Collaborative Attack Detection over MANET Nodes Using Enhanced Routing Protocol for Efficient Data Transmission

Haripriya Nair[1], Dr.B.Arunkumar[2], Dr. GKD Prasanna Venkatesan[3]

[1] Research Scholar, Department of Computer Science and Engineering, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu
[2] Associate Professor, Department of Computer Science and Engineering, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu
[3] Dean, Faculty of Engineering, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu

Abstract: MANETs possess a high degree of node mobility due to dynamic fluctuations in the network topology. It is difficult to construct a stable and reliable network path in such cases so data security plays a crucial role in such dynamic networks. In the proposed research methodology, an efficient collaborative attack detection scheme is proposed to identify the possible threats and attacks introduced by the malicious nodes in the network. Further, an optimization technique involving a hybrid CSA and GA algorithm is employed for enhancing the performance of the proposed CBD technique by improving the network strategy.

Keywords: Attack Detection, MANET, Routing Protocol, Data Transmission

1. INTRODUCTION

MANETs are a class of wireless networks that are configured without any physical network connectivity. In the ad hoc network, every single node behaves as a router to send/receive information from other nodes. Routing is a difficult task in MANETs because there is a high degree of node mobility resulting in frequent change in the network topology. Nodes in the ad hoc network can move in any direction when the complexity of the network increases, which in turn makes routing a problematic task. The act of gathering information and delivering it to the destination is known as routing. Routing involves two concepts: to find the routing paths and to transfer the gathered information in the form of packets. There are different protocols used in routing. These protocols make use of many metrics to find suitable networking paths for moving the information. The process of creating network paths involves the creation of networking algorithms which make use of routing tables and contain routing path information. There are two prominent types of protocols: proactive protocol and on-demand protocol. Proactive protocols keep updating routing data to all nodes by spreading the updates throughout the network. On-demand protocols, also called reactive protocols, discover a routing path only when the route is required. Due to node mobility which results in rapid alterations in the network topology and due to network partitions designing network routing protocols for MANETs has become a challenging functionality. In addition to this, packet losses and variable capacity of wireless networks contribute to the complexity of the design, which can be addressed by designing effective routing protocol. MANETs are useful for applications in hostile and combative environments where there is no established infrastructure. There is active research work in the field of routing, power control, resource management, and application of MANETs in these fields. Mobile ad hoc network concentrates on improving the network transmission capacity by providing users with an efficient transmission channel which has sufficient bandwidth and which is safe and reliable (Kaur & Kumar, 2013). The major concern related to MANETs is security or data provenance in communication systems. The security issue is due to frequent exposure of MANETS to various vulnerabilities (Dureja & Dahiya, 2014). Some of the characteristics such as absence of proper validation system, infrastructure less network environment and dynamic random node movement and non-availability of authorization functionality makes MANETs more sensitive to attacks. Different vicious attacks target the data transmission system in the network and there are various secured routing protocols to withstand few attacks. But it is challenging to tackle two or more attacks acting simultaneously on a network system. Such types of attacks are known as Collaborative attacks (Rana et al., 2015).

1.1 Collaborative attacks in MANETs:

Collaborative attacks influence performance degradation of MANETs and have more significant effect than relatively singular attacks. Due to an increase in the demand for MANETs based applications, a wide range of routing protocols and different algorithms for securing MANETs were developed. However, there is no availability of completely secured protocols to strengthen the security system of data transmission (Kumar & Kumar, 2015). The nodes in the ad hoc network are capable of forwarding the data packets on their own and these nodes support intermittent network connection with the association of numerous routing such as AODV, DSR and DSDV etc. (Aldaej & Ahamad, 2016). However, most of these protocols failed to deliver satisfactory security performance. Fundamentally, two prominent threats affect the performance of the routing protocols (Pathan, 2016). The primary threat to MANET is from the nodes which do not belong to the network group and the later threat is from the unauthorized nodes which belong to the network group. Besides, there are predominant chances of injecting a false and unauthorized routing information into the network by an attacker due to which there can be security meltdown or increase in data load which prevents efficient functioning of routing protocols (Poongodi & Karthikeyan, 2016). Different routing protocols are developed to address the routing issue, which is discussed in the Literature Review Section. In the proposed research methodology, a Cooperative Bait Detection technique is adopted for detecting the collaborative attack over MANET. The proposed technique mainly focuses on identifying the attacks during data transmission. However, the threat in routing systems still exists and to overcome this limitation, an efficient collaborative attack detection scheme is proposed. This technique adopts an enhanced routing protocol for securing the data transmission by preventing the possible routing attack. The proposed methodology aims in improving the network performance by improving the routing strategy. An optimization technique combining Hybrid CSA and Improved GA is adopted for improving the performance of the MANET by enhancing the routing mechanism.

2. LITERATURE REVIEW:

The process of detecting vicious nodes in MANET is very complex. Several literary works have studied the complexities of detecting vicious nodes in the MANETs. Most of the previous studies discussed the identification of a single vicious node in the MANET network. Besides, most of the discussed research works require a pre-defined environment or constraints to operate. Detection schemes presented by various researches previously are categorized into proactive and reactive faulty node detection methods. The proactive detection technique requires constant detection or monitoring of the nodes. In this technique, irrespective of the existing vicious nodes, the detection overhead is created frequently and thus predominant amount of data is wasted in detecting malicious nodes. Nevertheless, it helps in avoiding the attack in the preliminary stage. Reactive detection techniques activate themselves only when the destination nodes identify or detect an important drop in the packet delivery ratio (Kumar & Kumar, 2008). Routing in MANETs is challenging because of the high node mobility and stable networking is not possible with minimum resource cost and with high efficiency. An efficient genetic algorithm (GA) based intelligent route optimization technique for MANET was proposed by (Haider & Shabbir, 2014). This research study provides a multidimensional approach to address the network complexities in MANETs by using an evolutionary GA algorithm. The preliminary aim of employing GA is to find an optimal network path with minimum resource utilization. The proposed approach finds its relevance beyond the specific constraint and is regarded as an efficient algorithm because of its simplicity and reliability in solving the optimization issues. Various researchers regard Quality of service (QoS) as an important aspect in MANETs and the necessity for optimizing QoS through routing. Preferentially, optimization of QoS enhances the lifetime of the network by consuming less energy and by distributing additional data packets with less routing overhead and low rate of Bit Error Ratio (Metri & Agarwal, 2014). An efficient DSR routing protocol is proposed by (Mahajan et al., 2016) to enhance the performance of the network routing by improving QoS in MANETs. A Bacterial Foraging Optimization (BFO) technique is applied to the DSR routing protocol and simulation results are used to prove the enhancement achieved due to the optimization technique. A comparative analysis of the performance of the DSR routing protocol with BFO and without BFO is performed to validate the efficiency of the BF optimization technique. Results show that there was increase in the lifespan of the MANETs and the data packets were transferred efficiently with very little BER which significantly reduced the possible cases of node failure. Security along with efficient energy utilization in MANETs is attracting significant attention among various researchers. A network coding mechanism is employed to mitigate energy utilization by considering fewer data transmissions in a MANET network. Encryption schemes are gaining popularity in achieving robust secured data transmission networks (Sachdeva & Kaur, 2016). Among various encryption schemes, the P-coding encryption mechanism is used widely which is discussed in (Patel & Khatiwala, 2016). This technique is a lightweight encryption method that is used to obtain confidentiality in data transfer networks. P-coding enables the source to alter the symbol of each packet randomly so that it becomes challenging for the attackers to hack important information without realizing the permutation encryption function and coding vector. Identifying a stable and secure path between a source and destination invites more complexities in MANETs due to the abrupt fluctuation in node stability and frequent alterations in the network topology (Kumar & Gopal, 2016). Besides, there is a major dependency on the intermediate nodes to transfer the data packets safely from the source to the destination which invokes trust issues in the network. It is important to utilize a trust mechanism to obtain secure routing and to simulate the intermediate nodes to associate in the process of packet forwarding (Liang et al., 2016). An evaluation of utilizing trust mechanisms in choosing the optimized path between two nodes is discussed by (Gharib et al., 2017). The proposed study mainly concentrates on selecting the most stable and secure routing path depending on the multidimensional trust evaluation mechanism which includes the percentage of hubs, evaluation of trust confidence in developing trust of nodes on the routing path. The proposed technique resolves the constraint of including only the trustworthiness of the intermediate nodes on the routing path and adopts a route optimization technique to find an efficient network route between source and destination. The factual observations showed phenomenal robustness and precision in the proposed trust approach in the dynamic MANET system.

3. RESEARCH METHODOLOGY:

The preliminary objective of the proposed research methodology is to strengthen the security mechanism of the MANET nodes against collaborative attacks. The proposed research methodology adopts an enhanced Cooperative Bait Detection technique (CBD) to detect the collaborative attack in the MANET system. An efficient optimization technique combines two optimization algorithms, Hybrid CSA and Improved GA to enhance the performance of the MANET by improving the proposed CBD technique.

3.1 Cooperative Bait Detection Approach:

The proposed approach presents an improved CBD technique, to identify and eliminate the launching of collaborative node attack through vicious nodes in the MANETs. In the present study, the source node contingently appoints a node as its adjacent node to cooperate in identifying any suspicious nodes that may compromise the security of the network. In this technique the source node generates a false RREQ to reach a known neighbor node which is falsely designated as the destination node. This RREQ will act like a bait to trigger any potential malicious node in the network to transmit a RREP message. This will help in detecting and preventing the malign or harmful nodes from involving themselves in the routing process by employing a reverse tracing mechanism (Dumne & Manjaramkar, 2016). This process goes on until the packet delivery ratio goes down suspiciously. Soon after the drop occurs, an alarm is triggered and an alarming signal is sent to the source node through destination node to initiate the faulty node detection process again. During the early stages of its operation the proposed CBDS technique takes advantage of a proactive scheme that prevents a malicious activity. Later on it switches over to another mechanism which is reactive in nature. This action significantly reduces the wastage of resources (Prasad, 2016). The CBD approach is based on the DSR scheme. This means that the RREP helps the proposed mechanism to identify the IP address of every node present in the route established between the source and destination. But the source node is not equipped to be able to identify the intermediate node which was responsible for redirecting the data packets through an unauthorized shortest route selected by the malicious node. It is important to resolve this complexity and to solve this, a HELLO message is sent to the CBD technique to assist every node to identify their respective neighboring nodes in the vicinity of single hop. This functionality enables the nodes to send the bait address to persuade the harmful nodes while utilizing the reverse tracing mechanism to identify the address of the vicious nodes (Usmani & Deshmukh, 2015). The properties of the baiting RREQ packets are the same as that of fundamental RREQ packets and the only difference is the change in the destination IP address which is now modified to function as a bait IP address. Refer the Table 1 that depicts the modified RREQ packet.

Table 3.1. Modified format of RREQ Packet

Type of message	Data Length	Request node Id
Destination Address (RREQ’: Bait address)		
Address 1		
Address 2		
Address 3		

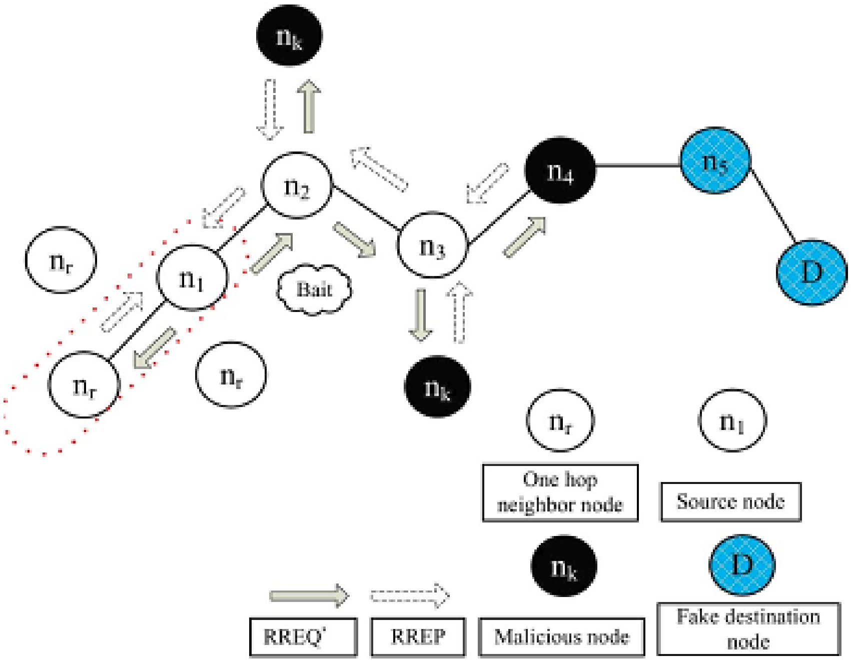


Fig 3.1Random selection procedure in CBD technique

The CBD technique consists of three stages: The first step is called as the bait step, the next step is called as initial reverse tracing and in the final phase it shifts to a reactive defense step. The first two phases are considered as proactive defense steps and the last step is regarded as a reactive scheme that responds to a possible attack.

(i) Initial Bait Step: The main aim of this step is to provoke a vicious node to transmit a reply message to RREP by forwarding the bait RREQ'. The source node contingently appoints a particular node as its adjacent node n_r within a hop. This node associates itself with the source node by considering its address as the destination address of the bait RREQ (Chetan et al., 2016) (Naveeda & Saraswathi, 2016)'. The baiting phase of selecting the adjacent nodes is illustrated in the figure 3.1. The analysis of the follow-up bait phase is explained as: Initially if the node n_r has not introduced any attack once the source node forwards the RREQ then there exists a reply RREP from neighboring nodes along with the node n_r, which indicates the existence of the vicious node in the reply routing path (figure 3.1). In such cases, a reverse tracing scheme is initiated to identify the affected network path. Consider the scenario in which only the node n_r responded to the RREQ by sending a RREP, then it is understood that vicious nodes are absent in the given network. Second, suppose if the node nr itself is the vicious node responsible for the black hole attack then, after sending the RREQ by the source node (along with nr node) other nodes would also send reply RREPs which clearly defines the presence of the vicious node in the reply routing path. In that state, the mechanism of the reverse tracing is executed in the later stages to identify the affected path. If the n_r node does not send any reply RREP, then the node is directly regarded as faulty node by the source node (Aadithiya, B. N., & Suganthi, 2016).

(ii) Initial Reverse Tracing Step: In this step, the RREP which is received in response to the RREQ is utilized to analyze the behavior of the malicious nodes. In a case where a vicious node receives the RREQ and the node replies with a false RREP and as a counter action, reverse tracing operation is executed to retrieve the false path. For example, when the malicious node n_m sends a reply with the wrong RREP, an address list $X = \{n_1,....n_k,....n_r\}$ is registered in the RREP.

(iii) Shifted to Reactive Defense Phase: The next significant step is to activate the path finding process. After the process of path definition if the packet delivery ratio is at the destination node equals the threshold value, the mechanism of detecting the invalidated node is initiated to identify the affected network path (Saini & Devi, 2016) (Jhaveri et al., 2018). The threshold value considered in this study is 0.5. If the dynamic threshold value of the node is above the set threshold (Above 0.5) then the route is considered as best route whereas, if the node threshold value is less than the set value (Below 0.5) then the route where the node is traversing is regarded as false route. The operation of the CBD technique is given in the figure 3.2

The operational process of CDB scheme involves retrieving the information related to false path, trusted nodes and malicious nodes to simplify the process of identifying the trusted zone by validating the reply of malicious node to every RREP.

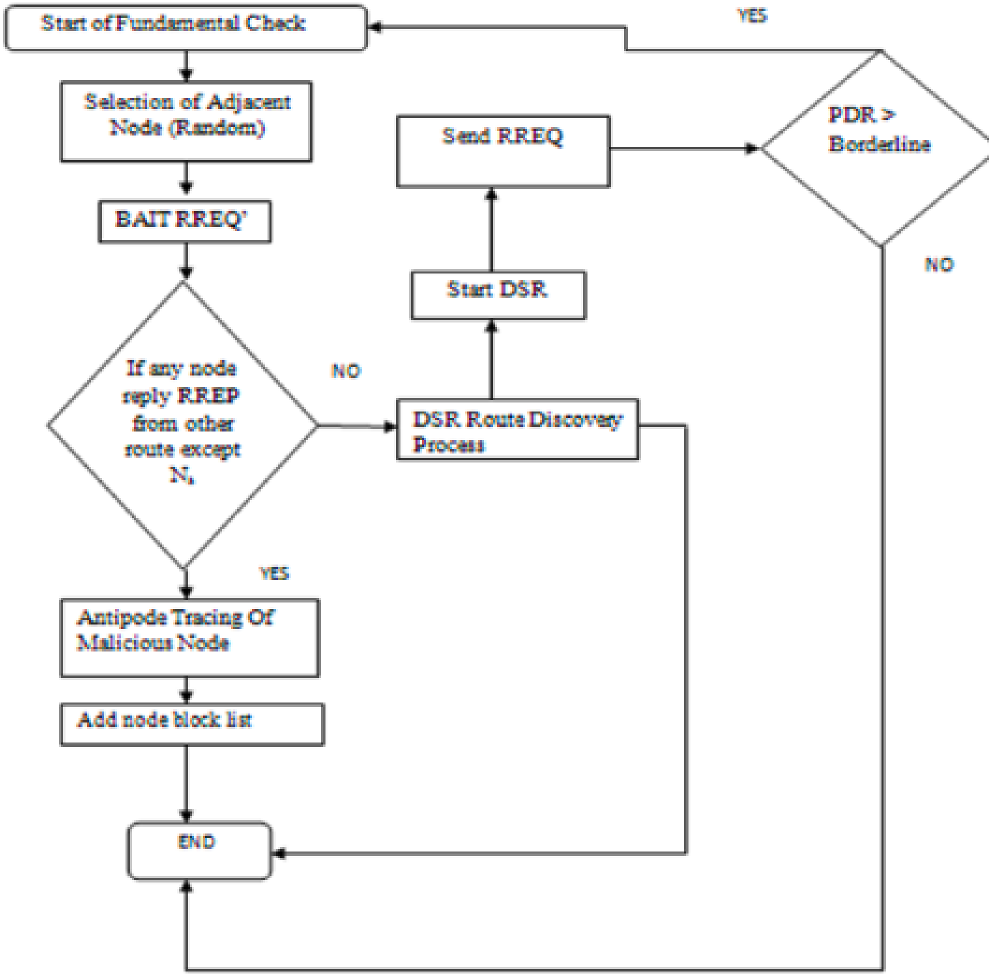

Start of Fundamental Check
YES
Selection of Adjacent Node (Random)
Send RREQ
PDR > Borderline
BAIT RREQ'
NO
Start DSR
If any node reply RREP from other route except N,
NO
DSR Route Discovery Process
YES
Antipode Tracing Of Malicious Node
Add node block list
END

Figure 3.2 Operation process of CBD technique

3.2 Implementation procedure:

- The random values are generated based on the bandwidth limits.
- Random number generation is bounded by the upper and lower limits of the calculated bandwidth.
- The highest and lowest values of bandwidth are calculated as per the following mathematical expression.

  I=min_val+ (max_val-min_val) *rand, which is employed in MATLAB.
- The initial size (I) is defined based on the population size.

- An objective function is employed for optimizing the routing process in MANET. The optimization is processed by using Ad-Hoc On Demand Distance Vectoring hybridization approach of CSA and Improved GA.
- Using an evolutionary algorithm GA, the best value is selected from the fitness function.
- The initial random values are updated by integrating the parameters of the optimization algorithm.
- The optimum value is selected by repeating the procedure until the iteration process is completed.
- The performance of the routing protocol optimized by the optimization algorithm GA is evaluated and the results are displayed.

3.3 Performance Metrics:

The performance of the proposed technique is evaluated based on the performance defining parameters given below:

(i) **Packet Delivery Ratio (PDR):** It is calculated as the ratio of the actual number of packets transmitted from the source to the number of packets received at the destination. The PDR is expressed as:

$$\textbf{PDR}= \frac{1}{n}\sum_{i=1}^{n}\frac{pktd(i)}{pkts(i)} \qquad \textbf{(1)}$$

Where, $pktd_i$ is the number of packets received by the destination node in the i^{th} application, and $pkts_i$ represents the packet count for transmissions that originated at the source node.

(ii) **Routing Overhead:** It is constituted as the ratio of the amount of routing-related control packet transmissions to the amount of data transmissions. The expression for average routing overhead is defined as:

$$\textbf{RO}= \frac{1}{n}\sum_{i=1}^{n}\frac{cpk(i)}{pkt(i)} \qquad \textbf{(2)}$$

Where, pk_i is the count of control packets generated in the traffic (i)

And pkt_i is the number of data packets transmitted in the traffic (i)

(iii) **Average End-to-End Delay**: It is represented as the average time taken for the transmission of the data packet from source node to the destination node. The Average End-to-End Delay is expressed as:

$$\textbf{E}= \frac{1}{n}\sum_{i=1}^{n}\frac{d(i)}{pktd(i)} \qquad \textbf{(3)}$$

Where, d_i is the total delay incurred. $pktd_i$.

(iv)Throughput:The actual amount of data received at the destination from a given source node within a particular time limit is termed as throughput of the system. Throughput of the system is defined as the total amount of received data. Throughput gives the number of bits that is transmitted per second, expressed as given below:

$$T=\frac{1}{n}\sum_{i=1}^{n}\left(\frac{b_i}{t_i}\right)....(4)$$

3.4 Optimization Algorithm:

The optimization technique in the proposed research combines two optimization algorithms: Hybrid CSA and Improved GA to enhance the performance of the network by improving the routing strategy.

3.4.1 Cuckoo search Algorithm (CSA):

CSA is a bio-influenced algorithm borrowed from the nature of cuckoos. The cuckoos opt to utilize the nests of other host birds to lay their eggs. Besides, there are different examinations that have demonstrated that flight conduct of numerous creatures and insects has shown the typical attributes of L'evy flights. Exceptionally, the behavior of cuckoo species is implemented to optimize and to perform the optimal search. The initial results exhibit the promising capability. Below is the pseudocode for the cuckoo search via Levy flights (Zhang et al., 2016).

The rules of CSA are described by the following steps:

(i) The egg laid by the cuckoo represents a feasible solution to the problem. The nest required to hold this egg is randomly chosen. The number of eggs that can be laid by a cuckoo is restricted to 1. .

(ii) Those nests which carry the best quality eggs are given priority and are carried over for further processing.

(iii) The number of host nest that actually exists is defined in advance. The host bird may recognize the cuckoo egg with a probability denoted by $P \in (0,1)$.

3.4.2 Genetic Algorithm (GA):

GA is an evolutionary algorithm profoundly used for optimizing the network systems. In GA, a swarm of chromosomes provides an efficient solution to optimize the output. These solutions are in the form of binary strings (0 and 1). Initially, the evolution of particles is randomly generated, and the process continues until the halting condition is reached. The FV of every swarm is evaluated, and the particles with high FV are selected to optimize the solution. The selected particles undergo mutation to allow the evolution of new particles having good FV and proximity. Consequently, these particles are evaluated in the next iteration, and the process is continued till the iteration reaches halting condition (Kaliappan et al., 2016).

The execution steps of the genetic algorithm are defined by the following steps:

(i) Generation of random initial population

(ii) Evaluation of the fitness function of every individual node in the node population within the network

(iii) Validation of predefined halting criteria

(iv)The existing population undergoes crossover and mutation that leads to the formation of a new set of individuals that constitutes the next generation.

3.4.3 Hybrid CSA and improved GA optimization algorithm:

The motivation behind combining the CSA and GA algorithm is to amalgamate the positive attributes of the cuckoo search and genetic algorithm. In the presented methodology, the hybrid CSA and GA is employed to find the optimal routing path in MANET and to enhance the performance of the proposed Cooperative Bait Detection technique. The proposed (CS-GA) optimization algorithm is based on the population search technique which swarms through the node population to arrive at the global optimum (Kanagaraj et al., 2013). The stages involved in this study are:

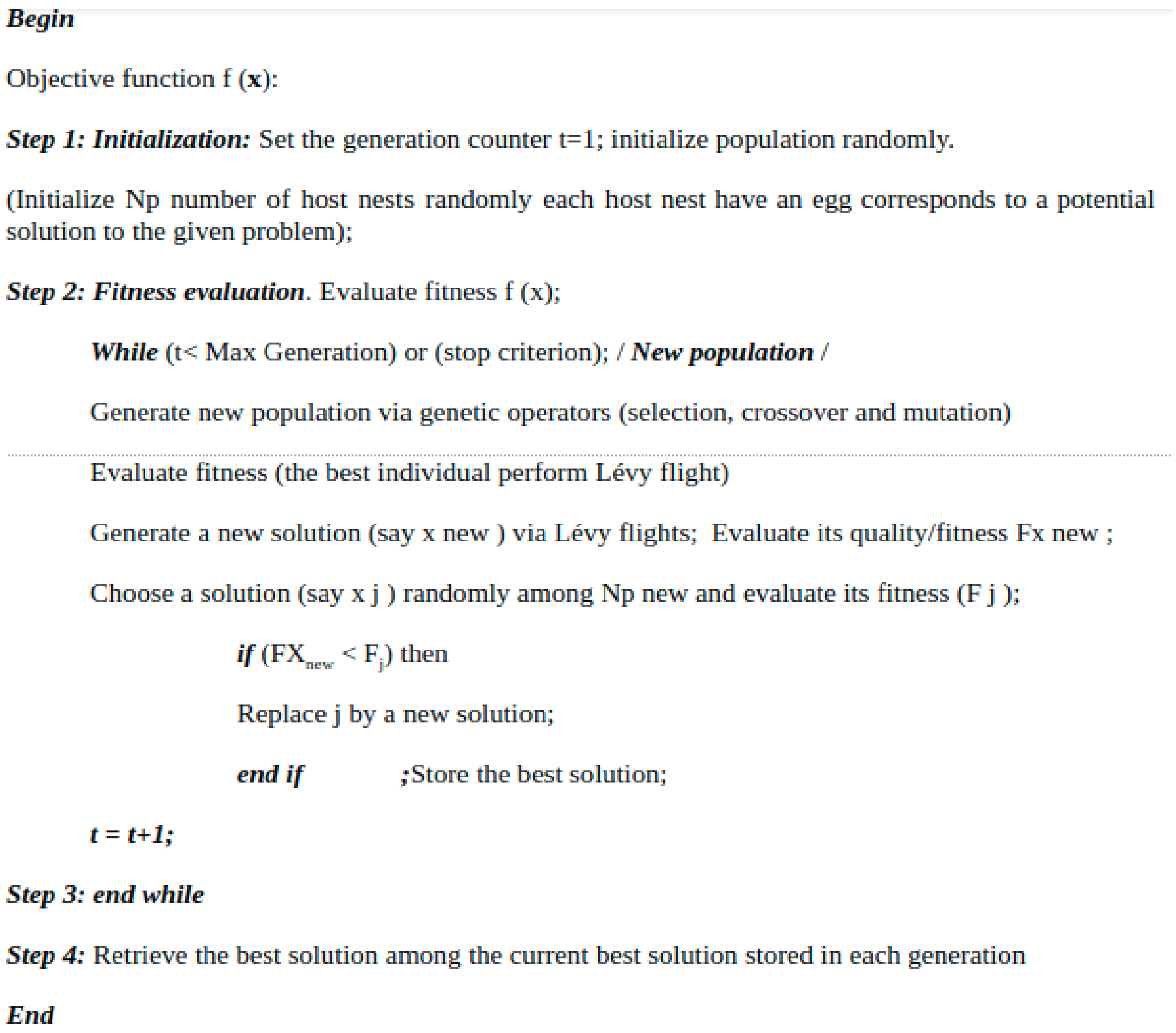
(i) Creation of initial population: The initial population constitutes with randomly distributed host nests which are generated first. The egg represents the solution which is stored in the nest.

(ii) Generation of new population: It consists of two stages; crossover and mutation. In crossover, 2 parent particles are involved in the generation of a new particle whereas in mutation, it is the effect of changes which takes place during replication process with very less probability. The probability of crossover and mutation essays an effective role in selecting GA particles (Garg et al., 2015). Parameters of high value get attracted towards forming a primitive random search model. To reduce the computational time GA process continues till 95% of the particles obtain high FV.

(iii) Elitism technique: The offspring population is formed by the initializing, selecting, reproduction, and mutation which restore the genuine population of the parental nodes. The crossover is done in order to replace the parent cuckoo with the newly generated cuckoo egg if the performance/characteristics of the cuckoo egg outperform its own parent.

The pseudocode for the hybrid CSA and GA is given below:

Begin



```
Begin

Objective function f (x):

Step 1: Initialization: Set the generation counter t=1; initialize population randomly.

(Initialize Np number of host nests randomly each host nest have an egg corresponds to a potential solution to the given problem);

Step 2: Fitness evaluation. Evaluate fitness f (x);

      While (t< Max Generation) or (stop criterion); / New population /

      Generate new population via genetic operators (selection, crossover and mutation)

      Evaluate fitness (the best individual perform Lévy flight)

      Generate a new solution (say x new ) via Lévy flights;  Evaluate its quality/fitness Fx new ;

      Choose a solution (say x j ) randomly among Np new and evaluate its fitness (F j );

                  if ($FX_{new}$ < $F_j$) then

                  Replace j by a new solution;

                  end if        ;Store the best solution;

      t = t+1;

Step 3: end while

Step 4: Retrieve the best solution among the current best solution stored in each generation

End
```

4. RESULTS AND DISCUSSION:

4.1 End to End delay:

The Figure 4.1 shows the end-end delay experienced by the network under the proposed scheme. From the results, it is observed that the delay time in the network decreases with the increase in number of nodes. CBD technique needs more time in detecting the malicious nodes.

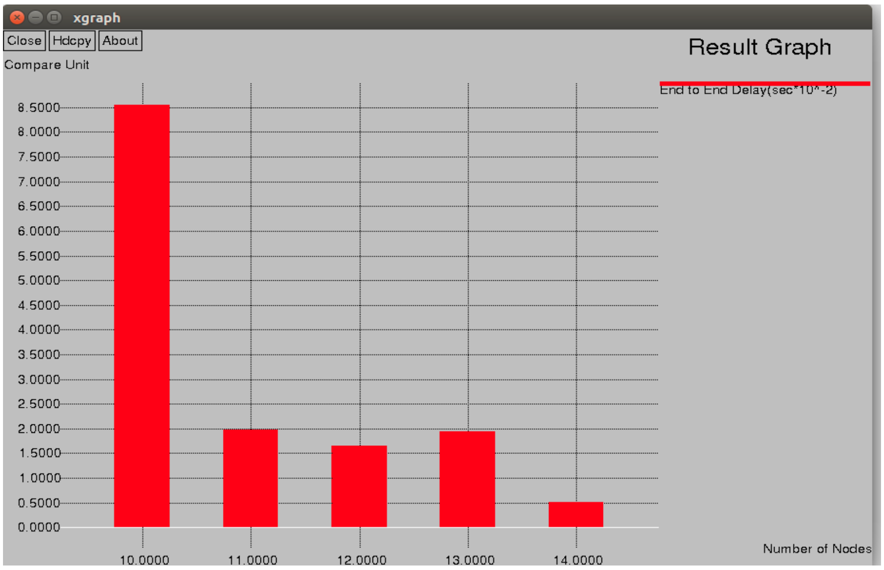


Fig 4.1 End to End delay

4.2 Energy drain rate:

The analysis of energy drain rate is represented in the figure 4.2. It is observed that, the energy fluctuation depends on the packet energy ratio which is sensitive to node mobility due to which the energy proportion fluctuates constantly throughout the network.

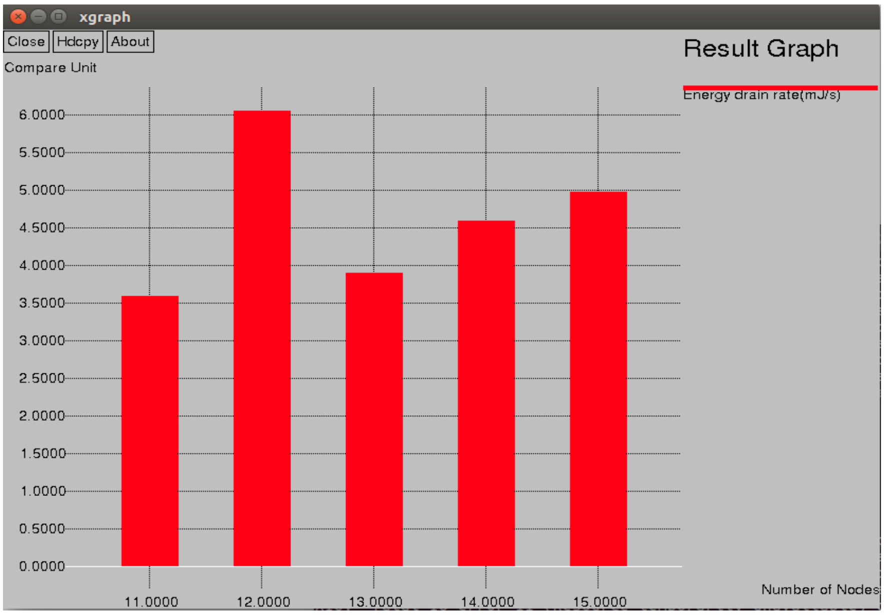


Fig 4.2 Energy drain rate

4.3 Routing overhead:

An increase in the population of malignant nodes will further degrade the performance of the network by increasing the routing overhead. The proposed CBD technique is capable of achieving the proactive detection at the first stage and then shifts itself to the reactive response stage and contributes towards reducing the wastage of resources.

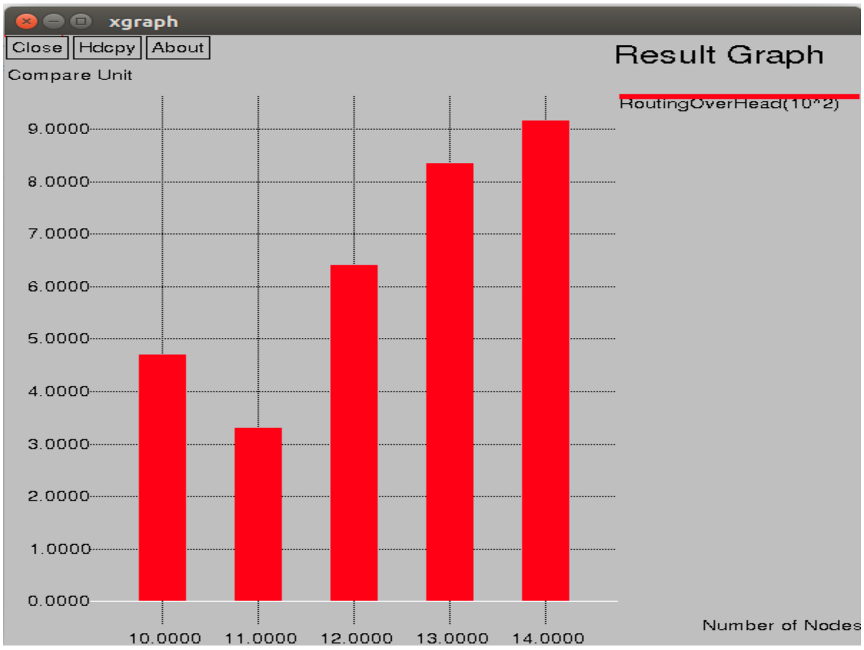


Fig 4.3 Routing Overhead in CBD technique

4.4 Throughput:

The throughput of the network depends on the threshold value. From the results it is observed that the CBD technique effectively manages and tolerates an increase in the number of nodes in the network without compromising on the threshold efficiency which is maintained at 85%.

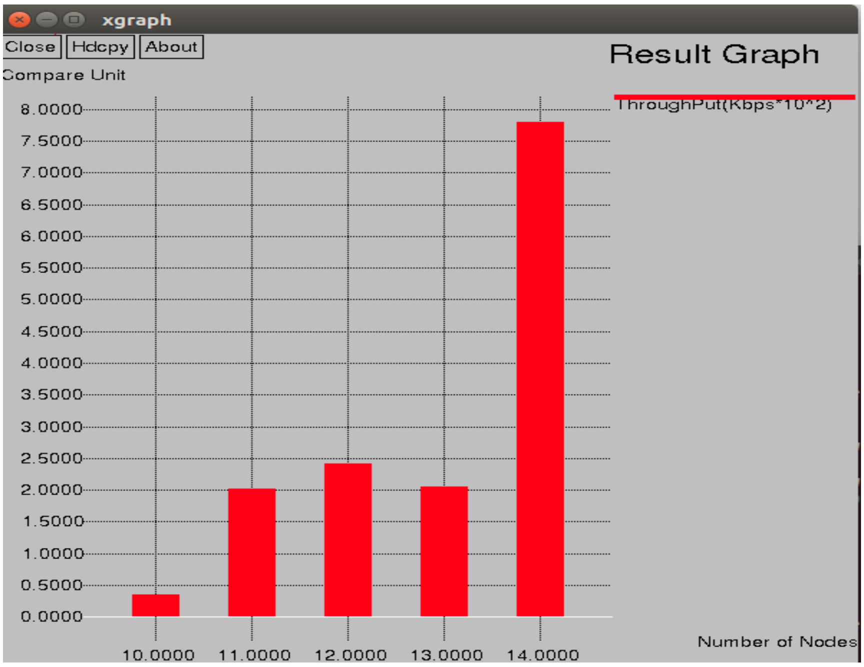


Fig 4.4 Analysis of network Throughput

5. CONCLUSION

The proposed research methodology presents an efficient routing protocol to detect collaborative attack in the MANET environment. An enhanced Cooperative Bait Detection Approach is presented in the study to identify the possible attacks initiated by the vicious nodes in the network. The proposed CBD approach is able to detect the node's address from the identified route between source and destination with help of the information stored in the

RREP message. The performance of the routing protocol is optimized using an efficient optimization technique (Hybrid CSA and Improved GA) which improves the network routing strategy resulting in a reduced end to end delay, reduced routing overhead and an improved throughput. The performance of the proposed technique was evaluated from the simulation results. Results show the enhancement in the throughput value and routing overhead irrespective of increase in the number of nodes.

6. REFERENCES:

[1] Kaur, D., & Kumar, N. (2013). Comparative analysis of AODV, OLSR, TORA, DSR and DSDV routing protocols in mobile ad-hoc networks. *International Journal of Computer Network and Information Security*, *5*(3), 39.

[2] Dureja, A., & Dahiya, V. (2014). Performance evaluation of collaborative attacks in MANETS. *Procedia Computer Science*, *50*, 120-145

[3] Rana, A., Rana, V., & Gupta, S. (2015). EMAODV: Technique to prevent collaborative attacks in MANETs. *Procedia Computer Science*, *70*, 137-145.

[4] Kumar, V., & Kumar, R. (2015). An adaptive approach for detection of blackhole attack in mobile ad hoc network. *Procedia Computer Science*, *48*, 472-479.

[5] Aldaej, A., & Ahamad, T. (2016). AAODV (aggrandized Ad hoc on demand vector): A detection and prevention technique for MANETs. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *7*(10), 2016.

[6] Pathan, A. S. K. (Ed.). (2016). *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press.

[7] Poongodi, T., & Karthikeyan, M. (2016). Localized secure routing architecture against cooperative black hole attack in mobile ad hoc networks. *Wireless Personal Communications*, *90*(2), 1039-1050.

[8] Kumar, S. D., & Kumar, B. V. (2008, December). Energy-aware multicast routing in MANETs based on genetic algorithms. In *2008 16th IEEE International Conference on Networks* (pp. 1-5). IEEE.

[9] Haider, Z., & Shabbir, F. (2014, January). Genetic based approach for optimized routing in Maritime Tactical MANETs. In *Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th-18th January, 2014* (pp. 488-492). IEEE.

[10] Metri, R., & Agrawal, S. (2014, April). Ant colony optimization algorithm based an intelligent protocol to improve QoS of MANETs. In *2014 International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA)* (pp. 121-125). IEEE.

[11] Mahajan, S., Dahiya, N., & Kumar, D. (2016, July). A mechanism of preventing sybil attack in MANET using bacterial foraging optimization. In *2016 Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN)* (pp. 1-5). IEEE.

[12] Sachdeva, S., & Kaur, P. (2016). Routing Attacks and their Countermeasures in MANETs: A Review. *International Journal of Advanced Research in Computer Science*, *7*(4).

[13] Patel, S., & Khatiwala, F. (2016, March). A review paper of an encryption scheme using network coding for energy optimization in MANET. In *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)* (pp. 1054-1058). IEEE.

[14] Kumar, A., Gopal, K., & Aggarwal, A. (2016). Design and Analysis of Lightweight Trust Mechanism for Secret Data using Lightweight Cryptographic Primitives in MANETs. *IJ Network Security*, *18*(1), 1-18.

[15] Liang, W., Ruan, Z., Wang, Y., & Chen, X. (2016). RESH: A secure authentication algorithm based on regeneration encoding self-healing technology in WSN. *Journal of Sensors*, *2016*.

[16] Gharib, M., Lollini, P., & Bondavalli, A. (2017, June). Towards an approach for analyzing trust in cyber-physical-social systems. In *2017 12th System of Systems Engineering Conference (SoSE)* (pp. 1-6). IEEE.

[17] Dumne, P. R., & Manjaramkar, A. (2016, September). Cooperative bait detection scheme to prevent collaborative blackhole or grayhole attacks by malicious nodes in MANETs. In *2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)* (pp. 486-490). IEEE.

[18] Sarvesh S. Joshi Sagar Ghodechor, Amol Barbade, Prof. Rahinj P.L. (2017) Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach *International Journal of Innovative Research in Computer and Communication Engineering* Vol. 5, Issue 4, April 2017, pp. 7163-7167

[19] Usmani, M. A., & Deshmukh, M. (2015) Defending against Attacks in MANETs using Cooperative Bait Detection Approach, *International Journal of Advanced Research in Computer and Communication Engineering Vol*, *4*.

[20] Chetan S. Arage, K. V. V. Satyanarayana & J. Amudhavel (2016). Improved Cooperative Bait Detection Method using Multiple Disjoint Path Technique. Indian Journal of Science and Technology, Vol 9(41), DOI: 10.17485/IJST/2016/v9i41/94793

[21] K. Naveeda & B. Saraswathi. (2016). A Cooperative Bait Detection Approach for Detection of Malicious Node in MANET. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. Vol. 5, Issue 5

[22] Aadithiya, B. N., & Suganthi, N. Enhanced Cooperative Bait Detection Scheme for Disclosure of Black and Grayhole Attacks in Manets. *Journal of Chemical and Pharmaceutical Sciences ISSN*, *974*, 2115.

[23] Saini, R., & Devi, P. S. (2016) Malicious Node Detection in MANETs using Cooperative Bait Detection Approach and Trust Model. *International Journal of Research and Scientific Innovation (IJRSI)*, *3*.

[24] Jhaveri, R. H., Desai, A., Patel, A., & Zhong, Y. (2018). A sequence number prediction based bait detection scheme to mitigate sequence number attacks in MANETs. *Security and Communication Networks*, *2018*.

[25] Zhang, X., Wang, X., Cui, G., & Niu, Y. (2016, October). A Hybrid IWO Algorithm Based on Lévy Flight. In International Conference on Bio-Inspired Computing: Theories and Applications (pp. 141-150). Springer, Singapore.

[26] Kanagaraj, G., Ponnambalam, S. G., & Jawahar, N. (2013). A hybrid cuckoo search and genetic algorithm for reliability–redundancy allocation problems. *Computers & Industrial Engineering*, *66*(4), 1115-1124.

[27] Kaliappan, M., Augustine, S., & Paramasivan, B. (2016). Enhancing energy efficiency and load balancing in mobile ad hoc network using dynamic genetic algorithms. *Journal of Network and Computer Applications*, *73*, 35-43.

[28] Garg, H. (2015). An approach for solving constrained reliability-redundancy allocation problems using cuckoo search algorithm. *Beni-Suef University Journal of Basic and Applied Sciences*, *4*(1), 14-25.