

# 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-EIAR), 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-EIAR) system is planned in MANETs. The t-EIAR 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-EIAR system to form the clusters with mobile nodes. Besides, the Intuitionistic Fuzzy TOPSIS (IFT) method is used in t-EIAR scheme to discover the trust value for each node in the

*Algorithm: Enhanced Intrusion Identification and Response system*

*Input:* Mobile Nodes ' $MN_i = MN_1, MN_2, \dots, MN_n$ ', Source Node ' $SN$ ', Destination Node ' $DN$ ', , Data Packets ' $DP_i = DP_1, DP_2, \dots, DP_n$ '

*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*

cluster [2]. After that, t-EIAR 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-EIAR scheme is measured in terms of stricture such as intrusion detection rate, energy consumption and network lifetime. The simulation analysis shows that the t-EIAR 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-EIAR systems efficiently discover the multiple malicious adversaries in route path and also isolate the malicious node in network [6]. As a result, t-EIAR 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-EIAR) system is put into the practice in NS2.34 network simulator. In t-EIAR system, 500 mobile nodes are randomly deployed in the network variety of the 1500 m\*1500 m size. The t-EIAR system used Ad hoc on demand distance vector routing protocols (AODV) [9] as routing protocol for detecting diverse

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 1  
Simulation parameters

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

The performance of t-EIAR 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 EIAR 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-EIAR) system is developed with objective of detecting the multiple intrusions in MANETs with reduced energy consumption. Initially, FCM algorithm is employed in t-EIAR system to create a cluster and then IFT method utilized to determine the trust value for each node in the cluster [11]. Next, t-EIAR 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-EIAR 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-EIAR system is tests with the metrics such intrusion detection rate, energy expenditure and network lifetime. With the simulations performed for t-EIAR system, it is pragmatic that the t-EIAR

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-EIAR 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

- [1] A. V. Santhosh Babu, P. Meenakshi Devi, Sharmila B & Suganya D, "Performance Analysis on Cluster based Intrusion Detection Techniques for Energy Efficient and Secured Data Communication in MANET", International Journal of Information Systems and Change Management, vol. 11, no. 1, pp. 56-69, 2019.
- [2] A. Pratapa Reddy and N. Satyanarayana, "Energy-efficient stable multipath routing in MANET", Wireless Networks, Springer, 2016, pp. 1-9
- [3] Abdulsalam Basabaa, Tarek Sheltami and Elhadi Shakshuki, "Implementation of A3ACKs Intrusion Detection System under Various Mobility Speeds", Procedia Computer Science, Volume 32, 2014, pp. 571-578.
- [4] Adnan Nadeem and Michael P. Howarth, "An intrusion detection and adaptive response mechanism for MANETs", Ad Hoc Networks, Volume 13, 2014, pp. 368-380.
- [5] Santhosh Babu A. V. & Meenakshi Devi P, "Energy aware Intrusion Detection System for MANETs", International Journal of Applied Engineering Research, vol. 10, no. 29, pp. 22300-22304, 2015.
- [6] A. V. Santhosh Babu, Meenakshi Devi P & Sharmila B, "Efficient enhanced Intrusion identification and response system for MANETs", International Journal of Business Information Systems, vol. 29, no. 4, pp. 535-546, 2018.
- [7] Santhosh Babu A. V. & Meenakshi Devi P, "Gene Populated Spectral Clustering for Energy Efficient Multiple Intrusion Detection and Responsive Mechanism for MANET", Journal of Electrical Engineering, vol. 17, no. 4, pp. 1-13, 2017.
- [8] A. V. Santhosh Babu, Meenakshi Devi P & Sharmila B, "Comparative Study of Manet Routing Protocols", Asian Journal of Research in Social Sciences and Humanities, vol. 6, no. 6, pp. 1924-1934, 2016.
- [9] Santhosh Babu A. V, Meenakshi Devi P & Sudhakar K, "Performance Enhancements for Pre-emptive Ad- Hoc On-demand Multipath Distance Vector Routing", International Journal of Latest Research in Engineering and Computing, vol. 1, no. 1, pp. 21-25, 2013.
- [10] A. V. Santhosh Babu & P. Meenakshi Devi, "Swarm optimised energy hubness clustering to detect and respond to intrusive attack variants in MANET", International Journal of Business Innovation and Research, vol. 18, no. 3, pp. 369-391, 2019.
- [11] B. Sharmila, "Effective Audio Steganography Based On LSBMR Algorithm," in International Journal of Research in Engineering, Science and Management, vol. 3, no. 4, pp. 37-40, April 2020.