International Journal of Research in Advent Technology, Vol.7, No.1, January 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Detection of Black Hole Attack in DSR Routing Protocol by modified cooperative bait detection scheme

R.Saranya[1], Dr.R.S.Rajesh[2]
[1,2]*Department of Computer Science & Engineering, Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India.*
Email: saranya.shantha@gmail.com[1], rs_rajesh1@yahoo.co.in[2]

Abstract- The main purpose of this paper is to provide security algorithms against Malicious Node Attack in Mobile Adhoc Network. The node must cooperate with each other to meet the need in the ad-hoc mobile network (MANETs) which provide communication between nodes. The arrival of abnormal nodes (harmful nodes) can cause serious security problems. To resolve this issue, this paper provides a new security network algorithm. The proposed approach consists of three steps: 1) Initial Setup Step; 2) Attack Identification Step using Reverse Tracing, and 3) reactive protection step. The first step detects the existence of potential nodes along the way. The second step finds non-harmful nodes and nodes that are dangerous in the transfer path. Finally, the last step locates a malicious location based on the energy price. To analyze the effectiveness of the suggested method uses the Detection accuracy Misclassification rate, Detection time, Packet Delivery Ratio, Routing Overhead, End-to-End Delay, Throughput, and Packet Loss. Experimental results show that the proposed method offers the best results from the existing approach.

Keywords- Mobile ad hoc network (MANET); malicious node; black hole attack; Cooperative bait detection scheme (CBDS); Packet Modification

1. INTRODUCTION

Mobile ad hoc networks (MANET) is one of the important networks in wireless communication. The main and serious problem of the wireless network is security. MANET is a decentralized network. MANET's main feature is topology and message publishing created by the node itself. MANET use different positions and can be installed via the air. MANET's use is a separate high-end mobile network. MANETs are exclusive among inaccessible communication networks, as experimental from the crucial application areas. On the other hand, the exclusive characteristics required by MANET applications require distinctive solutions and separate MANETs from other predictable networks. There are different challenges may take for an account while designing a MANET.

It is well known that node detection of hackers in MANET is difficult because nodes are all mobile. Traffic may be affected by a joint attack provided by a node in a mobile network (MANET). Malicious nodes are defined as nodes that want to exclude services to other nodes on the network. This type of node offers many security issues such as gray hole and black hole attacks in collaboration. The attack is a network operator in which hackers attempt to change the target data or data on the path to the target.

For an attack in a gray hole, this node is not recognized for the first time because it is endangered, but only afterward protect its presence in a network of security solutions based on trust. Then, rejection data entry of data when the packet passes through it. In this article, identifying common black holes using the Dynamic Navigation Integration (DSR) technique is focused.

DSR has two main steps. The first step is path detection and the second step is path preservation. In order to run the path and to find the node on the route, the RREQ packet is transmitted in the network. From the total number of nodes, the only partial node contains information about the path and pass this information to the destination for taking action with RREP which should be transmitted to the source node. The time when RREQ is transferred to the node which added its address data to the RREQ route is recorded. After receiving RREQ, the address of each point between the roads can be obtained. The target node is based on collecting data between packets and send the RREP response to the source node along with all path information in the path. The DSR does not have a detective method, except the source node be able to obtain the entire path data. In this work, these aspects have been utilized. The nanomaterial node

demonstrates the possibility of a new route, regardless of the roadmap. In this case, the attack unit will respond to the road proposal, thus passing the packet and holding it. For flood-based protocols, abuse responses will be received from the request module before receiving a response from the actual node. In this way, the path of malice and falsehood is being created. When this is set, it depends on the node whether the packet is forwarded or forwarded to an unknown address. Generally, harmful nodes are inserted into the router.

The following section summarizes previous related work.

2. RELATED WORK

Tsou et al. [13] have provided a mechanism for finding dangerous nodes that have launched black/gray/ black attack attacks and CBDS (CBD) attacks. It includes active defense architecture and reaction and collaboration with neighboring nodes. By addressing the vulnerability of the neighboring nodes due to the manipulation of bait, he lures bad intentions to encounter RREP and finds programs evaluating malicious nodes for traceability and thus preventing their attacks. Deng et al [7] planned an answer to the part drawback for an ad-hoc on-demand routing protocol. One limitation of the planned methodology is that it supports an assumption where malicious nodes would not work as a bunch, though this might happen throughout a true situation and presently gazing this drawback of team attacks. Xue and Nahrstedt et al [22] planned a replacement routing service named best-effort fault-tolerant routing (BFTR) the look goal of BFTR is to produce packet routing service with high delivery quantitative relation and low overhead in presence of misbehaving nodes. Rather than distinguishing a path is nice or unhealthy, BFTR evaluates the routing challenges of a path by its end-to-end performance (e.g. packet delivery quantitative relation and delay). BFTR dynamically routes the packets via the foremost possible path. BFTR provides an economical and uniform resolution for a broad variety of node misbehaviors with only a few security assumptions. The BFTR formula is evaluated through each analysis and intensive simulations. The results show that BFTR greatly improves the ad-hoc routing performance in the presence of misbehaving nodes. Baadache and Belmehdi et al. [3] predicted that when the area was attacked by a mechanical mechanism, it was sure to check the gloomy packet intersection. Anticipated responses avoid attacks by regions and areas of cooperation. An analytical indicator was noted in the simulation to illustrate the effectiveness of the suggested responses.

Liu et al [10] introduce a 2AK o chain that examines the weaknesses of MANET. In this method, two node neighbor distance data are transmitted on the contrary way of the track to show that the data package is successful. This project belongs to an active project and therefore creates additional paths, regardless of the presence of harmful nodes. S. Ramaswamy, H. Fu, Sreekantaradhya, J. Dixon and K. Nygardet al. [17] CBDS in the Hybrid Defense design. How to find hackers Introducing a joint attack and black hole attack is called CBDS (Collaborative Threat). It unites active architecture and reactions and works with any random nodes. Through the bad address of the neighboring node due to the address of the bait and the detection of harmful nodes through the tracker, thus preventing the attack. K.Vishnu and A.J.Paul et al [11] found the black/gray hole in the mobile network. Pull down to expand, so it requires the nearest BMP. RREP responses are distributed to all BIPs and destinations without end. If the power node receives a response from the direction of the direction, it shows that there is no part of the route. When the node receives a BIP response that indicates that Blackhole attacks then is in the path. Finally, transportation found parts of the road. When you find a private attack, the power node sends blind knowledge to the destination. No nodes found nearby. Here, the algorithm finds the status on the package. In the Gregorian calendar month, there are Wang Wang, Bang Phavi, and Emmanuel, and others. [21] To stop spontaneous network attacks. Hash works significantly on the basis of the mechanism used to locate small drops in the network. It stores information about transmitted and transmitted information. At W. Kozma and L. Lazos et al. [19], REAct has been announced. The study considers the question of faulty cluster detection that rejects the packet without directing it to its destination. To top off, the strategy is listed as REACT. REAct detects harmful nodes through a number of random audit mechanisms in the event of a decrease in performance. A service node and destination will be ready to perform a dangerous node with the REAct mechanism. This indicator is made up of a filter for abnormalities and minimizes top-line communication to detect harmful nodes.

Mamatha et al. [6] explore the behavior of degradation due to the existence of this dangerous (bad attitude) at Manet. They are designed and evaluated in a specified way (AODV + ACK + PFC) to observe and mitigate the results of professional misconceptions. In the future, improvements can also be achieved by evaluating various nodes and web parameters. In addition, the topic can be expanded to identify and prevent multiple attacks on layer layers to allow methods to generate more force against attacks. Rajaram et al. [2] Requested a security certificate based on trusted confidentiality and authentication of the packet both in the transmission and in the MANET's connection layer. In the initial stage of the protocol, they developed a trustworthy bait scheme to detect and isolate dangerous nodes using layered layers of data. It employs a trust value to facilitate transmitted by preserving trust for each other. A node is penalized or rewarded by reducing or increasing trust. If the confidence value falls below the corresponding node confidence level, it is flagged as risky. The next phase of the protocol provides layer protection using the Cipher Block Chaining (CBC-X) authentication method and encryption method.

Anandukey et al [16] investigated the wrong practice of the node and plan a completely new approach to the detection and isolation of the node configured badly. Planned approaches are often combined with high-level protocols, protocols, estimated DSRs and reliance packages for the causation to receive victimization packets into individualized accounts, how to package volumes, triumphal problems Of bad nodes. Joint planning methods that are less loaded on roads and many advantages, such as smaller size packages required for claiming. In the future, any authentication mechanisms is accepted to make sure the ack square packages really measure and together as a mechanism to punish a malicious node. Single et al. [8] Proposed double-track detection schemes for nodes detected. Suggested schema features include high detection of nonsensical nodes, minor irregularities, slight changes in the application layer and easy-to-implement hardware programs. Only after set the time and the number of users. The project can be implemented at a very low price. Manvi et al [18] investigated the deterioration in productivity caused by such selfish (bad) nodes in MANET. They have analyzed and evaluated a technique called 2ACK to detect and mitigate the effects of such bad behavior. They have embedded some aspects of security with 2ACK to verify the privacy of the message by checking the original hash code with the GSC code generated in the destination. One of the advantages of the 2ACK scheme is its flexibility to control overhead costs. Pirzada et al [1] Display a new trusted framework for identifying and isolating nodes that generate sockets on the network without having to implement crypto devices. With extensive experiments, they have shown that their projects work efficiently in the face of harmful nodes and do not require unnecessary conditions in the network's construction and operation. Ren et al [20] protection topics with detection and response mechanisms. Signs of detection include the frequency of RTS / CTS packages, busy frequencies (signal disturbances), and the transmission of various RTS / DATA messages. The response theme is based on the Acceleration labeling mechanism. Through a deeper networking experiment of ns2, tend to show the presence of a high level of delays and delays under this type of attack.

N.Venkatadri et al [12] Adhoc's wireless network is a type of wireless network with no fixed infrastructure. Ad Hoc network devices can work on networks within a specific range. Currently, most of the transactions are done via a computer network so they are more susceptible to physical security threats. One of the major DOS attacks that destroy MANET's entire performance is the Black Hole attack. In the case of attack, the node black hole does not forward packets forward but packaged. In this work, black hole attacks were detected and deleted by the use of digital signatures with two fish algorithms. Authors have modified the transfer protocol on a request called a TORA, and call it STORA. Our STORA works well under normal conditions and in the black hole from the original TORA. Pham Thi Ngoc Diep et al [14] the tolerance network is designed to handle unconnected connections and latency in the wireless network. Due to limited connections, DTN is susceptible to black hole holes and deceptive slots, where there is an accidental key, all or part of a package of deliberate intent. Although the existing proposals may find an attack initiated by individuals, they cannot solve the problem that is working together to defeat the defense system. In this article, plan to handle both individual and contractual agreements is proposed. Nodes are required to change notes from previous meetings and evaluate others based on their message transmission ratios. A malicious node may not be found by a mixed group to hide the proportion of the redirected aspect ratio. In order to downgrade the package permanently

and raise the meter at the same time, the attacker must create a high-frequency meeting record and a large number of messages sent. This leads to the abnormal behavior of fake meetings, which contradicts the assertions and gives signs of collusion. Extensive experiments indicate that our solution can work with a variety of dropouts and a high number of highly precise and low-level moderators. Harsh Pratap Singh, et al [9] the special mobile network is a collection of mobile nodes that temporarily creates a network and has a few infrastructure networks. Because of self-motivation or mobility in nature, nasal forces are vulnerable to security threats that drive network performance. This article discusses the review of various types of coordinated attacks such as Blackhole / Blackjack attack, the most serious threat in the mobile network. In more than one node, the nucleus attacks more than one negotiation, which is why it is difficult to identify. This article provides an overview of several safety mechanisms to remove the black hole / black hole attacks from the network. Yanzhi Ren, (2014) et al [4] The Delay Tolerant Networks (DTNs) are of paramount importance in providing essential services, including emergency scenarios and battle applications. However, DTNs are vulnerable to malware attacks, which are malicious nodes, packet records in the same location, and download them to other shared nodes that keep them on the web. The Wormhole attack is a serious threat to DTN's normal network operations. In this article, various methods developed to detect worms is covered. Most of them, however, cannot work effectively in DTN. To detect the presence of a worm attack, a mechanism to detect the existence of a prohibited network topology is offered. Using the road route and the Zebranet model is approached through extensive experiments. Our results show that the suggested method can detect Worm attacks in DTNs effectively and efficiently. KanuGeete et al [15] Wireless networks are multi-hotspot networks and can be used as synonyms for Adhoc networks. This is a network that has many links to the ability to cope with web design. Security is a challenge for wireless networks. The nature of the configuration itself makes the wireless network vulnerable to various attacks. Exploiting WMN may result in damages to network performance. In this article, some attacks occurring on different layers of the TCP / IP model is discussed. Comparative survey for specific attacks on the network layer is discussed. Gray hole attacks are often difficult to detect and recover. There are different detection techniques that have advantages and disadvantages. Arul Kumaran et al [5] propose a new strategy to detect black hole attack based on energy auditing, packet veracity check and trust node to improve the performance of AODV.

3. PROPOSED WORK

The proposed method is based on DSR. Therefore, detection of all nodes along the path is possible by sending RREP information in the network. It is possible that the new nodes do not identify the average nodes with path information, responding to RREP or bad nodes by creating RREP. This scenario can cause the outcome of the node to send packets on the shortest path chosen by the node that could cause black hole attacks. To overcome this problem, HELLO was included in CBDS to help each node recognize neighbor nodes. This feature can send an email address to trigger a malicious key and reverse the CBDS video reverse trick to find a malicious URL. The RREQ library packages, similar to the original RREQ package, except their receiving addresses, are obscene. The proposed approach consists of three steps: 1) Initial setup step; 2) attack identification step using reverse tracing, and 3) reactive protection step. These three steps are discussed in the most detailed way below.

3.1. *Initial Setup Step*

The purpose of this step is to emulate the malicious way which sends fake RREP for the RREQ packet. To achieve this, the next approach is established to create goal RREQ packet. The output node selects the stochastic i node. The node in the one-hop neighborhood and collaborate with the node, taking its address for the address of the RREQ. Since any trick is done stochastic and neighboring nodes will change if nodes move the bait will not be changed. The bubble function is activated when sending the RREQ_ bait before finding the original route. First, if the node does not start a black hole attack after the source network sends RREQ_, adds to the node's node, it will have an RREP response to the other node. This shows that harmful nodes are on the way.

3.2. *Attack Identification Step using Reverse Tracing*

Tracker is used for detecting harmful node behavior responding to RREQ_ paths. If a malicious node is accidentally receiving RREQ it will respond with fake RREP. Therefore, the reverse transaction process will be performed for the node getting RREP to reveal

suspicious data about the route and the trusted transit area on the road. It supposed to be stressed that CBDS can identify additional dangerous nodes and in which time these nodes have transmitted RREPs. To show that the malicious node is in the S sequences, the initial node will transmit the hello package to the path and forward the message to the second node of the last node in the T series. By checking transmit and returned back signals up to final node in T series, decision made on each nodes. The next node saves the black hole list and broadcasts network notifications to warn every node on the node. If the last node drops packets instead of forwarding, the original node will keep it in the blacklist.

3.3. *Reactive Protection Phase*

3.3.1 Malicious Node Detection using Energy Value

After initial protection, the DSR path discovery method has been stimulated. The particular time where the path is recognized in addition to the energy value is discovered which is important for the system boot level, then the discovery will be re-enabled to find untrusted support and real-time response. The energy value is calculated for all nodes including both normal node and attacker nodes. Then these energy value is compared with an energy threshold value. Threshold is different in [30%, 70%]. The initial level is 90%. Dynamic Threshold Algorithm that executes the time when power-sharing is broadcasted to a similarly low level. If the limit value is reduced, this indicates that the malicious nodes stay in the network. In such a situation, the lowest level should be corrected. Or else, the limit value will be reduced.

4. PERFORMANCE EVALUATION

To analysis the performance the proposed following performance metrics are used. Average Delay, Degree of Aggregation, Packet Loss, Network Lifetime and Energy Consumption.

5. EXPERIMENTAL EVALUATION

The proposed system is implemented using Network Simulator (NS2). In the simulation experiments, several parameters are used. They are listed in the table given as follows.

Table 1. The planning and control components.

No of Nodes	50
Area Size	1000m x 1000m
Target Size	[500,500] x [500,500]
Simulation Duration	150 seconds
Queue Limit	20
Packet Size	552 Bytes
Packet Interval	2
Communication Range	30 m
Buffer Size	20 packets

5.1. *Packet Delivery Ratio (PDR)*

Packet Delivery Ratio defines the total number of delivered packets from the available packets. This is one of the performance metrics. This metric is used to analyze the performance of this proposed method. It is calculated by using the below formula

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

5.2. *Average Throughput (AT)*

Average throughput is described as the average ratio of successful message delivery through a communication channel. This is one of the performance metrics. This metric is used to analyze the performance of this proposed method. It is calculated by using the following formula

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

Fig.6. shows that the proposed method gives higher performance than AODV and Fuzzy Logic. The value of the average throughput of other system and the proposed system is given in Table 3.

5.3. *Trust Value Computation*

The difference in the number of sent packets and received packets can be noticed easily. That difference might be caused by the loss of packets, inserted packets or multiplied packets. The probability of packets being lost, inserted and multiplied can be computed by the following equation:

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

Where $\pi_{dn}$is obtained by Number of Received packets – Number of Sent Packets. Fig.7. shows that the proposed method gives higher performance than O AODV and Fuzzy Logic. Table 4. Summarizes the trust value computation of other techniques and the proposed system.

5.4. *Control Overhead*

This metric is a proportion of the amount of control packet distribution to a number of data transmissions.

5.5. *Detection Accuracy*

Detection Accuracy is the measurement system, which measures the degree of closeness of measurement

between the original malicious node and the detected malicious node by the proposed method.

$$\text{Accuracy} = \frac{\text{Number of Correctly Detected Malicious Node}}{\text{Total No of Malicious Node}} \quad (4)$$

5.6. *Varying the Number of Nodes with a Fixed Mobility*

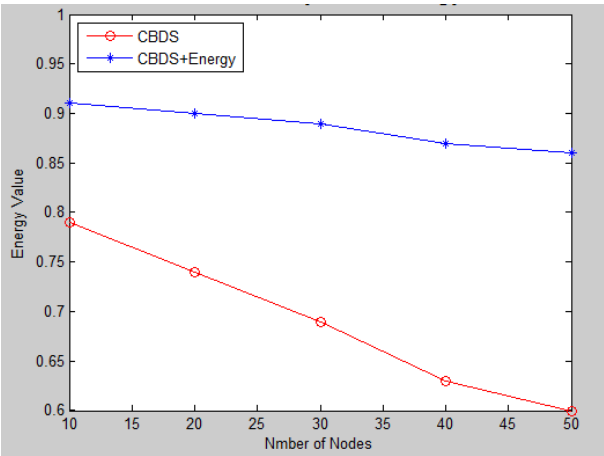

Fig.1. Energy value of CBDS and CBDS+Energy for different Number of Nodes

This paper study the energy value of the CBDS and CBDS+Energy for a different number of nodes. The results are captured and showed in Fig. 1. In this study, the total number of malicious nodes are taken in this work from 0 to 10 in percentage. The highest node speed is taken as 20 m/s. Here, the energy threshold value is set to 30%, 70%. From the above Fig.1, it can be observed that our CBDS+Energy scheme shows a higher energy value compared with that of CBDS. Although 10 percent of all nodes on the network is at risk, CBDS + Energy remains successful in detecting these malicious nodes while maintaining more than 90 percent of its energy.

This paper study the detection accuracy value of the CBDS and CBDS+Energy for a different number of nodes. The results are captured and showed in Fig. 2. In this study, the total number of malicious nodes are taken in this work from 0 to 10 in percentage. The highest node speed is taken as 20 m / s. Here, the energy threshold value is set to 30%, 70%. From the above Fig.2, it can be observed that our CBDS+Energy scheme shows a higher detection accuracy value compared with that of CBDS. Although 10 percent of all nodes on the network is at risk, CBDS + Energy remains successful in detecting these malicious nodes while maintaining more than 90 to 93 percent of accuracy value.

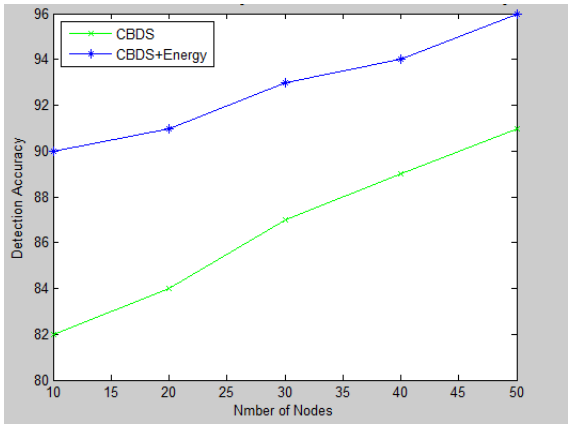

Fig.2. Detection Accuracy of CBDS and CBDS+Energy for different Number of Nodes

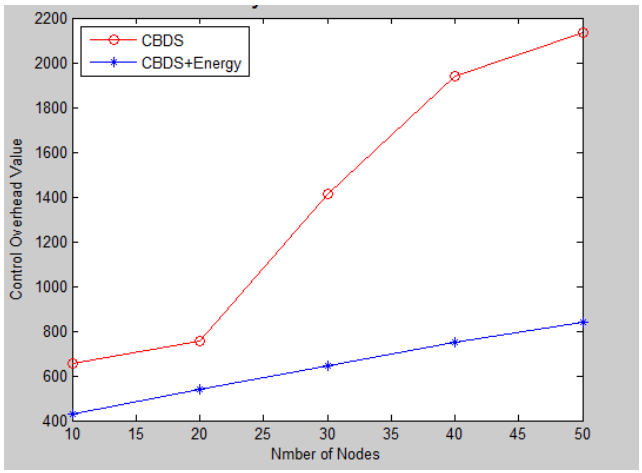

Fig.3. Control Overhead of CBDS and CBDS+Energy for different Number of Nodes

This paper study the control overhead value of the CBDS and CBDS+Energy for a different number of nodes. The results are captured and showed in Fig. 3. In this study, the total number of malicious nodes are taken in this work from 0 to 10 in percentage. The highest node speed is taken as 20 m / s. Here, the energy threshold value is set to 30%, 70%. From the above Fig.3, it can be observed that our CBDS+Energy scheme shows a higher trust value compared with that of CBDS. Although 10 percent of all nodes on the network is at risk, CBDS + Energy remains successful in detecting these malicious nodes while maintaining less value of control overhead with 500.

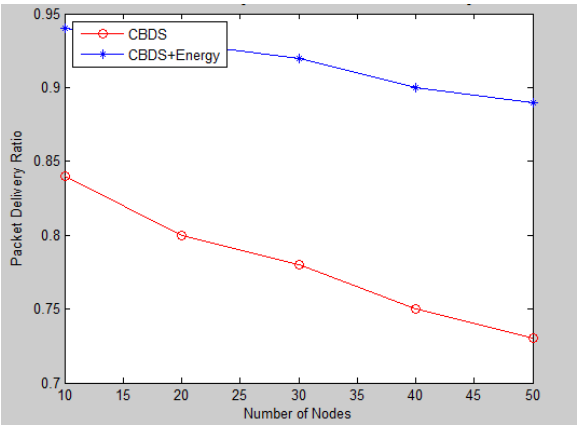

Fig.4. Packet Delivery Ratio of CBDS and CBDS+Energy for different Number of Nodes

This paper study the packet delivery ratio of the CBDS and CBDS+Energyfor a different number of nodes. The results are captured and showed in Fig. 4. The total number of malicious nodes are taken in this work from 0 to 10 in percentage. The highest node speed is taken as 20 m / s. Here, the energy threshold value is set to 30%, 70%. From the above Fig.4, it can be observed that our CBDS+Energy scheme gives a superior packet delivery ratio than the CBDS. Among the entire nodes, only 10 percent are at risk, CBDS + Energy remains successful in detecting these malicious nodes while maintaining more than 92 percent of packet delivery ratio.

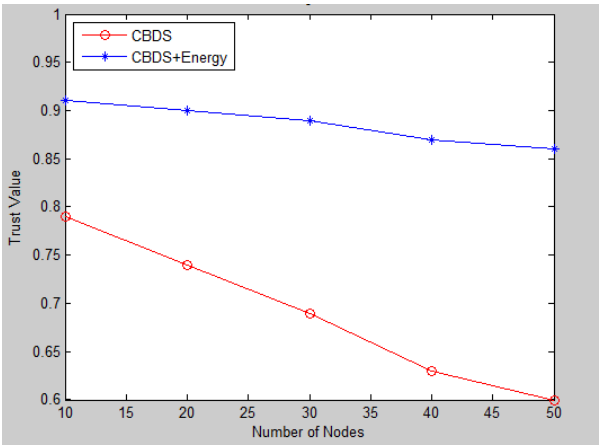

Fig.5. Trust Value of CBDS and CBDS+Energy for different Number of Nodes

This paper study the trust value of the CBDS and CBDS+Energy for a different number of nodes. The results are captured and showed in Fig. 5. In this study, the total number of malicious nodes are taken in this work from 0 to 10 in percentage. The highest node speed is taken as 20 m / s. Here, the energy threshold value is set to 30%, 70%. From the above Fig.5, it can be observed that our CBDS+Energy scheme shows a higher trust value compared with that of CBDS. Although 10 percent of all nodes on the network is at risk, CBDS + Energy remains successful in detecting these malicious nodes while maintaining more than 90 percent of trust value.

5.7. *Varying the Number of Nodes with a Different Threshold*

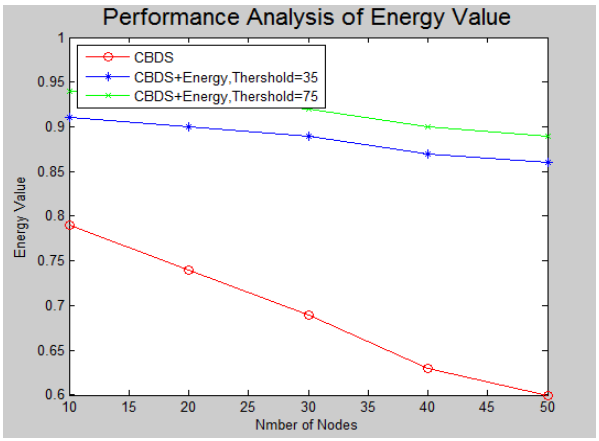

Fig.6. Energy value of CBDS and CBDS+Energy for different threshold

This paper study the energy value of the CBDS, CBDS+Energy-Threshold 35 and CBDS+Energy-Threshold75 for a different number of nodes. The results are captured and showed in Fig. 6. In this study, the total number of malicious nodes are taken in this work from 0 to 10 in percentage. The highest node speed is taken as 20 m / s. Here, the energy threshold value is set to 35%, 75%. From the above Fig.6, it can be observed that our CBDS+Energy-Threshold 75 scheme shows a higher energy value compared with that of the other two schemes. Although 10 percent of all nodes on the network is at risk, CBDS+Energy-Threshold 75remains successful in detecting these malicious nodes while maintaining more than 92 percent of its energy.

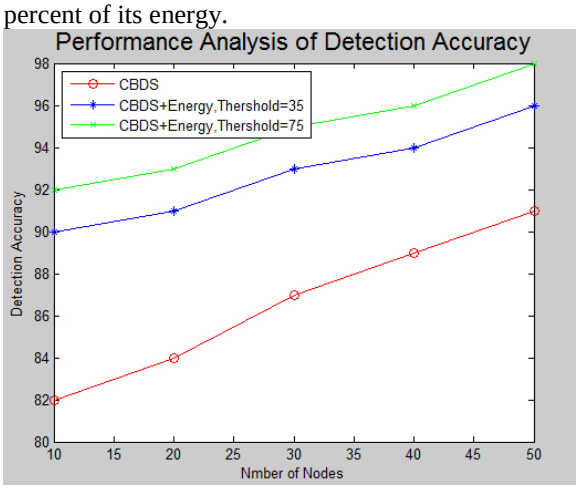

Fig.7. Detection Accuracy of CBDS and CBDS+Energy for different threshold

This paper study the detection accuracy value of the CBDS, CBDS+Energy-Threshold 35 and CBDS+Energy-Threshold 75 for a different number of nodes. The results are captured and showed in Fig. 7. In this study, the total number of malicious nodes are taken in this work from 0 to 10 in percentage. The highest node speed is taken as 20 m / s. Here, the energy threshold value is set to 30%, 70%. From the above Fig.7, it can be observed that our CBDS+Energy-Threshold 75 scheme shows a higher detection accuracy value compared with that of the other two schemes. Although 10 percent of all nodes on the network is at risk, CBDS+Energy-Threshold 75 remains successful in detecting these malicious nodes while maintaining more than 92 to 97 percent of the accuracy value.

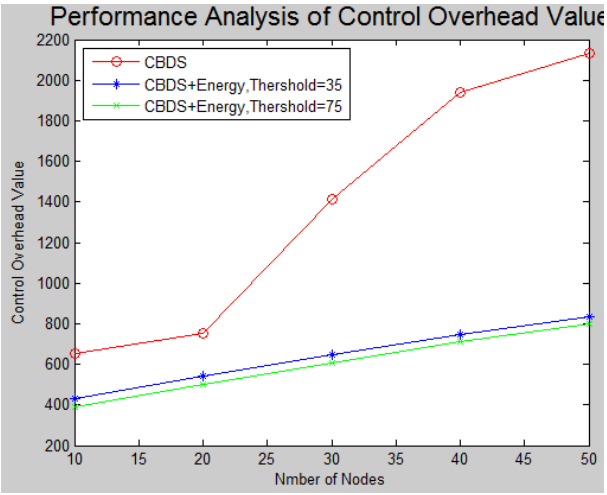

Fig.8. Control Overhead of CBDS and CBDS+Energy for different threshold

This paper study the control overhead value of the CBDS, CBDS+Energy-Threshold 35 and CBDS+Energy-Threshold75 fora a different number of nodes. The results are captured and showed in Fig. 8. In this study, the total number of malicious nodes are taken in this work from 0 to 10 in percentage. The highest node speed is taken as 20 m / s. Here, the energy threshold value is set to 30%, 70%. From the above Fig.8, it can be observed that our CBDS+Energy-Threshold 75 method shows a higher trust value compared with that of the other two schemes. Although 10 percent of all nodes on the network is at risk, CBDS+Energy-Threshold 75 remains successful in detecting these malicious nodes while maintaining less value of control overhead with 400.

This paper study the packet delivery ratio of the CBDS, CBDS+Energy-Threshold 35 and CBDS+Energy-Threshold 75 of malicious nodes vary from 0% to 10% for all network. The highest node speed is taken as 20 m / s. Here, the energy threshold value is set to 30%, 70%. From the above Fig.9, it can be observed that our CBDS+Energy-Threshold 75 scheme gives a superior packet delivery ratio than the other two methods. Among the entire nodes only 10 percent are at risk, CBDS+Energy-Threshold 75remains successful in detecting these malicious nodes while maintaining more than 97 percent of packet delivery ratio.

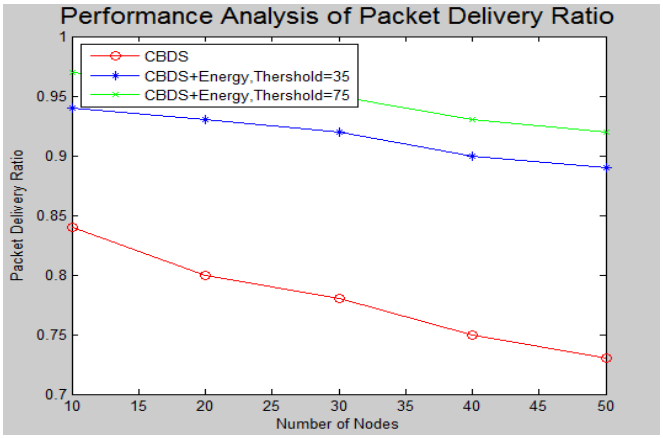

Fig.9. Packet Delivery Ratio of CBDS and CBDS+Energyfor different threshold

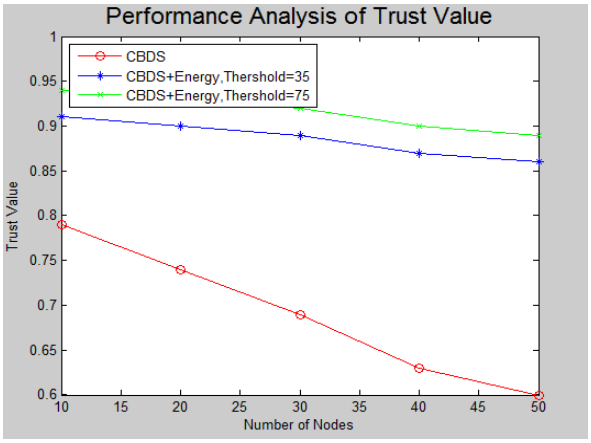

Fig.10. Trust Value of CBDS and CBDS+Energy for different threshold

This paper study the trust value of the CBDS, CBDS+Energy-Threshold 35 and CBDS+Energy-Threshold 75 for a different number of nodes. The results are captured and showed in Fig.10. In this study, the percentage of malicious nodes varies from 0% to 10% for all network. The highest node speed is taken as 20 m / s. Here, the energy threshold value is set to 30%, 70%. From the above Fig.10, it can be observed that our CBDS+Energy-Threshold 75 scheme shows a higher trust value compared with that of the other two schemes. Although 10 percent of all nodes on the network is at risk, CBDS+Energy-Threshold 75 remains successful in detecting these

malicious nodes while maintaining more than 90 percent of trust value.

6. CONCLUSION

In this paper, a new approach is proposed for finding and avoiding malicious node attack in MANETs. In this work, the node source selects a highly valuable node for collaboration, in that the node's address is employed as a trap to track malicious nodes to launch RREP messages as a response. In this case, a malicious node was detected and prevented from participating in the operation of the input using energy-based reverse tracing technology. The performance metrics shows the result of the existing and proposed system. From the experimental setup, it is shown that the proposed approach gives the best result than the existing approaches.

REFERENCES

[1] A. Pirzada and C. McDonald, "Detecting and evading wormholes in mobile ad hoc wireless networks," International Journal of Network Security, vol. 3, no. 2, pp. 191-202, 2006.

[2] A.RajaramandS.Palaniswami, "Malicious node detection system for mobile ad hoc networks," International Journal of Computer Science and Information Technologies, vol. 1, no. 2, pp. 77-85, 2010.

[3] Baadache and A. Belmehdi, "Avoiding Blackhole and cooperative Blackhole attacks in wireless ad hoc networks," Intl. J. Comput. Sci. Inf. Security, vol. 7, no. 1, 2010.

[4] Bansi S. Kantariya1, Dr. Narendra M. Shekokar," Detection and Mitigation of Greyhole Attack in Wireless Sensors Network Using Trust Mechanism", 2013.

[5] G. Arulkumaran& R. K. Gnanamurthy, "Fuzzy Trust Approach for Detecting Black Hole Attack in Mobile Adhoc Network ", 2017.

[6] G.S.MamathaandS. C.Sharma, "Anew combination approach to secure manets against attacks," International Journal of Wireless & Mobile Networks, vol.2, no.4, pp. 71-80, 2010.

[7] H. Deng, W. Li, and D. Agrawal, "Routing Security in Wireless Adhoc Network," IEEE Commun. Mag., vol. 40, no. 10, Oct. 2002.

[8] H. Liu, J. G. Delgado-Frias, and S. Medidi, "Using two-timer scheme to detect selfish nodes in ad-hoc networks," in 6th IASTED International Conference Communication, Internet, and Information Technology, pp.179-184, Alberta, Canada, 2007.

[9] JaydipSen," Detection of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", Bengal Intelligent Park, Salt Lake Electronic Complex, Kolkata, India,2014.

[10] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[11] K. Vishnu and A. J Paul, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks," Int. J. Comput. Appl., vol. 1, no. 22, pp. 28–32, 2010.

[12] N.Venkatadri, Reham Abdellatif Abouuhogail, and Ahmed Yahya, "Secure TORA: Removal of Black Hole Attack using Twofish Algorithm", International Journal of Software Engineering and its Applications, 2016.

[13] P.-C. Tsou, J.-M. Chang, H.-C. Chao, and J.-L. Chen, "CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture," in Proc. 2nd Intl. Conf. Wireless Commun., VITAE, Chennai, India, Feb. 28–Mar. 03, pp. 1–5,2011.

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

[15] Pham Thi Ngoc Diep," Detecting Colluding Blackhole and Greyhole Attack in Delay Tolerant Networks", 2015.

[16] 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.

[17] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative blackhole attacks in wireless ad hoc networks," in Proc. Int. Conf. Wireless Netw., pp. 570–575, Jun. 2003.

[18] S. S. Manvia, L. B. Bhajantrib, and V. K. Vagga, "Routing misbehavior detection in manets using 2ACK," Journal of Telecommunication and Information Technology, vol 4, no. 1, pp. 105-111, 2010.

[19] 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.

[20] W. Ren, Dit-Yan Yeung, Hai Jin, and Mei Yang, "PulsingRoQDDoSattack and defense scheme in mobile ad hoc networks," International Journal of Network Security, vol. 4, no. 2, pp. 227-234, 2007.

[21] 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.

[22] Y. Xue and K. Nahrstedt, "Providing fault-tolerant Adhoc routing service in adversarial environments," Wireless Pers. Commun. vol. 29, pp. 367– 388, 2004.