*International Journal of Latest Engineering and Management Research (IJLEMR)*
*ISSN: 2455-4847*
*www.ijlemr.com || Volume 05 - Issue 09 || September 2020 || PP. 04-09*

# Detection and Prevention of System Intrusion in Wireless Ad-hoc Networks

Prof. Adilakshmamma
*M Tech, Ph.D.*

**Abstract:** Wireless communication technologies are undergoing fast advancements. A wireless ad hoc network is a decentralized type of wireless network. The network is ad hoc because it does not depend on a pre-existing infrastructure. An ad hoc network is a type of temporary computer-to-computer connection. In ad hoc mode, you can set up a wireless connection directly to another computer without having to connect to a Wi-Fi access point or router. An ad hoc network can have a variety of signs, whereas an Infrastructure network will always show an antenna. As wireless ad-hoc networks have different characteristics from a wired network, the intrusion detection techniques used for wired networks may no longer be sufficient and effective when adapted directly to a wireless ad-hoc network. Existing methods of intrusion detection have to be modified and new methods have to be defined in order for intrusion detection to work effectively in this new network architecture. Wireless ad-hoc networks need to be secured and use Intrusion Detection Systems (IDS) for detecting rogue access points. On a managed wireless network, a centralized network device is used to scan the radio frequencies of the network and reports and rogue access-points. For an ad-hoc network, an intrusion detection system solution needs to be implemented on a host based system to prevent network intruders. This paper will present various existing intrusion detection techniques that can be adapted to wireless ad-hoc networks and finally propose Effective Intrusion Detection and Prevention System in Wireless Ad hoc Networks.

**Keywords:** Wireless Communication, Wireless Ad Hoc Network, Intrusion Detection System, Host Based System, Access Points.

## I. Introduction

A wireless ad hoc network (WANET) is a decentralized type of wireless network. The network is ad hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity.

In addition to the classic routing, ad hoc networks can use flooding for forwarding data. Wireless mobile ad hoc networks are self-configuring, dynamic networks in which nodes are free to move. Wireless networks lack the complexities of infrastructure setup and administration, enabling devices to create and join networks anywhere and anytime.

A wireless ad-hoc network is a computer network in which the communication links are wireless shown in figure 1. The network is ad-hoc because each node is willing to forward data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. This is in contrast to older network technologies in which some designated nodes, usually with custom hardware and variously known as routers, switches, hubs, and firewalls, perform the task of forwarding the data.

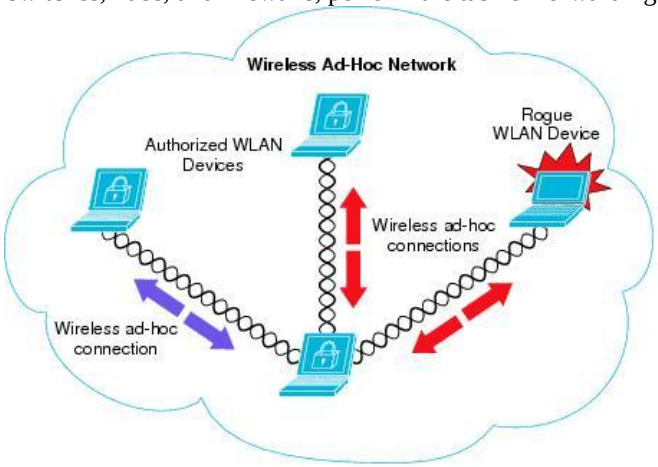


Figure 1 Wireless Ad-Hoc Network

## II. Effective Detection and Prevention System Intrusions

In wireless ad-hoc network, the various intrusions are occurred at the network transmission due to the node mobility. A network intrusion is also known as the unauthorized activity on a computer network. In several cases, such unwanted activity utilizes the network resources for other uses, and for all time threaten the data for deficiency of the network security. Properly designing and organizing a network intrusion detection system is mostly used to avoid the intruders from the network. Therefore, an efficient IDS uses Effective Intrusion Detection and Prevention System(EIDPS) technique for anomaly intrusion detection in wireless ad-hoc network. Starting with a network model, followed by the problem formulation and the proposed method is explained in detail.

### 2.1 System Model

Let us consider a wireless Ad hoc Network with number of nodes '$N_i = N_1, N_2, \dots, N_n$' distributed in a given rectangular area of '$M * N$' with a communication range '$R$'. The objective of Effective Intrusion Detection and Prevention Systemtechnique is to detect the anomaly intrusion that allows any source node '$SN$' to send to any destination node '$DN$' through intermediate nodes '$IN_i = IN_1, IN_2, \dots, IN_n$' a set of data packets '$DP_i = DP_1, DP_2, \dots, DP_n$'.

### 2.2 Problem Definition

One of the challenging issues when dealing with the nodes that are distributed in wireless ad-hoc network is the intrusion detection. With increases the anomalous in ad-hoc network, the performance of network gets reduced. The fundamental issue for intrusion detection in ad-hoc network is anomaly intrusion detection. The problem considered in this work is to distinguish the normal and anomalous during the data transmission with the objective of efficient intrusion detection accuracy using Effective Intrusion Detection and Prevention Systemclassifier technique.

The conventional intrusion detection techniques are difficult for classifying the activities as normal or anomalous. Similarly, the swarm intelligence approach is used for selecting the optimal feature to identify the network intrusion. But the malicious activity utilizes the network resources for other uses and failed to compromise a classification. Therefore, an effective intrusion detection system (IDSs) is needs to improve the performance of network activities by classifying the normal and anomalous behavior.

### 2.3 Optimal feature selection model

The first model in the design of the EIDPS classifier technique is the optimal feature selection model. In general, the optimal feature selection is the method of choosing relevant features for intrusion detection. The feature selection model is used to make easier for classifying the intrusion. The ensemble learning method used for determining a global optimum features about the nodes in wireless ad-hoc network from the number of features related with the network intrusion detection. Followed by, an efficient intrusion detection and classification is carried out to improve the detection accuracy. Optimal Feature selection is often used in network where several features and relatively selects the few features.

Let us consider, the network consist number of nodes $N_i = N_1, N_2, \dots, N_n$ and the network data consists of several features $F_1, F_2, F_3 \dots . F_n$ . In the wireless ad-hoc network environment, each node receives a network data. Among the multiple features, only a small fraction of features represents the intrusion performance. In order to reduce the irrelevant feature, feature selection is essential for improving the intrusion detection. Therefore, the optimal feature selection function is described as follows,

$$F_n(d) = \frac{W_t * tf_d * \log\left(\frac{N_d}{n_k} + 0.001\right)}{\sqrt{\sum_{d=1}^{n} (W_t * tf_d)^2 \log\left(\frac{N_d}{n_k} + 0.001\right)}} * \left(1 - \frac{1}{L_{th}}\right) \quad (1)$$

From (1),$F_n(d)$ is the function of feature selection, $W_t$ denotes weight factor of the data packet from the dataset d. $tf_d$ is the frequency that appears in dataset. $N_d$ Is the number of data packet and $n_k$ is the frequency that containing the specific approach and $L_{th}$ is the length of the data packet. Therefore, the packets with larger weight are chosen as the training samples.

**Input:** Number of Nodes$N_i = N_1, N_2, \dots, N_n$,weight factor of data packet ($W_t$), $tf_d$ , number of data packet ($tf_d$), length of the data packet ($L_{th}$), $n_k$, Data packet $DP_i = DP_1, DP_2, \dots, DP_n$
**Output :** Discover the optimal feature for intrusion detection
**Step 1**: Begin
**Step 2:** For each features
**Step 3:** Measure optimal feature selection function using (1)

**Step 4:** Selects optimal feature and remove the irrelevant feature
**Step 5**: End for
**Step 6: End**

Figure 2 Optimal Feature Selection Algorithm

## III. Simulation Settings

Effective Intrusion Detection and Prevention Systemclassifier technique is simulated using NS2.3 network simulator for improving the anomaly intrusion detection accuracy in wireless ad-hoc network intrusions. For the simulation settings, KDD cup 1999 dataset is considered for detecting the intrusion. This dataset is taken from UCI repository. The KDD cup 1999 dataset employed for the third International Knowledge Discovery and Data Mining Tools Competition, which was held in combination with KDD-1999 Fifth International Conference on Knowledge Discovery and Data Mining. The task to construct a network intrusion detector, a predictive approach is used to distinguish the ``bad" connections, which is called as intrusions or attacks, and "good" as normal connections. Based on this separation, the node which is normal or anomalous is detected in a network environment.

In Wireless ad-hoc network, totally 500 nodes are deployed over a square area of $A^2$ (1500 m * 1500 m) in a random manner that generates traffic for every 20 m/s. The nodes are distributed using Random Way point mobility model, whereas the link layer provides the link between two nodes. A number of data packets are considered from 10 to 100 and forwards the data packets. The simulation time is set as 1500sec. the simulation parameter is shown in below table.

**Table1: simulation parameter**

| **Parameters** | **Values** |
|---|---|
| Simulator | NS 2.34 |
| Network area | 1500 m * 1500 m |
| Number of nodes | 50,100,150,200,250,300,350,400,450,500 |
| Number of data packets | 10,20,30,40,50,60,70,80,90,100 |
| Size of data packet | 100 – 512 KB |
| Range of communication | 30m |
| Speed of node | 0 – 20 m/s |
| Simulation time | 1500 s |
| Mobility model | Random Way Point |
| Traffic type | Constant bit rate |
| Number of runs | 10 |

## IV. Results and Discussion

The Effective Intrusion Detection and Prevention System technique is evaluated with the existing Multicriterion Fuzzy Approach [1] and SVM-IDS [2]. The experimental evaluation is carried out with the different parameters such packet delivery ratio and classification time. Simulation analysis is carried out with the help of tables and graph values.

### 4.1 Impact of Packet Delivery Ratio

Packet delivery ratio using EIDPS technique is defined as the ratio of numbers of packets sent by source nodes to the number of packets correctly received at the destination nodes. The mathematical formula for packet delivery ratio is shown below,

$$PDR = \frac{No.of\ packet\ \ received}{No.of\ packet\ \ sent} * 100 \qquad (1)$$

From (1), packet delivery ratio $PDR$ is number of packet received to No. of packet sent. It is measured in terms of percentage (%). Higher the packet delivery ratio more efficient the method is said to be.

**Table 2 Tabulation For Packet Delivery Ratio**

| No. of packet sent | Packet Delivery ratio (%) | | |
|---|---|---|---|
| | EIDPS | Multi-criterion Fuzzy Approach | SVM-IDS |
| 10 | 84.36 | 74.65 | 66.49 |
| 20 | 86.75 | 76.79 | 69.63 |
| 30 | 88.79 | 79.46 | 71.21 |
| 40 | 91.21 | 81.10 | 72.47 |
| 50 | 91.76 | 82.67 | 73.76 |
| 60 | 93.47 | 83.47 | 78.35 |
| 70 | 95.79 | 86.76 | 79.31 |
| 80 | 97.58 | 87.35 | 81.21 |
| 90 | 98.49 | 89.74 | 83.79 |
| 100 | 99.79 | 91.47 | 85.68 |

The simulation values of packet delivery ratio with respect to the number of packet sent is illustrated in table 2. From the table value, the packet delivery ratio is higher in proposed EIDPS technique than the existing Multi-Criterion Fuzzy Approach [1] and SVM-IDS [2]. The convergence plot of ten different values is shown in figure 2.

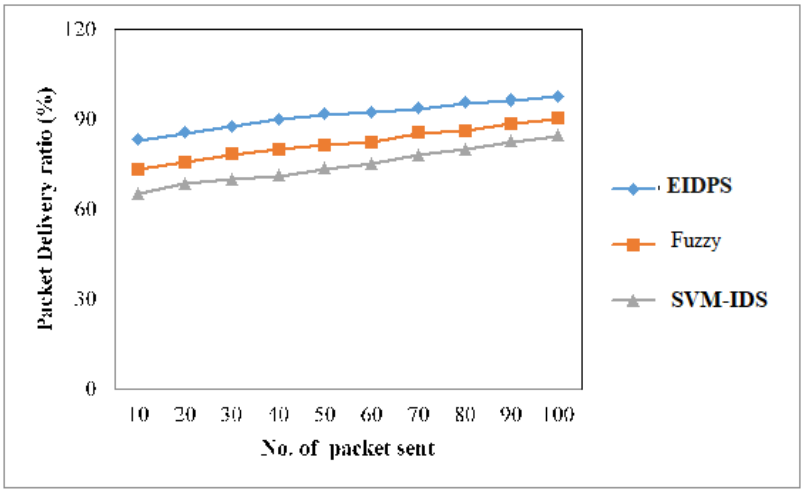


Figure 2 Measure of Packet Delivery Ratio

The simulation results of packet delivery ratio based on three methods namely, proposed EIDPS technique than the existing Multi-Criterion Fuzzy Approach [1] and SVM-IDS [2] is illustrated in figure 2. From the figure, it is clearly evident that, while increasing the number of packet being sent, the packet delivery ratio gets increased in all the three methods. But comparatively, the proposed EIDPS technique improves the performance level.Therefore, EIDPS technique increases the packet delivery ratio by 13% and 17% compared to existing Multi-Criterion Fuzzy Approach [1] and SVM-IDS [2] respectively.

### 4.2 Impact of Classification Time

It is defined as the amount of time required to classify the intrusion as normal or anomalous using EIDPS classifier. It is measured in terms of milliseconds (ms). The classification time is measured as follows,

$CT = No.of\ nodes * time\ (classifying\ normal\ or$ anomalous node)(2)From (2),Classification time (CT) is measured with number of nodes in the network.

**Table 3 Tabulation for Classification Time**

| No. of nodes | Classification time(ms) | | |
|---|---|---|---|
| | EIDPS | Multi-criterion Fuzzy Approach | SVM-IDS |
| 50 | 29.42 | 33.46 | 36.21 |
| 100 | 32.35 | 37.25 | 39.71 |
| 150 | 34.69 | 41.23 | 43.32 |

| | | | |
|---|---|---|---|
| 200 | 35.68 | 44.46 | 47.67 |
| 250 | 37.31 | 46.31 | 51.21 |
| 300 | 41.21 | 48.96 | 53.47 |
| 350 | 43.68 | 49.97 | 55.43 |
| 400 | 45.79 | 51.31 | 57.46 |
| 450 | 50.76 | 53.47 | 59.31 |
| 500 | 54.46 | 58.76 | 61.23 |

As shown in table 3, the analysis of classification time based on the number of node ranges from 50 to 500. The targeting results of classification time using proposed EIDPS technique than the Multi-criterion Fuzzy Approach [1] and SVM-IDS [2] is shown in following figure 3.

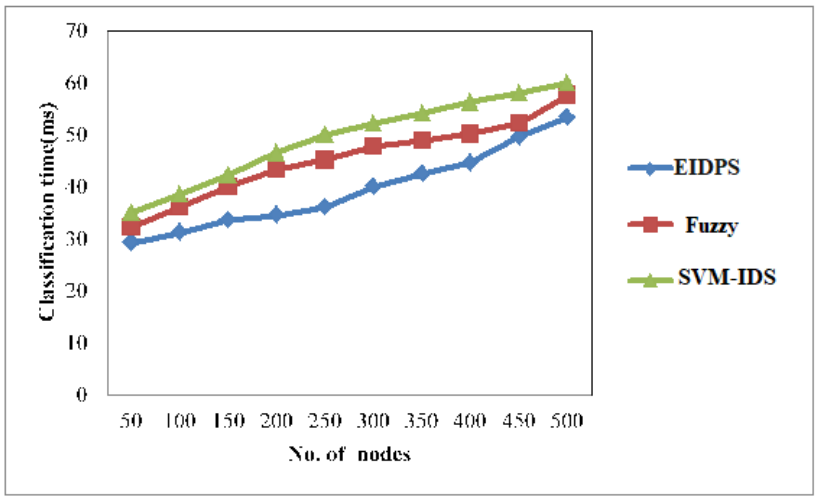


Figure 3 Measure of Classification Time

Figure 3 depicts the simulation results of classification time to classify the normal node or anomalous with respect to number of nodes in wireless ad-hoc network. The figure illustrates, the proposed EIDPS technique improved the performance with reducing the classification time than the state-of-art- methods [1] [2]. Due to, the classifier is used in EIDPS technique for efficiently classifies the intrusion in wireless ad-hoc network with minimum time. From that, the EIDPS classifier takes minimum time for separating the normal and anomalous using optimal hyper plane. Therefore, the classification time is reduced by 18% and 28% compared to existing Multicriterion Fuzzy Approach [1] and SVM-IDS [2] respectively.

## V. Conclusion

An efficient technique is called as Effective Intrusion Detection and Prevention System (EIDPS) for Anomaly Intrusion Detection in wireless ad-hoc network.An anomaly-based intrusion detection system is used for monitoring the system activities and classifying it as either normal or anomalous node. This helps to improve the intrusion detection accuracy in wireless ad-hoc network. Simulated annealing is applied in EIDPS technique for selecting the optimal feature of the node to detect the intrusion. Based on the optimal feature, the classifier is used to distinguish the malicious node and normal node by using the support vectors that outline the hyper plane in the feature space is more efficient for detecting the network intrusions and monitoring system and classifying the node as either normal or anomalous. The simulation is carried out for different parameters such as packet delivery ratio, classification time, false positive rate and anomaly intrusion detection accuracy. The performance results show that the EIDPS technique improves the packet delivery ratio, and reduces the classification time.

## References

[1]. El-Sayed M. El-Alfy, Feras N. Al-Obeidat, "Multicriterion fuzzy classification method with greedy attribute selection for anomaly-based intrusion detection", Procedia Computer Science, Elsevier, Volume 34, 2014, Pages 55 – 62.

[2]. Erfan A. Shams and Ahmet Rizane, "A novel support vector machine based intrusion detection system for mobile ad hoc networks", Wireless Networks, Springer, 2017, Pages 1–9.

[3]. ConstantinosKolias, Vasilis Kolias, GeorgiosKambouraki, "SVM-IDS: a distributed swarm intelligence-based approach for wireless intrusion detection", International Journal of Information Security, Springer, 2016, Pages 1–16.

[4]. Bandana Mahapatra, Srikanta Patnaik, "Self Adaptive Intrusion Detection Technique Using Data Mining concept in an Ad-Hoc Network", Procedia Computer Science, Elsevier, Volume 92, 2016, Pages 292 – 297.

[5]. Vishnu Balan E, Priyan M K, Gokulnath C, Usha Devi G, "Fuzzy Based Intrusion Detection Systems in MANET", Procedia Computer Science, Elsevier, Volume 50, 2015, Pages 109 – 114.

[6]. Binod Kumar Pattanayak and MamataRath, "Mobile Agent based Intrusion Detection System Architecture for Mobile Ad hoc Networks", Journal of Computer Science, Volume 10 Issue 6, 2014, Pages 970-975.

[7]. AbdulsalamBasabaa, Tarek Sheltami and ElhadiShakshuki, "Implementation of A3ACKs intrusion detection system under various mobility speeds", Procedia Computer Science, Elsevier Volume 32, 2014, Pages 571 – 578.

[8]. Anusha, K., Jayaleshwari, N., Arun Kumar, S., &Rajyalakshmi, G. V., "An Efficient and Secure Intrusion Detection Method in Mobile Ad-hoc Network using Intuitionistic Fuzzy", International Journal of Engineering and Technology (IJET) Volume 5, Issue 3, July 2013, Pages 2575-2584.

[9]. ConstantinosKolias, Vasilis Kolias, GeorgiosKambouraki, "SVM-IDS: a distributed swarm intelligence-based approach for wireless intrusion detection", International Journal of Information Security, Springer, 2016, Pages 1–16.

[10]. Malik N. Ahmed, Abdul Hanan Abdullah, OmprakashKaiwartya, "FSM-F: Finite State Machine Based Framework for Denial of Service and Intrusion Detection in MANET", PLoS ONE journal, Volume 11, Issue 6, 2016.

[11]. UjwalaRavale, NileshMarathe and Puja Padiya, "Feature Selection Based Hybrid Anomaly Intrusion Detection System Using K Means and RBF Kernel Function"Procedia Computer Science, Elsevier, Volume 45, 2015, Pages 428 – 435.

[12]. SedighehKhajoueiNejad, Sam Jabbehdari, Mohammad Hossein Moattara, " hybrid intrusion detection system using particle Swarm optimization for feature selection", International Journal of Soft Computing and Artificial Intelligence, Volume 3, Issue 2, 2015, Pages 55-58.

[13]. Khaled Badran and Peter Rockett, "Multi-class pattern classification using single, multi-dimensional feature-space feature extraction evolved by multi-objective genetic programming and its application to network intrusion detection", Genetic Programming and Evolvable Machines, Springer, Volume 13, Issue 1, 2012, Pages 33–63.

[14]. Alexandros G. Fragkiadakis, Vasilios A. Siris, Nikolaos E. Petroulakis and Apostolos P. Traganitis, "Anomaly-based intrusion detection of jamming attacks, local versus collaborative detection", Wireless Communications and Mobile Computing, Wiley communication and mobile computing, Volume 15, Issue 2, 2015, Pages 276–294.

[15]. Chun-Wei Tsai, "Incremental particle swarm optimization for intrusion detection", IET Networks, Volume 2, Issue 3, 2013, Pages 124 – 130.

[16]. Amin Hassanzadeh and RaduStoleru, "On the optimality of cooperative intrusion detection for resource constrained wireless networks", computers & security, Elsevier, Volume 34, 2013, Pages 16-35.

[17]. M. Usha and P. Kavitha, "Anomaly based intrusion detection for 802.11 networks with optimal features using SVM classifier", Wireless Networks, 2016, Pages 1–16.

[18]. PanosLouvieris, Natalie Clewley, Xiaohui Liu, "Effects-based feature identification for network intrusion detection", Neuro computing, Elsevier, Volume 121,2013, Pages 265–273.

[19]. VaishaliChahar, Rita Chhikara, YogitaGigras and Latika Singh, "Significance of Hybrid Feature Selection Technique for Intrusion Detection Systems", Indian Journal of Science and Technology, Volume 9, Issue 48, 2016, Pages 1-7.

[20]. ShrutiDubb and YaminiSood, "Feature selection approach for intrusion detection system based on pollination algorithm", International Journal of Advanced Engineering Research and Technology (IJAERT), Volume 4, Issue 6, 2016, Pages 209-213.