IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

Identifying Black Hole Attack Based On Energy Consumption and Packet delivery ratio in the Routing Protocol

R.Saranya[1*], R.S.Rajesh[2]

[1,2]Dept. of Computer Science & Engineering, Manonmaniam Sundaranar University, India

[*]*Corresponding Author: saranya.shantha@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7i3.711718 | Available online at: www.ijcseonline.org

Accepted: 12/Mar/2019, Published: 31/Mar/2019

***Abstract*—** The main objective of this paper is to provide a secure-aware routing algorithm for mobile ad hoc networks. The cooperation and communication between MANET nodes are vital. This paper discusses the new algorithm which addresses the security threat in the communication networks. The proposed algorithm has three stages: 1) the Initial bait Stage; 2) Detection Stage using Reverse Tracing, And 3) Ensuring security and protection stage. The first stage is to find the existence of a malicious node on the transfer path. The Second Stage is used to find the nonmalicious node and malicious node in the transfer path. Finally, the last stage decides the malicious node in terms of the packet delivery ratio and energy value. These three stages are designed and executed using commercial software and the outputs of the proposed method are acquired. The important parameters such as Packet Loss, Misclassification rate, Detection accuracy, Packet Delivery Ratio, Throughput, and Routing Overhead is involved to discuss the performance of the proposed method. The Simulation is executed with the given parameters and final results are used to compare with the existing methods. From the comparison, it is apparent that the proposed approach has better performance than the existing methods.

***Keywords*—** Mobile ad hoc network (MANET), malicious node, black hole attack, Cooperative bait detection scheme, Packet Modification

I. INTRODUCTION

The Ad Hoc Network is a multi-hop wireless network that automatically connects each other via a wireless system with no fixed infrastructure. Rapid and easy deployment in a situation that is unlikely to create a consistent infrastructure network has increased the potential used in other applications in many key scenarios. Like a battlefield, disaster relief, conferences and more. The Mobile Network Specialist (MANET) can be distinguished by a mobile node that is free to move in any direction and has the ability to self-identify, self-supporting, and self-organizing through the network by means of a radio link without the infrastructure. Constants such as fixed stations, routers, and central servers. Since there is no base station or intermediary on the network, so each node acting as a router responsible during the relationship must be played by each node that is involved in network communication. Thus, all nodes are integrated with the Input Mechanism to provide packets from source to destination.

It is well known that to detect the hacker node in MANET is difficult because all nodes have mobility. The routing process may be affected because of the collaboration attacks which are provided by a malicious node in Mobile Adhoc Network (MANET). Harmful node provides many security problems like a gray hole and collaborative black hole attacks. The attack is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target. In gray hole attacks, the nodes should not be recognized first, as it later became malicious, defending a confidentiality-based solution to detect its presence in the network. The package is removed/forwarded when the packet passes through it.

DSR is a simple and efficient navigation protocol designed specifically for use on a wireless network node. The DSR allows the network to be self-managed and organized without the need for existing network infrastructure or administration. DSR has two main steps: road clearance and road maintenance. To end the route to the intersection of the RREQ route, send the route to the network. If half the node has path information to the destination in the repository it will respond with RREP to the receiving node. When RREQ checks the road record RREQ. When you get RREQ, you know the point across the road. The target node is based on data collection data between the packages to send the RREP response to the source node along with all path information. The DSR does not have a detection mechanism, but the source advice can get all the information on the road. In our approach, we use this feature. In the case of a dangerous black hole attack, use its own protocol to broadcast live. Use the shortest route to the target node or packet that wants to

interrupt. This aerodynamic node underlines the chance of creating an original route not based on the roadmap. In this way, the attack unit will have to provide in response to the Street Request, so cross the packet and hold it. In a flood-based protocol, the response from harmful nodes reaches the requesting node earlier than the actual response from the nodes. Thus, the paths of malicious and false are created. In general, harmful nodes are inserted into the data router. The following section II summarizes previous related work, section III explains the proposed method, section IV discusses and analyses the performance and section V concludes the proposed work.

II. RELATED WORK

Jin-Man Kim and Jong-Wook Jang [1] have requested the AODV Power Protocol, which uses the average cost-effectiveness algorithm to enhance network life. Each node plays an important role in the Adhoc Network. In particular, the state of the energy of each node has a profound effect on the whole life of the network. An attempt was made to extend the network's lifespan by adjusting the timing of RREQ delays, based on data derived from the comparison of the energy of the node and the average energy cost of the entire network. The results show that by implementing a cost-effective energy algorithm to the AODV protocol, it has had a positive impact on the overall network lifespan. Tripti Nema et al. [2] develops energy based on the Adhoc lead algorithm to require energy stability between the nodes as a result in preserving at least one energy level between the node and the life of the net expander. The focus of the algorithm is to increase the broader existence of the node in the network. Energy is limited to a minimum of a mobile unit. When a node reaches the node, switch to sleep, save energy and join the event as long as possible, thus increasing the life of the nets. Estimates of the effectiveness of these strategies show a significant reduction in energy utilization, with fewer reductions in productivity, but an increase in MANET's performance. Ordinary AODV simple sparse life or energy also sends RREQ. While life expires after I've spent some time. Number. Cannot send RREP (Response Path) to Spoof. Thus, the source node begins to retransmission RREQ for the purpose of communicating with the target resulting in unrecorded RREQ retransmission, at least the proportion of the supply (Laos), as well as the bandwidth and extension delay from the edge to the edge. The best routing protocols, AODV (OAODV) [3], are the solution to those problems, where the node does not transmit RREQ unless it has sufficient power (battery life) and the density of the node in its atmosphere exceeds a certain level. By adding both parameters, the new protocol is better than AODV related to battery life and bandwidth.

Syed Muhammad Sajjada et al. [4] This shows an aggressive search pattern based on a dependency process in which to find nesting nodes in the network. In addition, the trusted node updates the relay mechanism for packet forwarding activities. The main advantage of this model is to find flood attacks, attacks, and attacks by recruits by analysing nuclear activities and network statistics. Jian- Ming Zhang and friends [5] the common algorithms for the search for hazardous bees in MANET were proposed by preventing a joint attack. The author tries to solve this problem by creating a flexible mechanism based on a dynamic current source (DSR) called CBDS, which incorporates the benefits of Active, Protective, and Active Architecture. Sandip Chakraborty et al. [6] Algorithms to resolve issues that are caused by hidden wireless networks. The author achieved 28.50 mJ of energy use and an 88.02% medium-sized relay to look for hidden nodes in the middle of MANET. Renyong Wu et al. [7] suggested discovering the nodes scanned in the network using trust-based authentication algorithms. Anamal trajectories are found based on viral theories and evidence-based theories. By monitoring the behaviors of multi-dimensional nodes and integrating these pieces of information, these endangered genes in the network can be determined and normal network operations can be verified. W. Wang, B. Bhargava, and M. Linderman et al [8] to stop cooperative pack drop attacks in the spontaneous network is introduced. The hash operates based mostly on a mechanism which is used to determine the batch location of packets on the network. It stores information about package traffic in addition to knowledge forwarding routes. In W. Kozma and L. Lazos et al [9], REAct was announced. This study is the subject of reporting the question of the detection of the wrong grid, which rejects the packet without sending them to the target. To beat the higher than downside the tactic referred to as REAct is introduced. REAct detects harmful nodes in the quantity of random verification mechanisms. Assignments and directions will be ready to carry out harmful nodes through the REAct mechanism that keeps the evidence. This indicator was created by a filter for the spread of misconduct and mitigated the linkage error of finding nesting nodes.

Anandukey Al [10] underscores the false practice of linking and drawing new methods for finding and parsing nodes that have not been configured. Planned approaches are often integrated with the DSR protocol and linking reasons to get victimized packages in each account to address the issue of knot success. Appropriate approaches to the roadmap and many advantages such as small packages. In the future, they will accept all oversight mechanisms to ensure that these measures and measures together form the mechanism of malicious punishment. Single and more. [11] The proposed find scheme of two traces for the node opens. Suggested features of this scheme include high detection of nonsense nodes, slight changes, little changes to easy-to-use programs and applications. Pham Thi Ngoc Diep et al. [12] The Network of Patience is designed to work with unrelated connections and delays in wireless networks. Due to limited connections, DTNs are set to holes in random, random, random focal pitches and focal points, all indications or

deliberations. Although existing requests may find attacks initiated by individuals, they cannot solve a working problem together to get rid of the system. In this article, we propose a plan to work on personal arrangements and contracts. JaydipSen [13] Dedicated mobile networks are a collection of mobile nodes that temporarily create networks and network infrastructure. Janschi Ray, (2014) and others. [14] Patient networks (DTNs) are essential for the provision of basic services, including rescue scenarios and combat programs. A generic forensic model based on network and management log analysis is proposed in [15] for the cloud environment. The proper study of deep learning and shallow learning methods to identify spam is given in [16] for communication network privacy.

III. PROPOSED METHOD

The proposed method is based on DSR. This way it detects all nodes on selected paths from source to the destination after the source receives RREP. It is very likely that the new nodes cannot find the average nodes in terms of either path information, or those who reply RREP or bad nodes which creates RREP. This situation would lead to a black hole attack due to nodes select the shortest package of boxes. To solve this issue, HELLO was employed with CBDS to enable each node to recognize a neighbor. This facility sends an email address. By sharing an email address, triggers a malicious key and also identify malicious URL by reversing the CBDS video reverse technique. The RREQ library packages are like the original RREQ package, excluding that receiving addresses are in the graphic. The proposed method has three steps: 1) Initial bait step; 2) Detection Stage using Reverse Tracing, and 3) Ensuring security and protection stage.

A. Initial Bait Step

The purpose of this step is a malicious way of sending a response to RREP by sending RREQ. Used to distribute the shortest route to the packaged node. In order to realize that an approach is initiated which creates goal RREQ. The stochastic i node is chosen by the output node. The node presents in the Hip Hop neighborhood involve itself with the node, which taking its address for the address of the RREQ. Though the method is employed in a stochastic way if nodes shift the bait did not change then neighbor nodes would get changed. When sending the RREQ_ bait, the bubble function is started prior to the original route discovery.

At first, if the node does not initiate attack after the network sends RREQ_, joins to the node's node, it will have an RREP response to the other node. This indicates that misbehaving nodes exist in the network. Therefore, the trackback program in the next step will be initiated to find the route. If only RREP response, it means there are no other nodes in the network, and CBMS has begun to establish the DSR path. Second, if this number is a risk factor for an attack hole slot, the source sends an RREQ_ node to send RREPs. This means there are bad caves on the road. In this case, the tracker in the next step will begin to search the route. If the number does not provide an RREP response it will be inserted directly into the black hole list from the receiving node. If only the RREP response node means no harmful nodes on the network unless it does not. In this case, the start-up phase of the DSR will begin. The specified routes will not be included in the options provided during the trip.

Pseudo Code: Black Hole Attack Detection

1. Procedure BAD ( )
2. Set S as Source Node
3. Set D as Destination Node
4. calculate initial Bait
5. Calculate reverse tracing
6. Detect Malicious Node using Packet delivery Ratio Value
7. Detect Malicious Node using energy Value
8. Calculate the best path BP based on Malicious Node Detection
9. Transfer data through BP

B. Detection Step using Reverse Tracing

The detector is implemented for tracking misbehaving nodes in the network. If an attacking node receives RREQ then there is very much possible that it will circulate message with fake RREP. By conducting the reverse transaction process for the node attains RREP, detects suspicious data about the route and also the trusted transit area on the road. It is worth mentioning that more RREPs spread by attacker node then the probability of the CBDS catching harmful nodes is also increased. Moreover, to display misbehaving nodes are in the S series, test package is formed and shared with the path as well as with the next node of the final node which is a member of series of trusted T's. It is required to enter a node in null mode. The system heard about the last node in T, sends packets and returns the results back to the nodes that are received. The following node gets information about black hole infected nodes and circulates messages which notify it to other nodes present in the network. If the following node fails to perform as a normal node, then the original node will list this node as misbehaviour.

C. Ensuring security and protection stage

The DSR path discovery method has been realized with the help of NS2 software platform. The time when the path is routed, the energy value of the nodes is considered for the system boot level. Furthermore, the data will be re-entered to identify non-confidential support and real-time response. The energy value parameter is found for all members present in the network both normal nodes and harmful nodes. Threshold is different in [30%, 70%]. The initial level is

fixed as 90%. In order to make a decision on the nodes, the calculated energy value of each node is made a comparison with the threshold level. In addition, when power-sharing is broadcasted to a similarly low-level Dynamic Threshold Algorithm will calculate the time. If the malicious modes exist in the network then limit value will be reduced. In such a situation, the lowest level should be corrected otherwise the limit value will be reduced.

IV. PERFORMANCE ANALYSIS

The following discussion brief about a few important parameters used as a metric to analyze and compare the proposed system.

A. Experiment Analysis

The proposed system is implemented using Network Simulator (NS2). The proposed system is compared with the ADOV and Fuzzy Logic Approach. In the simulation experiments, several parameters are used. The number of nodes is given as 50, Area size is notified as 1000m*1000m, Target size is given as [500,500] x [500,500], Simulation times are set as 150 seconds, Queue Limit is given as 20, The Queue size is set as 100, The packet size is considered as 552 Bytes, Packet interval is 2, communication range is given as 30m, and Buffer size is given as 20 packets. The above parameter's value is given as input for simulation purpose.

1. Packet Delivery Ratio (PDR)

Packet Delivery Ratio term can be defined ratio between transported packets from the existing packets. This parameter is employed in the next section to brief the performance of this proposed method. The following expression is involved in determining the packet delivery ratio

$$SP= \frac{\text{Total no of delivered packets}}{\text{Total no of available packets}} \quad (1)$$

2. Average Throughput (AT)

Average throughput is regarded as the rate of completed message delivery over a communication network. This parameter is involved in the next section to brief about the comparison between the proposed method and other. The following expression is involved in finding the average throughput

$$AT= \frac{\text{Total no of Successfully received packets}}{\text{Total no of transmit Packets}} \quad (2)$$

3. **Trust Value Computation**

The discrepancy in the number of sent packets and received packets is caused because of loss of packets, inserted packets or multiplied packets. The following expression gives the probability of the trust value in the network

$$p_n = \frac{\pi_{dn}}{\pi_{ns}} \quad (3)$$

4. **Control Overhead**

This parametric indicates the picture between control packets and data packets in the communication network.

5. **Detection Accuracy**

Detection Accuracy is one of the parameters which gives the true relation between the original malicious node present in the defined network and the detected malicious node from the defined network by the proposed method.

A. Variable Number of Nodes versus Stable Mobility

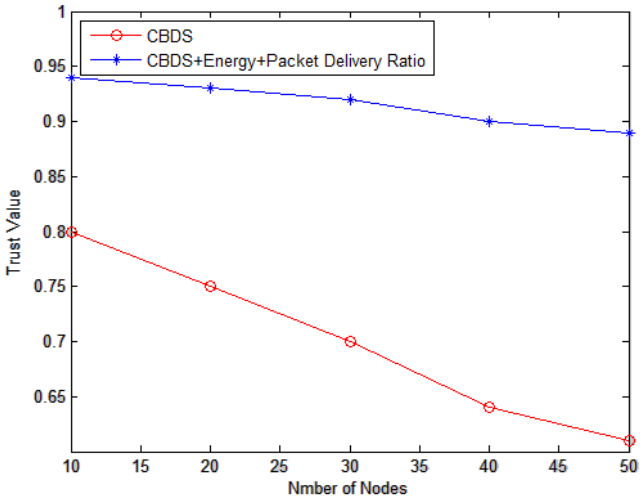

Fig.1. Energy value of CBDS and CBDS+Energy+Packet Delivery Ratio for different Number of Nodes

The following section discusses and illustrates the energy value of the CBDS and CBDS+Energy+Packet Delivery Ratio. Fig. 1. illustrates the acquired results for the various number of the nodes. The overall percent of the malicious node in the network is chosen consciously from 0 to 10 in percentage. The maximum mobility speed of the nodes is given as 20 m/s. In the next step, 30%, 70% is considered as a threshold for the energy metric. Fig.1 clearly indicates that the CBDS+Energy+Packet Delivery Ratio scheme expresses a higher energy value related to conventional CBDS. It can be understood, that CBDS+Energy+Packet Delivery Ratio prevails because 92 percent of energy is preserved while detecting the harmful nodes.

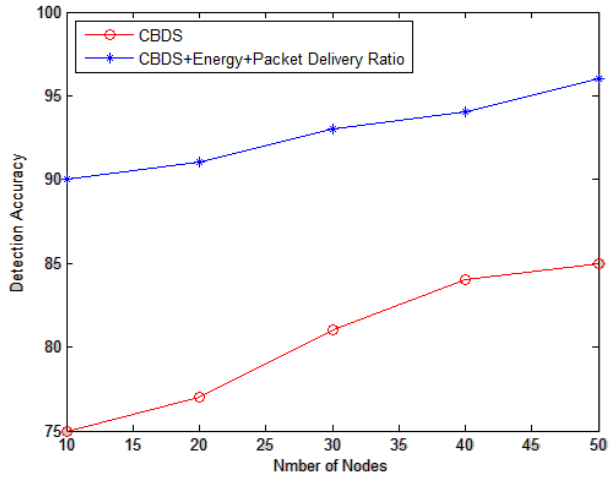

Fig.2. Detection Accuracy of CBDS and CBDS+Energy+Packet Delivery Ratio for different Number of Nodes

The following section discusses and illustrates the detection accuracy value of the CBDS and CBDS+Energy+Packet Delivery Ratio. Fig. 2. Illustrates the acquired results of detection accuracy parameter for the dissimilar number of nodes. The overall percent of a malicious node in the network is chosen consciously from 0 to 10 in percentage. The maximum mobility speed of the nodes is given as 20 m/s. In the next step, 30%, 70% is considered as the threshold for the energy metric. Fig.2 clearly indicates that the CBDS+Energy+Packet Delivery Ratio scheme displays a higher energy value related to typical CBDS. Despite 10 percent of nodes are facing threat, it can be understood that the CBDS+Energy+Packet Delivery Ratio attains good result because it has been preserved more than 90 to 95 percent of accuracy value in the process of finding malicious nodes.

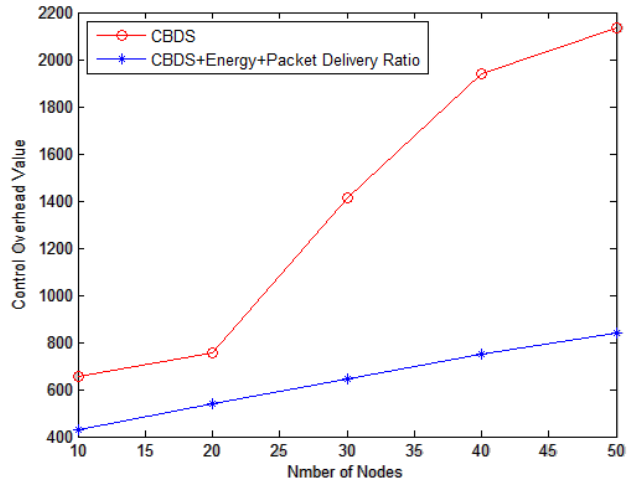

Fig.3. Control Overhead of CBDS and CBDS+Energy+Packet Delivery Ratio for different Number of Nodes

The following section discusses and illustrates the control overhead value of the CBDS and CBDS+Energy+Packet Delivery Ratio. Fig. 3. Displays acquired results for the various number of nodes. The overall percent of the malicious node in the network is chosen consciously from 0 to 10 in percentage. The maximum mobility speed of the nodes is given as 20 m/s. In the next step, 30%, 70% is considered as a threshold for the energy metric. Fig.3 clearly indicates that the CBDS+Energy+Packet Delivery Ratio scheme performs a higher trust value related to conventional CBDS. Despite 10 percent of nodes facing threat, it can be understood that the CBDS+Energy+Packet Delivery Ratio outperforms because it has been given less value for control overhead parameter with 400 in the process of identifying the attacker nodes.

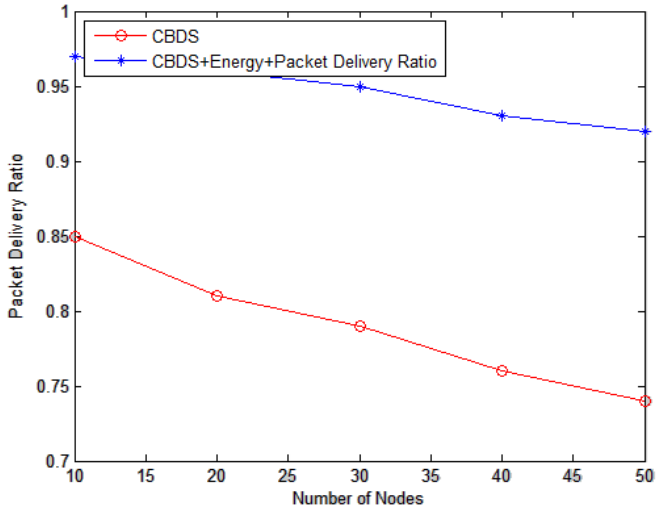

Fig.4. Packet Delivery Ratio of CBDS and CBDS+Energy+Packet Delivery Ratio for different Number of Nodes

The following section discusses and illustrated the packet delivery ratio of the CBDS and CBDS+Energy+Packet Delivery Ratio. Fig. 4. Illustrates the acquired results for the various number of the nodes. The overall percent of the malicious node in the network is chosen consciously from 0 to 10 in percentage. The maximum mobility speed of the nodes is given as 20 m/s. In the next step, 30%, 70% is considered as a threshold for the energy metric. Fig.4 clearly indicates that the CBDS+Energy+Packet Delivery Ratio scheme provides good packet delivery ratio related to other mechanisms. Despite 10 percent of nodes is a threat, it can be understood that the CBDS+Energy+Packet Delivery Ratio displays good performance because it has been shown 93 percent of packet delivery ratio in the mission of finding malicious nodes.

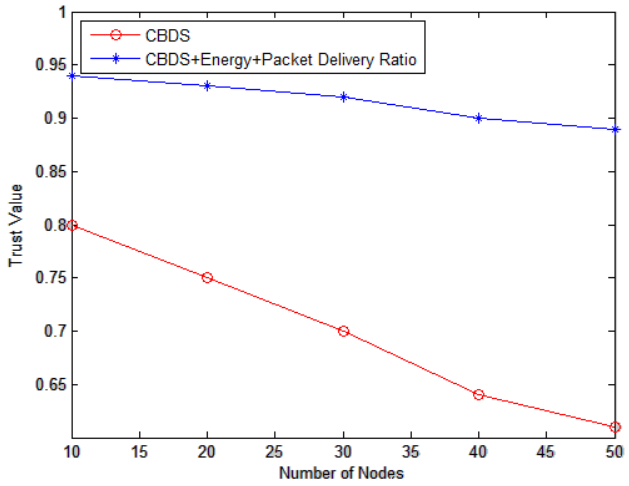

Fig.5. Trust Value of CBDS and CBDS+Energy+Packet Delivery Ratio for different Number of Nodes

The following section discusses the trust value of the CBDS and CBDS+Energy+Packet Delivery Ratio. Fig. 5 illustrates the acquired results for the various number of nodes. The overall percent of a malicious node in the network is chosen consciously from 0 to 10 in percentage. The maximum mobility speed of the nodes is given as 20 m/s. In the next step, 30%, 70% is considered as the threshold for the energy metric. Fig.5 clearly indicates that the CBDS+Energy+Packet Delivery Ratio scheme performs a higher trust value related to typical CBDS. Despite 10 percent of nodes facing threat, it can be understood that the CBDS+Energy+Packet Delivery Ratio outperforms because it has been preserved more than 94 percent of trust value in the process of finding attacker nodes.

B. Variable Number of Nodes versus Dissimilar Threshold

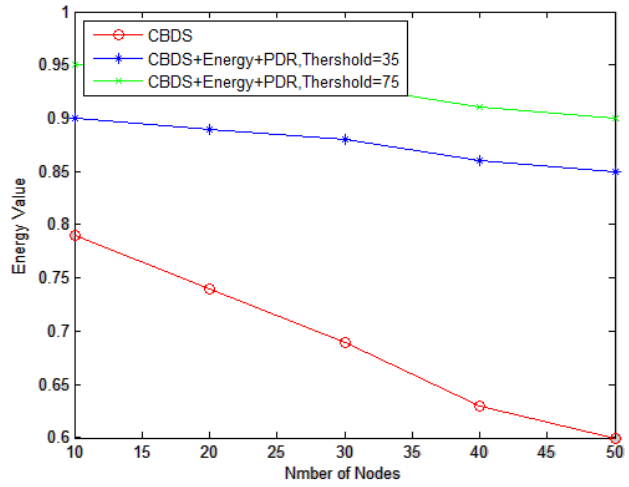

Fig.6. Energy value of CBDS and CBDS+Energy+Packet Delivery Ratio for different threshold

The following section discusses and compares the energy value of the CBDS, CBDS+Energy+Packet Delivery Ratio - Threshold 35 and CBDS+Energy+Packet Delivery Ratio - Threshold 75. Fig. 6. Illustrates the acquired results for the various number of nodes. The overall percent of the malicious node in the network is chosen consciously from 0 to 10 in percentage. The maximum mobility speed of the nodes is given as 20 m/s. In the next step, 30%, 70% is considered as a threshold for the energy metric. Fig.6 clearly indicates that the CBDS+Energy+Packet Delivery Ratio - Threshold 75 scheme displays a higher energy value related to the other mechanisms. Despite 10 percent of the nodes facing threat, the CBDS+Energy+Packet Delivery Ratio - Threshold 75 outperforms because it has been preserved more than 95 percent of its energy in the process of finding attacker nodes.

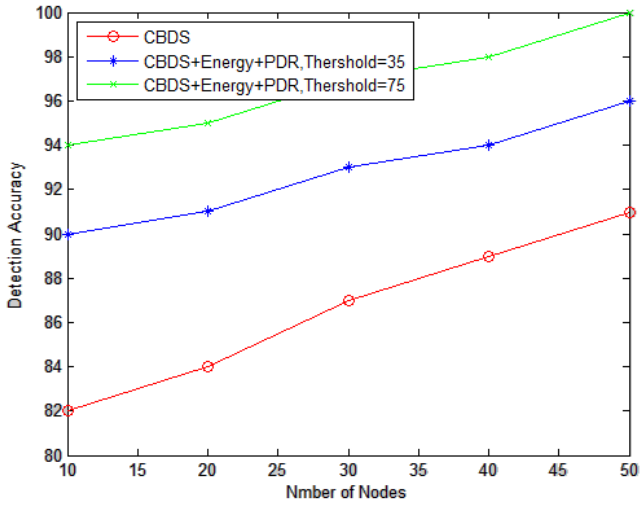

Fig.7. Detection Accuracy of CBDS and CBDS+Energy+Packet Delivery Ratio for different threshold

The following section discusses the detection accuracy value of the CBDS, CBDS+Energy+Packet Delivery Ratio - Threshold 35 and CBDS+Energy+Packet Delivery Ratio - Threshold 75. Fig. 7. Illustrates the acquired results for the various number of nodes. The overall percent of a malicious node in the network is chosen consciously from 0 to 10 in percentage. The maximum mobility speed of the nodes is given as 20 m/s. In the next step, 30%, 70% is considered as the threshold for the energy metric. Fig.7 clearly indicates that the CBDS+Energy+Packet Delivery Ratio -Threshold 75 scheme has a higher detection accuracy value related to the other mechanisms. Despite 10 percent of the nodes facing threat, CBDS+Energy+Packet Delivery Ratio -Threshold 75 outperforms because it has been preserved more than 94 to 98 percent of accuracy value in the process of searching the attacker nodes.

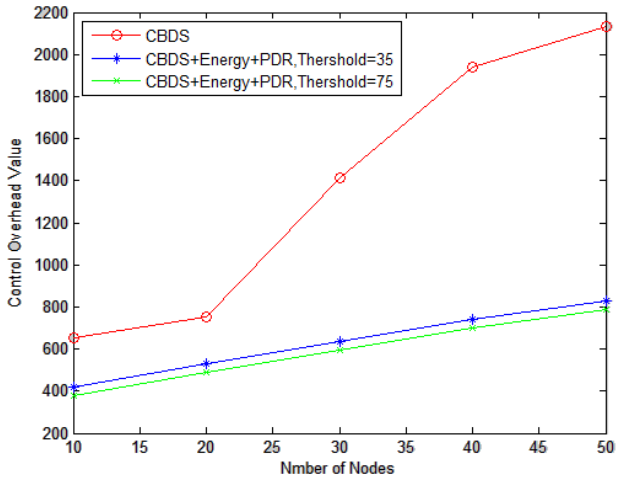

Fig.8. Control Overhead of CBDS and CBDS+Energy+Packet Delivery Ratio for different threshold

The following section discusses the control overhead value of the CBDS, CBDS+Energy+Packet Delivery Ratio - Threshold 35 and CBDS+Energy+Packet Delivery Ratio - Threshold 75. Fig. 8 illustrates the acquired results for the various number of nodes. The overall percent of the malicious node in the network is chosen consciously from 0 to 10 in percentage. The maximum mobility speed of the nodes is given as 20 m/s. In the next step, 30%, 70% is considered as the threshold for the energy metric. Fig.8 clearly indicates that the CBDS+Energy+Packet Delivery Ratio -Threshold 75 scheme has a higher trust value. Despite 10 percent of the nodes facing the threat, the CBDS+Energy+Packet Delivery Ratio -Threshold 75 outperforms it has been preserved less value of control overhead with 380 in the process of finding the attacker nodes.

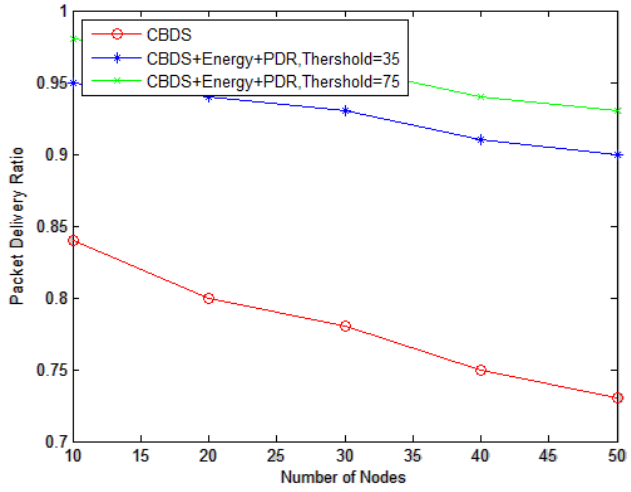

Fig.9. Packet Delivery Ratio of CBDS and CBDS+Energy+Packet Delivery Ratio for different threshold

The following section discusses the packet delivery ratio of the CBDS, CBDS+Energy+Packet Delivery Ratio - Threshold 35 and CBDS+Energy-Threshold 75. The overall percent of a malicious node in the network is chosen consciously from 0 to 10 in percentage. The maximum mobility speed of the nodes is given as 20 m/s. In the next step, 30%, 70% is considered as the threshold for the energy metric. Fig.9 indicates that the CBDS+Energy+Packet Delivery Ratio -Threshold 75 scheme has a superior packet delivery ratio related to the other mechanisms. Despite 10 percent of the nodes facing the threat, the CBDS+Energy+Packet Delivery Ratio -Threshold 75 outperforms because it has been preserved more than 98 percent of packet delivery ratio in the process of finding the attacker nodes.

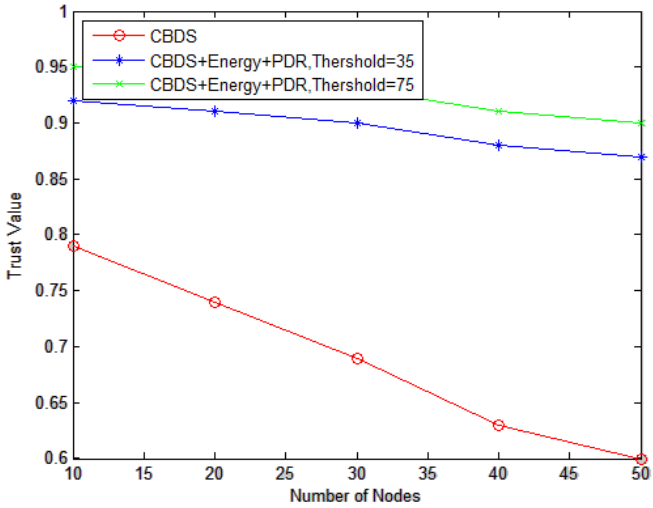

Fig.10. Trust Value of CBDS and CBDS+Energy+Packet Delivery Ratio for different threshold

The following section discusses the trust value of the CBDS and the other methods. Fig.10. illustrates the acquired results for the various number of nodes. The overall percent of a malicious node in the network is chosen consciously from 0 to 10 in percentage. The maximum mobility speed of the nodes is given as 20 m/s. In the next step, 30%, 70% is considered as a threshold for the energy metric. Fig.10 indicates that CBDS+Energy-Threshold 75 scheme has a higher trust value related to the other techniques. Despite 10 percent of the nodes facing threat, the CBDS+Energy-Threshold 75 outperforms because it has been preserved more than 94 percent of trust value in the process of finding the attacker nodes.

V. CONCLUSION AND FUTURE SCOPE

In this article, the new approach is a network algorithm for a particular mobile network. In this work, the node source selects a valuable network node because the node address is

used as a malicious node trap to process the RREP message as a response. Finally, malicious devices based on the proportion of supply and energy prices is found. Performance indicators show the results of existing and proposed systems. From the experimental parameters, it has been shown that the best-proposed approach produces an existing method approaches.

REFERENCES

[1] Jin-Man Kim and Jong-Wook Jang, "AODV based Energy Efficient Routing Protocol for Maximum Lifetime in MANET", Proceedings of the Advanced International Conference on Internet and Web Applications and Services 2006.

[2] Tripti Nema et al., "Energy Efficient Adaptive Routing Algorithm in MANET with Sleep Mode", International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970) Volume-2 Number-4 Issue-6 December-2012.

[3] Suvarna P Bhatsangave and V R Chirchi, "OAODV Routing Algorithm for Improving Energy Efficiency in MANET", International Journal of Computer Applications 51(21):15-22, August 2012.

[4] Syed Muhammad Sajjada, Safdar Hussain Boukb, Muhammad Yousaf, "Neighbor Node Trust Based Intrusion Detection System for WSN", Procedia Computer Science 63, pp 183 – 188,2015.

[5] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, " Defending Against Collaborative Attacks by Malicious Nodes in MANETs: Cooperative Bait Detection Approach", IEEE Systems Journal, Vol.9, Issue.1, 2015.

[6] Sandip Chakraborty, Sukumar Nandi, and Subhrendu Chattopadhyay, "Alleviating Hidden and Exposed Nodes in High-Throughput Wireless Mesh Networks". IEEE Transactions on Wireless Communications, Vol.15, Issue.2, Feb 2016.

[7] Renyong Wu, Xue Deng, Rongxing Lu, and Xuemin (Sherman) Shen, "Trust-Based Anomaly Detection in Emerging Sensor Networks," International Journal of Distributed Sensor Networks, vol. 2015, Article ID 363569, 14 pages, 2015.

[8] W. Wang, B. Bhargava, and M. Linderman, "Defending against collaborative packet drop attacks on MANETs," in Proc. 28th IEEE Int. Symp. Reliable Distrib. Syst., New Delhi, India, Sep. 2009.

[9] W. Kozma and L. Lazos, "REAct resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in Proc. WiSec, pp. 103–110, 2009.

[10] S. Anandukey and M. Chawla, "Detectionofpacket dropping attack using improved acknowledgment based scheme in MANET, "International Journal of Computer Science Issues I, Vol. 7, No. 1, pp. 12-17, 2010.

[11] H. Liu, J. G. Delgado-Frias, and S. Medidi, "Using two-timer scheme to detect selfish nodes in ad-hoc networks," in the proceedings of International Conference Communication, Internet, and Information Technology, pp.179-184, Alberta, Canada, 2007.

[12] Pham Thi Ngoc Diep, Monika Sachdeva, "Detecting Colluding Blackhole and Greyholeattack in Delay Tolerant Networks", ICRTEDC, Vol. 1, Special Issue. 2, 2015.

[13] JaydipSen," Detection of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", International Journal of simulations, systems, science and technology, Vol.12, No. 4, Aug 2011.

[14] Yanzhi Ren, Mooi Choo Chuah, Jie Yang, Yingying Chen "Detecting Wormhole Attacks In Delay-Tolerant Networks" IEEE Wireless Communications, Volume 17, Issue.5, October 2010.

[15] P.Santra, "An expert forensic investigation system for detecting malicious attacks and identifying attackers in cloud environment", International Journal of Scientific Research in Network Security and Communication, Volume 6, Issue.5, Oct 2018.

[16] Afzal Ahmad, Mohammad Asif, and Shaikh Rohan Ali, "Review paper on shallow learning and deep learning methods for network security", International Journal of Scientific Research and Computer Science and Engineering, Volume.6, Issue.5, pp. 45-54, Oct 2018.

Authors Profile

R.Saranya received her B.E degree from Anna University, M.E degree from Manonmaniam Sundaranar University in 2011 and 2013 respectively. Currently, she is working towards a Ph.D. in Manonmaniam Sundaranar University, India. Her research topics are wireless networks, network security, and Network Routing Protocol.

Dr. R. S. Rajesh received his B. E and M. E degrees in Electronics and Communication Engineering from Madurai Kamaraj University, Madurai, India in the year 1988 and 1989 respectively. He is currently the Professor and Head of Department of Computer Science and Engineering, Manonmaniam Sundaranar University where he earned his Doctorate degree in the field of Computer Science and Engineering in the year 2004. He has 22 years of PG teaching experience. He has published 100 articles in leading international journals. His research areas include Vehicular Adhoc Networks, Wireless networks, Digital image processing, and Pervasive computing.

