Detection and Isolation of Selfish Nodes in MANET Using Collaborative Contact-Based Watchdog With Chimp-AODV

Bismin V Sherif (bisminsherif@gmail.com)
College of Engineering https://orcid.org/0000-0001-8451-6917
P. Salini
Pudhucherry Engineering College

Research Article

Keywords: Ad-hoc On-Demand Distance Vector, Mobile Ad-hoc Network, Chimp optimization algorithm, Collaborative Contact based Watchdog, selfish node.

Posted Date: August 10th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-754829/v1

Detection and Isolation of Selfish Nodes in MANET using Collaborative Contact-based Watchdog with Chimp-AODV

[*1]Bismin V Sherif, [2]P. Salini
[1]Dept. of Computer Science and Engineering.
Pondicherry Engineering College, Puducherry, India
[2]Dept. of Computer Science and Engineering
Pondicherry Engineering College, Puducherry, India
[*1]bisminsherif@gmail.com, [2]salini@pec.edu

Abstract. Mobile Ad-hoc Network (MANET) is one of the most important self-configuring and independent wireless network. Numerous intermediate nodes are used among MANET to interchange the information without the requirement of any centralized infrastructure. But some nodes act selfishly and utilize the resources only for their own purposes and do not share with the neighbors. This selfish nodes might delay or drop the packet and do not perform routing. Though watchdog is a well-known selfish node detection technique, it causes false negatives and false positives that can affect the performance in terms of precision and speed. To eliminate the drawbacks of existing approaches in selfish node detection, this paper integrates both Ad-hoc On-Demand Distance Vector (AODV) protocol incorporated with chimp optimization algorithm and Collaborative Contact based Watchdog to propose a novel technique called Chimp-CoCoWa-AODV in order to improve the performance of MANET. The main role of chimp optimization algorithm in AODV is to undergo optimal route selection process. The performance of the proposed Chimp-CoCoWa-AODV approach is compared with existing approaches in terms of average routing load, Average Packet Delivery Fraction (PDF), Average End-to-end Delay (EED), Average Throughput, Total packet drop in the application layer, and maliciously dropped packet in the routing layer. The simulation results shows that the proposed approach is effective with 82% PDF and 7.4 ms EED at 50 nodes in detection and isolation of selfish nodes in MANET even in the presence of malicious node.

Keywords: Ad-hoc On-Demand Distance Vector, Mobile Ad-hoc Network**,** Chimp optimization algorithm**,** Collaborative Contact based Watchdog, selfish node.

1. Introduction

In recent years, Ad-hoc networks get more attention due to their self-healing, self-configuring and self-organizing nature. An Ad-hoc network that connects several devices in wireless means is called Wireless Ad-hoc network (WANET). Mobile Ad-hoc Network (MANET) is a type of wireless Ad-hoc network that consists of arbitrarily located mobile nodes. These nodes are wireless connected in a self-healing and self-configured network without any fixed infrastructure [1]. The routing protocols developed for MANET are mainly classified into three categories like reactive protocols, proactive protocols and hybrid protocols [2]. The proactive protocols are based on periodic exchange and the reactive protocols are based on on-demand route discoveries. The benefits of the proactive and reactive protocols are combined in the hybrid protocols. The reactive protocols has more advantages than others such as less routing overhead and consuming less resources due to the absence of large routing tables. The two common types of reactive routing protocol are on-demand and bandwidth efficient protocol. The main functions of this protocol includes route discovery for discovering new routes and route maintenance for existing route repairing and detecting the link breaks.

Ad-hoc On-Demand Distance Vector (AODV) is a best reactive routing protocol that support both multicast and unicast packet transmissions [3]. It requires less computational requirements and bandwidth as it generate route to a destination only when it is necessary. The two operating modes of AODV are route maintenance and route discovery. The source node sends the Route Request (RREQ) packet to all the neighbors only when there is no valid route to the destination node. The node sends a Route Reply (RERR) packet to the source if it detects a link failure

in route maintenance mode. The four types of vulnerabilities in the AODV protocol are (i) forge reply: the attacker sends a fake route reply in response to the received routing request, (ii) modify and forward: the attacker modifies one or more fields in the packet and forward to the neighbors, (iii) drop: the attacker drops all the received packets and active forge: the attacker misuse the RREP and RREQ messages. In addition, the attacker sends a fake routing packet without being triggered of any routing packet receipts. Moreover, it does not provide optimal path though the protocol contain more features [4]. This may further results in wastage of power, low and unstable packet delivery. Therefore, nature inspired algorithms such as Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), Genetic Algorithm (GA) and Whale Optimization algorithm (WOA) are applied for optimal path selection in Ad-hoc networks [5]. The main features of the bio-inspired optimization algorithms include high performance, speed as well as flexibility in search. The recent popular chimp optimization algorithm (ChOA) is inspired from the sexual motivation and group hunting intelligence of individual chimps [6]. In this paper, ChOA is combined with AODV to get the optimal path.

Each node in the MANET needs the help of other nodes to forward the packets to the destination. In this network topology, rapid changes may occur due to highly dynamic nodes of MANET. MANET has a routable networking environment on the top of the link layer of Ad-hoc network. It can be a part of large internet or it may operate in a standalone fashion. Every node in the MANET behaves like a router though it forwards the traffic to the neighbor nodes. Nevertheless, some nodes act selfish and do not cooperate with other nodes [7]. These selfish nodes are involved in drop and delay of packets rather than participating in the process of AODV routing [8]. The deviation from original forwarding and routing is called as node misbehavior. The other behavior of selfish nodes includes not forwarding or delaying different messages like RREQ data, and RREP. The performance of MANET in routing is seriously affected by this behavior of the selfish nodes. The deviation from original forwarding and routing is called as node misbehavior. As a result, there is a need of selfish node detection approach to promote the cooperation of nodes in MANET. A number of selfish node detection techniques are suggested by researchers in the state-of-the-art works [7-10]. The most renowned selfish node detection approach commonly used among the MANET community is called watchdog [11]. The collaboration of AODV with local watchdog can improve the route recovery process [12]. However, it is reported that the watchdogs generate false positives and false negatives due to the presence of malicious node. Besides, local watchdogs show poor performance in terms of speed and precision if the detection is dependent only on the local watchdogs. A Collaborative Contact-based Watchdog (CoCoWa) technique is found to reduce the effects of false positives and false negatives and improve the performance of local watchdogs [13]. This approach combines the information diffusion among nodes and local watchdog. In this paper, CoCoWa is collaborated with Chimp-AODV routing protocol to eliminate the drawbacks of existing approaches.

The main contributions of this paper are given as follows:

1. AODV is integrated with chimp optimization algorithm for the optimal path selection.
2. The CoCoWa is utilized to detect and isolate the selfish nodes with the chimp-AODV that can greatly increase the reliability of selfish node detection during route discovery process and quickly propagates the information about selfish nodes.
3. The performance of the proposed Chimp-CoCoWa-AODV approach is compared with existing approaches in terms of average routing load, Average ~~Packet Delivery Fraction~~ (PDF), Average ~~End-to-end Delay~~ (EED), Average Throughput, Total packet drop in the application layer, and maliciously dropped packet in the routing layer.

The rest of this paper is arranged as follows. Section 2 gives the review of related works. The background of algorithms and techniques used in the proposed methodology is detailed in Section 3. The Section 4 described the proposed methodology. The simulation results are discussed in Section 5. Section 6 concludes this paper.

2. Related Works

The collection of mobile nodes called MANET can be formed without the support of any fixed infrastructure. However, some nodes in MANET will not forward the packets from other nodes. This type of nodes are called as selfish nodes that will affect the performance of the whole network. A secure trust model is introduced with private keys and credentials to identify and isolate the malicious nodes [14]. Wang et al. [15] introduced a light weight trust based (Quality of Service) QoS model with aspects like neighbor node recommendation and direct trust computation. Various techniques and researches proposed to detect and isolate the selfish nodes are addressed in this paper. Wu et al. [16] proposed a threshold based method that reduced the false detection rate and improved the selfish node detection rate. A token-based umpiring technique is introduced in [17] to detect and isolate the selfish nodes. An intrusion detetcion system is proposed in [18] to prevent and recognize the selfish nodes.

The two major classification of selfish node mitigation techniques presented in several works are reputation-based and incentive-based techniques. [19] addressed the stimulating cooperation problem for civilian applications in self-organizing MANETs. The tamper resistant hardware module and a nuglet counter are maintained in this approach. The counter increses when a packet is forwarded by the node, and decreases when own packet is send by the node. An incentive-based method for mobile nodes is proposed in [20] to report and cooperate with honest actions. The receipt of the message is kept in the node whenever it receives a message. On the other hand, watchdog is used in many works to detect the selfish nodes [11-12]. Hernandez-Orallo et al. [21] proposed a collaborative watchdog approach for the evaluation of selfish node detection time. The information about the selfish node in one node is transmitted to warn all other nodes in the CoCoWa method proposed in [13]. This method minimizes the detection time and improves the precision. Hence, this technique is chosen as the selfish node detection approach in this paper.

The AODV routing protocol is used in many research works and found to outperform other routing protocols [3, 4, 18]. However, route failure may occur in conventional AODV due to routing overhead and data loss. The combination of DSDV and DSR routing protocol is the reason for the better performance characteristics of AODV [23]. RREP and RREQ are the two types of control packets used in AODV to link two nodes. The performance of reactive routing protocol has been analyzed under various types of attacks. The Packet Delivery Ratio (PDR) and throughput results show that the performance is decreased with the presence of attacks. The neighbor credit value based AODV (NCV-AODV) and its improved version are introduced in [8] to minimize the false detection rate. These methods show effective performance on the detection of selfish nodes in MANET. The application of evolutionary algorithms in optimal route selection will improve the performance of AODV protocol. Sarkar et al. [4] proposed an enhanced-Ant-AODV for MANET to enhance the QoS and improve the optimal route selection. This method calculates the pheromone value of a route based on the congestion, path reliability, residual energy of nodes and hop count. The highest pheromone value path is selected for data packet transmission. Similarly, PSO [24] and GA [25] are used to improve the performance of AODV through optimal selection of route in MANET. Due to the effective performance characteristics of AODV, it is chosen as the routing protocol in this paper. In addition, the chimp optimization algorithm is integrated with AODV for optimal path selection.

3. Preliminaries

~~This section details the algorithms and methods used in the proposed methodology.~~

3.1 CoCoWa Watchdog

Watchdog is one of the best monitoring mechanisms in wireless ad-hoc network to detect the misbehaving and selfish nodes in the networks. The transmitter and receiver are overheard by the watchdog in terms of calculating the ratio between transmitted packets and received packets in order to detect the anomalies. The performance of local watchdog can be improved by the dissemination of information about the selfish node when a contact occurs between pairs of nodes. The diffusion between a node pair is defined as a contact. The improved CoCoWa can quickly propagate the selfish node information and hence provides enhanced precision within less time. A node is noted as positive if watchdog detects that node as selfish node whereas it is noted as negative if watchdog detects

that node as non-selfish node. The node transmits the information about the selfish behavior when it contact with other nodes through the collaborative information transmission.

The Figure 1 shows the example for the operation of CoCoWa. The information diffusion and local watchdog are the two functions of CoCoWa. The transmission opportunity between a node pair is defined as contact. To know the working process of CoCoWa, the Figure 1 is assumed with one selfish node and initiated with no transmission of information about the selfish node. The detected selfish node is noted as a positive and non-selfish node noted as a negative. The information is transmitted to another node when contact occurs between the node and another node. Thus, the awareness about selfish node is transmitted to all nodes directly through watchdog or indirectly using collaborative information transmission. The fast diffusion of wrong information is produced by the uncontrolled negative and positive detection diffusion under this scheme. This leads to a poor performance of network. The last state 4 of Figure 1 shows that node b and c have a positive detection and node d has a negative detection. No other nodes are aware of the selfish behavior of node. The node a will get a positive detection when it contacts with node b and c. It will get negative detection when it contact with node d. The node a will detect the selfish node if it contact with the selfish nodes.

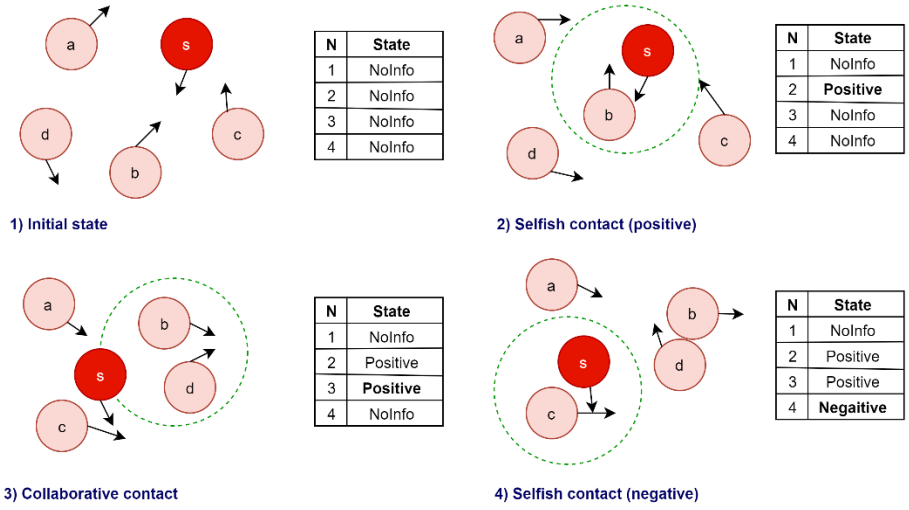

Figure 1. Example for Working of CoCoWa

3.2 Chimp Optimization Algorithm

The four types of chimps in a chimp colony are driver, chaser, barrier and attackers. The prey is followed by the driver. A dam is built by the barriers themselves in a tree across the prey progression. The chasers move rapidly to catch up the prey. At last, the attackers hunt the prey. Different abilities of the chimps are considered for a successful hunt. The chimps' hunting process is mainly categorized into two phases: exploration and exploitation. Chasing, driving and blocking the prey comes under exploration and attacking the prey is taken as exploitation. Thus, the prey is hunted during the exploitation and exploration phases. The driving and chasing of the prey can be written in mathematical form as given in Equations (1) and (2).

$$\mathrm{d} = \left| c.x_{prey}(t) - m.x_{chimp}(t) \right| \quad (1)$$

$$x_{chimp}(t+1) = x_{prey}(t) - \mathrm{a.d} \quad (2)$$

Where, the count of current iteration is indicated by t. c, m and a represents the vector coefficients. The position vector of chimp is represented by x_{chimp}. The prey position vector is represented by x_{prey}. The vectors c, a and m are calculated by using the Equations (3), (4) and (5).

$$c = 2.r_2 \quad (3)$$

$$a = 2.f.r_1 - f \quad (4)$$

$$m = \text{chaotic value} \quad (5)$$

Here, the iteration process f is non-linearly reduced from 2.5 to 0. The vectors r_1 and r_2 represents the random vectors in the range between 0 and 1. The chaotic vector m is measured with different chaotic map. The sexual motivation effect of chimps in the hunting process is represented by this vector. The participation of the chaser, barrier and driver chimps in the process of hunting is irregular and there is no data about the prey's best location. For mathematical modeling, it is assumed that the optimum location of the prey is informed to the chaser, driver and barrier by the first attacker. The best four solutions are saved as given in Equations (6-9) and positions of other chimps are updated based on the location of best chimps.

$$x_1 = x_a - a_1(d_a) \quad (6)$$

$$x_2 = x_b - a_2(d_b) \quad (7)$$

$$x_3 = x_c - a_3(d_c) \quad (8)$$

$$x_4 = x_d - a_4(d_d) \quad (9)$$

Here, the a_1, a_2, a_3, a_4 values are calculated using Equation (4). The d_a, d_b, d_c, d_d values can be calculated using Equations (10-13).

$$d_a = |c_1 x_a - m_1 x| \quad (10)$$

$$d_b = |c_2 x_b - m_2 x| \quad (11)$$

$$d_c = |c_3 x_c - m_3 x| \quad (12)$$

$$d_d = |c_4 x_d - m_4 x| \quad (13)$$

Here, the d_a, d_b, d_c, d_d values are calculated using Equations (6-9). The m_1, m_2, m_3, m_4 are chaotic values that can be calculated using Equation (5). The values of c_1, c_2, c_3, c_4 are calculated using Equation (3). The optimum location of new chimps can be obtained using Equation (14).

$$x(t+1) = \frac{x_1 + x_2 + x_3 + x_4}{4} \quad (14)$$

4. Proposed Methodology

The proposed methodology is discussed in this section. The architecture of the proposed model and mathematical modeling of system are discussed.

4.1 Architecture of Proposed Model

The detection of selfish node and new contact are the two functions of local watchdog. The watchdog generates no detection event if the information about a node is not enough or enough messages is not overheard by the watchdog due to less contact time. Neighborhood packet overhearing is used to detect the new contacts. A packet is assumed as new contact when a new contact is overheard by the watchdog. Hence, an event will be generated for the information module of network. An information diffusion module is used to isolate the selfish nodes. The transmission and reception of negative and positive detections are the two functions of information diffusion module. The main challenge in the proposed approach is diffusion of information. The positive detections are always transferred to a low overhead as the selfish node count is less compared to the total node count. This will lead the negative detections to cover the network quickly. Hence, it is important to transmit negative detections to

neutralize the effect of false events. If all the negative detections are transmitted, it will make fast transmission of false negatives or produce excessive messaging. The architecture of the proposed methodology is presented in Figure 2.

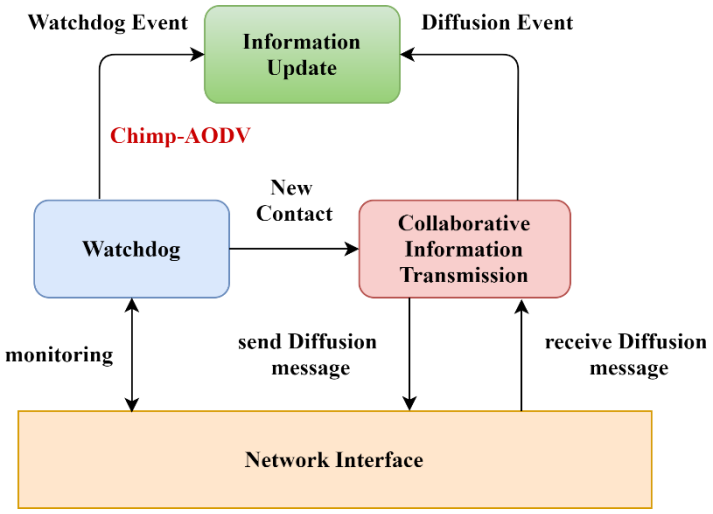

Figure 2. Architecture of the Proposed Methodology

A low value of negative diffusion factor γ can equalize the effects of false negatives and false positives. The negative transmission factor γ is defined as the ratio of actually transmitted negative detections. If any negative detections are not transmitted, the value of γ is 0 and value of γ will be 1 if all the negative detections are transmitted. When an event of new contact is received by the diffusion module, the watchdog transmits a message to the new neighbor node. The new neighbor node makes an event to the information module of network with the negative and positive detection list when it receives a message. The information updating is the role of the data update module. Negative state, Positive state and No information state are the internal information in a node about the other nodes. If there is no information about a node, then it is no information state. If a node is selfish then it is positive state and if the node is not selfish it is negative state. Local watchdog give direct information to the node and neighbor nodes indirectly give the information about the node. The node state is updated when there is negative or positive event from the diffusion modules and local watchdog. The value of reputation ρ is updated with these events as shown in Equation (15).

$$\rho = \rho + \Delta \tag{15}$$

Where,

$$\Delta = \begin{cases} +\delta & (\text{PositiveEvent, Local}) \\ +1 & (\text{PositiveEvent, Indirect}) \\ -\delta & (\text{NegativeEvent, Local}) \\ -1 & (\text{NegativeEvent, Local}) \end{cases} \qquad \delta \geq 1$$

The reputation value ρ increases with the positive event and decreases with the negative event. If $\rho \geq \theta$, then the state of node changes to positive, if $\rho \leq -\theta$ then the state of node changes to negative; otherwise the state remains no information state. Here θ is a threshold value. The parameters θ and δ combination permits a dynamic and flexible behavior. In order to change the state, several events are required when $\delta < \theta$ and $\theta > 1$. Only one event is required when $\theta = 1$. Otherwise, more trust should be given to the indirect information or local watchdog. The wrong local decisions can be compensated by this approach that has two advantages. The fast transmission of false negatives and false positives can be reduced with θ is the first advantage. Otherwise, a delay on the detection will happen. The decision taken about a selfish node with the help of most recent information is the second advantage.

4.2 System Model

The proposed MANET is modeled with AODV protocol, CoCoWa watchdog and N number of wireless mobile nodes. The nodes consist of selfish node, collaborative nodes and malicious node represented by S, C and M respectively.

4.2.1 Architecture of CoCoWa

Three parameters are used to model the local watchdog like false negative ratio p_{fn}, false positive ratio p_{fp} and detection probability p_d. The detection probability p_d represents the probability that the watchdog has enough data to create a Negative event or Positive event when a contact occurs between two nodes. This probability is based on the traffic load, mobility pattern of nodes and efficiency of watchdog. If a node does not act selfish then the watchdog generates false positive. If a node acts selfish then the watchdog generates false negative. p_{fp} is the ratio of generated false positives and p_{fn} is the ratio of generated false negatives. The probability of generating negative event and positive event with the watchdog can be modeled as: (i) Positive event: The selfish node detected by the watchdog with the probability $p_d(1-p_{fn})$ or $p_d \cdot p_{fp}$. (ii) Negative event: The non-selfish node detected by the watchdog with the probability $p_d(1-p_{fp})$ or $p_d \cdot p_{fn}$.

The collaboration probability is represented as p_c. The probability of indirectly generating negative event and positive event through collaborative information transmission can be modeled as: (i) Positive event: The probability of positive state when a node contact with other node is p_c. (ii) Negative event: The probability of negative state when a node contact with other node is $\gamma \cdot p_c$.

4.2.2 Malicious node

The CoCoWa system is attacked by the malicious nodes with the incorrect information generated about the nodes. The capability or behavior of these malicious nodes' can be addressed by the attacker model. The negative about a selfish node and positive about a non-selfish node is transmitted on malicious node attack with the aim of generating false negatives and false positives on all other nodes. The knowledge about the working of CoCoWa is required for this process. The effectiveness of this behavior is determined based on the precision and rate. It is assumed that malicious nodes have communications hardware similar to all other nodes. From receiver perspective, the modeling of malicious node behavior depends on the wrong information receiving probability about a given node when a malicious node contact occurs. This behavior can be noted as the probability of maliciousness p_m. The various aspects affecting this probability are: (a) all contacts not generating the reception is considered by the reception of information. This is same as the collaboration degree but increase in malicious nodes' communication range will increase the reception of information. (b) The malicious nodes do not aware about all nodes. ~~So that~~, a message from other nodes must have received by this node or other nodes must have contacted this node previously to transmit a negative or positive about a node.

4.2.3 Selfish Nodes

4D Continuous Time Markov chain (4D-CTMC) is used to model the proposed MANET. The collaborative nodes are divided into destination node D and intermediate node E. The states of 4D-CTMC are: $d_p(t)$, $d_n(t)$, $e_p(t)$, $e_n(t)$. The count of intermediate nodes with positive state is represented by $e_p(t)$, the number of intermediate node with negative state is represented by $d_n(t)$, the number of destination nodes with positive state is represented by $d_p(t)$ and the number of destination node with negative state is represented by $d_n(t)$. $d_p(t) + d_n(t) \leq D$ and $e_p(t) + e_n(t) \leq E$ are the conditions for the verification of state. The initial state of all the states is considered as zero. When $d_p(t) = D$, then it is considered as the final state.

The number of absorbing state is represented by $\upsilon = P^S$(E) = 0.5 * (E+2)* (E+1). Similarly, the count of transient state can be represented by τ which can be derived with Q as the generator matrix as given in equation (16).

$$Q = \begin{pmatrix} T & R \\ 0 & 0 \end{pmatrix} \quad (16)$$

Where $\tau \times \tau$ matrix is represented by T. $\tau \times \upsilon$ matrix is represented by R. $\upsilon \times \tau$ matrix is represented by left 0. $\upsilon \times \upsilon$ matrix is represented by right 0.

4.3 Chimp-AODV

At first, the populations of chimp (route paths) are initialized randomly in the search space (MANET). The objective function between destination node and the source node is used to calculate the fitness of each path. In the chimp-AODV, the route path is represented by chimps and the fitness of optimal path is represented by the prey. The chimp-AODV considers the bandwidth availability bw_a and path distance D along the path as the objective function to construct an optimal source towards destination route. The path distance D is the overall distance between destination node and source node with the hop counts. It can be calculated using Equation (17).

$$D = \sqrt{(x_2 - x_1)^2 - (y_2 - y_1)^2} \quad (17)$$

Here x_1 and y_1 are the coordinate of the source node and x_2 and y_2 are the coordinate of the destination node. The availability of bandwidth bw_a can be calculated based on the consumed bandwidth and total bandwidth as given in Equation (18).

$$bw_a = bw_{tt} - bw_u \quad (18)$$

Here, the total bandwidth is represented as bw_{tt} and overall consumed bandwidth is represented as bw_u. The fitness value can be calculated based on this objective function as per Equation (19).

$$ft = (minD)\&\&(bw_a > \delta) \quad (19)$$

Here, δ represents the threshold. Then the best four searching agents d_a, d_b, d_c, d_d are selected based on the fitness value using Equations (6-9). The position x_{chimp} (t+1) is updated based on the best searching agents. Then the parameters a, c, m, f are updated. The final updated position of chimp is expressed in Equation (14). This process is repeated until the maximum iteration condition is reached. The optimal route path is selected using this process that satisfies the fitness criteria. The algorithm 1 explains the Pseudo code for chimp optimization based optimal path selection.

Algorithm 1: Pseudo code for chimp optimization based optimal path selection

Input: Data packets $Dp_i = Dp_1, Dp_2, Dp_3, Dp_4, \ldots Dp_n$, Route paths $p_1, p_2, p_3, p_4, \ldots p_n$.
Output: optimal route path
Start
1. Initialize population of route paths $p_1, p_2, p_3, p_4, \ldots p_n$
2. **for** each route path p_i
3. Calculate bandwidth availability bw_a and distance D
4. Measure the fitness ft
5. Select four best searching agents d_a, d_b, d_c, d_d based on ft
6. **while** (t < maximum iteration)
7. **for** each searching agent
8. update the position x_{chimp} (t+1) with the chaotic sequence map
9. update the position of all searching agents x(t+1)

10. update the parameters a, c, m, f
11. Compute fitness
12. Replace the worst fit chimp with the best fit chimp
13. t=t+1
14. **end for**
15. **end while**
16. Return optimal
17. **end for**
18. Source node sends Dp_i along optimal route path

End

5. Experimental results and discussion

The model parameters used in the simulation is shown in Table 1. The software used for simulation is Network simulator NS2.35. At first, 50 nodes are generated randomly where some nodes are set as selfish node. The performance of proposed Chimp-CoCoWa-AODV is compared with existing algorithms such as traditional AODV with selfish node, traditional AODV without selfish node and CoCoWa-AODV.

Table 1. Parameters of Simulation

Routing protocol	AODV
Channel	Wireless channel
Phy	Wireless phy
Propagation	Two ray ground
Mac	802_11
Link Layer	LL
Antenna	Omni antenna
Queue	Drop Tail-PriQueue
Length of Queue	50
Traffic type	CBR(constant bit rate)
Total number of nodes	30, 40, 50
Number of selfish node	5

5.1 Performance metrics

Packet Drop: The number of malicious dropped packets due to the selfish attack is calculated for both the routing layer and the application layer.

Throughput: It is defined as the count of successfully arriving packets at the destination per unit time. The constantly reaching data to the destination is calculated using this metric. The unit of this measure is in megabits per second or kilobits per second.

Packet delivery Fraction (PDF): The ratio between the counts of packets successfully arrived to the destination and the entirely generated packets by source nodes.

End-to-End Delay: It is defined as the time period exists between the sender node packet production and successful delivery of destination node packet. The unit of this measure is in millisecond.

Routing load: It is defined as the number of every node generated routing messages and the successfully arrived packets at the destination node.

5.2 Simulation Results

The dropped malicious packets are counted at the routing layer. The performance comparison in terms of maliciously dropped packets at routing layer is shown in Figure 3. The CoCoWa-AODV and Chimp-CoCoWa-AODV have less maliciously dropped packets. The maliciously dropped packets at routing layer of the proposed Chimp-CoCoWa-AODV are equal to traditional AODV without selfish node. The dropped packets are counted at the application layer. The performance comparison in terms of total dropped packets at application layer is shown in Figure 4. The CoCoWa-AODV and Chimp-CoCoWa-AODV have less dropped packets at application layer. The total dropped packets at application layer of the proposed method are equal to that of traditional AODV without selfish node.

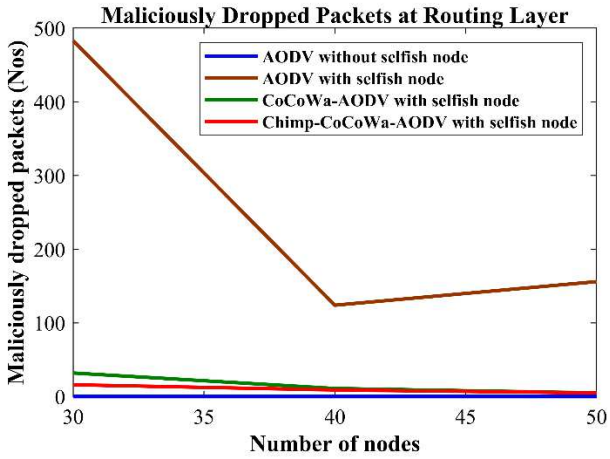

Figure 3. Comparison with Maliciously dropped packets at routing layer

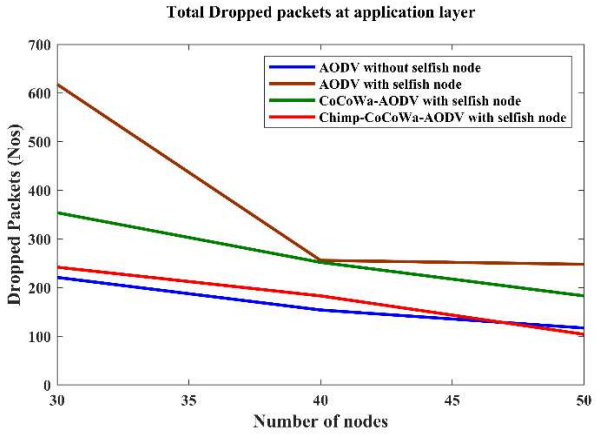

Figure 4. Comparison with Total dropped packets at application layer

The Average throughput is shown in Figure 5. The CoCoWa-AODV and Chimp-CoCoWa-AODV have higher average throughput. The traditional AODV with selfish node has less average throughput. The throughput of Chimp-CoCoWa-AODV is 52 kbps at 30 nodes and increased to 60 kbps at 50 nodes. The throughput of traditional AODV

is 61kbps at 50 nodes that is almost equal to the proposed method. The throughput of traditional AODV and CoCoWa-AODV at 50 nodes is 54 kbps and 58 kbps respectively that is less than the proposed approach. The average end to end delay (EED) of the proposed methodology is shown in Figure 6. The CoCoWa-AODV and Chimp-CoCoWa-AODV have low average EED. The traditional AODV with selfish node shows higher average EED of 54 ms. The average EED of proposed Chimp-CoCoWa-AODV is 52 ms at 30 nodes. It is increased with the increase in the number of nodes. The average EED of the proposed method is equal to that of traditional AODV without selfish node. The EED is higher for traditional AODV with selfish node than the proposed approach.

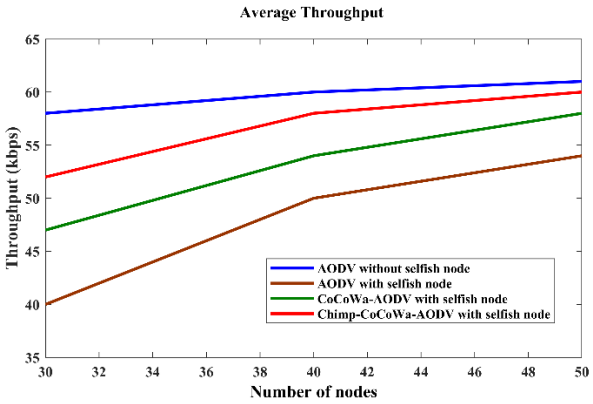

Figure 5. Comparison with Average throughput

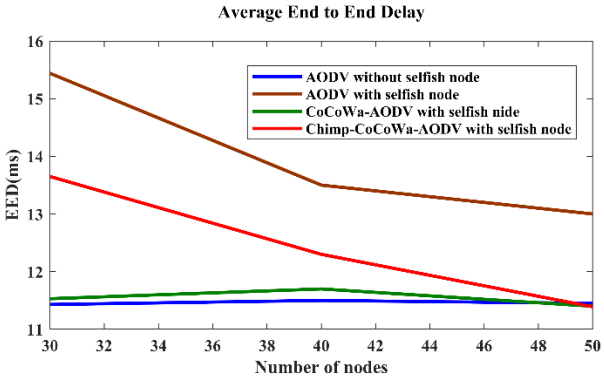

Figure 6. Comparison with EED

The average PDF of the proposed methodology is shown in Figure 7. The CoCoWa-AODV and Chimp-CoCoWa-AODV have higher average PDF. The average PDF at 30 nodes is 76% and increased to 82% at 50 nodes. In case of traditional AODV with selfish node, average PDF is 73% at 50 nodes that is lower than other approaches. The performance of the proposed method is similar to the traditional AODV without selfish node at 50 nodes. The average routing load of proposed methodology is shown in Figure 8. The performance of CoCoWa-AODV and Chimp-CoCoWa-AODV with selfish node is not affected with increase in the average routing load. The traditional AODV shows poor performance with the increase in the average routing load.

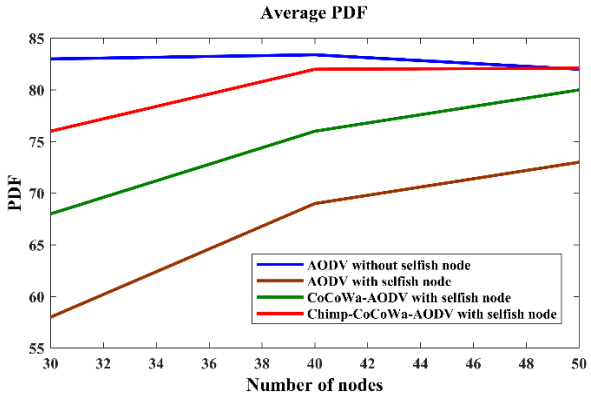

Figure 7. Comparison with Average PDF

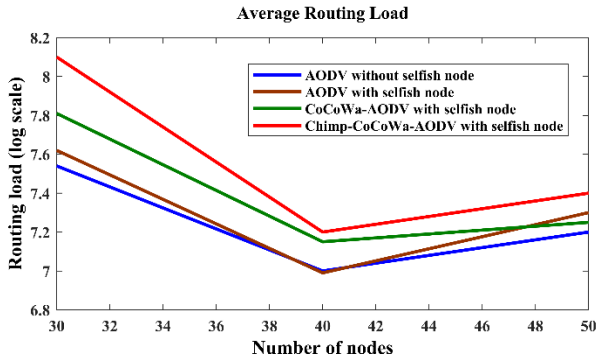

Figure 8. Comparison with Average routing load

The proposed Chimp-CoCoWa-AODV shows less maliciously dropped packets at routing layer, total dropped packets at the application layer and average EED and higher average PDF, throughput and routing load. From the above experimental results, it can be concluded that the proposed selfish node detection model shows better performance than the existing approaches.

6. Conclusion

One of the challenging security issues in MANET is selfish behavior of nodes. In this paper, a novel Chimp-CoCoWa-AODV approach is proposed to detect and isolate the selfish nodes in the MANET. The selfish node is detected by the local watchdog in the CoCoWa. The information about this selfish node is transmitted to all nodes directly or indirectly. Then the selfish node is isolated from the packet transmission. AODV is integrated with Chimp optimization algorithm for the purpose of optimal path selection. The proposed approach shows better performance than existing algorithms even in the presence of malicious node. The performance of the proposed approach is analyzed in terms of average routing load, Average PDF, Average EED, Average Throughput, Total packet drop in the application layer, maliciously dropped packet in the routing layer. The future work of this paper aims at extending the application of proposed approach in various attacks in MANET.

Conflict of interest:

The authors declare that they have no conflict of interest.

References

1. Gaurav, A., & Singh, A. K. (2018). Light weight approach for secure backbone construction for MANETs. Journal of King Saud University - Computer and Information Sciences. doi:10.1016/j.jksuci.2018.05.013.
2. Gandhi, S., Chaubey, N., Tada, N., & Trivedi, S. (2012). Scenario-based performance comparison of reactive, proactive & Hybrid protocols in MANET. 2012 International Conference on Computer Communication and Informatics. doi:10.1109/iccci.2012.6158842.
3. Moudni, H., Er-rouidi, M., Mouncif, H., & El Hadadi, B. (2016). Performance analysis of AODV routing protocol in MANET under the influence of routing attacks. 2016 International Conference on Electrical and Information Technologies (ICEIT). doi:10.1109/eitech.2016.7519658.
4. Sarkar, D., Choudhury, S., & Majumder, A. (2018). Enhanced-Ant-AODV for Optimal Route Selection in Mobile Ad-Hoc Network. Journal of King Saud University - Computer and Information Sciences. doi:10.1016/j.jksuci.2018.08.013.
5. Farooq, H., & Tang Jung, L. (2013). Energy, Traffic Load, and Link Quality Aware Ad Hoc Routing Protocol for Wireless Sensor Network Based Smart Metering Infrastructure. International Journal of Distributed Sensor Networks, 9(8), 597582. doi:10.1155/2013/597582.
6. Khishe, M., & Mosavi, M. R. (2020). Chimp Optimization Algorithm. Expert Systems with Applications, 113338. doi:10.1016/j.eswa.2020.113338.
7. Nobahary, S., Garakani, H. G., Khademzadeh, A., & Rahmani, A. M. (2019). Selfish node detection based on hierarchical game theory in IoT. EURASIP Journal on Wireless Communications and Networking, 2019(1). doi:10.1186/s13638-019-1564-4
8. Rama Abirami, K., & Sumithra, M. G. (2018). Evaluation of neighbor credit value based AODV routing algorithms for selfish node behavior detection. Cluster Computing. doi:10.1007/s10586-018-1851-6.
9. Hollick, M., Schmitt, J., Seipl, C., & Steinmetz, R. (2004). On the effect of node misbehavior in ad hoc networks. 2004 IEEE International Conference on Communications (IEEE Cat. No.04CH37577). doi:10.1109/icc.2004.1313244.
10. Buchegger, S., & Le Boudec, J.-Y. (2005). Self-policing mobile ad hoc networks by reputation systems. IEEE Communications Magazine, 43(7), 101–107. doi:10.1109/mcom.2005.1470831.
11. Meeran, A., Praveen A, N., & Ratheesh T, K. (2017). Enhanced system for selfish node revival based on watchdog mechanism. 2017 International Conference on Trends in Electronics and Informatics (ICEI). doi:10.1109/icoei.2017.8300943.
12. Varshney, T., Sharma, T., & Sharma, P. (2014). Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network. 2014 Fourth International Conference on Communication Systems and Network Technologies. doi:10.1109/csnt.2014.50.
13. Hernandez-Orallo, E., Olmos, M. D. S., Cano, J.-C., Calafate, C. T., & Manzoni, P. (2015). CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes. IEEE Transactions on Mobile Computing, 14(6), 1162–1175. doi:10.1109/tmc.2014.2343627.
14. Ren, Y. & Boukerche, A. (2008) Modeling and Managing the Trust for Wireless and Mobile Ad Hoc Networks. IEEE International Conference on Communications, 2008. ICC'08, Beijing, 19-23 May 2008, 2129-2133. http://dx.doi.org/10.1109/icc.2008.408.
15. Wang, W., Huang, K., & Zou, Y. (2016). Cooperation incentive mechanism for selfish users based on trust degree. 2016 Sixth International Conference on Information Science and Technology (ICIST), 2(1), 12-25.
16. Wu, L.-W., & Yu, R.-F. (2010). A threshold-based method for selfish nodes detection in MANET. 2010 International Computer Symposium (ICS2010). doi:10.1109/compsym.2010.5685389.
17. Josh Kumar, J. M. S. P., Kathirvel, A., Kirubakaran, N., Sivaraman, P., & Subramaniam, M. (2015). A unified approach for detecting and eliminating selfish nodes in MANETs using TBUT. EURASIP Journal on Wireless Communications and Networking, 2015(1). doi:10.1186/s13638-015-0370-x.
18. Pakzad, F., & Rafsanjani, M. K. (2010). Intrusion Detection Techniques for Detecting Misbehaving Nodes. Computer and Information Science, 4(1). doi:10.5539/cis.v4n1p151.
19. Buttyán, L., & Hubaux, J.-P. (2003). Mobile Networks and Applications, 8(5), 579–592. doi:10.1023/a:1025146013151.
20. Chong C.N., Peng Z., Hartel P.H. (2003) Secure Audit Logging with Tamper-Resistant Hardware. In: Gritzalis D., De Capitani di Vimercati S., Samarati P., Katsikas S. (eds) Security and Privacy in the Age of Uncertainty.

SEC 2003. IFIP — The International Federation for Information Processing, vol 122. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-35691-4_7.
21. Hernández-Orallo, E., Olmos, M. D., Cano, J., Calafate, C. T., & Manzoni, P. (2013). A Fast Model for Evaluating the Detection of Selfish Nodes Using a Collaborative Approach in MANETs. Wireless Personal Communications, 74(3), 1099-1116.
22. Kumar, A., Varadarajan, V., Kumar, A., Dadheech, P., Choudhary, S. S., Kumar, V. D. A., … Veluvolu, K. C. (2020). Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. Microprocessors and Microsystems, 103352. doi:10.1016/j.micpro.2020.103352.
23. Yasin, A., & Abu Zant, M. (2018). Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique. Wireless Communications and Mobile Computing, 2018, 1–10. doi:10.1155/2018/9812135.
24. Pati, B., Panigrahi, C. R., Buyya, R., & Li, K.-C. (Eds.). (2020). Advanced Computing and Intelligent Engineering. Advances in Intelligent Systems and Computing. doi:10.1007/978-981-15-1483-8.
25. Yang, H., & Liu, Z. (2017). A Genetic-Algorithm-Based Optimized AODV Routing Protocol. Geo-Spatial Knowledge and Intelligence, 109–117. doi:10.1007/978-981-10-3966-9_12.