ADAPTIVE ASSOCIATION RULE MINING BASED CROSS LAYER INTRUSION DETECTION SYSTEM FOR MANET

V. Anjana Devi[1] and R. S. Bhuvaneswaran[2]

[1]St. Joseph's College of Engineering, Chennai
anjanadevi_anne@yahoo.com
[2]Anna University, Chennai
bhuvan@annauniv.edu

ABSTRACT

Mobile ad-hoc wireless networks (MANET) are a significant area of research with many applications. MANETs are more vulnerable to malicious attack. Authentication and encryption techniques can be used as the first line of defense for reducing the possibilities of attacks. Alternatively, these approaches have several demerits and designed for a set of well known attacks. This paper proposes a 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. This approach uses a fixed width clustering algorithm for efficient detection of the anomalies in the MANET traffic and also for detecting newer attacks generated . In the association process, the Adaptive Association Rule mining algorithm is utilized. This helps to overcome the more time taken for performing the association process.

KEYWORDS

Intrusion Detection System (IDS), Mobile ad hoc network (MANET), Ad Hoc On-Demand Distance Vector (AODV), Adaptive Association Rule Mining, Fixed Width Clustering Algorithm

1. INTRODUCTION

Because of the introduction of the mobile ad hoc networks (MANETs), IP-based networks with fairly high bandwidths have become deployable as platforms for communication and information processing applications, even in the absence of fixed infrastructure. Therefore, supporting networks with mobile nodes have become an attractive approach for supporting military scenarios, like command post networking, communication of vehicle convoys and autonomous robot systems, as well as for supporting infantry missions. Reliable transmission of essential information such as sensor data, equipment status information, and tactical orders to the required places, in order to support the paradigm of Network Enabled Capabilities is very important in the security purposes. The ability to handle multimedia data (e.g., voice, video) in these networks allows the efficient substitution of ancient technologies using highly interoperable IP-based networks and applications.

In MANET, in order to implement end-to-end communication along dynamic paths composed by multi-hop wireless links, a set of interacting nodes should cooperatively implement routing functions. Several multi-hop routing protocols have been proposed for MANET, and most popular ones include:

- Dynamic Source Routing (DSR),
- Optimized Link-State Routing (OLSR),

DOI : 10.5121/ijnsa.2011.3519

- Destination-Sequenced Distance-Vector (DSDV) and
- Ad Hoc On-Demand Distance Vector (AODV).

MANETs are also subjected to different types of threats like any other radio-based networking technology [13, 15]. These threats include outside attackers as well as misbehaving entities on the inside. Therefore, many different information assurance technologies need to be applied to protect these kinds of networks, such as data encryption, access control, identity management, and intrusion detection [11, 12]. Unfortunately, many of the well established intrusion detection approaches and implementations are not immediately transferrable from infrastructure-based IP networks, since there are many extensive implications to the usage of radio links and the mobility of the respective devices. Not only has the attack surface for broadband and smart jamming been enlarged, but the danger of impersonation and MITM (man-in-the-middle) attacks in the network has also increased. Due to the possibility of unsuccessful transfer of protocol packets, the probability for false alarms and false accusations of nodes in the networks is very significant. This possibility increases with physical motion in the network which leads to interruption of transmissions and fluctuation of routes. Moreover, there are no key locations in the network, where all relevant traffic may be observed and analyzed in order to detect malicious behavior, which was the case for routers, switches, and firewalls in wired IP networks.

To overcome these problems, a novel Intrusion Detection System (IDS) based on cross layers are proposed in this paper. These will helps in detecting the abnormalities occurred in the wireless networks. For the linkage between the OSI protocol stack and the IDS module, the association algorithm is implemented in this paper. This paper uses Adaptive Association Rule Mining algorithm in order to perform the association algorithm faster. The fixed width clustering algorithm [21] is applied in this paper in order to detect the intrusion efficiently in the adhoc network.

2. RELATED WORKS

Hong et al., [1] proposed a Real-time cooperation intrusion detection system for MANETs. It is very common that lot of intrusion detection systems are required for mobile ad hoc networks (MANETs) [16]. In recent times, Real-time Intrusion Detection for Ad hoc Networks (RIDAN) has been proposed to detect malicious activity which is less error prone than other detection techniques, such as the behavior-based. But, RIDAN lacks central monitor and cooperation function; the nodes couldn't share information with each other. In this paper, the author proposes an improved RIDAN based on cooperative idea, Real-time Cooperation Intrusion Detection system for MANETs (RCID MANET). The simulation results show that the RCID MANET achieves more detecting accuracy and success than the RIDAN.

Identification of critical nodes for MANET intrusion detection systems is presented by Karygiannis et al., [2]. The general design goal of reactive, proactive, and hybrid ad hoc routing protocols is to faithfully route packets from a source node to a destination node while maintaining a satisfactory level of service in a resource-constrained environment. Detection of malicious nodes in an open ad hoc network in which participating nodes have no previous security associations presents a number of challenges which are not faced by traditional wired networks. Traffic monitoring in wired networks is generally executed at switches, routers and gateways, but an ad hoc network does not have these types of network elements where the intrusion detection system (IDS) [5, 6] can collect and analyze audit data [7] for the entire network. A number of neighbor-monitoring, trust-building, and cluster-based voting techniques have been proposed in the research to enable the detection and reporting of malicious activity in ad hoc networks. The resources utilized by ad hoc network member nodes to monitor, detect, report, and diagnose malicious activity, however, may be greater than simply rerouting packets through a different available path. This paper proposes a method for determining conditions

under which critical nodes should be monitored, describes the details of a critical node test implementation, presents experimental results, and offers a new approach for conserving the limited resources of an ad hoc network IDS.

Cabrera et al., [3] put forth infrastructures and methodologies for distributed anomaly-based intrusion detection in mobile ad-hoc networks. This paper addresses one aspect of the problem of defending mobile ad-hoc networks (MANETs) [9, 10] against computer attacks, namely, the development of a distributed anomaly-based intrusion detection system [20]. In a general sense, the proposed system is a co-located sensor network, in which the monitored variable is the health of the network being monitored. A three level hierarchical system for data collection [8], processing and transmission is described. Local IDSs (intrusion detection systems) are attached to each node of the MANET, collecting raw data of network operation, and computing a local anomaly index measuring the difference between the current node operation and a baseline of normal operation. Anomaly indexes from nodes which belong to a cluster are periodically transmitted to a cluster head, which fuses the node indexes producing a cluster-level anomaly index. In the same way, cluster heads periodically transmit these cluster-level anomaly indexes to a manager node, which fuses the cluster-level indexes into a network-level anomaly index. Due to network mobility, cluster membership and cluster heads are times varying. The paper describes:

- Clustering algorithms to update cluster centers;
- Machine learning approaches for computing the local anomaly indexes;
- A statistical technique for fusing the anomaly indexes at the cluster heads and at the manager.

The statistical technique is formally shown to increase detection accuracy under idealized assumptions. These approaches were implemented and tested under the following conditions. Routing techniques: AODV (ad-hoc on demand distance vector routing) and OLSR (optimized link state routing); mobility patterns: random walk mobility model and reference point group mobility at various speeds; types of attacks: traffic flooding denial-of-service and black hole. The ROC (receiver operating characteristics) for several operational conditions at the nodes, cluster heads and manager is determined for the performance evaluation. The overall results shows the effectiveness of the infrastructures and algorithms described in the paper, with detection accuracy generally improving as it move up in the hierarchy, i.e. detection accuracy at the cluster level is very higher than at local level, while network-level detection outperforms cluster-level detection.

3. METHODOLOGY

3.1. Cross Layer Techniques in Ids

For efficient intrusion detection, we have used cross layer techniques in IDS. 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. 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. 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.

3.2. 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. 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.

This approach relies on information about relationships between different normal and abnormal nodes in order to achieve traffic features.

The new AR (Adaptive Rule) consists of two parts: AR-1 and AR-2.

AR-1 With the intention of mining only a normal and abnormal node of most capable rules for each target web site, AR-1 is used to control the minimum support count and discover the rules with the highest supports. The minimum support count is the smallest amount of nodes that convince a rule with the aim of making that rule frequent, specifically; it is the multiplication of the minimum support and the whole number of nodes. It consists of three parts:

1. AR-1 starts the minimum support count based on the frequency of the target nodes and calls AR-2 to mine rules.
2. When AR-2's output is returned, AR-1 will initially verify if the number of rules returned is equivalent to maxRulenum (as described below, AR-2 terminates the mining process when the number of rules generated is equal to maxRulenum). If it is, that means the minimum support count is small which causes above maxRulenum rules, as a result the AR-1 will keep rising the minimum support count and calling AR-CRS-2 until the number of rules is less than maxRulenum.
3. Lastly, AR-1 will verify if the number of rules is fewer than minRulenum; if it is, it will keep diminishing the minimum support count until the rule number is better than or equal to minRulenum.

Within a specified support, rules with smaller bodies are mined initially. Therefore, if with minimum support count say 15 nodes there is no rule available, but with minimum support count 16 nodes there are at least maxRulenum rules, then AR-1 will return the shortest maxRulenum rules with support count of at least 16 nodes.

AR-2 is an alternative of Classification Based Association-Rule Generation (CBA-RG) and as a result of the Apriori algorithm also. AR-2 is a alternative of CBA-RG in the sense that rather than mining rules for all target nodes, it only mines rules for one target node. It varies from CBA-RG in that it will simply mine a number of rules within a particular range. When it attempts to produce a new rule after having acquired maxRulenum rules previously then it just terminates its execution and returns the rules it has mined until now.

```
Input: Nodes, targetNode, minConfidence, minRulenum, maxRulenum
Output: minedRulenum
1)      set initial minsuppoatCount based on targetItem's
        like ratio;
2)      r=AR-2();
3)      while (R,rulenum=maxRulenum) do
4)      minusupportCount++;
5)      R1=AR-2();
6)      if R1.rulenum > minRlenum then R= R1;
7)      else return R;
8)      end
9)      while(R.rulenum<minRulenum) do
10)     minsupportCount--;
11)     R=AR-2();
12)     end
13)     return R;
```

Figure 1: The AR-1 Algorithm

```
Input: Nodes, targetNode, minConfidence, maxRulenum, minsupportCount
Output: mined association rules
1)      F1={frequent1-condsets};
2)      R=genRules(F1);
3)      if R.rulenum=maxRulenum then return R;
4)      for (k=2; Fk-1≠∅;k++) do Begin
5)      Ck =candidateGen(Fk-1);
6)      for each transaction t∈ Ct contained in t;
7)       Ct =all candidate condsets of Ck contained in t;
8)      for each candidate c∈Ct do Begin
9)            C.condsupCount++;
10)    If t contains targetNode then c.rulesupCount++;
11)     end
12)     end
13)     Fk={ c=Ck|c.rulesupCount ≥minisupportCount};
14)     R=R ∪ genRules(Fk);
15)     if R.rulenum=maxRulenum then return R;
16)     end
17)     return R;
```

Figure 2: The AR-2 Algorithm

Here k-condset is used to indicate a set of nodes of size k which possibly will form a rule: k-condset ⇒target-node. The support count of the k-condset called condsupCount is the amount of nodes that include the k-condset. The support count of the equivalent rule (also called rulesupCount of this k-condset) is the number of transactions that include the condset in addition to the target node.

AR-2 is extremely like CBA-RG as stated above. Association rules are produced by making multiple passes over the nodes. The initial pass calculates the rulesupCounts and the condsupCounts of all the particular nodes and discovers the frequent 1-condsets. For pass $k \geq 1$, it produces the candidate frequent k-condsets by making use of the frequent $(k-1)$-condsets; after that it scans all transactions to count the rulesupCounts and the condsupCounts of all the candidate k-condsets; at last, it will go over the entire k-condsets, choosing those whose rulesup is above the minimum support as frequent k-condsets and simultaneously generating rules k-condset ⇒target-node, if the confidence of the rule is above the minimum confidence. The algorithm is presented in Figure 2.

3.3. INTRUSION DETECTION MODULE

The data mining techniques is used in intrusion detection module in order to improve the efficiency and effectiveness of the MANET nodes. It if found out that among all the data mining intrusion detection techniques [18], 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.

The association algorithm such as Adaptive Association Rule Mining is used which can be utilized to achieve traffic features which is then followed by clustering algorithm. It is previously observed 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. The proposed IDS architecture is shown in Figure 3 and the IDS module is described below.

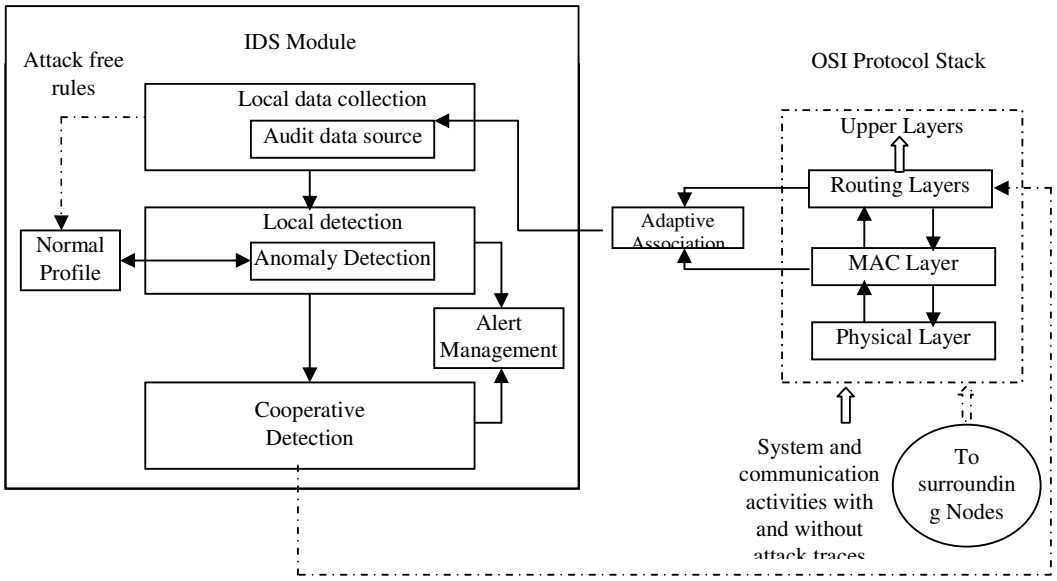

Figure 3. Proposed IDS Architecture in MANET

3.3.1. 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.

3.3.2. 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.

3.3.3. 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.

3.3.4. 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.

3.4. 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. The process of anomaly detection comprises of two phases: training and testing. The basic framework for normal behavior is constructing by collecting the noticeable characteristic from the audit data. The data mining technique is used for building Intrusion detection system to describe the anomaly detection mechanism.

3.4.1. 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. The few assumptions have to be done so that the traced traffic from the network contains no attack traffic:

- The normal traffic occurs more frequently than the attack traffic.

- The attack traffic samples are statistically different from the normal connections.

Since, two assumptions are used; 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.

3.4.2. Feature construction

For feature construction, an unsupervised method is used to construct the feature set. The clustering algorithm is used 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, the traffic related features as well as non-traffic related features which represent routing conditions are collected. Some of the features are used 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.

3.5. Training normal data using cluster mechanism

Fixed-width clustering algorithm is used in this paper as a technique for anomaly detection which is proposed by Shrestha et al., [21]. Fixed-width clustering algorithm is shown in Figure 4. 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. The cluster width w is chosen as the maximum threshold radius of a cluster.

3.5.1. Fixed width algorithm

A set of network traffic sample ST are obtained from the audit data for training purpose. Each sample si 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 si. For every succeeding point, the distance of each traffic sample si to the centroid of each cluster $\psi 1^*$ that has been generated by the cluster set Ψ is measured. If the distance to the nearest cluster ψn 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 τ % 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; the points that are outliers are only considered.

Algorithm:
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 samples si∈ST
If C=0 then
Make new cluster Ψ1 with centroid Ψ_1^* *from si*
Ψ1:={s1}, Ψ_1^* *=si, Ψ:= {Ψ1}, C=C+1*
Else
Find the nearest cluster Ψn to si
n:=argmink{Distance(si, Ψ_1^* *)}, where k=1,…,C*
If distance to nearest cluster Distance(si, Ψ_1^**)<w then*
Add si to cluster Ψn and update cluster centroid Ψ_1^*
Ψn:={si}UΨn
Else
Make new cluster ΨC+1 with centroid Ψ_{C+1}^* *from si*
ΨC+1:={si},
Ψ_{C+1}^**:=si,*
Ψ:={ΨC+!}UΨ,
C:=C+1
For each cluster Ψk
Find the outermost point smax in cluster Ψk
*smax:=argmini{Distsnce(si, Ψk *)}, where si∈Ψk and i=1,…,NT*
Set width wk of cluster Ψk
wk:=Distance(smax, Ψ_k^**)*
Cluster Labeling:
If |Ψk|/NT<classification threshold τ then
Label Ψk as anomalous
Else
Label Ψk as normal

Figure 4. Fixed width algorithm

4. EXPERIMENTAL RESULTS

The proposed technique is experimented with 25 similar wireless mobile nodes and attack is provided with single node. The routing protocol used for all the nodes is AODV routing protocol. The experiment s carried in the campus with the area of 800m x 800m. AODV routing protocol is used here because of its low message overhead. The experiment is carried for around 350 seconds.

Table 1 shows the simulation statistics used for the proposed technique. The custom application is used here with a streaming multimedia of packet size 1024. For experimentation, the UDP

traffic is used as a primary transport protocols. UDP data traffic is sent in bytes/sec during simulation from the source node to the destination. Also, in order to disturb the normal data traffic, the traffic attack is introduced. In this scenario, UDP flooding attack is introduced along with normal traffic. Mobility configuration module is used here in order to define random way point and random direction mobility to the mobile nodes. The mobility makes the network topology to be highly dynamic which helps in detecting the attacks with low false positive and negative rates by the detector. These settings are typical ad-hoc settings with sufficient mobility and data load overhead and they are used in all the experiments. Two simulations are performed for experimentation, one not including the attacker node and other including the attacker node. Training set is obtained by single execution of normal data. For experimentation, some normal data and some kind of attack are used.

Table 1: Simulation Statistics

Statistics	**Value**
Scenario Size	800m X 800m
802.11b Data Rate	11 Mbps
Transmission Range	<250 meter
Power of each Node	0.005 W
Simulation Time	350 seconds
No. of Mobile Nodes	25
Mobility	Random Waypoint, Random Direction Mobility

In the proposed association model, the common control packets and data packets from MAC and network layer are combined into single category as either routing control packets or routing data packets using Adaptive Association Rule Mining. For evaluating the Intrusion Detection, the packets are sent to IDS module. The fixed width algorithm included in IDS module is helpful in detecting the anomalous behavior. The normal traffic behavior is considered as normal profile and if the traffic abnormal, the packets are processed for intrusion detection.

In the experiment case that is considered, AODV routing protocol is used in 25 mobile nodes and the random mobility is implemented using mobility configuration. For evaluation, the source, destination and attacker node is considered. At the same time, other nodes have their own purpose. In order to train the system with normal traffic, the attacker node is disabled during the training phase.

The streaming multimedia UDP data traffic sent by the source to the destination node along with the anomalous traffic is shown n Figure 5. The red color in figure 5 indicates the UDP data traffic. 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 increase 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 the proposed method, the anomaly is detected and IDS treats this anomalous activity as an intrusive behavior.

Figure 5. UDP traffic analysis in destination node

In the figure 6, during the testing process, the abnormal behavior can be seen in the wireless data traffic received after 3 minutes interval time. The simulation is run in two setups, one with attacker node and other without the attacker node. The red color in the figure indicates 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.

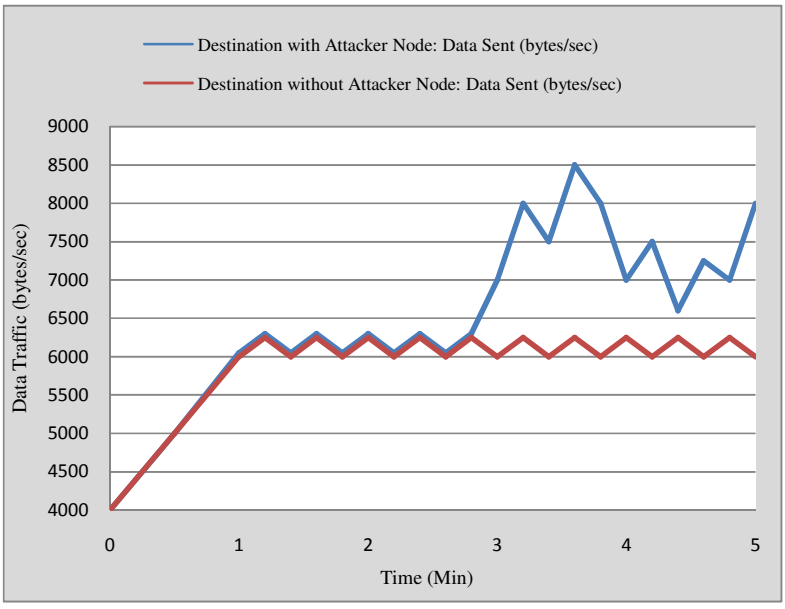

Figure 6. Wireless LAN Data Traffic Received in bits/sec

From these 25 nodes, node 3 is chosen for consideration. The traffic is introduced in the network and the performance of the proposed technique is evaluated. Figure 7 shows the AODV routing traffic for the existing technique, proposed technique and the traffic introduced by the attacker. From the figure, it can be clearly observed that the AODV routing traffic for the proposed technique is lesser when compared to the AODV routing traffic produced in the existing technique. This case continues even after the introduction of traffic in the wireless network. This clearly indicates that the proposed technique for intrusion detection will yield only lesser traffic when compared to the conventional techniques.

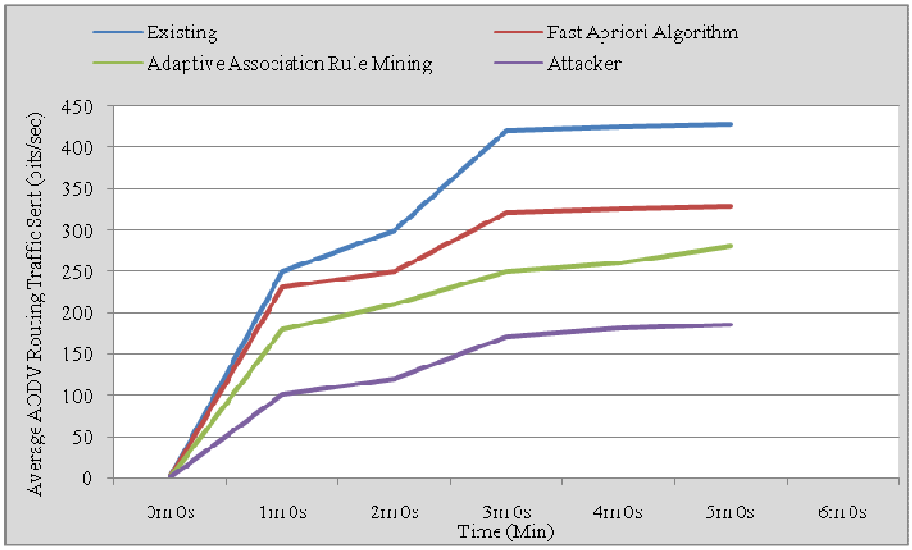

Figure 7. Time-Average in AODV Routing Traffic Sent

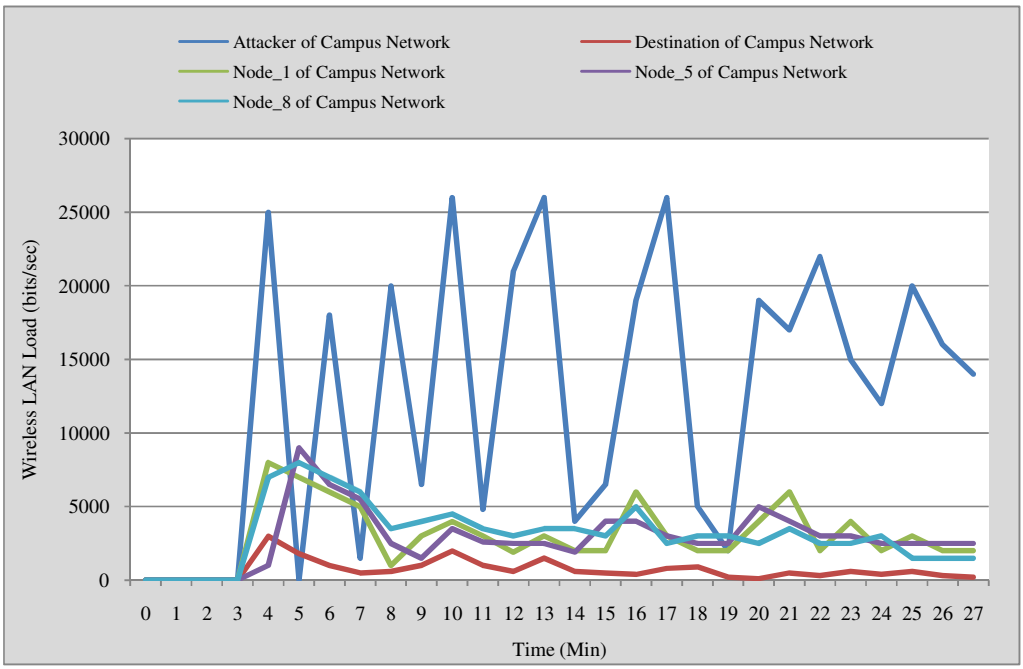

Figure 8. Wireless LAN load on Random nodes

At the same time examining the load on different nodes in this circumstance, it is found from the Figure. 8, that the load of the attacker node is high than any other nodes. It is because of the fact that the attacker node is sending UDP flooding attack to in the direction of the destination node.

5. CONCLUSION

Because of their significance in military and other applications, Mobile Ad-Hoc Wireless Networks or MANETs have caught the attention of considerable attention in the research community. It is very complicated to design the Intrusion detection system for MANETs since these networks change their topologies dynamically due to node mobility, lack concentration points where traffic can be analyzed for intrusions, utilize self-configuring multi-party infrastructure protocols that are susceptible to malicious manipulation and rely on wireless communications channels that provide limited bandwidth and are subject to noise and intermittent connectivity. The Intrusion detection systems for MANETs based on cross layers which satisfy these challenges are proposed in this paper. This paper utilizes clustering and data mining techniques for detecting the occurrence of intrusion. The proposed technique uses the fixed width algorithm for clustering process. The usage of fixed width algorithm helps in finding the DoS attacks and sink hole attack at different layers of the protocol stack. The proposed techniques will make use of Adaptive Association Rule Mining algorithm for the association process. This helps in increasing in speed for detecting the intrusion occurred in the network when compared to the conventional techniques. The various types of UDP flooding attack can also be detected efficiently using the proposed Intrusion detection system. The experimental results shows that the proposed technique undergoes lesser traffic when the intrusion is included in the network than the traffic occurred in the existing Intrusion detection systems.

REFERENCES

[1] Hong Ding and Xiaomei Xu,"Real-time cooperation intrusion detection system for MANets", IET International Conference on Wireless, Mobile and Multimedia Networks, pp.1-4, 2006.

[2] Karygiannis. A, Antonakakis. E and Apostolopoulos. A, "Detecting critical nodes for MANET intrusion detection systems", Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, pp.9-15, 2006.

[3] Cabrera. J.B.D, Gutierrez. C and Mehra. R.K, "Infrastructures and algorithms for distributed anomaly-based intrusion detection in mobile ad-hoc networks", IEEE Military Communications Conference, pp. 1831 – 1837, 2005.

[4] Puttini. R, Percher. J.M, Me. L and de Sousa. R, "A fully distributed IDS for MANET", Ninth International Symposium on Computers and Communications, pp.331-338, 2004.

[5] C. Endorf, E. Schultz and J. Mellander,"Intrusion Detection & Prevention", McGraw-Hill, 2004.

[6] M. Esposito, C. Mazzariello, et.al. "Evaluating Pattern Recognition Techniques in Intrusion Detection Systems". The 7th International Workshop on Pattern Recognition in Information Systems, pp. 144-153, 2005.

[7] N. Ye, X. Li, et.al. "Probabilistic Techniques for Intrusion Detection Based on Computer Audit Data". IEEE Transactions on Systems, Man, and Cybernetics, pp. 266-274, 2001.

[8] G. Florez, S.M. Bridges, and R.B. Vaughn, "An Improved Algorithm for Fuzzy Data Mining for Intrusion Detection". The North American Fuzzy Information Processing Society Conference, New Orleans, LA, 2002.

[9] A. Mishra, K. Nadkarni, and A. Patcha. "Intrusion Detection in Wireless Ad Hoc Networks", IEEE Wireless Communications, Vol. 11, Issue 1, pp. 48-60, 2004.

[10] Y. Zhang, W. Lee, and Y. Huang. "Intrusion Detection Techniques for Mobile Wireless Networks". Wireless Networks Journal (ACM WINET), 9(5): 545-556, 2003.

[11] Y. Zhang, W. Lee, "Intrusion detection in wireless ad-hoc networks", The 6th Annual International Conference on Mobile Computing and Networking, pp. 275–283, 2000.

[12] S. Bo, W. Kui, U.W. Pooch. "Towards adaptive intrusion detection in mobile ad hoc networks". IEEE Global Telecommunications Conference, pp. 3551–3555, 2004.

[13] H. Yang, H.Y. Luo, et.al. "Security in Mobile Ad Hoc networks: challenges and solutions", IEEE Wireless Communications, pp.38–47, 2004.

[14] T. Anantvalee and J. Wu. "A Survey on Intrusion Detection in Mobile Ad Hoc Networks", Book Series Wireless Network Security, Springer, pp. 170 – 196, 2007.

[15] P. Albers, O. Camp, et al. "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches". Proceedings of the 1st International Workshop on Wireless Information Systems, pp. 1-12, April 2002.

[16] D. Sterne, P. Balasubramanyam, et al. "A General Cooperative Intrusion Detection Architecture for MANETs". In Proceedings of the 3rd IEEE International Workshop on Information Assurance, pp. 57-70, 2005.

[17] B. Sun, K.Wu, and U. W. Pooch. "Alert Aggregation in Mobile Ad Hoc Networks", ACM Workshop on Wireless Security in conjuction with the 9th Annual International Conference on Mobile Computing and Networking (MobiCom'03), pp. 69-78, 2003.

[18] C. Krugel and T. Toth. "Applying mobile agent technology to intrusion detection". In ICSE Workshop on Software Engineering and Mobility, 2001.

[19] R. Ramanujan, S. Kudige, T. Nguyen, S. Takkella, and F. Adelstein, "Intrusion-Resistant Ad Hoc Wireless Networks", Proceedings of MILCOM, 2002.

[20] O. Kachirski, R. Guha, "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks,"Proceedings of the 36th Annual Hawaii International Conference on System Sciences, 2003.

[21] R. Shrestha, Kyong-Heon Han, Dong-You Choi and Seung-Jo Han, "A Novel Cross Layer Intrusion Detection System in MANET", 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), Pp. 647 – 654, 2010.