Efficient Anomaly Intrusion Detection Using Hybrid Probabilistic Techniques in Wireless Ad Hoc Network

K. Murugan[1,2] and P. Suresh[3]

(Corresponding author: K. Murugan)

Research Scholar, Bharathiar University[1]

Coimbatore, Tamil Nadu 641046, India (Email: mkcsresearch@gmail.com)

Department of Computer Science, Government College for Women, Kolar-563101, Karnataka, India[2]

Department of Computer Science, Salem Sowdeswari College, Salem 636010, Tamil Nadu, India[3]

(Received Mar. 26, 2017; revised and accepted June 26, 2017)

Abstract

A wireless ad-hoc network includes huge number of mobile nodes that structure temporary networks. Due to the dynamic nature of wireless ad-hoc network, security and efficient intrusion detection system (IDS) is a challenging task to detect the intruder nodes. The classification algorithm is used to detect the intrusions in an efficient manner. However, the network is characterized by high mobility they also introduce many vulnerabilities that increase their accurate detection risks. The optimization technique is performed to attain effective model for intrusion detection. But, the IDS continuously use additional resources to monitoring intruder activity in the network. In order to overcome the above issues in wireless ad-hoc network, Simulated Annealing based Naive Bayes Classifier (SA-NBC) technique is proposed for Anomaly Intrusion Detection. An anomaly-based intrusion detection system is used to detect the network intrusions and monitoring network activities in an exact manner. At first, the optimal features are chosen for classifying and detecting the intrusion by means of Simulated Annealing (SA) method when performing packet transmission. Based on these selected features, the accuracy and efficiency of traffic pattern analysis is improved using intrusion detection. Next, the Naive Bayes classifier is employed to classify the attack depends on features to identify the malicious behavior accurately from normal node in a testing environment by using the Bayes theorem. This in turns, the network traffic is minimized and increases the accuracy of anomaly intrusion detection. The SA-NBC technique conducts the simulations work on parameters such as anomaly intrusion detection accuracy, execution time, and throughput. The simulation results demonstrate that the SA-NBC technique is able to improve the accuracy of intrusion detection and also improves the throughput when compared to state-of-the-art works.

Keywords: Anomaly Intrusion Detection; Bayes Theorem; Intrusion Detection System (IDS); Naive Bayes Classifier; Wireless Ad-Hoc Network

1 Introduction

A wireless ad hoc network (WANET) is a decentralized network without having any fixed infrastructure. Wireless ad-hoc networks are essentially used in the tactical battlefield, emergency explore and civilian ad-hoc locations. The nodes in wireless ad-hoc network communicate with each other nodes through the intermediate node. Due to the diverse characteristic of mobile ad hoc networks, the various intrusions affect the network performance thus increases the traffic. In addition, limited transmission range of wireless network introduces the communication traffic over a number of nodes.

A novel IDS called as Adaptive Three Acknowledgements (A3ACKs) was introduced in [17] for MANETs. In A3ACKs, watchdog technique was applied to solve the issues in data transmission. However, the packet delivery ratio was not improved. In [15], a novel intrusion-detection system called as Enhanced Adaptive ACKnowledgment (EAACK) was developed to increase the malicious-behavior-detection rates in MANETs. However, the network overhead was high and the normal or anomalous behavior activities are difficult to identify.

A new method called as hash message authentication code (HMAC) was introduced in [4] to overcome the primary user attack in cognitive radio networks. However, the interferences are occurred in the HMAC through the transmission process. Security assurance process properties unification was developed in [12] to solve the security demands when handling logical vulnerability in system.

However, some network issues are not exposed or identified.

In [16], Intrusion detection systems were introduced to solve the availability attacks in ad-hoc networks. However, the performance of the network was not improved. A hybrid detection system called Hybrid Intrusion Detection System (H-IDS) [13] was developed to detect the DDoS attacks. The H-IDS uses both anomaly-based and signature-based detection methods. However, the detection accuracy of intrusion detection is not efficient.

In [1], a new intrusion detection system was introduced based on neuro-fuzzy classifier for avoiding the packet drops in mobile ad hoc networks. Anomalous node in network is isolated from the normal activities by using SVM classifier. An IDS based on anomaly based intrusion detection was developed in [8] by protecting the network node behavior to overcome the attacks. However, the packet delivery ratio was not sufficient.

Intrusion detection in MANETs using statistical classification algorithms [10] was developed to improve the classifier performance. A normalized gain based IDS was introduced in [19] for MAC Intrusions (NMI) detection to choose an optimal feature subset in training the classifier. However, the time consumed for classification was high.

The contribution of the paper is organized as follows: Simulated Annealing based Naive Bayes classifier (SA-NBC) technique is developed in wireless ad-hoc network for Anomaly Intrusion detection. Initially, with the aid of Simulated Annealing (SA) in SA-NBC technique, the optimal features of the nodes are selected to classify the intrusion in packet transmission. Next, by considering optimal feature selection, the traffic pattern accuracy is improved in the network. Finally, NB classifier is used to classify the node whether it is normal or anomalous by using the conditional probability function and therefore improves the intrusion detection accuracy and reduces the execution time for intrusion detection.

The rest of the paper is organized as follows. Detailed description of the method is provided in Section 2. In Section 3 the simulation environment is presented and the results are explained in Section 4. Section 5 presents a brief introduction of related works. Finally, the concluding remarks are presented in Section 6.

2 Methodology

Due to the higher mobility of nodes in wireless ad-hoc network, the different intrusions are occurred at the network transmission. A network intrusion is also called as the unauthorized activity on a computer network. The aim of intrusion detection is identify the various types of misbehavior activity. This misbehavior activity utilizes the network resources and accesses the data through the transmission for reducing network performance. Generally efficient modeling and organizing a network intrusion detection system is used to detect the intruders from the network. Therefore, an efficient IDS uses Simulated Annealing based Naive Bayes Classifier (SA-NBC) technique for anomaly intrusion detection in wireless ad-hoc network.

2.1 System Model

In this section, a system model for designing with Naive Bayes classifier is presented. Let us consider a WANET with number of node, $N_i = N_1, N_2, \cdots, N_n$, distributed in a given rectangular area.

2.2 Problem Definition

The major challenging problem in wireless ad-hoc network includes the lack of reliable data transmission due to its mobility and hence it is more prone to intrusion threats. With increases of anomalous in ad-hoc network leads to degrade the network performance. The anomaly intrusion detection is a basic issue for intrusion detection in ad-hoc network. The problem of classify the normal and abnormal nodes during the data transmission is considered in this work with the aim of obtaining improved intrusion detection accuracy using Simulated Annealing based Naive Bayes classifier technique.

Generally, intrusion detection techniques are difficult to distinguish the activities whether it is normal or anomalous. However the network resources are utilized by malicious activity and unable to compromise a classification. Hence, efficient intrusion detection system (IDSs) is needs to increase the throughput of network by means of classifying behavior of the nodes.

2.3 Simulated Annealing Based NB Classifier

A Simulated Annealing based NB classifier (SA-NBC) technique is developed with the aim of increasing the anomaly intrusion detection accuracy in wireless ad-hoc networks. Due to the different features of node the computational complexity is occurred in the network. In order to overcome the above issues, the SA-NBC technique uses the simulated annealing (SA) method that extracts the optimal feature. Each feature contains the different values in data packets that are produced by different attacks. The group of feature values is separated into various classes. Hence, an optimal feature is selected efficiently and reduces the computation time of IDS thus improves the detection accuracy using classifier.

The NB classifier is used to classify the malicious behavior accurately using SA-NBC technique. It reduces the failure of unidentified process and mainly employs the classification task that directs to lack of cascade classification in the intrusion classification process. Therefore, the NB classifier performs an intrusion classification process by means of separating the optimal features through monitoring the malicious activities in precise manner. The architecture of SA-NBC technique for anomaly intrusion detection and classification is shown in Figure 1.

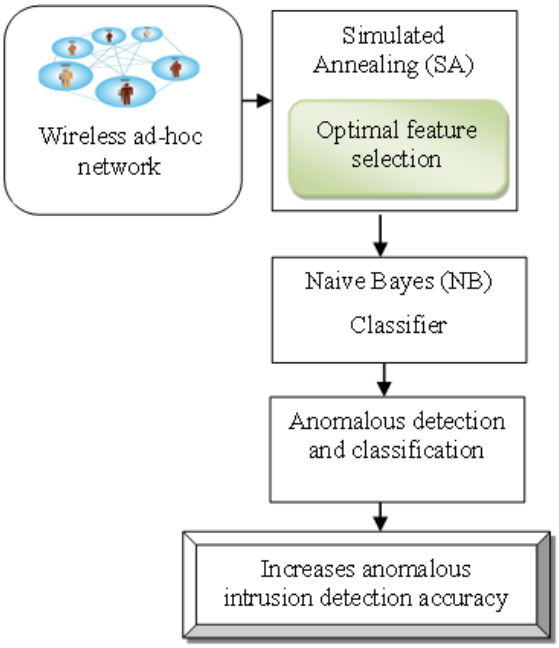

Figure 1: Architecture diagram of simulated annealing based NB classifier

As shown in Figure 1 the process of Simulated Annealing based NB classifier is used to detect the intrusion in the network. There are two phases in SA-NBC technique. The primary phase performs optimal feature selection and secondary executes attack detection and classification to improve the anomaly intrusion detection in wireless ad-hoc network. Initially, the feature of node is extracted through the simulated annealing. After that, the attack is identified and classified using NB classifier by considering selected optimal features. The brief explanation about the SA-NBC technique is presented in next subsections.

2.3.1 Simulated Annealing Method

In SA-NBC technique, the primary phase is used to perform the optimal feature selection with the aid of simulated annealing method. Generally, simulated annealing is a method used to solve the optimization issues.The global optimum feature from the number of features in the node is identified with the aid of SA method. After that, an efficient attack detection and classification is processed to increase the intrusion detection accuracy. In addition, SA is a probabilistic technique to detect the optimal results and avoiding the local optima when searching the solution space. In such a case, simulated annealing is an efficient technique in order to improve the network performance. The solid is efficiently heated to provide high temperature, then left to cool down slowly in simulated annealing process. During this process, a solid particle is travel into disordered state through heating the solid with higher temperature. This in turns, the internal energy gets improved. When gradually cool down, particles return to the order and it attains the equilibrium state at each temperature level. Lastly, the particle arrives a ground state at normal temperature and thus the internal energy minimized to a minimum level. Therefore, Simulated Annealing is applied in SA-NBC technique. The objective function value F with a simulated internal energy E, temperature T as control parameter, then frequent iteration as slowly decays of values thus provides the estimated optimal solution.

For allowing sufficient development, the initial temperature (T) is higher adequate. The temperature reduction function using SA is defined and it is formulated as follows,

$$T \leftarrow \gamma \times T. \tag{1}$$

In Equation (1), T denotes temperature it is based on the current temperature multiplied with the constant factor (γ). Initial solution is randomly chosen and it is taken as an optimal solution in SA. Next, the energy of the initial solution is calculated. A neighboring node of the initial state is chosen to calculate the energy when temperature T does not satisfies the termination condition.

The current state is replaced with a recently chosen state when the energy of newly selected neighboring node is less than or equal to the current state.If the energy of the new state is higher than the current state, a random value R is selected within the range of (0, 1). When random value R is less than the transition probability of the state, the optimal solution is achieved with the aid of simulated annealing method. After the temperature is decreased by using Equation (1), this process is continued until the termination condition T satisfied.

Consider the initial state of the node is'x' and the new state of the node is 'y', then the energy of the node is E(x) and E(y), the state transition probability is formulated as

$$P_{xy} = \exp(-\frac{E(y) - E(x)}{KT}). \tag{2}$$

From Equation (2), K represents the Boltzmann constant and T denotes the temperature of the material. The objective function value F is applied to describe the SA based feature selection algorithm for providing optimal solution. SA is a cooling scheme for finding optimal solutions to avoid local optima while searching the solution space. Based on the state transition using simulated annealing in SA-NBC technique, the optimal energy of the node is selected for classifying the network intrusion.

Algorithm 1 explains the process of finding an optimal state of the node with the aid of simulated annealing. The state transition carried out through the optimal state transition in the network. The energy of the new state is lesser than the current state and the current state is modified into new one. If the R value is less than the state transition probability, then the random number is generated. Hence, optimal feature of the node is chosen from the entire features. Then the intrusion detection and classification is processed with an optimal feature using NB classifier to detect the normal and anomalous node behavior in wireless ad-hoc network.

Algorithm 1 Simulated annealing algorithm

Input: Initial temperature (T), Number of nodes? $N_i = N_1, N_2, \cdots, N_n$, constant γ, a random number R
Output: Detect the optimal features for intrusion detection
for each node **do**
  Generate new state to choose optimal feature
  while Temperature > 0.001 **do**
    begin
    arbitrarily choose neighboring node state
    if $E(y) < E(x)$ **then**
      transition probability is calculated
    else
      produce R uniformly in the range (0, 1)
      if R < State transition probability **then**
        $x \leftarrow y$
        $T \leftarrow \gamma \times T$
      end if
    end if
  end while
end for

2.3.2 Naive Bayes Classifier For Anomaly Intrusion Detection

After selecting the optimal feature about the node, then the attacks detection and classification process is carried out using Naive Bayes Classifier. A Bayesian classifier is works on the design of a role of (natural) class that predict the values of features for nodes in the class. The nodes are grouped in classes since they include common values for the features. Such classes are further called natural kinds. If an organizer knows the class, the other features value of a node is predicted. If it unable to know the class, Bayes rule can be applied to predict the given class feature values of a node. The learning agent constructs a probabilistic model for classifying the node features whether it is normal or anomalous using Bayesian classifier. It also uses to predict the classification of a new pattern.In a probabilistic model, the classification is a latent variable in which the variable is probabilistically related to the detected variables.

Naive Bayes is a conditional probability model. The Naive Bayes classifier performs on optimal feature selection for the node. This means that the probability of one node feature does not affect the probability of the other. The independence of the Naive Bayesian classifier is realized in a certain trust network where the features are the nodes.

The nodes in the network is classified and represented by a vector $X = (x_1, x_2, \cdots, x_n)$. It denotes some optimal features of a node and assigns to this instance probabilities $p(C_{k|x_1}, x_2, \cdots, x_n)$ for each k possible classes C_k. For each example, the prediction can be computed by conditioning on detected values for the input features and by querying the classification.

In order to find the large number of optimal feature nodes n, the conditional probability can be expressed as,

$$p(C_{k|X}) = \frac{p(C_k)p(X|C_k)}{p(X)} \tag{3}$$

From Equation (3), $p(C_{k|X})$ denotes the posterior probability of class given predictor (feature), $p(C_k)$ represents prior probability of class features and $p(X|C_k)$ is the likelihood which is the probability of predictor given class. Then the $p(X)$ is a prior probability of features.

If the denominator is a normalizing constant then the probabilities provides the value greater than 1 means the node is normal. If else, the probabilities provides the value lesser than 1 means node is anomalous. Therefore, the intrusion detection accuracy is improved by using Naive Bayes classifier while monitoring the nodes behavior in wireless ad-hoc network.

The algorithmic process of NB classifier for anomaly intrusion detection is explained as follows,

Algorithm 2 Naive Bayes classifier algorithm

Input: Number of nodes $N_i = N_1, N_2, \cdots, N_n$
Output: normal and anomalous node classification
Begin
for each node **do**
  Evaluate t optimal feature nodes in vector X
  Measure conditional probability value using Equation (3)
  if $p(C_{k|X}) \geq 1$ **then**
    the node is normal
  else
    the node is anomalous
  end if
end for

Algorithm 2 shows the process of Naive Bayes classifier for detecting anomalous intrusion in wireless ad-hoc network. The vector representation is used to divide the nodes in different class. After that the conditional probability is applied to take optimal features of a node and classify the node is normal or anomalous. This in turns efficiently improves the anomaly intrusion detection accuracy. Therefore, Simulated Annealing based Naive Bayes Classifier (SA-NBC) technique is used to detect the intrusions and monitoring the network activities in an efficient manner.

3 Simulation Settings

In order to detect anomaly intrusion detection in wireless ad-hoc network, Simulated Annealing based NB Classifier (SA-NBC) technique is proposed and simulated using NS2 network simulator. The KDD cup 1999 dataset is taken from UCI repository for performing the simulation. KDD cup 1999 dataset contains standard set of data is audited, which comprises a number of intrusions in a network environment. The features are duration, src_bytes, dst_bytes,

number of urgent packets, srv_count, diff_srv_count and so on. Based on these features, the connection is separated in strong or feasible.

In wireless ad-hoc network, the number of nodes 500 is randomly arranged in an area $1500m \times 1500m$. Then speed of the node generates a traffic is maintained at a specific level as 20 m/s. The mobile nodes are distributed using Random Way point model in an area for simulation. Data packets used in the ranges from 10 to 100. The simulation time is taken as 1500sec. In each scenario, totally 500 nodes are used to identify the node interference and intrusion in the network. Table 1 illustrates simulation parameters.

Table 1: Simulation parameter

Parameter	Value
Network range	$1500m \times 1500m$
Simulation time	1500 ms
Number of mobile 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
Data Packets Size	100 - 512 KB
Range of communication	30 m
Speed of node	0 - 20 m/s
Mobility model	Random Way Point
Traffic type	Constant bit rate
Number of runs	10

4 Results and Discussion

Simulated Annealing based Naive Bayes Classifier (SA-NBC) technique is evaluated with the existing A3ACKs [17] and EAACK [15]. The experimental evaluation is carried out with the different parameters such anomaly intrusion detection accuracy, execution time and throughput. Performance is evaluated along with the following metrics with the help of tables and graph values.

4.1 Impact Of Anomaly Intrusion Detection Accuracy

The anomaly intrusion detection accuracy is measured as the ratio of the number of node accurately detected as anomalous to the total number of nodes in network. The anomaly intrusion detection accuracy is mathematical formulated as follows

$$AIDA = \frac{\text{No. of node accurately detected as anomalous}}{\text{No. of nodes}} \times 100. \quad (4)$$

From Equation (4), anomaly intrusion detection accuracy (AIDA) is measured in terms of percentage (%). If the anomaly intrusion detection accuracy is higher, then the method is said to be more efficient

Table 2: Tabulation for Anomaly intrusion detection accuracy

No. of nodes	Anomaly intrusion detection accuracy (%)		
	SA-NBC	A3ACKs	EAACK
50	84.20	75.24	70.22
100	86.54	78.16	72.35
150	87.16	80.30	74.55
200	89.52	82.54	75.63
250	90.41	85.28	77.22
300	92.10	86.86	79.46
350	93.47	89.45	81.42
400	95.32	91.36	83.53
450	97.27	93.44	86.40
500	98.14	94.27	89.18

Table 2 shows the tabulation for anomaly intrusion detection accuracy using proposed SA-NBC compared with existing A3ACKs [17] and EAACK [15] methods in wireless ad-hoc network. Number of nodes is taken from the range of 50 to 500 for experimental purpose. From table, it is clear that anomaly intrusion detection accuracy is increased for the respective increase in number of nodes using all the methods.

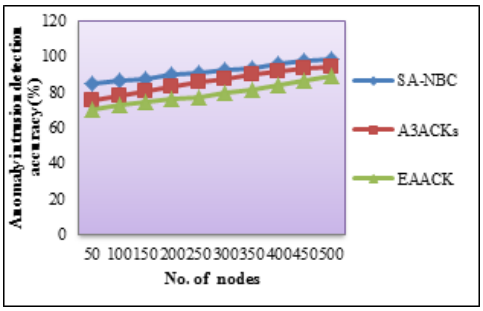

Figure 2: Measure of anomaly intrusion detection accuracy

Figure 2 shows the performance of anomaly intrusion detection accuracy using three methods such as proposed SA-NBC and existing A3ACKs [17] and EAACK [15] methods. From the figure, it is clearly illustrated that the anomaly intrusion detection accuracy is improved in SA-NBC technique. This efficient improvement in SA-NBC technique is attained with the help of simulated annealing based classification in wireless ad-hoc network. Then the Naive Bayes classifier is used to classify the normal and anomalous nodes in the network based on the optimal feature selection. The condition probability values are considered to detect the anomalous nodes accurately. There-

fore, the anomaly intrusion nodes are detected in wireless ad-hoc network and thus improve accuracy of anomaly intrusion detection using SA-NBC technique by 6% and 14% compared to existing A3ACKs [17] and EAACK [15] methods respectively.

4.2 Impact of Execution Time

Execution time is measured by product of time taken for detecting an intrusion or attacks in a network with respect to number of nodes participate in that network. It is formulated as given below.

$$ET = n \times \text{Time (intrusion detection)}. \quad (5)$$

From Equation (5), Execution Time 'ET' is measured in terms of milliseconds (ms). Lower execution time ensures the effectiveness of method.

Table 3: Tabulation for Execution time

No. of packets	Execution time (ms)		
	SA-NBC	A3ACKs	EAACK
50	9.53	11.21	13.76
100	13.59	14.68	17.28
150	17.24	18.57	20.63
200	19.48	20.65	22.69
250	22.47	23.58	26.49
300	25.38	27.49	29.66
350	28.32	29.37	32.52
400	30.26	32.56	34.25
450	33.26	35.26	37.24
500	35.12	37.31	39.15

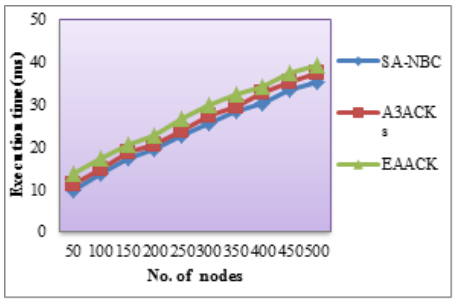

Figure 3: Measure of execution time

Table 3 and Figure 3 show the measure of execution time with respect to varying number of nodes in proposed SA-NBC technique compared with existing A3ACKs [17] and EAACK [15] methods. As shown in Figure 4, the proposed SA-NBC technique provides better reduction in execution time for intrusion detection when compared to other existing methods. This efficient reduction of execution time is achieved by the application of Naive Bayes classifier for MANETs. Data packets are transmitted through network from source node to destination node and entire information successfully transferred using proposed SA-NBC technique due to the detection of abnormal node in the network. Hence delay time for transmitting data packets to destination node is reduced effectively. Therefore, execution time for intrusion detection using proposed SA-NBC technique is reduced by 8% when compared to A3ACKs [17] and 19% when compared to EAACK [15] method respectively.

4.3 Impact of Throughput

Throughput is measured by the ratio of successfully received data packets at destination node and total number of data packets sent through source node. Throughput rate in wireless ad-hoc network is calculated as shown below.

$$T = \frac{\text{successfully received data packets}}{\text{total number of data packets sent}} \times 100. \quad (6)$$

From Equation (6), throughput 'T' is measured in terms of percentage (%). If throughput rate is high, then the network is said to be more secure and efficient.

Table 4: Tabulation for throughput

No. of packet sent	Throughput (%)		
	SA-NBC	A3ACKs	EAACK
10	77	70	62
20	79	72	64
30	82	75	66
40	84	77	67
50	85	78	69
60	88	80	71
70	91	83	74
80	93	85	76
90	95	86	78
100	96	87	81

Table 4 shows the measure of throughput using proposed SA-NBC technique compared with existing A3ACKs [17] and EAACK [15] methods. The number of data packets is taken as the ranges from 10 to 100 for the experimental purpose. From the table, the throughput of the network is increased with the respective increase in data packets. Proposed SA-NBC technique provides higher throughput when compared to state-of-the-art methods.

Figure 4 depicts the result analysis of the throughput with number of data packets are considered for evaluation process. From the figure, it is clearly evident that the proposed SA-NBC technique accurately classifies the node as normal or anomalous. This technique improves the performance results when compared to existing methods due to NB classifier in SA-NBC technique. The NB

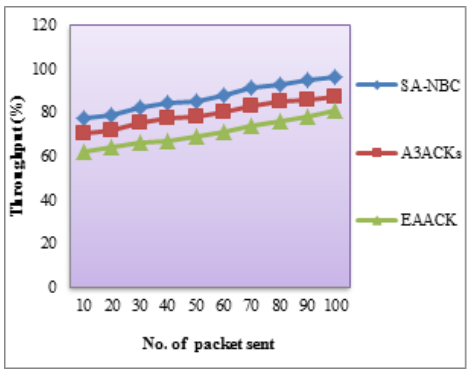

Figure 4: Measure of throughput

model classifies the nodes as normal or anomalous in vector consideration in which the nodes are selected with optimal features. With the aid of selected optimal features of a node, the traffic pattern is analyzed in the network. In addition, simulated annealing is used to perform the optimal feature selection process for further classify the node is normal or anomalous in the wireless ad-hoc network. Hence, efficient communication is achieved while transmitting the data packets through the normal node and thus improves the performance of the network. This in turns efficient throughput is achieved in wireless ad-hoc network. Therefore, proposed SA-NBC technique improves the throughput by 9% and 19% compared to existing [17] and EAACK [15] respectively.

5 Related Works

The security attacks and intrusion detection systems method was introduced in [11] for self-configurable networks. However, the applications are used in the method was affected by intruders. A novel intrusion detection system based on the trust rates was introduced in [5] to detect the intrusive action in MANET. But, the execution time for intrusion detection was remained unaddressed.This issue is overcome by the SA-NBC technique for improving the performance through identifying the anomalous node behavior.

Distributed combined authentication and intrusion detection was designed in [2] to maximize security in MANET. But, trust values from all nodes were not combined effectively. A behavior-rule specification-based technique was introduced in [9] for intrusion detection in medical devices. However, the large numbers of nodes are does not handled effectively. The SA-NBC technique improves the optimal feature for classifying large number the anomalous and normal activities in wireless ad-hoc network.

An intelligent multi-level classification technique was introduced in [3] to detect the intrusion detection in MANET. The mixture of tree classifier with labeled training data and enhanced multiclass classifier algorithm was designed to prevent the network from the intrusion. But, the intrusion detection was does not efficiently carried out. This problem is solved by SA-NBC technique by using Naive Bayes classifier. Neural network method was introduced in [14] to distinguish the normal and attacked behavior of the system based on MLP. But, the normal and anomalous of the system was not distinguished.

TermID, a distributed rulebased network intrusion detection system was developed in [6] for performing intrusion detection applications in wireless networks. But, the classification was not enhanced using distribution of the tasks in wireless networks.The SA-NBC technique used to improve the intrusion detection effectively by means of selecting optimal features of a node in the network. In [7], IDS based on self-learning technique was developed to detect the attacks in the network where the system uses unknown data pattern classifier (Neuro-fuzzy approach) thus reduces the dimensionality of the dataset. However, the classification was not efficient.

A novel IDS technique of cluster leader election process and a hybrid IDS was introduced in [18]. It provides the intrusion detection service by means of Vickrey Clarke-Groves mechanism in MANET. However, the intrusion detection rate was not enhanced and reduces the false positive rate. The cross-layer based distributed machine learning anomaly detection system was developed in [**?**] to protect the system. However, the throughput was not improved. This problem is addressed and it reduced in SA-NBC technique using Simulated annealing based Naive Bayes classifier.

6 Conclusion

A novel technique is called Simulated Annealing based Naive Bayes classifier (SA-NBC) is proposed to detect Anomaly Intrusion Detection in wireless ad-hoc network. An anomaly-based intrusion detection system is an essential one to observe the network activities and classify whether it either normal or anomalous node. Hence, the accuracy of intrusion detection is enhanced. In proposed SA-NBC technique, simulated annealing is used to choose the optimal feature of the node and thus detect the intrusion in the network. Based on these optimal features, the Naive Bayesclassifier is used to classify the malicious node and normal node with the aid of calculating conditional probability. It outlines the vector representation for detecting the network intrusions and observes network behavior and classifying the node as either normal or abnormal (anomalous). The experiments are conducted on different parameters such as anomaly intrusion detection accuracy, execution time and throughput. The performance results show that the proposed SA-NBC technique improves the anomaly intrusion detection accuracy, throughput and reduces the execution time than the state-of-art methods.

References

[1] V. N. T. AlkaChaudhary and A. Kumar, "A new intrusion detection system based on soft computing techniques using neuro-fuzzy classifier for packet dropping attack in MANETs," *International Journal of Network Security*, vol. 18, no. 3, pp. 514–522, May 2016.

[2] S. Bu, F. R. Yu, X. P. Liu, P. Mason, and H. Tang, "Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 3, pp. 1025–1036, Mar. 2011.

[3] S. Ganapathy, P. Yogesh and A. Kannan, "An intelligent intrusion detection system for mobile ad-hoc networks using classification techniques," *Advances in Power Electronics and Instrumentation Engineering*, vol. 148, pp. 117–122, 2011.

[4] W. R. Ghanem, M. Shokair and M. I. Dessouky, "Defense against selfish PUEA in cognitive radio network based on hash message authentication code," *International Journal of Electronics and Information Engineering*, vol. 4, no. 1, pp. 12–21, 2016.

[5] D. G. Gopal1 and R. Saravanan, "A novel trust based system to detect the intrusive behavior in MANET," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 31–43, 2015.

[6] C. Kolias, V. Kolias, G. Kambouraki, "TermID: A distributed swarm intelligence-based approach for wireless intrusion detection," *International Journal of Information Security*, vol. 16, no. 4, pp. 401–416, 2017.

[7] B. Mahapatra, S. Patnaik, "Self adaptive intrusion detection technique using data mining concept in an ad-hoc network," *Procedia Computer Science*, vol. 92, pp. 292–297, 2016.

[8] S. Mamatha and A. Damodaram, "Intrusion detection system for mobile ad hoc networks based on the behavior of nodes," *International Journal of Grid Distribution Computing*, vol. 7, no. 6, pp. 241–256, 2016.

[9] R. Mitchell and I. R. Chen, "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 16–30, 2015.

[10] A. Mitrokotsa and C. Dimitrakakis, "Intrusion detection in MANET using classification algorithms: The effects of cost and model selection," *Ad Hoc Networks*, vol. 11, pp. 226–237, 2013.

[11] N. Mohd, S. Annapurna, H. S. Bhadauria, "Taxonomy on security attacks on self configurable networks," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 44–52, 2015.

[12] F. Nabi, M. M. Nabi, "A process of security assurance properties unification for application logic," *International Journal of Electronics and Information Engineering*, vol. 6, no. 1, pp. 40–48, 2017.

[13] S. OzgeCepheli G. Kurt, "Hybrid Intrusion detection system for DDoS attacks," *Journal of Electrical and Computer Engineering*, vol. 2016, pp. 1–8, 2016.

[14] K. Pavani and A. Damodaram,. "Multi-class intrusion detection system for MANETs," *Journal of Advances in Computer Networks*, vol. 3, no. 2, pp. 93–98, 2015.

[15] E. M. Shakshuki, N. Kang and T. R. Sheltami, "EAACK - A secure intrusion-detection system for MANETs," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 3, pp. 1089–1098, 2013.

[16] N. Shah and S. Valiveti, "Intrusion detection systems for the availability attacks in ad-hoc networks," *International Journal of Electronics and Computer Science Engineering*, vol. 1, no. 3, pp. 1850–1857, 2012.

[17] T. Sheltami, A. Basabaa and E. Shakshuki, "A3ACKs: Adaptive three acknowledgments intrusion detection system for MANETs," *Journal of Ambient Intelligence and Humanized Computing*, vol. 5, no. 4, pp. 611-620, 2014.

[18] B. Subba, S. Biswas, S. Karmakar, "Intrusion detection in mobile ad-hoc networks: Bayesian game formulation," *Engineering Science and Technology*, vol. 19, pp. 782–799, 2016.

[19] M. Usha and P. Kavitha, "Anomaly based intrusion detection for 802.11 networks with optimal features using SVM classifier," *Wireless Networks*, vol. 23, no. 8, pp. 2431–2446, 2017.

Biography

K. Murugan is Assistant Professor and Head of the Department of Computer Science at Government College for Women, Kolar. His current area of research interest is Computer Networks and its applications. He has successfully guided 15 candidates for M.Phil. He has been teaching computer Science for the past 18 Years. He completed his Master Degree in Computer Science at Bharathidasan University, Master of Philosophy in Computer Science at Manonmaniam Sundaranar University, Master of Engineering in Computer Science and Engineering at Anna University.

P. Suresh is Associate Professor and Head, Department of Computer Science, Salem Sowdeswari College [Govt. Aided], Salem. He received the M.Sc, Degree from Bharathidasan University in 1995, M.Phil Degree from Manonmaniam Sundaranar University in 2003. The M.S (By Research) Degree from Anna University, Chennai 2008 in Science and Humanities. PGDHE Diploma in Higher Education and Ph.D Degree from Vinayaka Missions University in 2010 and 2011 respectively in Computer Science. He is an Editorial Advisory Board Member of Elixir Journal. His research interest includes Data Mining and Natural Language Processing. He is a member of Computer Science Teachers Association, New York.