Study for Enhanced Intrusion Detection and Response System for MANET

A. V. Santhosh Babu*

Assistant Professor, Dept. of Information Technology, Sengunthar College of Engineering, Tiruchengode, India

*Corresponding author: santhoshbabu.av@gmail.com

Abstract: A mobile ad hoc network (MANET) is a configuration of smaller amount network in which the mobile nodes are randomly enthused in any direction within the transmission range of the network. Due to the mobility of the nodes, MANETs are susceptible to diverse types of attacks. Therefore, Intrusion detection and prevention technique is required to look after the MANETs beginning attack by external or internal intruders. Presented Intrusion Detection & Adaptive Response (IDAR) mechanism was designed for performing intrusion detection and effective retort with minimum network performance deprivation. Still, the energy consumed for detecting the intrusion was high which affects the natural life of network. Further, Enhanced Adaptive ACKnowledgment (EAACK) was intended for intrusion detection in MANETs. But, intrusion detection recital was not efficient which lacks intrusion detection rate.

Keywords: Two phase Enhanced Intrusion Identification and Response (t-EIIAR), Mobile Adhoc NETwork (MANET), Enhanced Adaptive ACKnowledgment (EAACK), Intuitionistic Fuzzy TOPSIS (IFT).

1. Introduction

In order to overcome on top of the mentioned confines, a two phase Enhanced Intrusion Identification and Response (t-EIIAR) system is planned in MANETs. The t-EIIAR system comprises of two phases namely cluster configuration and cluster head selection, the enhanced identification and response system [1]. The fuzzy c means (FCM) algorithm is old in t-EIIAR system to form the clusters with mobile nodes. Besides, the Intuitionistic Fuzzy TOPSIS (IFT) method is used in t-EIIAR scheme to discover the trust value for each node in the cluster [2]. After that, t-EIIAR system chooses the cluster head and detects the intrusion levels based on trust value. Finally, the intrusion response action is performed from the intrusion level classifications. The performance of t-EIIAR scheme is measured in terms of stricture such as intrusion detection rate, energy consumption and network lifetime. The simulation analysis shows that the t-EIIAR system is able to improve the intrusion detection rate of all attacks and also decrease the energy consumption when compared to the state-of-the-art works [5].

2. Performance of Enhanced Intrusion Identification and Response System

By means of the above algorithmic procedure, t-EIIAR systems efficiently discover the multiple malicious adversaries in route path and also isolate the malicious node in network [6]. As a result, t-EIIAR system better intrusion detection rate and reduced energy consumption in an able method [8].

3. Performance of Enhanced Intrusion Identification and Response System

In order to evaluate the presentation of the future, two phase Enhanced Intrusion Identification and Response (t-EIIAR) system is put into the practice in NS2.34 network simulator. In t-EIIAR system, 500 mobile nodes are randomly deployed in the network variety of the 1500 m*1500 m size. The t-EIIAR system used Ad hoc on demand distance vector routing protocols (AODV) [9] as routing protocol for detecting diverse

Algorithm: Enhanced Intrusion Identification and Response system

Input: Mobile Nodes ‘MN = MN1,MN2,...,MNn’ Source Node ‘SN’, Destination Node ‘DN’, , Data Packets ‘DP1 = DP1,DP2,...,DPn’

Output: Improved Intrusion Detection Rate and Network Lifetime

Step 1: Begin
Step 2: For all the mobile nodes in MANETs
Step 3: Cluster formation is performed with aid of FCM algorithm
Step 4: Cluster Head is selected in formed cluster using IFT method
Step 5: Computes trust values for each mobile nodes using (3.29)
Step 6: Classify intrusion levels based on trust values of mobile nodes
Step 7: Perform Intrusion response action to improve network performance
Step 8: End for
Step 9: End
types of routing attacks, i.e., black hole (BH), gray hole (GH), wormhole (WH), sleep deprivation (SD) and rushing attacks (RH) in MANETs. The simulation restrictions used for experimental labor is shown in below table.

<table>
<thead>
<tr>
<th>Simulation parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulator</td>
<td>NS2.34</td>
</tr>
<tr>
<td>Protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>50,100,150,200,250,300,350,400,450,500</td>
</tr>
<tr>
<td>Simulation time</td>
<td>2000sec</td>
</tr>
<tr>
<td>Mobility model</td>
<td>Random Way Point</td>
</tr>
<tr>
<td>Nodes speed</td>
<td>0-20m/s</td>
</tr>
<tr>
<td>Network area</td>
<td>1500m * 1500m</td>
</tr>
<tr>
<td>Data packets</td>
<td>10,20,30,40,50,60,70,80,90,100</td>
</tr>
<tr>
<td>Number of runs</td>
<td>10</td>
</tr>
<tr>
<td>Traffic type</td>
<td>CBR</td>
</tr>
</tbody>
</table>

The performance of t-EIIAR system is evaluate the against with obtainable intrusion detection & adaptive response (IDAR) instrument [3] by Adnan Nadeem and Michael P. Howarth (2014) and Enhanced Adaptive ACKnowledgment (EAACK) [4] by Elhadi M. Shakshuki et al. (2013). The efficiency of EIIAR system is measured in terms of intrusion detection rate, energy consumption and network lifetime.

4. Conclusion and Future Enhancement

A two phase Enhanced Intrusion Identification and Response (t-EIIAR) system is developed with objective of detecting the multiple intrusions in MANETs with reduced energy consumption. Initially, FCM algorithm is employed in t-EIIAR system to create a cluster and then IFT method utilized to determine the trust value for each node in the cluster [11]. Next, t-EIIAR systems desire the cluster head within cluster and identifies the intrusion levels depends on the trust value. At last, the intrusion answer action (i.e. no punishment, route around attack and isolation) is carried out from intrusion level classifications (i.e. very high, high, medium and low). Thus, t-EIIAR system professionally isolates assault such as black hole, gray hole, wormhole, sleep deprivation and rushing attacks with higher intrusion detection rate. The efficiency of t-EIIAR system is tests with the metrics such intrusion detection rate, energy expenditure and network lifetime. With the simulations performed for t-EIIAR system, it is pragmatic that the t-EIIAR system provide more accurate results for detecting the all kinds of adversaries in MANETs when compare to state-of-the-art works. The simulation results illustrate that t-EIIAR system provides enhanced performance with an improvement of intrusion detection rate by and decrease of energy consumption when compared to the state-of-the-art works. For further improving the performance of intrusion detection, Gene Populated Spectral Clustering (GPSC) technique is designed which detailed described in future enhancement [7, 10].

References