A MODEL FOR INTRUSION DETECTION IN MANET BASED ON DECISION TREE CLASSIFICATION

[1]P.Bharathisindhu, [2]S.Selva Brunda
[1]Research scholar, Bharathiar university, Coimbatore
[2]Professor and Head, Department of Computer Science Engineering,
Cheran College of Engineering, Karur

Abstract: In data communication, security plays a vital role when transmitting the data packets from one place to another. On the other hand intrusion on the networks makes the data communication vulnerable. MANET is a Mobile Ad hoc Network with wireless nodes that are communicated each other without any predefined infrastructure. Because of dynamic topology the security may very much challenging in MANETs and intrusion detection techniques become wide. The comprehensive analysis of security measures in MANET defines the various techniques that provide the intrusion detection techniques. In this paper we compare the proposed decision tree based model with Naive Bayes classifier which gives the better accuracy of finding the intrusion in Network. The decision tree based model works efficiently with Information gain that helps to find the relationship between the nodes. The malicious node is detected and the result shows that decision tree based models achieves the better results when compared with previous techniques.

Index Terms: MANET, Decision tree, Naive Bayes classifier.

I. INTRODUCTION

MANET is Mobile Adhoc Network, does not need wired infrastructure and centralization hub. The increase in wireless technology and network devices the growth of MANET becomes popular. Due to massive growth, the challenges on security become normal. The various attacks in MANETs are Black hole attack, Grey hole attack, routing attacks, Jamming attacks [1]. In MANET, the intrusion makes the node vulnerable towards various attacks. The IDS (Intrusion Detection System) monitor the network and helps to detect the malicious node from the MANET. In the proposed work, decision tree based IDS model helps to detect the malicious node at the earliest and isolate the misbehaving node from the network. Naive Bayes classifier [11] and Genetic based classifier [1] are used in various existing works. The classifiers were used to detect the various attacks. We proposed Decision tree based model provides the generalized solution for Intrusion detection system. The result shows that our work provides the better accuracy of detecting misbehaving node is better when compared with existing approaches.

II Related Works

In this section we discussed the various existing system that are more important for proposed system.

MANETs are categorized into three types that are Proactive, Reactive and Hybrid [3]. There are two types of MANETs such as open and closed system [7]. Open MANETs share the resources among the nodes in the networks. The closed MANETs do not share the resources globally in the networks. The routing misbehaviour in the network reduces the performance at the routing layer. The maintenance of the data packets becomes unreliable over the networks. Marti et al. [6] proposed the Watch dog mechanism for the Intrusion detection system and constructed based on Dynamic Source Routing Protocol (DSR). In this technique, Watch dog mechanism recognized the misbehaving nodes from the network and Path rater eliminates the intrusion nodes from the networks. In this paper, the node counter reaches the threshold value the nodes are said to be malicious or misbehaving nodes. The drawbacks of the Watch dog mechanism are it might not detect the misbehaving node with receiver collision, false misbehaviour report. Hasswa et al proposed an intrusion detection and response system for MANETS [4]. The combination of Watch dog mechanism and path rater [10] are categorized as fresh, member, unstable and suspect. The performance of the path rater is increased with this technique. Ramasamy et al [10] proposed the timer-based acknowledgement technique that isolated the misbehaving node and send the packets in alternate route. The packet delivery ratio with induced packet drop and overhead attained the better performance than the on-demand protocol.

Liu et al [5] proposed an acknowledgement based approach for the detection of misbehaviour nodes in MANETs. The approach overcomes the issues like receiver collision and limited transmission power in watchdog mechanism. The acknowledgement for every data packet over three consecutive nodes is sent from the source to destination. If the ACK (Acknowledgement) not received by the destination within the predefined time, the nodes are identified as malicious node.

The combined version of ACK and TWOACK has been proposed by Sheltami et al [13] as AACK(Adaptive Acknowledgement Scheme). The efficiency of the detection have increased and solved the limited transmission power and receiver collision problems. The Enhanced Adaptive Acknowledgement (EAACK) scheme was an improved version of the IDS schemes that overcomes the issues like false misbehaviour report authentication [9]. In paper [8] Niadiammai et al proposed the effective approach for the denial of service attacks in MANETs. The EDADT algorithm represents the less computational and false alarm rate was low. Also the algorithm reduces the less storage compared with c4.5 +PSO and SVM+PSO.

In paper [1], Ali et al surveyed the various security challenges in MANETs. The paper focussed and discussed the challenges and security services. Also the paper discussed various attacks that made MANET vulnerable and security issues. The security mechanism increases the performance when compared with existing mechanisms.

III Proposed Work

The existing Intrusion detection schemes were implemented based on Acknowledgement based schemes. In the proposed work the following steps take place in route establishment phase, Acknowledgement phase, Monitoring phase (MRA).

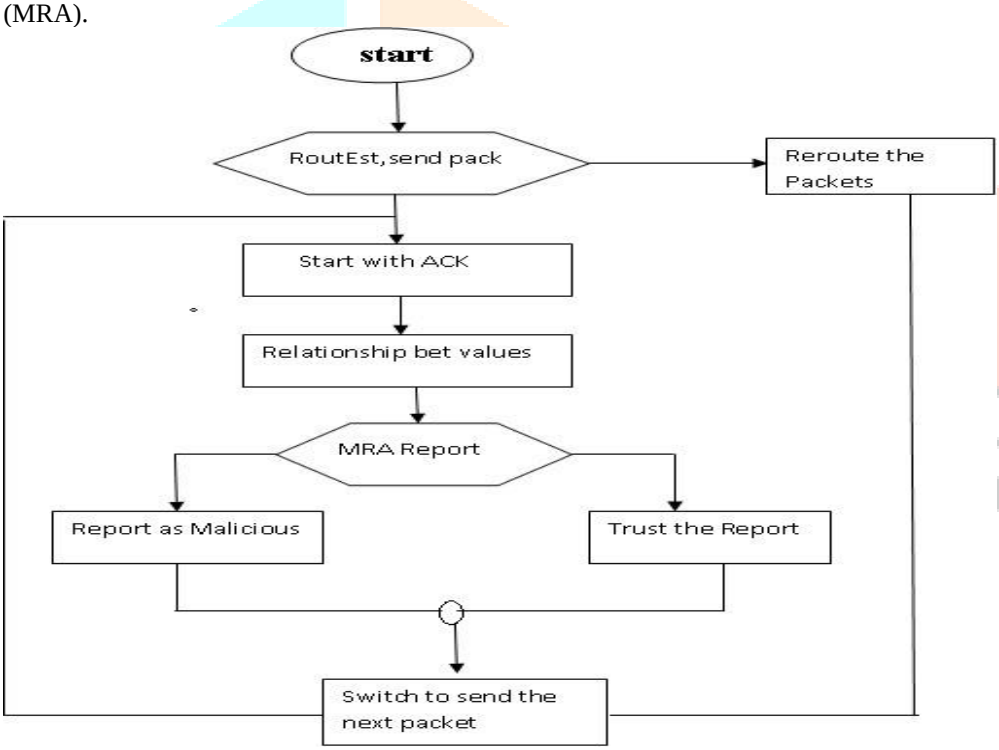

Fig.1 Proposed Model

1) Acknowledgement phase

The phase starts with route establishment. After the route got established, the sender start sends the packets. Once the packet reaches the next node, Ack is send to the sender node. The monitoring table maintains the number of packets, time taken to send the packets and time delay. Every node has the monitoring table with its routing information. In the monitoring table packet receiver count and packet send count is maintained.

2) Decision tree based model phase

The classification and regression based model identifies the relationship between the data values. The model generates the binary decision tree. The Entropy is used to calculate the values from the attributes. The Entropy is used to measure the amount of uncertainty or randomness or surprise in the set of data.

$$\text{Entropy } H(P_1, P2....Ps) = \sum^{s}_{i=1}(p_i \log (i/p_i)) \quad (1)$$

where $\sum^{s}_{i=1} p_i=1$ with the given probabilities. The values between 0 and 1.

The ID3 and CART follows the learning decision trees from the training tuples. The parameters used to construct the tree are as follows

i) R is the routing monitoring table

ii) Attributes_list is the list of attributes.

iii) Attributes_selection_method helps to select the attributes with selection measures.

The attribute selection measures are Information gain or GiniIndex. The method determines the splitting criterion. The value calculated from the split results in the network normal or abnormal. If the node is normal the packet is send to the next node. If the outcome of the split value is greater than threshold value the node is isolated from the network. The formula used for classify a tuples in D is given by,

$$\text{Info}_A(D) = \sum^{r}_{j=1} |D_j| / |D| * \text{Info}(D_j) \quad (2)$$

The information gain is defined with the difference of threshold value and trust value. The parameters used in the proposed work are packet generation rate, packet loss rate and packet delay.

The model propose the generalize solution for finding the misbehaving nodes from various attacks and isolate the node from the network.

IV Performance Analysis

We use the network simulator (NS2) for our proposed work.

Simulation Parameters	
No.of nodes	100
Area size	1000*1000
MAC	802.11
Simulation time	50 sec
Traffic source	CBR
Packet size	512
Speed	10 m/s

Table1. Simulation parameter

The 100 nodes were taken in the simulation and the nodes move within 1000*1000 meters region. The simulation time is 50 sec and the transmission range is 250 m. The traffic source used is CBR.

Performance Metrics

Packet generation rate = No. Of packets received/time

Packet loss rate = (No of packets generated - no of packets send)/time

Packet delay = Packet receive time – packet send time

Result :

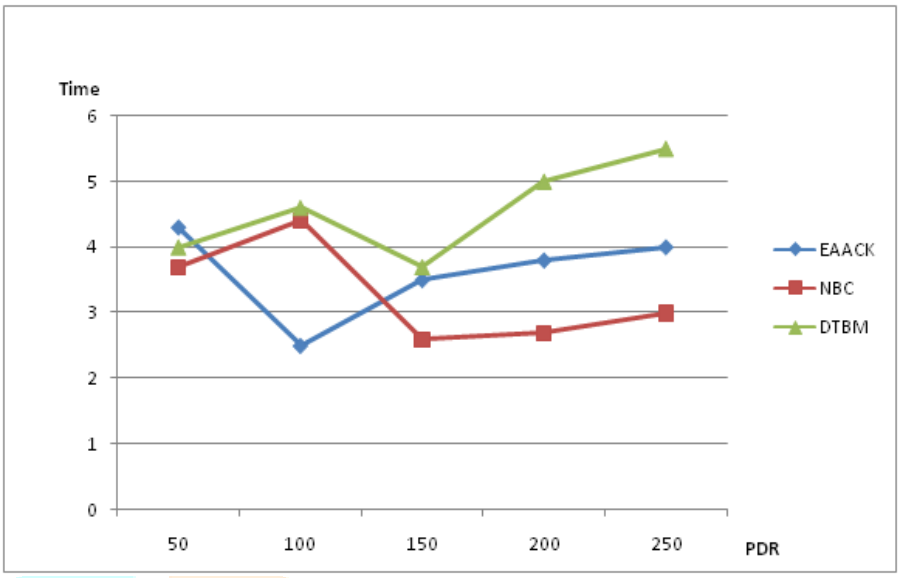

Figure 2 Packet Delivery Ratio

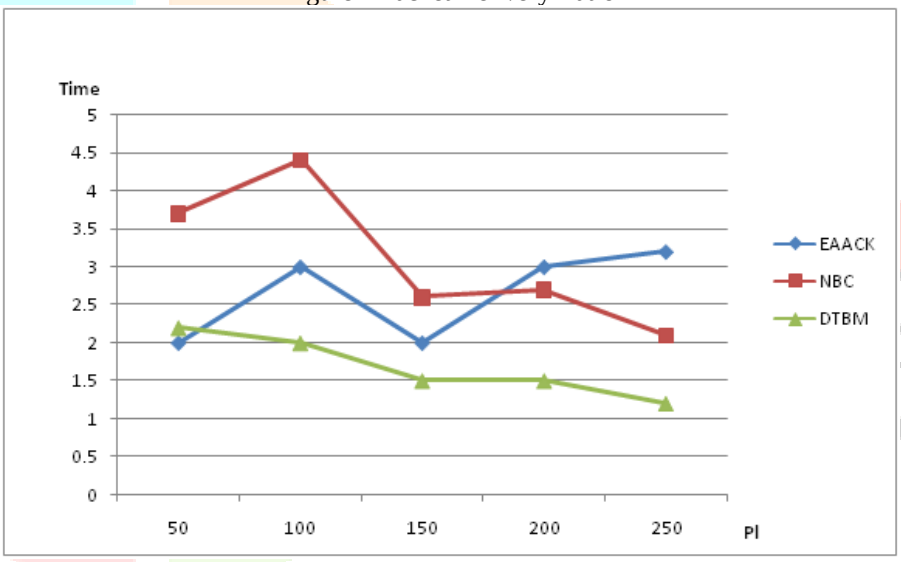

Figure 3 Packet loss Rate

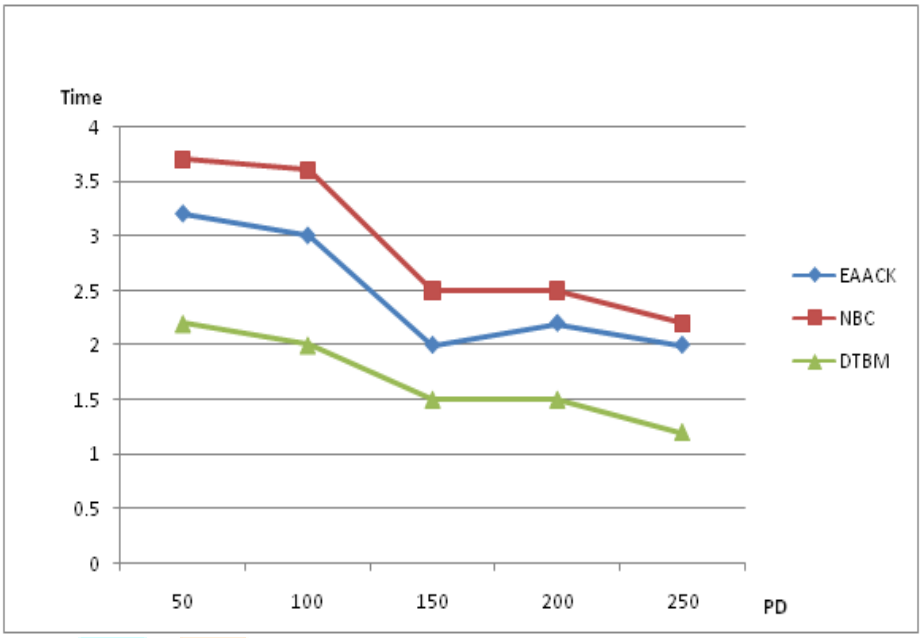

Figure 4 Packet Delay

Conclusion

The proposed model with decision tree based classification based Intrusion detection system helps to identify the malicious node better than the previous acknowledgement schemes. The information gain used to find the relationship between the values of the monitoring table which is used to identify the normal or abnormal behaviour of the nodes. The proposed mechanism improves the speed of the intrusion detection and implements the work in Network simulator (NS2). The data mining technique becomes more reliable for the intrusion detection and increases its performance than other techniques.

References

[1] Ali Dorri, S. R. (2015). Security challenges in Mobile Adhoc Networks: A Survey. *International Journal of Computer Science & Engineering Survey , 6* (1).

[2] Bharathisindhu P, S. B. (2018). An improved model based on genetic algorithm for detecting intrusion in mobile ad hoc network. *cluster computing,The Journal of Networks,Software Tools and Applications* .

[3] D, S. *Intrusion Detection in Mobile Adhoc Networks.* Texas,A M university.

[4] Hasswa A, Z. H. (2005). Routing Gaurd:An Intrusion detection and Response system for Mobile Adhoc Networks. *IEEE International Conference*, (pp. 336-343).

[5] Liu K, D. J. (2007). An Acknowledgement Based Approach for the detection of Routing misbehaviour in MANETs. *Mobile Computing* (pp. 536-550). IEEE Trans.

[6] Marti S, G. T. (2000). Mitigating Routing Misbehaving in Mobile Adhoc Networks. *Mobile Computing*, (pp. 255-265).

[7] Miranda H, R. L. (2001). Preventing selfishness in open Mobile Adhoc Networks. *Seventh CaberNet Radicals Workshop.*

[8] Nadiammai G.V, H. M. (2014). Effective approaches towards Intrusion Detection system using Data Mining techniques. *Egyptian Informatic Journal* , 37-50.

[9] NanKang, E. M. (2010). Detecting Misbehaving Nodes in MANETs. *iWAS* . Paris,France.

[10] Ramasamy Murugan, A. S. (2013). A TImer based Acknowledgement scheme for Node Misbehaviour Detection and isolation in MANET. *International Journal of Network Security* , 182-188.

[11] Saravanan S, C. R. (2005). Intrusion detection system using Bayesian approach . *International journalof engineering Innovtive Technology* , 108-116.

[12] Sheltami T, R. A. (2009). video transmission enhancement in presence of misbehaving nodes in MANETs. *International journalof Multimedia systems* , 273-282.