nodes and different types of DoS attacks by exploiting the information available across different layers of protocol stack in order to improve the accuracy of detection. We have used cooperative anomaly intrusion detection with data mining technique to enhance the proposed architecture. We have implemented fixed width clustering algorithm for efficient detection of the anomalies in the MANET traffic and also generated different types of attacks in the network. The simulation of the proposed architecture is performed in OPNET simulator and we got the result as we expected.

**Keywords**- MANET; AODV; DoS; IDS; Cross layer

### I. INTRODUCTION

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. 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. The medium access control (MAC) protocol allows mobile nodes to share a common broadcast channel. The network-layer holds the multi-hop communication paths across the network. All nodes must function as routers that discover and maintain routes to other nodes in the network.

It is difficult for Intrusion Detection system (IDS) to fully detect routing attacks due to MANET’s characteristics. So, the IDS needs a scalable architecture to collect sufficient evidences to detect those attacks effectively. A malicious node may take advantages of the MANET node to launch routing attacks as the node acts as router to communicate with each other. The wireless links between the nodes along

with the mobility raises the challenges of IDS to detect the attacks. Hence, we are motivated to design a new IDS architecture which involves cross layer design to efficiently detect the abnormalities in the wireless networks. We have proposed a new intrusion detection architecture which incorporates cross layer that interacts between the layers. In addition to this we have used association module to link between the OSI protocol stack and the IDS module which results in low overhead during the data collection. We have implemented the fixed width clustering algorithm in anomaly detection engine for efficient detection of intrusion in the ad-hoc networks. The rest of the paper is organized as follows. The related work is presented in section II. Section III gives brief description about cross layer techniques in IDS followed by association module in section IV. In Section V, a detailed description of intrusion detection module and its underlying architecture is dealt. The anomaly detection mechanism used in MANET is discussed in section VI. Section VII is dedicated on the performance evaluation under which the simulation scenario and evaluation of results are presented for the verification of the proposed architecture. Finally, section VIII concludes the carried out research and possible future works..

### II. RELATED WORKS

A lot of studies have been done on security prevention measures for infrastructure-based wireless networks but few works has been done on the prospect of intrusion detection [1]. Some general approach has been used in a distributed manner to insure the authenticity and integrity of routing information such as key generation and management on the prevention side. Authentication based approaches are used to secure the integrity and the authenticity of routing messages such as [2], [3]. There are some difficulties that have to be faced in realizing some of the schemes like cryptography and they are relatively expensive on MANET because of computational capacity. A number of intrusion detection schemes for intrusion detection system have been presented for ad-hoc networks. In [4], the paper proposed architecture for a distributed and cooperative intrusion detection system for ad-hoc networks based on statistical anomaly detection techniques but they have not properly mentioned about the simulation scenario and the type of mobility they have used. In [5], A. Mishra emphasizes the challenge for intrusion detection in ad-hoc network and purpose the use of anomaly

detection, but do not provide a detailed solution or implementation for the problem. In [6], Huang details an anomaly detection technique that explores the correlations among the features of nodes and discusses about the routing anomalies. Loo [7] presents an intrusion detection method using a clustering algorithm for routing attacks in sensor networks. It is able to detect three important types of routing attacks. They are able to detect sink hole attacks effectively which are intense form of attack. There are some flaws like there is absence of simulation platform that can support a wider variety of attacks on larger scale networks. Fixed width clustering algorithm has shown to be highly effective for anomaly detection in network intrusion [8]. It presents a geometric framework for unsupervised anomaly detection. This paper needs more feature maps over different kinds of data and needs to perform more extensive experiments evaluating the methods presented.

### III. CROSS LAYER TECHNIQUES IN IDS

In compared to wired networks, MANET has to face different challenges due to its wireless features and ad-hoc structure. The very advantage of mobility in MANET leads to its vulnerabilities. For efficient intrusion detection, we have used cross layer techniques in IDS. The traditional way of layering network approach with the purpose of separating routing, scheduling, rate and power control is not efficient for ad-hoc wireless networks. A. Goldsmith discussed that rate control, power control; medium access and routing are building block of wireless network design [9]. Generally, routing is considered in a routing layer and medium access in MAC layer whereas power control and rate control are sometimes considered in a PHY and sometimes in a MAC layer. If there is no cross layer inter action then the routing can select between several routes and have no information about congestion or malicious nodes. As a result, it selects a congested route or it selects a route that includes malicious nodes. With the help of cross layer interaction, the routing forwards possible route choices to MAC and MAC decides the possible routes using congestion and IDS information as well as returns the result to the routing.

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 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 behavioral 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 [10]. This cross layer technique incorporating IDS leads to an escalating detection rate in the number of malicious behavior of nodes increasing the true positive and reducing false positives in the MANET. It also alleviates the congestion which can adapt to changing network and traffic characteristics. In order to evade congestion and reroute traffic, MAC and routing layers have to cooperate with each other with the IDS in order to avoid 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 [11]. By combining cross layer features, attacks between the layers inconsistency can be detected. Furthermore, these schemes provide a comprehensive detection mechanism for all the layers i.e attacks originating from any layers can be detected with better detection accuracy.

### IV. ASSOCIATION MODULE

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 RREQ, RREP and RERR 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 routing CtrlPkt or routing DataPkt [12]. The feature set is foreshortened by associating one or more features from different layers to specific MAC layer feature so that the overhead of learning is minimized. The characteristics are assorted based on dependency on time, traffic and other features [13].

Our association rule is of the form  $X \rightarrow Y, c, s$ . Where  $X$  and  $Y$  are itemsets, and  $X \cap Y = \emptyset$  S-support (XUY) is the  $\frac{\text{sup}(X \cup Y)}{\text{sup}(X)}$  is 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 [14]. Support and confidence are generally used to measure the relevance of the association rules. 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 is agreed 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. Let  $F_k$  be the set of frequent  $k$ -itemsets having minimum support and  $C_k$  be the set of contender  $k$ -itemsets with potentially frequent itemsets and  $E$  be the events. Each of these itemsets has itemset and support count fields. The initial pass of the algorithm simply counts item occurrence to determine the frequent 1-itemsets. A succeeding pass  $k$  consists of two phases. The first phase consists of frequent itemsets  $F_{k-1}$  found in the  $(k-1)$ th permission that are used to generate the candidate itemsets  $C_k$ . In the other phase, the database is scanned and the support of candidates in  $C_k$  is counted.

The apriori algorithm is given below:

```

Fk := {frequent 1-itemsets};
k := 2; // k is the permission number
while (Fk-1 ≠ ∅) do begin
  Ck: =New contender of size k generated from Fk-1;
  forall transactions E ∈ D do begin
    Increment the count of all contenders in Ck that are
    contained in E.
  end
  Fk: = All contenders in Ck with minimum support.
  k := k+1;
end

```

The Apriori Contender Generation algorithm is as follows:

Given F<sub>k-1</sub>, the set of all frequent (k-1)-itemsets, the algorithm returns a superset of the set of all frequent k-itemsets. F<sub>k-1</sub> and F<sub>k-1</sub> are joined in the join step:

```

insert into Ck
select p.item1, p.item2, ..., p.itemk-1, q.itemk-1
from Fk-1 p, Fk-1 q
where p.item1 = q.item1, ..., p.itemk-2 = q.itemk-2, p.itemk-1 <
q.itemk-1;
Next in the prune step, remove all the itemsets c ∈ Ck such that
some (k-1)-subset of c is not in Fk-1:
for all itemsets c ∈ Ck do
  forall (k-1)- subsets s of c do
    if (s ∉ Fk-1) then
      delete c from Ck ;

```

Any subset of a frequent itemset has minimum support. The join step extends F<sub>k-1</sub> with each item in the database and deletes those itemsets for which the (k-1) - itemset obtained by deleting the (k-1)th item is not in F<sub>k-1</sub>. The condition p.item<sub>k-1</sub> < q.item<sub>k-1</sub> ensures that no duplicates are generated. Hence, after join step, C<sub>k</sub> ⊇ F<sub>k</sub>. Also, the prune step where all itemsets of C<sub>k</sub> are deleted whose (k-1)-subsets are not in F<sub>k-1</sub>, does not delete any itemset that could be in F<sub>k</sub>.

#### Basic algorithm for rule:

We find all non-empty subsets of f to generate rules for every frequent itemset f. For every subset a, we output a rule of the form a ⇒ (f-a) if the ratio of support (f) to support (a) is atleast minconf. All subsets of f are considered to generate rules with multiple consequents.

A simple rule algorithm is as follows:

```

forall frequent itemsets fk, k ≥ 2 do
  call genrules (fk, fk);
// The genrules generates all valid rules ā ⇒ (fk- ā), for all ā ⊂ am
procedure genrules (fk: frequent k-itemset, am: frequent m-itemset)
A := {(m-1)-itemsets am-1 | am-1 ⊂ am};
forall am-1 ∈ A do begin
  conf := support (fk)/support (am-1);
  if (conf ≥ minconf) then begin
    output the rule am-1 ⇒ (fk- am-1), with confidence=conf
    and support=support (fk);
    if (m-1 > 1) then
      call genrules (fk, am-1); // to generate rules with subsets of am-1
      // as the antecedents
    end
  end

```

## V. INTRUSION DETECTION MODULE

We have used data mining techniques in Intrusion detection module in order to improve the efficiency and effectiveness of the MANET nodes. With our studies, we have found out that among all the data mining intrusion detection techniques, clustering-based intrusion detection is the most potential one because of its ability to detect new attacks. Many traditional intrusion detection techniques are limited with collection of training data from real networks and manually labeled as normal or abnormal. It is very time consuming and expensive to manually collect pure normal data and classify data in wireless networks. [15].

We have used association algorithm such as Apriori which can be utilized to achieve traffic features which is then followed by clustering algorithm. In [15], it states that a good efficiency and performance is obtained with association algorithm and clustering algorithm. The association rule and clustering are used as the root for accompanying anomaly detection of routing and other attacks in MANET. Our proposed IDS architecture is shown in fig. 1 and the IDS module is described below [16].

### A. Local Data Collection

The local data collection module collects data streams of various information, traffic patterns and attack traces from physical, MAC and network layers via association module. The data streams can include system, user and mobile nodes' communication activities within the radio range.

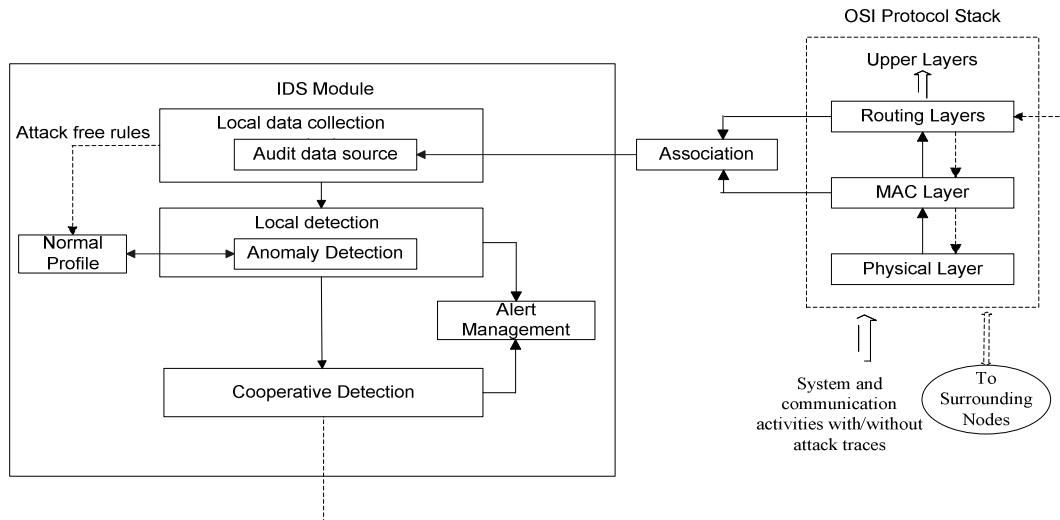


Figure 1. Proposed IDS Architecture in MANET

### B. Local Detection

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 profile is an aggregated rule set of multiple training data segments. New and updated detection rules across ad-hoc networks are obtained from normal profile. The normal profile consists of normal behavior patterns that are computed using trace data from a training process where all activities are normal. 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.

### C. Cooperative Detection

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.

### D. Alert Management

The alert management receives the alert from the local detection or co-operative detection depending on the strength of intrusion evidence. It collects them in the alert cache for  $t$  seconds. If there are more abnormal predictions than the normal predictions then it is regarded as “abnormal” and

with adequate information an alarm is generated to inform that an intrusive activity is in the system.

## VI. ANOMALY DETECTION MECHANISM IN MANET

The anomaly detection system creates a normal base line profile of the normal activities of the network traffic activity. Then, the activity that diverges from the baseline is treated as a possible intrusion. 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. Some of the advantages of anomaly detection system are it can detect new and unknown attacks, it can detect insider attacks; and it is very difficult for the attacker to carry out the attacks without setting off an alarm [17]. The process of anomaly detection comprises of two phases: training and testing. We try to build the basic framework for normal behavior by 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.

### A. Construction of normal Dataset

The data obtained from the audit data sources mostly contains local routing information, data and control information from MAC and routing layers along with other traffic statistics. The training of data may entail modeling the allotment of a given set of training points or characteristic network traffic samples. We have to make few assumptions so that the traced traffic from the network contains no attack traffic [18]:

- The normal traffic occurs more frequently than the attack traffic.
- The attack traffic samples are statistically different from the normal connections.

Since, we have used two assumptions; the attacks will appear as outliers in the feature space resulting in detection

of the attacks by analyzing and identifying anomalies in the data set.

### B. Feature construction

For feature construction, we use an unsupervised method to construct the feature set. We use clustering algorithm to construct features from the audit data. The feature set is created by using the audit data and most common feature set are selected as essential feature set which has weight not smaller than the minimum threshold. A set of considerable features should be obtained from the incoming traffic that differentiates the normal data from the intrusive data. Few and semantic information is captured which results in better detection performance and saves computation time. In case of feature construction, we collect the traffic related features as well as non-traffic related features which represents routing conditions. We use some of the features for detecting DoS attacks and attacks that manipulate routing protocol. The number of data packets received is used to detect unusual level of data traffic which may indicate a DoS attack based on a data traffic flood.

### C. Training normal data using cluster mechanism

We have implemented fixed-width clustering algorithm as an approach to anomaly detection. It calculates the number of 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 known as cluster width in the feature space [19]. The cluster width  $w$  is chosen as the maximum threshold radius of a cluster.

#### Explanation of the Fixed width algorithm:

A set of network traffic sample  $S_T$  are obtained from the audit data for training purpose. Each sample  $s_i$  in the training set is represented by a  $d$ -dimensional vector of attributes. In the beginning, the set of clusters as well as the number of clusters are null.

Since, there is significant variation in each attribute. While calculating the distance between points, normalization is done before mapping into the feature space to ensure that all features have the same outcome. It is obtained by normalizing each continuous attribute in terms of the number of standard deviations from the mean. The first point of the data forms the centre of the new cluster. A new cluster  $\psi_1$  is formed having centroid  $\psi_1^*$  from sample  $s_i$ . For every succeeding point, we measure the distance of each traffic sample  $s_i$  to the centroid of each cluster  $\psi_1^*$  that has been generated by the cluster set  $\Psi$ . If the distance to the nearest cluster  $\psi_n$  is within  $w$  of cluster center, then the point is assigned to the cluster, and the centroid of the closest cluster is updated. The total number of points in the cluster is incremented. Else, the new point forms the centroid of a new cluster. Euclidean distance as well as argmin is used because it is more convenient to have items which minimizes the functions. As a result, the computational load is decreased. Moreover, the traffic samples are not stored and only one pass is required through the traffic samples. In the final stage of training, labeling of cluster is done based on the initial

assumptions like ratio of the normal traffic is very small than attack traffic and the anomalous data points are statistically different to normal data points. If the cluster contains less than a threshold  $\tau$  % of the total set of points then it is considered as anomalous. Otherwise the clusters are labeled as normal. Besides, the points in the dense regions will be higher than the threshold; we only consider the points that are outliers.

Algorithm:

Training samples  $S_T = \{s_i, i = 1, 2, \dots, N_T\}$   
 where each sample has dimension  $d$ ,  $s_i = \langle x_{i1}, \dots, x_{id} \rangle$

Initial set of clusters  $\Psi = \{\}$ , the number of clusters  $C = 0$

Normalizing  $S_T$ ,

For each training sample  $s_i \in S_T$

**If**  $C=0$  then

Make new cluster  $\psi_1$  with centroid  $\psi_1^*$  from  $s_i$   
 $\psi_1 := \{s_i\}, \psi_1^* := s_i, \Psi = \{\psi_1\}, C = C+1$

**Else**

Find the nearest cluster  $\psi_n$  to  $s_i$   
 $n := \text{argmin}_k \{\text{Distance}(s_i, \psi_k^*)\}, \text{ where } k=1, \dots, C$

**If** distance to nearest cluster  $\text{Distance}(s_i, \psi_n^*) < w$  then  
 Add  $s_i$  to cluster  $\psi_n$  and update cluster centroid  $\psi_n^*$   
 $\psi_n := \{s_i\} \cup \psi_n$

**Else**

Make new cluster  $\psi_{C+1}$  with centroid  $\psi_{C+1}^*$  from  $s_i$   
 $\psi_{C+1} := \{s_i\},$   
 $\psi_{C+1}^* := s_i,$   
 $\Psi = \{\psi_{C+1}\} \cup \Psi,$   
 $C = C+1$

For each cluster  $\psi_k$ ,

Find the outermost point  $s_{\max}$  in cluster  $\psi_k$

$s_{\max} := \text{argmin}_i \{\text{Distance}(s_i, \psi_k^*)\}, \text{ where } s_i \in \psi_k \text{ and } i=1, \dots, N_T$

Set width  $w_k$  of cluster  $\psi_k$

$w_k := \text{Distance}(s_{\max}, \psi_k^*)$

Cluster Labeling:

**If**  $|\psi_k|/N_T < \text{classification threshold } \tau$  then  
 Label  $\psi_k$  as anomalous

**Else**

Label  $\psi_k$  as normal

### D. Testing Phase

The testing phase takes place by comparing each new traffic samples with the cluster set  $\Psi$  to determine the anonymity. The distance between a new traffic sample point  $s_i$  and each cluster centroid  $\psi_1^*$  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 less dense region of the feature space, and is labeled as anomalous.

While comparing our IDS module with [13], it has complexity of the system due to non linear pattern recognition where as the proposed IDS is simple using association rule to comply with the anomaly profiling. Similarly, [11] has message overhead as a result it consumes more power resulting battery constrains while the proposed IDS consumes low energy by adopting association rule.

## VII. PERFORMANCE EVALUATION

### A. Simulation Setup

The simulation is carried out in OPNET simulator in windows XP machine [20]. The experimental set up consists of 20 similar wireless mobile nodes stations with one attack node. 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. We have used custom application with a streaming multimedia of packet size 1024 which starts at around 20 sec. We have used UDP traffic as underlying transport protocols. During simulation UDP data traffic is sent in bytes/sec by the source node to the destination node as well as the attack traffic has been implemented to disrupt the normal data traffic. We have used UDP flooding attack along with the normal traffic in this scenario. We have used mobility configuration module for defining random way point and random direction mobility to the mobile nodes. 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. These settings are typical ad-hoc settings with adequate mobility and data load overhead and they are used in all our experiments. We run two simulations, one without the attacker node and other including the attacker node. We use one running trace of normal data as training set. For evaluation purposes, we use several other traces with normal data only and few traces composed with different types of attacks. The existing node model is modified at its IP layer and MAC layer for capturing the incoming and outgoing traffics for detecting intrusive activities because the IDS checks the payload of the traffics [21].

TABLE I. SIMULATION STATISTICS

Statistics	Value
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	21
Mobility	Random waypoint, random direction mobility

The association model combines the common control packets and data packets from MAC and network layer into one category as either routing control packets or routing data packets using association rules. The packet is then sent to the IDS module for evaluating and verifying the Intrusion Detection. The IDS module consists of fixed width algorithm for detecting anomalous behavior. The normal traffic behavior is recorded as a profile in normal profile. When packets arrive in this module, a stream of interrupts is issued and the packet is processed for intrusion detection.

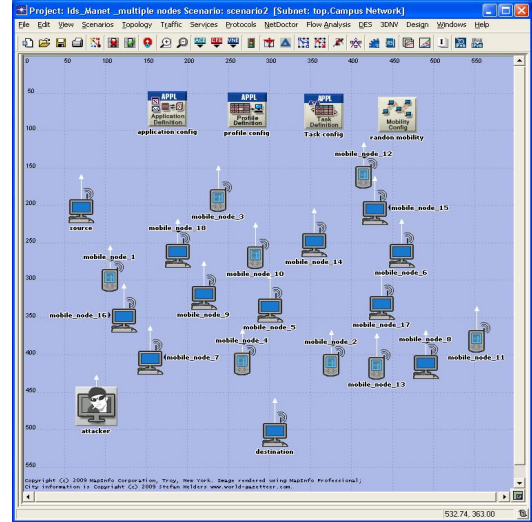


Figure 2. Simulation scenario

### B. Evaluation of results

Several evaluation methods have been proposed but there is no globally acceptable standard or metrics for evaluating an intrusion detection system [17]. In our case, we have used AODV routing protocol in 21 mobile nodes and implemented random mobility using mobility configuration. For evaluation purpose, we mostly consider source, destination and attacker node whereas other nodes assist in routing of the packets and have their own purpose. During the training phase, the attacker node is disabled so that the normal traffic can be trained without any interference.

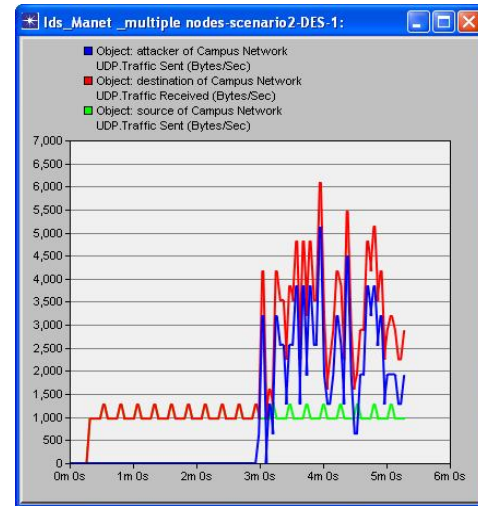


Figure 3. UDP traffic analysis in destination node

In the fig. 3, 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 seconds which is almost a consistent UDP data traffic indicated by green color. The attacker starts to send the custom anomalous unidirectional traffic to the

same destination node at around 3 minutes. 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 3 minutes it receives abnormal data traffic till the end of the simulation. These data traffic are collected and then sent to IDS specification where the data traffics are compared with the normal behavior of the normal profile. If the traffic samples at the destination does not match with the normal traffic generated by the fixed width algorithm and lies in the sparse region then an irregularity is detected. If any deviation is found from the normal behavior then an anomaly is observed and an alarm is generated indicating intrusive behavior. In our case, an anomaly is detected and IDS treats this anomalous activity as an intrusive activity.

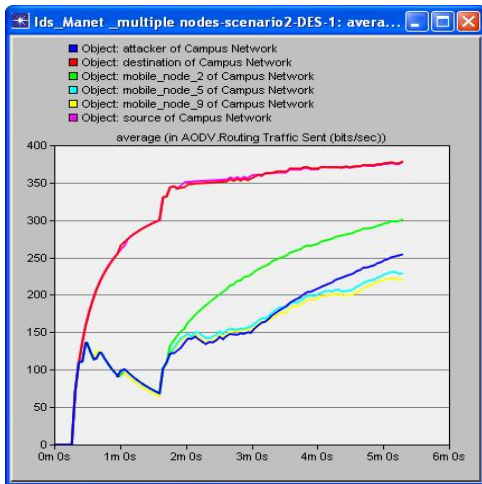


Figure 4. Time-average in AODV routing traffic sent

Fig. 4 shows the time-average in AODV routing traffic sent in bits/sec at source, attacker, destination and other mobile nodes. 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 sink hole attack causes artificial routes resulting other nodes to request route and a route request message is sent to the receiving node despite of the already existed path. So, there is increase in routing traffic in destination of campus node. Also, the attacker node starts to send anomalous traffic to the destination node at around 3 minutes so there is sudden raise in the routing traffic due to RREQ and RREP messages.

In the fig. 5, during the testing process, we can see the abnormal behavior in the wireless data traffic received after 3 minutes interval time. The simulation is run in two scenarios, one with attacker node and other without the attacker node. The red color shows the data traffic without the attacker node while the blue one is in the presence of the attacker node. In this case, there is a deviation between the normal and abnormal traffic in the destination node and the anomalous traffic is regarded as malicious behavior so an alarm is generated.

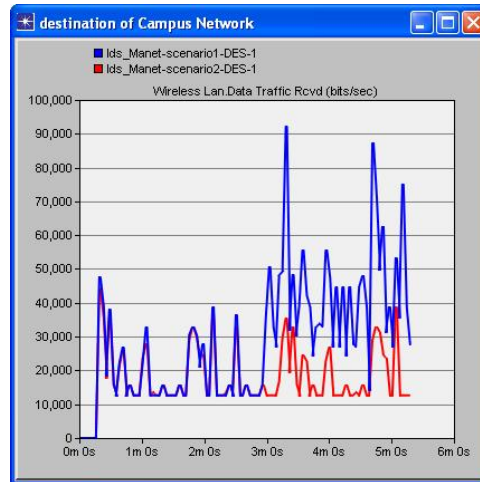


Figure 5. Wireless LAN Data Traffic Received in bits/sec

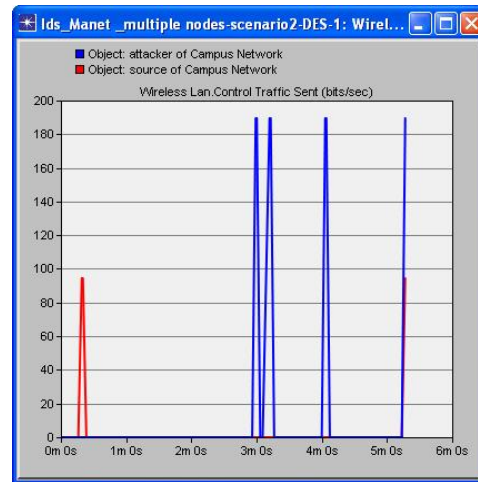


Figure 6. Wireless LAN Control traffic (bits/sec)

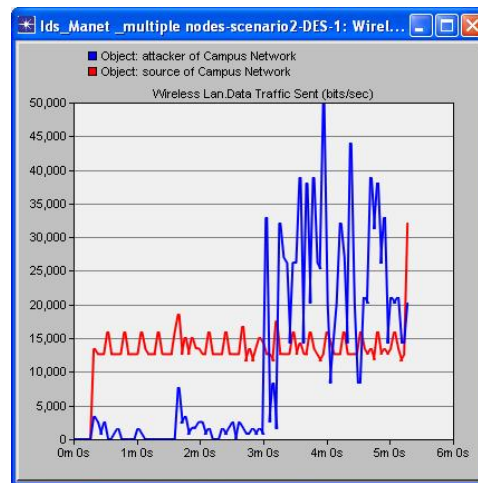


Figure 7. Wireless LAN Data traffic (bits/sec)

We have also captured the wireless LAN control and data traffic in bits/sec which are shown in fig. 6 and fig. 7. The

captured Control and data traffic of the attacker and the source are different from each other. The normal traffic occurs more frequently than the attacker traffic as well as the nature of the attacker traffic is statistically different. So, the anomaly technique can distinguish the normal behavior from the anomaly behavior by utilizing the fixed width clustering algorithm.

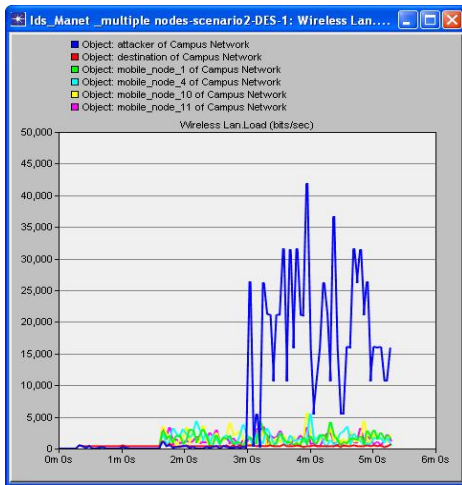


Figure 8. Wireless LAN load (bits/sec) on random nodes

While analyzing the load on different nodes in our scenario, we found that the load of the attacker node is higher than any other nodes. It is due to the fact that the attacker node is sending UDP flooding attack to towards the destination node.

### VIII. CONCLUSIONS AND FUTURE WORK

Hence, a better intrusion detection mechanism based on anomaly detection is presented in this paper utilizing cluster data mining technique. We have implemented the proposed architecture with fixed width algorithm and done the simulation and analyzed the result. Our proposed cross-layer based intrusion detection architecture is designed to detect DoS attacks and sink hole attack at different layers of the protocol stack. We are able to detect various types of UDP flooding attack and sink hole attack in an efficient way.

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

### REFERENCES

[1] S. Jacobs, S. Glass, T. Hiller, and C. Perkins, "Mobile IP authentication, authorization, and accounting requirements," Request for Comments 2977, Internet Engineering Task Force, October 2000.

[2] K. Sanzgiri, B. Dahill, B.N. Levine, E.B. Royer, and C. Shields, "A Secure Routing Protocol for Ad-hoc Networks," in the Proceedings of International Conference on Network Protocols (ICNP), 2002.

[3] Yih-Chun Hu, Adrian Perrig, and David Johnson. Ariadne: "A Secure On- Demand Routing Protocol for Ad Hoc Networks," in the Proceedings of MobiCom, 2002.

[4] Y. Zhang, W. Lee, and Y.-A. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," *ACM J. Wireless Networks*, pp. 545-556, 2003.

[5] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion Detection in Wireless Ad-Hoc Networks," in *IEEE Wireless Communications*, pp. 48- 60, February 2004.

[6] Y. Huang, W. Fan, W. Lee, and P. S. Yu, "Cross-feature analysis for detecting ad-hoc routing anomalies," in the Proceedings of the 23rd International Conference on Distributed Computing Systems (ICDCS) Providence, pp. 478-487, 2003.

[7] C. Loo, M. Ng, C. Leckie, and M. Palaniswami, "Intrusion Detection for Routing attacks in Sensor Networks," in *International Journal of Distributed Sensor Networks*, pp. 313-332, october-December 2006.

[8] E. Eskin, A. Arnold, M. Preray, L. Portnoy, S. Stolfo, "A geometric framework for unsupervised anomaly detection: detecting intrusions in unlabeled data," in *Applications of Data Mining in Computer Security*. Kluwe, 2002.

[9] A.Goldsmith and S.B. Wicker, "Design challenges for energy-constrained ad hoc wireless networks," in *IEEE Wireless Communications*, pp. 9(4):8-27, August 2002.

[10] C. J. John Felix, A. Das, B.C. Seet, and B.S. Lee, "Cross Layer versus Single Layer Approaches for Intrusion Detection in MANET," in *IEEE International Conference on Networks*, Adelaide, pp. 194-199, November, 2007.

[11] J. S. Baras and S. Radosavac, "Attacks and Defenses Utilizing Cross-Layer Interactions in MANET," in workshop on Cross-Layer Issues in the Design of Tactical Mobile Ad Hoc Wireless Networks: Integration of Communication and Networking Functions to Support Optimal Information Management, Washington, DC, June 2004.

[12] L. Yu, L. Yang, and M. Hong, "Short Paper: A Distributed Cross-Layer Intrusion Detection System for Ad Hoc Networks," in *Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks*, Athens, Greece, pp. 418-420, September 2005.

[13] C. J. John Felix, A. Das, B.C. Seet, and B.-S. Lee, "CRADS: Integrated Cross Layer Approach for Detecting Routing Attacks in MANETs," in *IEEE Wireless Communications and Networking Conference (WCNC)*, Las Vegas, CA, USA, pp. 1525-1530, March 2008.

[14] R. Shrikant, "Fast algorithm for mining association rule and sequential pattern," PhD Thesis , University of Wisconsin, Madison, 1996.

[15] S.J. hua and M.C. Xiang, "Anomaly Detection Based on Data-Mining for Routing Attacks in Wireless Sensor Networks," in *Second International Conference on Communications and Networking in China, CHINACOM '07*, pp. 296-300, August 2007.

[16] R. Shrestha, K.H. Han, J.Y. Sung, K.J Park, D.Y. Choi, S.J. Han, "An Intrusion Detection System in Mobile Ad-Hoc Networks with Enhanced Cross Layer Features," *KICS conference*, Suncheon University, pp. 264-268, May 2009.

[17] A. Patcha and J.M. Park, "An overview of anomaly detection techniques: existing solutions and latest technological trends," *Elsevier Computer Networks*, Vol. 51, Issue 12, pp. 3448-3470, 2007.

[18] L. Portnoy, E. Eskin, and S. Stolfo, "Intrusion detection with unlabeled data using clustering," in *proceedings of the Workshop on Data Mining for Security Applications*, November 2001.

[19] C. Loo, M. Ng, C. Leckie, and M. Palaniswami, "Intrusion Detection for Routing attacks in Sensor Networks," in *International Journal of Distributed Sensor Networks*, pp. 313-332, October-December 2006.

[20] OPNET modeler, <http://www.opnet.com>.

T. Phit and K. Abe, "Protocol Specification-based Intrusion Detection System for VoIP," *Technical Report of IEICE*, vol. 107, pp. 5-10, February 2008.