DESIGN OF NETWORK ARCHITECTURE FOR INTRUSION DETECTION USING SPANNING TREE MULTICLASS CLASSIFIER IN MANET

[1]V. UMA DEVI, [2]C. CHANDRASEKAR

[1]Scholar, Department of Computer Science, Karpagam University, Coimbatore, Tamil Nadu, India.
[2]Associate Professor, Department of Computer Science, Periyar University, Selam, Tamil Nadu, India.

E-mail: [1]vumadevi76@gmail.com , [2]ccsekar@gmail.com

ABSTRACT

Security in mobile ad-hoc network plays a strategic role to ensure high level of protection without any intrusions in computer networks. Most of the intrusions in mobile ad-hoc network are traced and detected by collecting traffic information and classified according to different classification algorithms. With individual traffic classifiers design, packet delay is expected to surely go up with overhead cost rate. These classification processes hosted on mobile ad-hoc network failed to develop multiclass classifier system under varied conditions and minimized the efficiency on detecting intrusions in network architecture. To present mobile ad-hoc network architecture, with multi-classifier intrusion detection system, a mechanism called, Tuning Spanning Tree Multiclass Classifier (TSTMC) is proposed in this paper. The TSTMC mechanism works with multiple classification process in MANET to detect the intruded distribution nodes. First, Multiclass Neural Shannon's Entropy based approach analyzes the network traffic properties based on the count of source destination pair, packet type, packet size and payload. After analyzing the traffic rate on MANET, the result are used in the next step to construct spanning tree network architecture. Secondly, the spanning tree is constructed with Tuning Tutte polynomial operations where the internal and external traffic over mobile ad-hoc network is classified. Tuning Tutte polynomial operation is used effectively to detect the abnormal activities through tuning spanning tree. Analysis is accomplished for different parameters, including the maximum node velocity and the average multiclass error rate they experience, node density and their true positive rate on detecting abnormal activities, packet delay and classification sensitivity rate. Simulations using NS2 were used to measure the performance of the mechanism to compare it with the performance of two other intrusion models for mobile ad-hoc networks, namely, GP and SSUM. The measured results signify the effectiveness of the proposed mechanism in terms of achieved multiclass error rate, classification sensitivity and low packet delay.

Keywords: *Multiclass Neural Shannon's Entropy, Mobile Ad-hoc Network, Tuning Spanning Tree, Intrusion Detection, Tutte Polynomial, Abnormal Activities*

1. INTRODUCTION

Enhanced Adaptive ACKnowledgement (EACK) was designed in [3] which were proven to be secured using digital signature with appendix and digital signature with message recovery. However, network overhead increased and security remained unaddressed with the increase in varying node density. Classification methods were used in [4] to detect the intrusion for varied traffic patterns and node density. The method proved to be efficient in terms of classification error generated that reduced with the increase in the node density.

A major drawback was the network degradation as it worked well with simulators but not using real data set. To address this issues, Intrusion Detection and Adaptive Responsive (IDAR) [5] mechanism was designed based on the level of attack, network degradation and so on. However, the accuracy of intrusion being detected was unaddressed. Hybrid Intrusion Detection (HID) model [6] addressed the intrusion detection rate with respect to accuracy using Tree Augmented Naïve Bayes (TAN). Reduced Error Pruning (REP) algorithm was used for efficient classification of intrusion being detected.

In the current scenario processing information based on Internet, are highly susceptible to several types of threats resulting in severe damages, namely the intrusion detection systems (IDS). Selection of features and classification based on intrusion was designed in [7] using rule-based attribute selection algorithm. Though efficient, multilayer model remained unaddressed. Maximum Overlap Discrete Overlap Transform (MODOT) [8] introduced clustering algorithm based on geometric properties to minimize the false positive and false negative rates. A signature based Intrusion Detector was designed in [9] to not only minimize the consumption of resources but also to improve the detection rate.

Based on the aforementioned techniques and methods, in this work, an effective network of design architecture called as Tuning Spanning Tree Multiclass Classifier (TSTMC) is designed in mobile ad-hoc network. The mechanism is implemented to identify the multiclass error rate by minimizing the packed delay by improving the classification sensitivity. The contributions of TSTMC mechanism are

(i) To provide multi-classifier intrusion detection system using mobile ad-hoc network architecture called, Tuning Spanning Tree Multiclass Classifier (TSTMC).

(ii) To detect intruded distribution nodes using multiple classification process in MANET.

(iii) To analyze the network traffic properties using the count of source destination pair, packet type, packet size and payload based on Multiclass Neural Shannon's Entropy based approach.

(iv) To efficiently classify the internal and external traffic over mobile ad-hoc network by constructing the spanning tree network architecture using Tuning Tutte polynomial operations.

(v) To detect the abnormal activities through tuning spanning tree using Tuning Tutte polynomial operation.

The rest of this paper is structured as follows: Section 2 discusses the techniques of intrusion detection and classification methods. Section 3 provides with the related works on intrusion detection system in mobile ad-hoc network. Section 4 presents experimental setting and section 5 illustrates the results for evaluating the proposed TSTMC mechanism. Finally, Section 5 gives concluding remarks.

2. RELATED WORKS

One of the most appealing mobile ad-hoc networks is the mobile ad-hoc network where the key issue to be handled is security. Securitizing mechanism against DDoS attack was provided in [10] at routing level based on the neighbor certification to increase the rate of throughput. An overview of intrusion detection systems in the purview of mobile ad-hoc network was designed in [11]. However, single classifier was taken into consideration to detect the level of intrusion in MANET. A hybrid intelligent approach [12] was designed to address the issues related to combination of classifiers and minimized the best possible false alarm rates using random forest model. Though false positive rate was improved with the application of multiple classifiers, with the increased node density at different interval of time, the method was not an efficient model.

With the most flexible in operation, mobile ad hoc networks (MANETs) are increasingly gaining higher amount of reception with respect to next-generation network arena. Also with the increasing mobility one of the key issues to be addressed is the anomaly detection rate. Anomaly-detection [13] based on dynamic learning process was designed to perform the process of identifying the intrusion at specific time intervals using multidimensional statistics. However, security remained unaddressed. To provide security, a fuzzy model was introduced in [14] by increasing the identification of intrusion rate. But, classification of normal and abnormal activities was not performed. Separate classification of normal and abnormal activities was concentrated on [15] with the help of proactive and reactive protocol. An enhanced protocol called as the Secured AODV (SAODV) was introduced in [16] using a Trust Based Mechanism (TBM) to improve the throughput level.

One of the serious problems posed in the Internet security is the Denial of Service (DoS) attack. Group Testing (GT) based approach was introduced in [17] to minimize the low negative rate while detecting the intrusion pattern. However, the distributed nature remained unaddressed. A novel trace back method for DDoS was introduced in [18] to identify the traffic patterns and the polluted packets. The model was not proved to be finer granularity. Optimal feature selection was introduced in [19] to address the problem related to penetrations in a illegal manner using k-means classifier.

Indeed, the absence of multiclass classifier system in mobile ad-hoc network under varied conditions and node density is a major threat that has to be resolved. It is, hence, significant to consider the above said concerns when scheming and establishing an intrusion detection system. With this, we design network architecture for intrusion detection using Spanning Tree Multiclass Classifier.

3. MOBILE AD-HOC NETWORK ARCHITECTURE WITH MULTI-CLASSIFIER FOR DETECTING INTRUSIONS

Mobile Ad-hoc network security is becoming an important factor. As a result, the proposed work is developed to detect the intrusions with minimal packet delay rate. Proposed Tuning Spanning Tree Multiclass Classifier mechanism identifies the intrusions by working with varied traffic data patterns. The entropy procedure is also introduced in the TSTMC mechanism to extract the traffic occurrence features on the mobile ad-hoc network architecture. The occurrences of features related to traffic taken for the research work are clearly depicted in Figure 1.

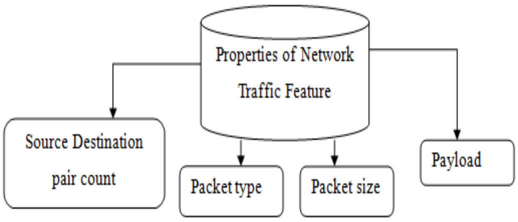
Properties of Network Traffic Feature
Source Destination pair count
Packet type
Packet size
Payload

Figure 1. Traffic Feature of Mobile Ad-hoc Network

As listed above, the properties of network traffic feature are considered and measured using Multiclass Neural Shannon's Entropy based approach. The TSTMC mechanism used this approach to easily identify the disorders (i.e.,) abnormal activity of the nodes in mobile ad-hoc network. Multiclass Neural Shannon's Entropy value in mobile ad-hoc network outranges the predefined range, and then the intrusion is placed on the network architecture. These entropy result measure is used as an input structure in TSTMC mechanism to construct the spanning tree and identify the abnormal activity in a precise manner. The spanning tree in TSTMC mechanism uses the polynomial operation to handle multiclass classifier and produce higher precision rate on detecting the intrusions in MANET.

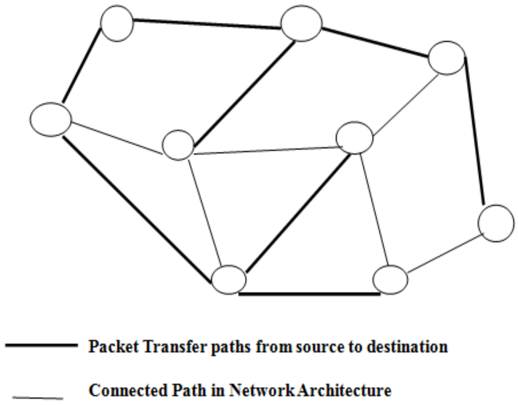
Packet Transfer paths from source to destination
Connected Path in Network Architecture

Figure 2. Diagrammatic Representation of Spanning Tree

Figure 2 depicts the diagrammatic representation of spanning tree developed in the proposed TSTMC mechanism to detect the intrusions easily through the sub graph edge points. As illustrated in the figure, the spanning tree is a connected graph where the network traffic features are connected with one another to detect the intrusions easily. A maximal set of edges are placed in the graph for easy transfer of the packet through several source-destination pair. Spanning tree uses the network traffic properties feature and performs the linear time breadth first search to detect the intrusions in MANET. Starting with the arbitrary root vertex 'AV', performs looping through the neighbor of the vertices (i.e., intermediate root paths of packet transfer) to detect the intruded nodes. The architecture diagram of Tuning Spanning Tree Multiclass Classifier (TSTMC) mechanism is depicted in Figure 3.

Journal of Theoretical and Applied Information Technology
10th June 2015. Vol.76. No.1
© 2005 - 2015 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

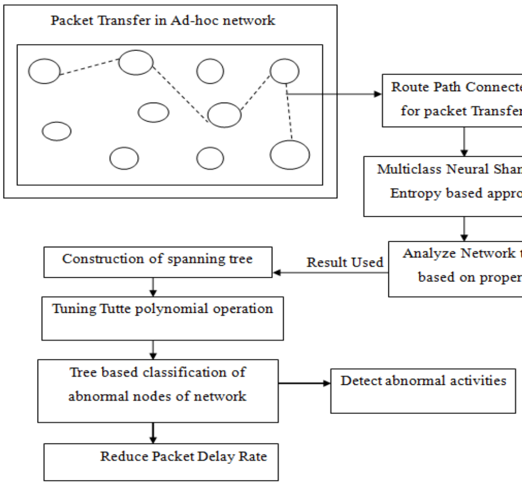
Packet Transfer in Ad-hoc network
Route Path Connected for packet Transfer
Multiclass Neural Shannon's Entropy based approach
Analyze Network traffic based on properties
Result Used
Construction of spanning tree
Tuning Tutte polynomial operation
Tree based classification of abnormal nodes of network
Detect abnormal activities
Reduce Packet Delay Rate

Figure 3. Architecture Diagram of TSTMC Mechanism

As illustrated in Figure 3, the intrusion nodes in the mobile ad-hoc network is traced and detected by collecting the information based on the network traffic properties. The route path is connected from source to the destination pair for packet transfer in mobile ad-hoc network. The traffic occurrence on the route path is analyzed by measuring the entropy value. The entropy measure in proposed TSTMC Mechanism uses the Multiclass Neural Shannon's Entropy based approach. Neural Shannon's Entropy based approach uses the input sensor node, intermediate nodes and destinations node of multiclass features to compute the value. The multiclass features used in the TSTMC Mechanism are source-destination pair, packet type, packet size and payload.

The network traffic measures the multiclass features and uses the result to construct the spanning tree. The spanning tree in TSTMC Mechanism uses the Tuning Tutte polynomial operation to handle multiclass features to classify the intrusion detected. Tuning Tutte polynomial clearly classifies the abnormal nodes in MANET. The abnormal nodes are also detected effectively with minimal delay time.

3.1. Multiclass Neural Shannon's Entropy Based Approach

Neural Shannon's Entropy based approach in TSTMC Mechanism identifies the uncertainties observed in mobile ad-hoc network architecture. The uncertainties results in the traffic occurrence on the route path while transferring packets from source to destination. In TSTMC mechanism, the traffic is measured based on entropy measure of network properties. The entropy measure of the network property is formularized as,

Entropy Source Destination Pair Count e(n1) = M (Source IP address ∩ Destination IP address) (1)

The source IP address and the destination IP address are compared with the predefined value and entropy measure 'M' is attained using TSTMC Mechanism.

$$Entropy\ Packet\ Type\ e(n2) = M(TCP, UDP, FTP, CBR) \quad (2)$$

According to (2), the packet type can be of Transfer Control Protocol (TCP), User Datagram Protocol (UDP), File Transfer Protocol (FTP), Constraint based Routing (CBR). The path selected for packet transfer and predefined structure is stored to measure the entropy value.

Entropy Packet Size e (n3) = M (Size of packet on source point) ∩ M (Size of packet on destination point) (3)

The entropy of packet size denotes the measure of packet size on the source point and destination point. The change on the values of packet size leads to the intrusion identification in mobile ad-hoc network.

Entropy of Payload e (n4) = M (No. of users involved in Network architecture) (4)

The users involved in transferring the packets are compared with the predefined value to measure 'M' the entropy of payload. All theses multiclass features are considered into the single output unit using the Neural Shannon's Entropy procedure. The single unit procedure is described as,

$$ShannonEntropy(SE) = \frac{-1}{N}\sum_{n=1}^{N}\log f(e(n)) \quad (5)$$

The summation of multiclass features together to get a neural (i.e.,) single output unit of the entropy value is provide in (5) where 'n' is the number of network features combined together using the log function 'f'. The total network features extracted in the mobile ad-hoc network structure is 'N' that denotes the total number of network features extracted in the ad-hoc network structure The result features of $e(n1)$, $e(n2)$, $e(n3)$, and $e(n4)$ together in a single output unit 'SH' are obtained in $e(n)$.

3.2. Spanning Tree based Multiclass Classifier

The result of the overall network entropy is used as the input procedure for easy classification of the intrusion. The spanning tree structure clearly detects the intrusions in a graphical form. The breadth first search procedure used to detect the intrusions in TSTMC mechanism. The minimal spanning tree spans the 'S' vertices from the arbitrary root (i.e.,) source vertices to detect the intrusion nodes. The delay is reduced in TSTMC mechanism by visiting only the fewest edges per vertices. The multiclass classification of intrusions is carried out using the Tuning Tutte Polynomial operation.

3.2.1. Tuning Tutte polynomial operation

Tuning step is used to adjust the network congestion and produce the effective classification of intrusions in MANET. Tuning Tutte polynomial plays the signification operation in TSTMC mechanism to perform multiclass classification of intrusions in proposed network architecture.

```
// Tuning Tutte Polynomial algorithm
Begin
Input: Graph –G, Arbitrary Vertex 'AV', 'S' – vertex, 'j'- Edges, 'n'- No. of network features
Output: Detected intrusions based on Tree classification with multiclass network Features
Step 1: Spanning Tree Graph (AV→ Start node)
Step 2: AV performs the Breadth First Search
Step 3: Polynomial Time processing of network Structure (Polynomial {internal & external root} path)
Step 4:
$Tuning\,Tutte(TT) = \sum (x)^{j(n)} + (x+1)^{j(n)} + \ldots + (x+n)^{j(n)}$
computed.
Step 5: Tuning Tutte sums up the vertices point on spanning tree to detect the intrusion nodes
End
```

The above algorithmic procedure describes about the Tuning Tutte Polynomial operation for effective classification of intrusion through tree structure. From the above algorithm, 'x' denotes the level of nodes that the detection is carried out based on the network features 'n'. Spanning tree used in the TSTMC mechanism improve the classification sensitivity rate. Sensitivity rate represents the detection of intrusions at a higher rate using the graph structure. Finally, higher rate of intrusion is detected with linear time in TSTMC mechanism using the polynomial operations.

4. PERFORMANCE ANALYSIS

Tuning Spanning Tree Multiclass Classifier (TSTMC) mechanism is evaluated in NS2 simulator to detect the intrusions in MANET. The network range of 1000*1000 mm size uses KDD Cup '99 dataset and DARPA Intrusion Detection System (IDS) Evaluation dataset for experimental work. DARPA dataset really appear like real network traffic information but contains synthetic data generates using a closed network. The data contains several proprietary network traffic generators, and hand inserted attacks.

In the Random Way Point (RWM) model, each mobile node moves to an irregularly chosen location. The irregular movement leads to the intrusion detection on some part of the network architecture. The RWM uses normal number of mobile nodes for scheduling the nodes. The chosen location with an arbitrarily chosen speed contains a predefined quantity and speed count. Proposed TSTMC mechanism is compared against the existing genetic Programming (GP) classification algorithms and Smart Server Update Mechanism (SSUM).

We now analyze the performance of our mechanism in terms of multiclass error rate, true positive rate on detecting abnormal activities, classification sensitivity rate and packet delay.

4.1 Multiclass error rate

We first describe how much iteration on an average is required in a network architecture to make a decision criteria as to whether uncertainty is observed in the traffic or not. Then, we will present the multiclass error rate of our mechanism. Let N denote the mobile network structure, with four entropy measure of network properties recorded in e(n1), e(n2), e(n3), e(n4) that represents the entropy of source destination pair count, packet type, packet size and payload respectively. Then the multiclass error rate using TSTMC is given as below

$$MER = e\,(N) - [e\,(n1),\, e\,(n2),\, e\,(n3),\, e\,(n4)] \quad (6)$$

From this equation we obtain the multiclass error rate for e(n1), e(n2), e(n3), e(n4) using (1), (2), (3) and (4) respectively.

4.2 True Positive Rate On Detecting Abnormal Activities

Let us consider network architecture with 700 nodes measured at a distance of 1000*1000 mm size using DARPA Intrusion Detection System (IDS) Evaluation dataset for experimental work. Each time when a packet has to be sent from source to destination based on the network traffic feature then there occurs a possibility of detection of both normal and abnormal activities. Let us assume that from a total of 700 nodes, 500 nodes are normal nodes and the remaining 200 nodes represent the abnormal nodes. But it 400 nodes are identified as normal and 300 nodes are identified as abnormal nodes, then the true positive rate is reduced. So, the true positive rate on detecting the abnormal activities is given as below

$$TFR_{detecting\ abnormal\ activities} = \frac{Abnormal_{correctly\ identified}}{Abnormal_{correctly\ identified} + Abnormal_{wrongly\ identified}} \quad (7)$$

4.3 Classification Sensitivity Rate

In a similar manner, the classification sensitivity rate using TSTMC mechanism is listed below

$$Classification_{sensitivity} = \frac{Classificaiton\ of\ intrusion_{correctly\ classified}}{Abnormal\ Classification_{correctly\ classified} + Abnormal\ Classification_{wrongly\ classified}} \quad (8)$$

4.4 Packet Delay

In order to measure the packet delay, the spanning tree model is used in TSTMC mechanism that considers fewest edges per vertices. Once the root has been selected in a spanning tree, each node determines the cost involved for each possible path from itself to the root. From these, it the smallest cost path is selected which becomes root port (RP) of the spanning tree.

$$ST = \sum_{path=1}^{p} Nodes_{path} \quad (9)$$

5. SIMULATION RESULTS

Tuning Spanning Tree Multiclass Classifier (TSTMC) mechanism is compared against the existing Genetic Programming (GP) [1] and Smart Server Update Mechanism (SSUM) [2]. The evaluation table given below through table value and graph form describes the TSTMC mechanism in mobile ad-hoc network minimizes the multiclass error rate. Table 1 evaluates the multiclass error rate measured in terms of percentage achieved with the different number of nodes ranging from 50 to 350 and comparison is made with the two existing schemes namely, Genetic Programming (GP) and Smart Server Update Mechanism (SSUM).

Table 1. Tabulation for Multiclass Error Rate

Node Density	Multiclass Error Rate (%)		
	TSTMC	GP	SSUM
50	45.81	51.84	62.86
100	48.35	54.38	65.50
150	51.25	56.28	67.28
200	53.35	59.34	70.36
250	50.25	56.24	67.26
300	54.25	60.25	71.27
350	58.85	64.83	75.85

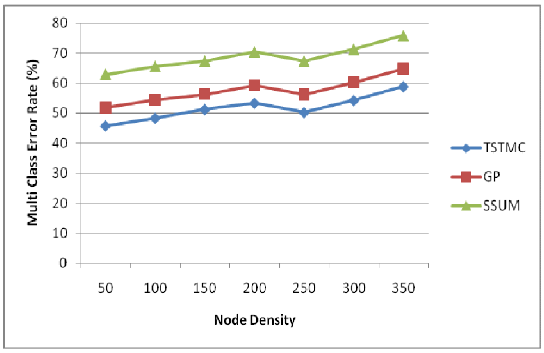

Figure 4. Measure Of Multiclass Error Rate With Respect To Node Density

Figure 4 describes the multiclass error rate based on the different node densities in mobile ad-hoc network. The entropy measure of network properties of each packet is measured based on packet size, packet type payload and source destination pair. With this network traffic feature, uncertainties are obtained and helps to reduce the multiclass error rate by 9 – 13 % compared to GP [1]. Using the entropy source destination pair (1), the entropy value is measured with the predefined path structures and path selected for packet transfer. The Neural Shannon's Entropy procedure considers the single output unit using the log function 'f' which reduces the multiclass error rate by 28 – 37 % compared to SSUM [2].

Table 2. Tabulation For True Positive Rate On Detecting Abnormal Activities

Maximum node velocity (m/sec)	True positive rate on detecting abnormal activities (%)		
	TSTMC	GP	SSUM
2	0.363	0.343	0.255
4	0.374	0.354	0.266
6	0.553	0.533	0.455
8	0.455	0.435	0.365
10	0.652	0.632	0.544
12	0.712	0.692	0.605
14	0.810	0.790	0.700

The True positive rate on detecting abnormal activities of our work TSTMC with the existing two schemes namely Genetic Programming (GP) [1] and Smart Server Update Mechanism (SSUM) [2] is provided in table 2.

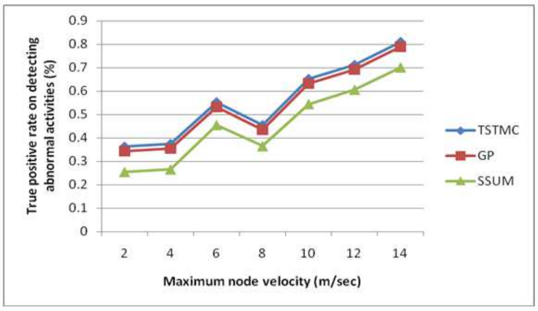

Figure 5. Measure Of True Positive Rate On Detecting Abnormal Activities Over Node Velocity

Figure 5 show that the proposed Tuning Spanning Tree Multiclass Classifier (TSTMC) mechanism provides higher true positive rate when compared to GP [1] and SSUM [2]. Though true positive rate increases with the increase in node velocity, comparatively TSTMC is proved to be efficient. The rate of efficiency achieves at a higher value when the node velocity is 6 m/sec. This is because of the application of Multiclass Neural Shannon's Entropy based approach that easily identifies the abnormal activities of the node in mobile ad hoc network. This in turn improves the true positive rate on detecting abnormal activities by 2 – 5 % and 13 – 29 % compared to GP and SSUM respectively.

Table 3.Tabulation For Classification Sensitivity Rate

Maximum node velocity (m/sec)	Classification Sensitivity Rate (%)		
	TSTMC	GP	SSUM
2	0.475	0.373	0.393
4	0.486	0.384	0.404
6	0.675	0.563	0.583
8	0.585	0.465	0.475
10	0.764	0.662	0.692
12	0.825	0.712	0.732
14	0.920	0.810	0.840

The higher influence of classification sensitivity rate with respect to the node velocity is listed in table 4 and comparison is made with two other existing schemes. It can also be seen that the classification sensitivity rate increases with the increase in the node velocity which is measured in terms of m/sec.

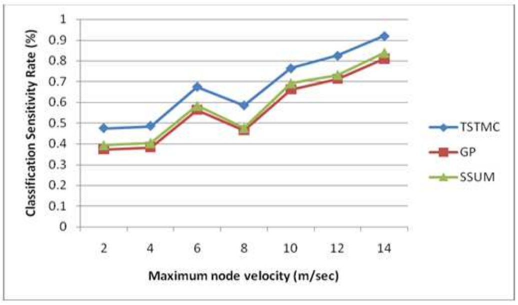

Figure 6. Measure Of Classification Sensitivity Rate Over Node Velocity

To measure the performance of the classification sensitivity rate over node velocity, comparison is two other existing techniques, GP [1] and SSUM [2]. In Figure 6, the node velocity is varied between 2 and 14. From the figure it is illustrative that the classification sensitivity rate is improved using the proposed Tuning Spanning Tree Multiclass Classifier (TSTMC) mechanism when compared to the two other existing works. This improvement rate is significant with the aid of Tuning Tutte polynomial operation. The polynomial time processing of network structure classifies accurately the internal and external traffic over mobile ad-hoc network and therefore improves the classification sensitivity rate by 11 – 21 % compared to GP. Finally, with the application of Spanning tree in the TSTMC mechanism that detects the intrusions through the sub graph edge points, further improves the classification sensitivity rate by 8 – 18 % compared to SSUM.

Table 4. Tabulation For Packet Delay

Node Density	Packet Delay (ms)		
	TSTMC	GP	SSUM
50	35.35	47.45	50.47
100	38.42	50.52	53.54
150	41.33	53.43	56.45
200	39.25	51.35	54.36
250	44.65	56.75	59.77
300	58.85	70.95	73.98
350	61.35	73.45	78.46

The results of packet delay are illustrated in table 4. It can be seen that our scheme TSTMC achieves higher packet delay with increase in the node density. But comparative analysis shows that the packet delay is lesser than the other two schemes.

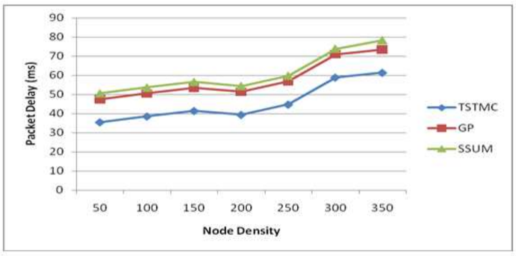

Figure 7. Measure Of Packet Delay Versus Node Density

In figure 7, we depict the packet delay for classifying the abnormal nodes from the network architecture observed in mobile ad-hoc network node using varying node densities with ranges between 50 and 35 nodes for experimental purpose and applied in NS2 simulator. From the figure, the value of packet delay achieved using the proposed Tuning Spanning Tree Multiclass Classifier (TSTMC) mechanism is lower when compared to two other existing techniques namely, Genetic Programming (GP) [1] and Smart Server Update Mechanism (SSUM) [2]. Besides we can also observe that by increasing the density of nodes, the packet delay also gets increased. But comparatively using the TSTMC mechanism it is comparatively less than two other methods. The packet delay is reduced by constructing a spanning tree model in TSTMC Mechanism that uses a polynomial operation referred to as the Tuning Tutte polynomial operation. This polynomial operation in turn classifies the intrusion being detected and therefore the occurrence of abnormal nodes in MANET. Therefore packet delay is gradually reduced by 19 – 34 % and 25 – 42 % compared to GP and SSUM respectively.

6. CONCLUSION

In this paper, an efficient design of network architecture for intrusion detection using Tuning Spanning Tree Multiclass Classifier (TSTMC) mechanism in MANET is provided. This mechanism provides multi-classifier intrusion detection system in mobile ad-hoc network. As the method uses multiple classification process in MANET, it increases coarser construction of true positive rate on detecting abnormal activities. As a result, the proposed Neural Shannon’s Entropy algorithm minimizes the multiclass error rate during packet transfer on the basis of packet type, packet size, payload and source destination pair count. The construction of spanning tree using Tuning Tutte polynomial operation in mobile ad-hoc network improves the classification rate of abnormal nodes in MANET. The spanning tree based classification using breadth first search reduces the time complexity in detecting abnormal activities and significantly reduces the packet delay rate. A series of simulation results are performed with varied node density and node velocity to test the multiclass error rate, bandwidth, true positive rate on detecting abnormal activities, classification sensitivity rate and packet delay to measure the effectiveness of the mechanism TSTMC. The multiclass error rate is reduced to 37.21 % when compared with the SSUM method. Efficient measure of node volume on mobile ad hoc network enable the true positive ratio with 29.75 % improved result when compared with the existing system.

REFERENCES:

[1] Sergio Pastrana., Aikaterini Mitrokotsa., Agustin Orfila., Pedro Peris-Lopez., “Evaluation of classification algorithms for intrusion detection in MANET,” Knowledge-Based Systems, Elsevier journal., 2012

[2] Khaleel Mershad., and Hassan Artail., “SSUM: Smart Server Update Mechanism for Maintaining Cache Consistency in Mobile Environments,” IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 6, JUNE 2010

[3] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami,” EAACK—A Secure Intrusion-

Detection System for MANETs", IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013

[4] Aikaterini Mitrokotsa, Christos Dimitrakakis," Intrusion detection in MANET using classification algorithms: The effects of cost and model selection", Ad Hoc Networks, Elsevier, Apr 2012

[5] Adnan Nadeema, and Michael P. Howarth," An Intrusion Detection & Adaptive Response Mechanism for MANETs", Elsevier, Sep 2013

[6] Mradul Dhakar and Akhilesh Tiwari," A Novel Data Mining based Hybrid Intrusion Detection Framework", Journal of Information and Computing Science Vol. 9, No. 1, 2014, pp. 037-048

[7] Sannasi Ganapathy, Kanagasabai Kulothungan, Sannasy Muthurajkumar, Muthusamy Vijayalakshmi, Palanichamy Yogesh and Arputharaj Kannan," Intelligent feature selection and classification techniques for intrusion detection in networks: a survey", EURASIP Journal on Wireless Communications and Networking, Elsevier, 2013,

[8] Mohamed Hamdi, AmelMeddeb-Makhlouf, and Noureddine Boudriga," Multilayer Statistical Intrusion Detection inWireless Networks", Hindawi Publishing Corporation EURASIP Journal on Advances in Signal Processing Volume 2009

[9] Mouhannad Alattar, Françoise Sailhan, and Julien Bourgeois," On Lightweight Intrusion Detection: Modeling and Detecting Intrusions Dedicated to OLSR Protocol", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013

[10] Prajeet Sharma, Niresh Sharma, Rajdeep Singh," A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network", International Journal of Computer Applications (0975 – 8887) Volume 41– No.21, March 2012

[11] Ehsan Amiria, Hassan Keshavarzb, Hossein Heidaric, Esmaeil Mohamadid, Hossein Moradzadehe," Intrusion Detection Systems in MANET: A Review", International Conference on Innovation, Management and Technology Research,
Malaysia, Elsevier, 22 – 23 September, 2013

[12] Mrutyunjaya Pandaa, Ajith Abrahamb, Manas Ranjan Patrac," A Hybrid Intelligent Approach for Network Intrusion Detection", International Conference on Communication Technology and System Design, Elsevier 2011

[13] Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour, Yoshiaki Nemoto, , and Nei Kato," A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 5, JUNE 2009

[14] A. Chaudhary1, V. N. Tiwari2 and A. Kumar3," Analysis of Fuzzy Logic Based Intrusion Detection Systems in Mobile Ad Hoc Networks", International Journal of Information Technology, Feb 2014

[15] Dina Sadat Jalali1, Alireza Shahrbanoonezhad2," A Novel Method Intrusion Detection Based on Sending and Checking Packet for Neighbored Nodes in MANET", Universal Journal of Communications and Network 2(1): 10-13, 2014

[16] Floriano De Rango, "Trust-Based SAODV Protocol with Intrusion Detection, Trust Management and Incentive Cooperation in MANETs", IGI PUBLISHING, Sep 2009

[17] Ying Xuan, Incheol Shin, My T. Thai, and Taieb Znati," Detecting Application Denial-of-Service Attacks: A Group-Testing-Based Approach", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 21, NO. 8, AUGUST 2010

[18] Shui Yu, Wanlei Zhou, Robin Doss, and Weijia Jia,," Traceback of DDoS Attacks Using Entropy Variations", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 3, MARCH 2011

[19] Khalil El-Khatib," Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 21, NO. 8, AUGUST 2010