International Journal of Research in Engineering, Science and Management
Volume 4, Issue 3, March 2021
https://www.ijresm.com | ISSN (Online): 2581-5792

# Comparison of Various Intrusion Identification and Response System for MANET

D. Suganya[1], A. V. Santhosh Babu[2*]

[1]Department of Information Technology, Velalar College of Engineering and Technology, Erode, India
[2]Department of Electronics and Communication Engineering, Erode Sengunthar Engineering College, Erode, India

***Abstract*: Mobile Ad hoc NETworks (MANETs) are the new creations of self-organize the networks that offer unrestricted mobility without any underlying infrastructure. It relies on the cooperation of all participate the nodes. Due to the diverse nature of MANET routing is the major challenge. Security for MANETS has become an easier said than done problem than the security in other networks. Authentication and encryption would be use as the major defence. Second level of defence to detect and respond to the safety difficulty called an intrusion identification system. In this paper, two phased enhanced intrusion identification and response (t-EIIAR) system for multi hop cluster based MANETs is planned. In order to improve energy efficient multiple intrusion detection and receptive mechanism, Gene Populated Spectral Clustering (GPSC) technique is introduced in MANET and finally, Swarm optimisation is used for providing energy efficient routing. Based on the nodes position and speed, association of nodes occurs. The fitness of each node is deliberate based on energy and trust for notice intrusion variants.**

***Keywords*: two phased enhanced intrusion identification and response (t-EIIAR), Gene population generation, Spectral clustering, Swarm optimization, Hubness clustering, Fitness function.**

## 1. Introduction

Mobile Ad Hoc Networks (MANETs) is a self-organize the system which consisting numerous mobile nodes that are communicate through wireless tie without any fixed infrastructure. The mobile nodes in MANETs are moving accidentally and frontward the data packet to another node in the network. Due to the node mobility and active network topology changes, the dissimilar types of attacks are occurred in the network direction path. Therefore, the intrusion detection scheme is required for reliable packet broadcast in MANETs. Intrusion Detection System (IDS) monitor the hateful activity in network and improves the security of data communication in the middle of the nodes in MANETs. A moment ago few research works are intended for detecting the intrusions in MANETs. But, conformist intrusion detection technique is not efficient for recognizing the numerous intrusion detection in MANETs. In order to conquer such kind of issues, three future methodologies called t-EIIAR system, GPSC technique and the SOEHC technique are designed.

### *A. Phase I method - two Phase Enhanced Intrusion Identification and Response*

two phase Enhanced Intrusion Identification and Response (t-EIIAR) system is intended in MANETs. The key purpose of t-EIIAR system is to get better the intrusion detection rate of manifold attacks in MANETs with smallest amount of energy consumption. The t-EIIAR system includes of two phases such as cluster configuration and cluster head collection, the enhanced discovery and response system. The Fuzzy C Means (FCM) algorithm is working in t-EIIAR system to generate the clusters with mobile nodes. In adding, the Intuitionistic Fuzzy TOPSIS (IFT) method is utilized in t-EIIAR system to calculate the trust value for each join in the cluster. Then, t-EIIAR system elects the cluster head and professionally identifies the multiple hateful intrusion attacks in MANETs using the strong-minded trust value. At last, the intrusion response deed is performed to isolate the detected intrusion attack nodes from the network. Thus, t-EIIAR system increase the intrusion detection rate of manifold attacks in MANETs with condensed energy consumption and also prolongs the network lifetime [1]. The efficiency of t-EIIAR system is deliberate in terms of parameter such as intrusion detection rate, energy expenditure and network lifetime. The simulation investigation demonstrates that the t-EIIAR scheme is able to enhance the intrusion detection rate of all attacks and also lessens the energy consumption when compare to the state-of-the-art works [2], [3].

### *B. Phase II method - Gene Populated Spectral Clustering*

Gene Populated Spectral Clustering (GPSC) technique is intended to improve presentation of multiple intrusion detection and responsive mechanism in MANETs with smallest amount of energy utilization. At first, GPSC technique generates gene population to form a cluster. Subsequently, the GPSC technique calculates the energy and trust value for each mobile node in MANETs. GPSC technique considerably identifies multiple attacks in MANETs with application of spectral clustering. Finally, the GPSC technique working intrusion response mechanism for isolating the intrusion nodes in MANETs. This helps for humanizing the network presentation with low

[*] Corresponding author: santhoshbabu.av@gmail.com

network poverty. As a result, the proposed GPSC technique enhances the intrusion detection rate of multiple attacks in MANETs through lower energy exploitation [4]. The effectiveness of GPSC technique is measured in terms of metrics such as energy consumption, intrusion detection rate and network lifetime. The simulation analysis illustrates that the GPSC technique is able to improve the intrusion detection rate and also decrease the energy expenditure while identifying the multiple intrusions in MANETs when compare to the state-of-the-art works.

### *C. Phase III method - Swarm Optimized Energy Hubness Clustering*

Swarm Optimized Energy Hubness Clustering (SOEHC)

Table 1
Network Lifetime

| **No. of nodes** | **Network lifetime (%)** | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **BH attack** | | | | **GH attack** | | | | **WH attack** | | | | **RH attack** | | | | **SD attack** | | | |
| | Existing IDAR | Proposed t-EIIAR | Proposed GPSC | Proposed SOEHC | Existing IDAR | Proposed t-EIIAR | Proposed GPSC | Proposed SOEHC | Existing IDAR | Proposed t-EIIAR | Proposed GPSC | Proposed SOEHC | Existing IDAR | Proposed t-EIIAR | Proposed GPSC | Proposed SOEHC | Existing IDAR | Proposed t-EIIAR | Proposed GPSC | Proposed SOEHC |
| 50 | 69 | 74 | 84 | 85 | 67 | 72 | 82 | 83 | 65 | 70 | 76 | 86 | 63 | 77 | 80 | 81 | 60 | 75 | 78 | 79 |
| 100 | 72 | 77 | 85 | 86 | 70 | 75 | 83 | 84 | 68 | 73 | 80 | 87 | 67 | 78 | 81 | 82 | 65 | 76 | 79 | 80 |
| 150 | 74 | 79 | 86 | 87 | 73 | 77 | 84 | 85 | 70 | 75 | 81 | 88 | 69 | 79 | 82 | 83 | 67 | 77 | 80 | 81 |
| 200 | 75 | 80 | 87 | 88 | 74 | 78 | 85 | 86 | 72 | 76 | 82 | 90 | 70 | 80 | 83 | 84 | 69 | 78 | 81 | 82 |
| 250 | 76 | 81 | 89 | 90 | 75 | 79 | 86 | 88 | 74 | 77 | 83 | 91 | 72 | 81 | 84 | 85 | 70 | 79 | 82 | 83 |
| 300 | 77 | 83 | 90 | 91 | 76 | 80 | 87 | 89 | 75 | 78 | 84 | 93 | 74 | 82 | 85 | 86 | 72 | 80 | 83 | 84 |
| 350 | 78 | 84 | 92 | 93 | 77 | 82 | 89 | 90 | 76 | 80 | 86 | 94 | 75 | 83 | 86 | 88 | 74 | 81 | 84 | 85 |
| 400 | 80 | 86 | 94 | 95 | 79 | 83 | 91 | 92 | 77 | 81 | 87 | 96 | 76 | 84 | 87 | 89 | 75 | 82 | 85 | 86 |
| 450 | 81 | 87 | 95 | 96 | 80 | 85 | 92 | 94 | 78 | 83 | 88 | 97 | 77 | 85 | 88 | 91 | 76 | 83 | 86 | 87 |
| 500 | 83 | 90 | 96 | 97 | 82 | 87 | 94 | 95 | 80 | 84 | 91 | 98 | 79 | 88 | 92 | 93 | 78 | 87 | 89 | 90 |

Table 2
Energy Consumption

| **No. of nodes** | **Energy Consumption (J)** | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **BH attack** | | | | **GH attack** | | | | **WH attack** | | | | **RH attack** | | | | **SD attack** | | | |
| | Existing IDAR | Proposed t-EIIAR | Proposed GPSC | Proposed SOEHC | Existing IDAR | Proposed t-EIIAR | Proposed GPSC | Proposed SOEHC | Existing IDAR | Proposed t-EIIAR | Proposed GPSC | Proposed SOEHC | Existing IDAR | Proposed t-EIIAR | Proposed GPSC | Proposed SOEHC | Existing IDAR | Proposed t-EIIAR | Proposed GPSC | Proposed SOEHC |
| 50 | 49 | 30 | 25 | 19 | 52 | 35 | 28 | 21 | 53 | 37 | 29 | 23 | 55 | 50 | 31 | 24 | 58 | 52 | 36 | 26 |
| 100 | 53 | 35 | 27 | 22 | 55 | 37 | 32 | 23 | 57 | 39 | 33 | 25 | 59 | 52 | 34 | 26 | 62 | 55 | 38 | 30 |
| 150 | 55 | 37 | 31 | 25 | 57 | 39 | 35 | 27 | 60 | 40 | 36 | 28 | 62 | 54 | 38 | 30 | 65 | 56 | 40 | 33 |
| 200 | 60 | 41 | 32 | 28 | 61 | 43 | 38 | 30 | 63 | 44 | 39 | 31 | 65 | 56 | 40 | 31 | 68 | 60 | 42 | 35 |
| 250 | 62 | 46 | 35 | 31 | 63 | 48 | 39 | 32 | 65 | 49 | 42 | 33 | 68 | 58 | 45 | 33 | 70 | 63 | 48 | 36 |
| 300 | 67 | 49 | 36 | 32 | 70 | 51 | 41 | 34 | 71 | 52 | 46 | 35 | 72 | 60 | 48 | 35 | 73 | 65 | 53 | 38 |
| 350 | 71 | 52 | 39 | 35 | 73 | 55 | 43 | 36 | 75 | 56 | 48 | 37 | 76 | 63 | 50 | 38 | 78 | 68 | 54 | 40 |
| 400 | 80 | 58 | 41 | 37 | 81 | 60 | 46 | 38 | 83 | 61 | 52 | 40 | 85 | 65 | 54 | 40 | 86 | 70 | 58 | 43 |
| 450 | 85 | 65 | 46 | 40 | 86 | 67 | 49 | 42 | 87 | 68 | 58 | 45 | 88 | 71 | 62 | 44 | 90 | 73 | 63 | 45 |
| 500 | 96 | 69 | 54 | 44 | 97 | 77 | 58 | 46 | 99 | 80 | 63 | 48 | 106 | 80 | 65 | 50 | 112 | 82 | 68 | 55 |

Table 1
Intrusion Detection Rate

| **No. of nodes** | **Intrusion Detection Rate (%)** | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **BH attack** | | | | **GH attack** | | | | **WH attack** | | | |
| | Existing IDAR | Proposed t-EIIAR | Proposed GPSC | Proposed SOEHC | Existing IDAR | Proposed t-EIIAR | Proposed GPSC | Proposed SOEHC | Existing IDAR | Proposed t-EIIAR | Proposed GPSC | Proposed SOEHC |
| 50 | 68 | 75 | 80 | 81 | 66 | 74 | 78 | 79 | 65 | 73 | 76 | 77 |
| 100 | 70 | 77 | 82 | 83 | 68 | 76 | 80 | 81 | 67 | 75 | 78 | 79 |
| 150 | 72 | 79 | 84 | 85 | 69 | 78 | 82 | 83 | 68 | 76 | 80 | 81 |
| 200 | 75 | 81 | 86 | 87 | 72 | 80 | 84 | 85 | 70 | 78 | 82 | 83 |
| 250 | 78 | 83 | 88 | 89 | 75 | 82 | 86 | 87 | 72 | 80 | 84 | 85 |
| 300 | 80 | 85 | 90 | 91 | 77 | 84 | 88 | 89 | 74 | 82 | 86 | 87 |
| 350 | 82 | 87 | 92 | 93 | 78 | 86 | 90 | 91 | 76 | 84 | 88 | 89 |
| 400 | 84 | 89 | 94 | 95 | 79 | 88 | 92 | 93 | 78 | 86 | 90 | 91 |
| 450 | 86 | 90 | 95 | 96 | 82 | 89 | 94 | 94 | 80 | 88 | 91 | 93 |
| 500 | 90 | 92 | 96 | 97 | 86 | 91 | 95 | 96 | 82 | 90 | 93 | 94 |

| **No. of nodes** | **RH attack** | | | | **SD attack** | | | |
|---|---|---|---|---|---|---|---|---|
| | Existing IDAR | Proposed t-EIIAR | Proposed GPSC | Proposed SOEHC | Existing IDAR | Proposed t-EIIAR | Proposed GPSC | Proposed SOEHC |
| 50 | 61 | 66 | 68 | 73 | 63 | 71 | 63 | 71 |
| 100 | 63 | 67 | 70 | 75 | 65 | 73 | 65 | 73 |
| 150 | 65 | 69 | 72 | 77 | 67 | 75 | 67 | 75 |
| 200 | 68 | 70 | 74 | 79 | 69 | 76 | 69 | 76 |
| 250 | 70 | 72 | 76 | 80 | 71 | 78 | 71 | 78 |
| 300 | 72 | 74 | 78 | 82 | 73 | 80 | 73 | 80 |
| 350 | 73 | 76 | 80 | 85 | 75 | 82 | 75 | 82 |
| 400 | 75 | 78 | 82 | 87 | 76 | 84 | 76 | 84 |
| 450 | 76 | 81 | 84 | 88 | 78 | 85 | 78 | 85 |
| 500 | 79 | 83 | 86 | 90 | 81 | 88 | 81 | 88 |

technique is intended to improve the presentation of intrusion attack variants in MANETs with smallest amount of energy utilization. The SOEHC technique is used swarm optimization for achieve energy efficient direction-finding in MANETs. The mobile nodes are arbitrarily moved in network depends on their place and velocity. In SOEHC technique, the strength of the value of each mobile node is predictable using energy and trust value in order to find out the intrusion variants attacks in MANETs. Then, the SOEHC technique is used Hubness clustering to professionally detect the attack variants in MANETs with superior intrusion detection rate. At last, the SOEHC technique is make use of the intrusion responsive mechanism to divide the intrusion nodes commencing the network. Hence, the SOEHC technique increases the network lifetime with lower energy expenditure [5]. The performance of SOEHC technique is deliberates in terms of energy consumption, intrusion detection rate and network lifetime. The simulation investigation shows that the GPSC technique provides improved performance with improvement of intrusion detection rate and reduction of energy utilization through discovering the intrusion attack variants in MANETs when compare to the state-of-the-art works.

## 2. Comparison of t-EIIAR, GPSC, SOEHC

The proposed three methods namely t-EIIAR system, GPSC technique and SOEHC technique is implemented in NS2 network simulator. Ad hoc On-Demand Distance Vector (AODV) routing protocols [9] is used as the routing protocol for conducting the experimental work. With different number of mobile nodes, Random Way Point (RWM) model is used as mobility model. The different number of mobile nodes is considered in the range of 50 to 500 randomly in rectangular area of 1500m * 1500m. The moving speed for mobile node in the network is about 0-20m/s. During the simulation process, five intrusive routing attacks (Gray Hole (GH), Black Hole (BH), Wormhole (WH), Rushing attacks (RH) and Sleep Deprivation (SD)) are efficiently identified.

With the simulations performed for three methods namely t-EIIAR system, GPSC technique and SOEHC technique, it is observed that the proposed SOEHC technique is presenting more accurate results for detecting the multiple intrusions in MANETs when compared to other two proposed and state-of-the-art works.

Thus, the proposed SOEHC technique improves the intrusion detection rate of BH, GH, WH, RH and SD are attacked by12%, 14%, 15%, 10%, and 15% respectively. Besides, the proposed SOEHC technique increases the lifetime of network with presence of BH, GH, WH, RH and SD are attacked by 14%, 13%, 15%, 17%, and 16% respectively. Furthermore, proposed SOEHC technique reduces the energy consumption of data transmission with occurrence of BH, GH, WH, RH and SD attacks by 43%, 40%, 40%, 34%, and 33% respectively [6]-[8].

## 3. Conclusion

A t-EIIAR system is developed for resourcefully detect the multiple attacks in MANETs. A t-EIIAR system selects the cluster head for identify the intrusion attacks. Nevertheless, the modification of the MANETs cluster head assortment mechanism to answer the various problems like detection of self-centered nodes in MANETs with senior intrusion detection correctness was remained unaddressed.

Besides, reducing the computational in the clouds of involved during the cluster head selection procedure was remaining unsolved. In addition, GPSC technique improves the performance of multiple intrusion discovery and responsive device in MANETs. However, intrusion detection performance of GPSC technique is not tested with a variety of conditions such as difference on mobility, size, and network traffic type and joins density. Moreover, SOEHC technique provides higher intrusion detection speed for identifying BH, GH, WH, RH and SD are attack in the MANETs. But, the other attack such as Sybil, flooding, denial of overhaul, IP spoofing is not considered in SOEHC technique which increases the energy consumption and too reduces the lifetime of network.

## 4. Future Work

Future work of t-EIIAR system can be proceed with enhancement of the cluster top collection mechanism to resolve the different issues and to further increase the presentation of multiple intrusion detection in MANETs. Supplementary, future work of GPSC technique can be preceded with varied the conditions such as disparity on mobility, size, network traffic type, and node thickness to professionally perform the multiple intrusion detection in MANETs with inferior false positive rate. In addition, the detection of dissimilar attacks like Sybil, flooding, denial of service, IP spoofing is also measured in future work of SOEHC technique for dropping the energy consumption and civilizing the lifetime of network.

## References

[1] Nadeem, A. and Howarth, M, “An intrusion detection & adaptive response mechanism for MANETs,” Ad Hoc Networks, vol. 13, pp. 368–380, 2014.

[2] Santhosh Babu A. V, Meenakshi Devi P and 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.

[3] Santhosh Babu A. V and Meenakshi Devi P, ‘Energy aware Intrusion Detection System for MANETs’, International Journal of Applied Engineering Research, vol. 10, no. 29, pp. 22300-22304, 2015.

[4] Santhosh Babu A. V and 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.

[5] Santhosh Babu A. V. and Meenakshi Devi P, ‘Swarm Optimized Energy Hubness Clustering to Detect and Respond Intrusive Attack Variants in MANET’, International Journal of Business Innovation and Research, vol. 18, no. 3, pp. 369-391, 2019.

[6] Santhosh Babu A. V, Meenakshi Devi P, Sharmila B and 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.

[7] Santhosh Babu A. V, Meenakshi Devi P and 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.

[8] Birundha K, Harini S, Hemalatha G, Kalaiselvi P and Santhosh Babu A. V, “A New Technique for Secured Authentication with PC Control through SMS,” International Journal of Engineering Research in Computer Science and Engineering, vol. 5, no. 3, pp. 445-447, 2018.

[9] Pavanya U, Ramya M, Surya N and Santhosh Babu A. V, ‘Protecting Location Privacy for Task Allocation’, International Journal of Innovative Research in Information Security, vol. 6, no. 3, pp. 208-214, 2019.

[10] Suganya D, Santhosh Babu A. V, “Performance Comparison of Secure Communication in Mobile Ad Hoc NETwork Using Intrusion Detection Techniques”, Sensor Letters, vol. 18, no. 4, pp. 273–279, 2020.

[11] Suganya D, Santhosh Babu A. V, “Investigation Study on Secured Data Transmission in 5g Networks with Internet of Things”, International Journal of Scientific and Technology Research, vol. 9, no. 6, pp. 1123-1129, June 2020.

[12] A. V. S. Babu, “Study for Enhanced Intrusion Detection and Response System for MANET”, International Journal of Research in Engineering, Science and Management, vol. 3, no. 5, pp. 252-253, May 2020.