IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-10, Oct 2018 E-ISSN: 2347-2693

Gwet Kappa Trust Factor-Based Repeated Node Taxonomy Scheme for Malicious Adversaries Detection

R. Saravanan[1*], E. Ilavarasan[2]

[1] Dept. of Computer Science and Engineering, Saveetha Engineering College, Chennai, Tamil Nadu. India

[2] Dept. of Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India

[*]*Corresponding Author: sararaju@hotmail.com*

Available online at www.ijcseonline.org

Accepted: 17/Oct/2018, Published: 31/Oct/2018

Abstract **-** There is a growing interest for mobile ad hoc network (MANET) in the recent years for many time-critical applications, such as military applications or during a disaster recovery scenario in a collaborative manner. In this paper, we proposed a Gwet Kappa Trust Factor-Based Repeated Node Taxonomy Scheme (GKRNTS) for malicious adversaries node detection which focuses on the discrimination of mobile nodes into malicious and benevolent nodes. The interactions between the mobile nodes are periodically monitored and the elucidated data are useful for determining the degree of collaboration between the mobile nodes through the computation of Gwet Kappa. The Gwet Kappa parameter used in this Repeated Node Taxonomy Scheme is stored with each node as an adjacency matrix that stores the interaction activity between the nodes of the network. This adjacency matrix quantifies the extent of cooperation existing between the mobile nodes of the network and they are considered as the taxonomy of the mobile nodes during data communication. The proposed GKRNTS is compared against the TPFPPDM and NPDRDS techniques by simulation using NS2 network simulator has led to promising results in terms of reduced packet rate, energy consumption and computational cost.

Keywords- MANETs, Node Taxonomy, Gwet Kappa, Malicious Nodes

I. INTRODUCTION

The advancement and evolution in the field of wireless technology have brought about dramatic changes in a person's life around the globe by facilitating reliable and trustworthy pervasive communication. This provision of pervasive communication helps the people to utilize technology in their day-to-day activities in order to reduce time during the accomplishment of tasks. Pervasive technology enables the people of the world to stay connected to the largely available networks of the world through their ready-made mobile equipment's like mobile phones, laptops, etc. One of such potential communication with the pervasive technology domain is the Mobile Ad hoc Network [1] that is devoid of base stations and mostly necessitates multi-hop communication for reliable data dissemination. The paper is organized by exploiting the vulnerabilities, decentralization and other aspects in this section.

II. COMPARATIVE STUDY

This section presents the details on some of the exiting methods relating to the proposed context of study.

II.I Naïve Probability-based Dynamic and Reactive Detection Scheme

A Naïve Probability-based Dynamic and Reactive Detection Scheme (NPDRDS) was proposed for handling the influence introduced by the emergence of jamming and selfish malicious nodes in the network [2]. This NPDRDS approach handles the process of detecting malicious nodes through the incorporation of two potent parameters, namely jamming and selfish parameter such that the maximum degree of network performance is ensured. The packet delay of the network is determined to high during the implementation of the NPDRDS approach since they fail to handle the impact of partial dropping selfish nodes.

II.II Threshold Packet Forwarding Potential Parameter-based Detection mechanism

The TPFPPDM approach is found to effectively detect malevolent nodes for improving the Quality of Service (QoS) in MANET[3]. In TPFPPDM, malicious adversaries are detected effectively based on the utilization of three parameters called Interaction Frequency Index (IFI), Index Of Intimacy (IOI) and Index Of Honesty **(**IOH). All the three factors are computed based on the past experiences derived through the interaction of each mobile node to the directly connected communicating nodes for sustaining reliable data dissemination [4].

II.II.I Computation of Interaction Frequency Index

The Interaction Frequency Index (IFI) refers to the degree of interaction or number of interactions that exists between the nodes of the network[5]. This IFI is determined using the

probe packets that are sent from the source to the destination nodes of the network. In this context, the probe packets help the monitoring nodes to estimate the degree of interaction made feasible by the monitored node at any particular point of time. The maximum number of interactions between the monitored nodes and its closer neighboring monitoring node infers better IFI. Thus IFI is calculated using Equation (2.1) which is the ratio of maximum number of interactions existing between the monitored and the monitoring nodes($M_{n(i)}$) to the cumulative number of interactions made possible by the monitored node to the other nodes of the network except the monitoring node (N_T).

$$TR_i^{IFI} = M_{n(i)} / N_T \quad (2.1)$$

II.II.II Calculation of Index Of Intimacy (IOI)

Index Of Intimacy (IOI) is the second factor essential for the computation of mobile nodes' trust. This IOI determines the time period in which the interaction between the monitored nodes and the monitoring nodes is maximum on par with the time period of interactions happening between the monitored nodes and the other neighboring nodes of the network. Thus IOI computed using Equation (2.2) represents the time incurred in the interaction between the monitored nodes and the monitoring nodes ($CTS_{l,m}$) to the cumulative time spent for interaction among the monitored node[6] and their interacting nodes($CTS_{l,m}$) of the network.

$$TR_i^{IOI} = CTS_{l,m} / CTS_{l,n} \quad (2.2)$$

II.II.III Calculation of Index Of Honesty (IOH)

Index Of Honesty **(**IOH) is the third factor used for quantifying the trust of the mobile nodes which is estimated using Equation (2.3) through the positive and negative interactions of the monitored mobile based on the viewpoint of the monitoring mobile nodes.

$$TR_i^{IOI} = f_i / f_{,i} + g_i \quad (2.3)$$

Where 'f_i' and 'g_i' represents the positive and negative interactions existing between the monitored and the monitoring mobile nodes of the network. Then, the Cumulative Trust Factor (CTF) [7]for quantifying a node as benevolent or malicious is determined based on Equation (2.4)

$$CTF_i = \alpha TR_i^{IFI} + \beta TR_i^{IOI} + \gamma TR_i^{IOH} \quad (2.4)$$

Finally, the estimated CTF is compared with the computed threshold parameter which is discussed in the forthcoming section.

II.II.IV Computation of Threshold Parameter

The estimation of the threshold parameter also depends on the past experience of the mobile node[8]. This past experience relates to the activity of the mobile node monitored over the number of session time 'k' till the recent past. Thus the threshold parameter is calculated based on Equation (2.5)

$$TH_p = \sum_{s=1}^{k}(PD_C)/ k \quad (2.5)$$

Where PD_c refers to the Packet delivery capability of the mobile nodes during the process of data dissemination. In this context, if the value of CTF_i is less than TH_P then the specific node is determined as malicious during data dissemination [9].

III. PROPOSED GKRNTS SCHEME

The proposed scheme uses Gwet Kappa trust factor for discrimination of mobile nodes into malicious and benevolent nodes which is done in order to eliminate malicious adversaries to improve the rate of data dissemination. The degree of collaboration between the mobile nodes through the computation of Gwet Kappa is the reliability factor based on which the mobile nodes is assigned taxonomical value for reliable data delivery. The Gwet Kappa parameter used in this Repeated Node Taxonomy Scheme is stored with each node as an adjacency matrix that stores the interaction activity between the nodes of the network. Further, this adjacency matrix quantifies the extent of cooperation existing between the mobile nodes of the network and they are considered as the taxonomy of the mobile nodes during data communication. The mobile node with the least taxonomical value (Gwet Kappa value) compared to the mean taxonomic value of all the mobile nodes under interaction is considered as the malicious node in the network.

The computation of Gwet Kappa value used in the proposed GKRNTS Scheme is as follows. Let 'k' be the number of mobile nodes under interaction with each mobile node of the network. This 'k' number of mobile nodes are periodically monitored for estimating the extent of collaboration rendered by them in terms of packet delivery capability. This degree of collaboration is quantified using the manipulation of Gwet Kappa which is an effective reliability factor of statistics proposed for eliminating the limitations of traditional Kappa reliability factors. Gwet Kappa estimates the trustworthiness of mobile nodes by multiple raters and it utilizes an agreement parameter that considers estimation errors and chance probability into account. Further, Gwet Kappa uses two rating factors named RF_1 and RF_2, in which RF_1 and RF_2 are determined by multiple number of raters (mobile nodes) using categorical methods and ordered categorical methods of rating respectively. Thus Gwet Kappa is calculated using Equation (3.1)

$$GK_{(i)} = P_0 - P_p / 1 - P_p \quad (3.1)$$

Where P_0 and P_P refers to the cumulative probability of rating and mean probability of the rating of the mobile nodes by the monitoring(Rating) mobile nodes over the monitored time. These probabilities depend on the manipulation of RF_1 and RF_2. The first influential factor called RF_1(First order agreement probability) is the modified form of $GK_{(i)}$ which is computed using Equation (3.2) based on Equations (3.3) to (3.5)

$$RF_1 = P_0 - P_{p(e)} / 1 - P_{p(0)} \quad (3.2)$$

$$P_{p(e)} = \frac{1}{R-1}\sum_{m=1}^{R}\pi_m(1-\pi_m) \quad (3.3)$$

$$\pi_m = \frac{1}{n}\sum_{i=1}^{n}\frac{f_{im}}{f} \quad (3.4)$$

$$P_o = \frac{1}{n}\sum_{i=1}^{R}(\sum_{m=1}^{R}\frac{f_{im}(f_{im}-1)}{f(f-1)}) \quad (3.5)$$

Where,f_{im} denotes the number of rating mobile nodes that categories the n^{th} interacting mobile node in the category 'm'. The categorizing index varies from 1 to m with 'm' varying from 1 to R. Furthermore, the reliability of the mobile nodes is again investigated using the second influential factor RF_2 (Second order agreement probability) derived from Equation (3.6) by adapting RF_1 based on Equations (3.7) to (3.11)

$$RF_2 = \frac{\hat{P}_0 - \hat{P}_{p(e)}}{1-\hat{P}_{p(0)}} \quad (3.6)$$

$$\hat{P}_{p(e)} = \frac{1}{R-1}\sum_{m=1}^{R}\hat{\pi}_m(1-\hat{\pi}_m) \quad (3.7)$$

$$\hat{\pi}_m = \sum_{i=1}^{R}\alpha_{m/g}\pi_p \quad (3.8)$$

$$\pi_P = \frac{1}{n}\sum_{i=1}^{n}\frac{f_{ip}}{f} \quad (3.9)$$

$$\alpha_{m/g} = \sum_{g=1}^{R}\beta\hat{P}_0 \quad (3.10)$$

$$\hat{P}_o = \frac{1}{n}\sum_{i=1}^{R}(\sum_{m=1}^{R}\frac{f_{im}(f_{im}-1)}{f(f-1)} + \sum_{g\neq 1}^{R}\sum_{g\neq 1}^{R}\frac{f_{ig}(f_{ig}-1)}{f(f-1)}) \quad (3.11)$$

Thus, the trust-based taxonomic value of the mobile nodes quantified using Gwet Kappa is computed depending on the number of mobile nodes interacting at the specific point of time with integration or without the integration of the influential factors RF_1 and RF_2 pairs. In case, if the number of nodes generally interacting with the mobile nodes is less than n(n-1) / 2 then RF_1 is used. In contrast, if the number of mobile nodes intersecting is greater than n(n-1) / 4, RF_2 is used. Else, the influential factors RF_1 and RF_2 pairs are normalized using formula defined in Equation (3.12)

$$RF_{norm} = RF_{(i)} - RF_{max} / RF_{min} - RF_{max} \quad (3.12)$$

Hence, the mobile node is determined to be malicious when the trust factor is less than the average of the quantified Gwet Kappa value evaluated cumulatively over the past history of interactions as defined in Equation (3.13) and then they are isolated from the network.

$$GK_{avg} = \frac{\sum_{i=1}^{s}GK_{(i)}}{k} \quad (3.13)$$

The taxonomic value computed using Gwet Kappa lies between the value of 0 and 1. The nodes acting maliciously have the possibility of infecting the other nodes of the network. Thus the nodes in the network should be classified repeatedly to avoid re-transmissions that affect the performance of the network. Thus Gwet Kappa-based repeated node classification method [10] detects the malicious nodes effectively and accurately. The algorithm of the proposed GKRNTS is given in below.

IV. PROPOSED GKRNTS ALGORITHM

Input: n-number of mobile nodes under interaction

Output: classification of nodes as malicious and benevolent

Step 1: For each of the mobile node '1' to 'n' in the network
Step 2: Compute Gwet Kappa for the monitored node
Step 3: Estimate RF_1 if the number of mobile nodes interacting with monitored node is less than $\frac{n(n-1)}{2}$.
Step 4: Estimate RF_2 if the number of mobile nodes interacting with monitored node is greater than $\frac{n(n-1)}{4}$
Step 5: Else
Step 6: Estimate $RF_{norm} = RF_{(i)} - RF_{max} / RF_{min} - RF_{max}$ for each of the mobile nodes
Step 7: If ($RF_{norm} < GK_{avg}$)
Step 8: Detect the mobile nodes as malicious adversary
Step 9: Else, The mobile node is benevolent.
Step 10: End If
Step 11:End For.

Pseudo Procedure of the propose algorithm

IV.I Experimental Setup

The potential of the proposed GKRNTS Scheme is explained based on the network topology as depicted below. Figure 4.1 presents the network topology of the ad hoc network used for explaining the process of GKRNTS Scheme implementation. It presents network topologies that consist of 9 mobile nodes labeled from 0 to 9. Initially, the Gwet Kappa-based taxonomic value ($GK_{(i)}$) represented through variable 's' is 0. Then the GKRNTS Scheme is implemented for detecting the malicious nodes. The mobile nodes 4, 8 and 9 are detected as malicious adversary from the network after iteration 2. Figure 4.2 highlights the computed ($GK_{(i)}$) of each mobile node in the considered network topology. Since, the mobile node '8' has less value of taxonomic value, it is detected as the malicious adversary and isolated from the network. This computation is performed for a predefined number of iterations (for example- 4) and are depicted in Figures 4.3, 4.4 and 4.5 respectively.

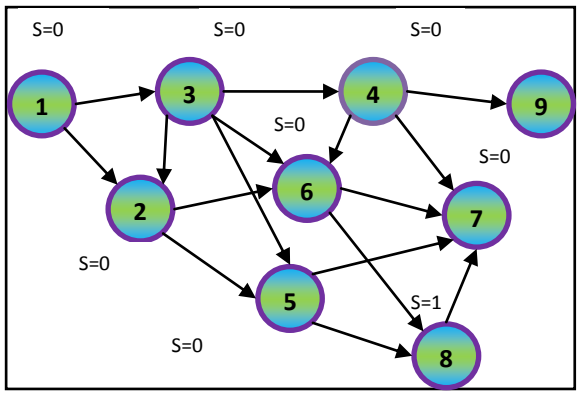

Figure 4.1: Network Topology used for presenting GKRNTS Scheme

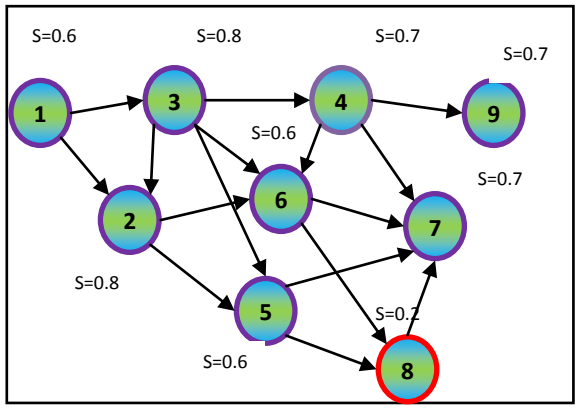

Figure 4.2: Node Taxonomy based Adversary Detection (First Iteration)

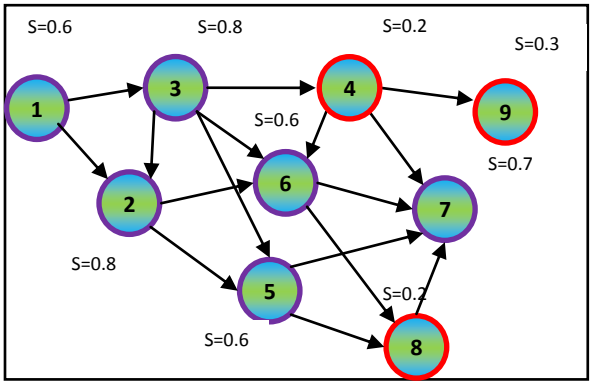

Figure 4.3: Node Taxonomy based Adversary Detection (Second Iteration)

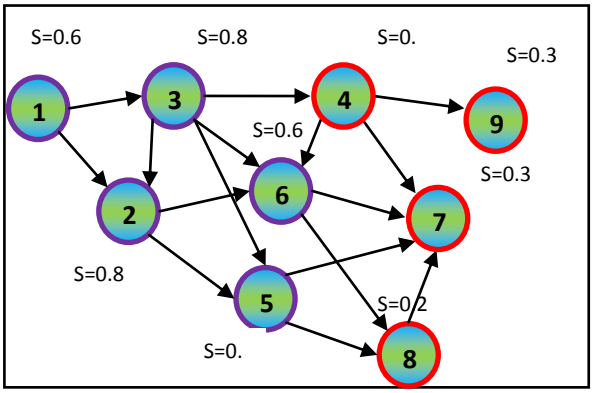

Figure 4.4: Node Taxonomy based Adversary Detection (Third Iteration)

The mobile nodes 4, 7, 8 and 9 are detected as malicious adversary from the network after iteration 3.

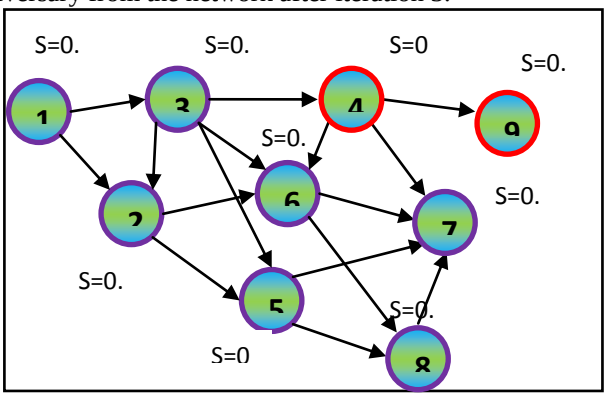

Figure 4.5: Node Taxonomy based Adversary Detection (Fourth Iteration)

Similarly, mobile nodes 4 and 9 are detected as malicious adversary from the network after iteration 4.

V. SIMULATION RESULTS AND DISCUSSION

The simulation experiments are conducted using the NS2 network simulator to evaluate the performance of the

proposed GKRNTS against existing TPFPPDM and NPDRDS techniques in terms of various performance metrics such as packet delivery ration, total overhead, packet loss rate and energy consumptions by varying the number of source and destination pairs. The following simulation setup is used for implementing the proposed GKRNTS, TPFPPDM and NPDRDS schemes. The simulation environment comprises of the network terrain area of 1500x1500 with 250 mobile nodes under the random motion in the network. The simulation parameters used for the experiment are tabulated in Table 5.1.

Table 5.1: GKRNTS method - Simulation Setup Parameters

Parameter	Value
Mobile nodes	250
Antenna type	Omni Antenna
Mobility model	Random Way Point
Model of Radio Propagation	Two Ray Ground
Traffic model	Constant Bit Rate (CBR)
Time for Simulation	300 Secs
Transmission Range	250 m
Type of MAC	802.11
Type of Network Interface	Wireless Phy Channel

Initially, the performance of the proposed GKRNTS method is studied using evaluation metrics defined as PDR, total overhead, and packet loss rate and energy consumptions. **Packet Delivery Ratio (PDR)** is defined as the ratio of data packets received by the destinations to those generated by the sources. Mathematically, it can be defined the eqn.(5.1) as:

$$PDR = \frac{\sum_0^n Packets\ Received}{\sum_0^n Packets\ Sent} \qquad (5.1)$$

Packet Loss Rate (PLR) is defined as the fraction of the total transmitted packets that did not arrive at the receiver node and it is mathematically defined by eqn.(5.2) as

$$PLR = \frac{Total\ Packets\ Dropped}{Total\ Packets\ Send} \qquad (5.2)$$

Energy Consumptions of mobile nodes are one of the most important issues that bring in catastrophic effects when not analysed. Higher consumptions of mobile node's battery power can lead to its failure that drastically disrupts the network performance. Thus, a considerable amount of focus needs to be given to the energy factor during the process of investigating security in the network. The mobile nodes of the network utilize its battery power for transmission and reception of data, node mobility and primitive node operation. The unnecessary retransmission of data packets caused by link failures, routing mishaps, link breakages and looping can cause draining of excessive amount of power during node operations. This unnecessary utilization of battery drain inculcates node failure possibility in the network. This energy utilization also leads to ample ways for a node to collapse or node failure state. This node failure probability needs to be avoided by proper utilization of available node battery level in a constrained and systematic manner. Novel schemes that consider node energy capacity during routing activity can avoid this problem. Reliable and secure schemes that generally require successive transmission and reception mechanisms until the node is recognized as a legitimate one is essential. These mechanisms also need to maintain trade off performance for preventing the activity of routing functionality induced by malicious nodes.

Figure 5.1 and Figure 5.2 shows the performance of GKRNTS method based on the PDR and total overhead compared to TPFPPDM and NPDRDS techniques. The PDR of GKRNTS technique is proved to be predominant than TPFPPDM and NPDRDS techniques since it is capable of detecting malicious adversaries even when the emergence of the monotonically increasing malicious adversaries are maximum in the network. Thus the PDR of GKRNTS technique is proved to be improved by 11% and 16% better to the existing TPFPPDM and NPDRDS techniques. The plots of total overhead have also proven the excellence of the proposed GKRNTS by a desirable minimum margin of 13% and 17% compared to TPFPPDM and NPDRDS techniques.

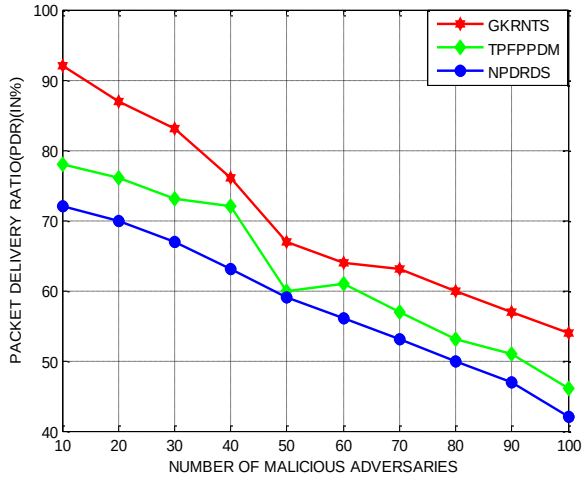

Figure 5.1 GKTFDM –PDR-Malicious adversaries

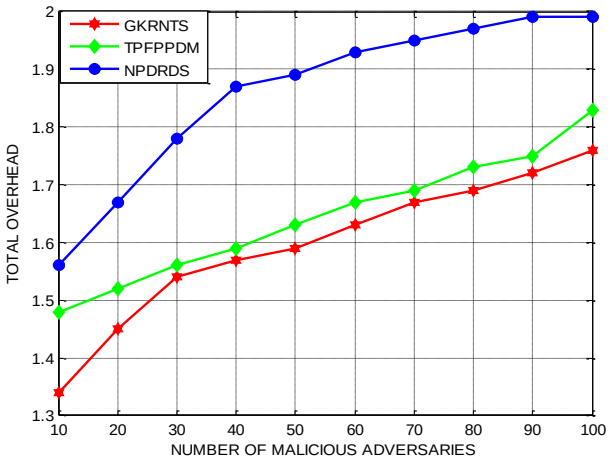

Figure 5.2: GKTFDM-total overhead-Malicious adversaries

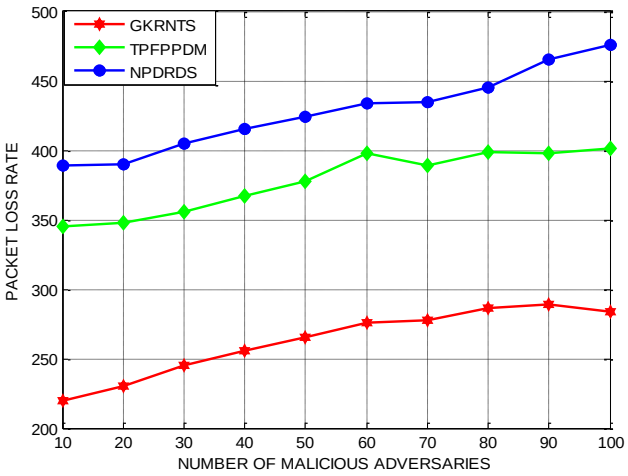

Figure 5.4-GKTFDM-packet loss rate-Malicious adversaries

Figures 5.3 and Figure 5.4 present the performance GKRNTS technique using packet drop rate and energy consumptions evaluated under a different number of malicious adversaries. The packet drop rate and the energy consumptions of the proposed GKRNTS technique is superior to the compared TPFPPDM and NPDRDS techniques since Gwet Kappa is capable of improving the rate of detection by using the concept of ordering categorical multiple rating factor. Thus the packet drop rate of GKRNTS method is determined to be minimized by 16% and 21% compared to TPFPPDM and NPDRDS techniques. Similarly, the energy consumptions of the proposed GKRNTS technique is drastically reduced
by 14% and 19% compared to the baseline TPFPPDM and NPDRDS techniques.

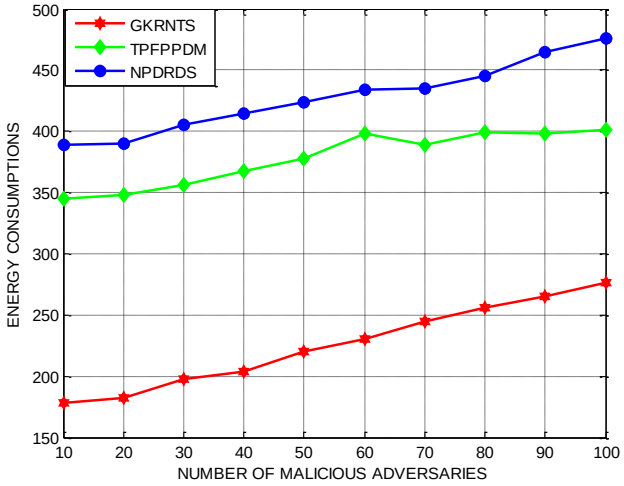

Figure 5.3- GKTFDM-Energy Consumptions-Malicious adversaries

Figures 5.5 and 5.6 explain the performance of GKRNTS technique using packet drop rate and energy consumptions evaluated under different numbers of CBR connections. The packet drop rate of GKRNTS method is reduced by 10% and 14% compared to TPFPPDM and NPDRDS techniques. Similarly, the energy consumptions of the proposed GKRNTS technique are also inferred to drastically reduced by 13% and 16% better to the compared detection schemes.

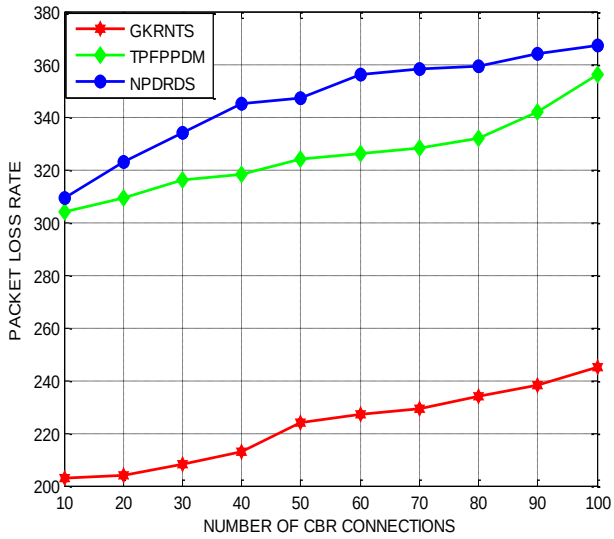

Figure 5.5-GKRNTS-Packet Loss Rate- Consumptions - Number of CBR connections

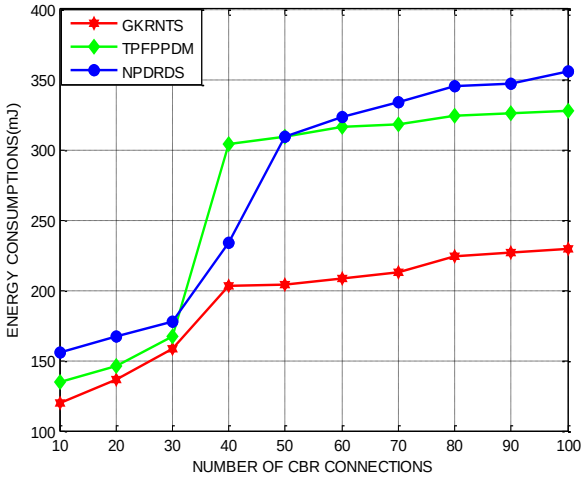

Figure 5.6-GKRNTS-Energy Number of CBR connections

VI. CONCLUSION

In this paper, we presented the Gwet Kappa-based Repeated Node Taxonomy Scheme (GKRNTS) for handling Malicious adversaries of the network. The algorithm and illustrations of the proposed Gwet Kappa-based Repeated Node Taxonomy Scheme is also presented. Simulation experiments for investigating the comparative performance of GKRNTS with TPFPPDM and NPDRDS techniques in term of various metrics such as PDR, total overhead, and packet loss rate and the performance of GKRNTS technique using packet drop rate and energy consumptions evaluated under different numbers of CBR connections. The implementation of the proposed GKRNTS technique and the computation of Gwet Kappa value for the reliable discrimination between the benevolent and malicious nodes of the network is also discussed. The proposed GKRNTS technique provide better results for various performance metrics when compared to TPFPPDM and NPDRDS techniques

REFERENCES

[1] Shailja Sharma , "A Review of Vulnerabilities and Attacks in Mobile Ad-Hoc Network", International Journal of Scientific Research in Network Security and Communication, Vol.6 , Issue.2 , pp.66-69, Apr-2018.

[2] Jaya, S and X. Deepak, " An Improved Naïve Bayes classifier for Intrusion DetectionSystem", *International Journal of Innovations & Advancement in Computer Science*, vol. 5, no.6, pp-128-134, 2016.

[3] Mitrokotsa, A., and Dimitrakakis, C., Intrusion detection in MANET using classification algorithms: The effects of cost and model selection, *Journal of Ad Hoc Networks*, 11(1), pp. 226-237, 2013.

[4] Youngseok Lee ; Ilkyu Park ; Yanghee Choi(2002),Improving TCP performance in multipath packet forwarding networks . Journal of Communications and Networks , Vol. 4(2)., pp 148 - 157 .

[5] Rebecca M. Warner,(1992) Dimensions of social interaction tempo: A factor analytic study of time and frequency domain indexes of interaction structure, The Journal of Psycholinguistic Research., Vol 21(3)., pp 173–191.

[6] K. Ravikumar, V. Manikandan , "Detection of Node Capture Attack in Wireless Sensor Networks", International Journal of Scientific Research in Computer Science and Engineering, Vol.6 , Issue.4 , pp.56-61, Aug-2018 .

[7] M. Natkaniec ; A.R. Pach (2000),An analysis of the influence of the threshold parameter on the IEEE 802.11 network performance , IEEE Wireless Communications and Networking Conference. Vol (3)., pp 23–28.

[8] Albers, P., Camp, O., Percher, J. M., Jouga, B., Me, L., and Puttini, R. S., Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches, *Journal of Wireless Information Systems*, pp. 1-12, 2002.

[9] Ishay Weissman,(2007), Confidence intervals for the threshold parameter, Journal of communications in statistics , Vol 1, pp 549-557 .

[10] Gopalakrishnan, S., and Kumar, P. M. (2016). Performance Analysis of Malicious Node Detection and Elimination Using Clustering Approach on MANET. *Circuits and Systems*, *07*(06), pp 748-758.

Authors Profile

R.Saravanan received Master's degree in Computer Applications from Manonmaniam Sundaranar University, Tirunelveli, India. Completed Master of Engineering degree in Computer Science and Engineering at Sathyabama University, Chennai, India. Working as a Associate Professor in the department of Computer Science Engineering at Saveetha Engineering College, Chennai, India. Area of interest includes Cloud Computing, Data Mining, Wireless Sensor Network, Mobile Computing, Networking, Specialization in Mobile Adhoc Network. Published 5 International Journals. Doing research on "Reliable Mitigation Techniques For Handling Malicious Adversaries In Mobile Ad Hoc Network" at Manonmaniam Sundaranar University ,Tirunelveli, India.He had more than twenty years of experience in teaching.

E. ILAVARASAN received the post graduate degree M.Tech. in Computer Science and Engineering from Pondicherry University, Puducherry, India, in 1997 and the Ph.D. degree in Computer Science and Engineering from the same University, in 2008. He is currently working as Professor in the Department of Computer Science and Engineering at Pondicherry Engineering College, Puducherry, India. His research interests include parallel and distributed systems, operating systems security, web services computing and embedded systems. He has organized National and International conferences with faculty members working in the Pondicherry Engineering College. He has published more than fifty research papers in the International Journals and Conferences. He had more than twenty five years of experience in teaching.

