Circuits and Systems, 2016, 7, 2070-2079
Published Online June 2016 in SciRes. http://www.scirp.org/journal/cs
http://dx.doi.org/10.4236/cs.2016.78180

Malicious Nodes Detection in MANET Using Back-Off Clustering Approach

A. R. Rajeswari[1*], K. Kulothungan[1], S. Ganapathy[2], A. Kannan[1]

[1]Department of Information Science and Technology, College of Engineering Guindy, Anna University, Chennai, India
[2]Department of Computer Science and Engineering, College of Engineering Guindy, Anna University, Chennai, India
Email: *arrajeswari.2015@gmail.com

Received 24 March 2016; accepted 20 April 2016; published 30 June 2016

Abstract

Mobile Ad hoc Networks (MANET) are infrastructure less networks which provide multi-hop wireless links between nodes. The main applications of MANET in real time environment are military and emergency areas where the fixed infrastructure is not required. It is a temporary communication infrastructure network for quick communication with minimal configuration settings among the group of nodes. The security is one of the primary concerns in MANET. The malicious nodes in MANET environment degrade the performance of the network. In this paper, the nodes in MANET are grouped using back-off duration technique and further the malicious nodes are detected using this algorithm. The proposed clustering based malicious nodes detection in MANET achieves higher performance in terms of packet delivery ratio, latency and energy consumption. The proposed method achieves 89.35% of packet delivery ratio, 36.2 ms latency and 26.91 mJ of energy consumption.

Keywords

MANET, Cluster, Malicious Nodes, Routing, Performance

1. Introduction

The idea of implementation of mobile wireless devices working collectively was proposed in the 1990s, when significant amount of research activities were carried out on mobile ad hoc networks (MANETs). The Mobile Ad hoc Networks Working Group [1] was created in 1997, with the aim of standardizing routing protocols for

*Corresponding author.

How to cite this paper: Rajeswari, A.R., Kulothungan, K., Ganapathy, S. and Kannan, A. (2016) Malicious Nodes Detection in MANET Using Back-Off Clustering Approach. *Circuits and Systems*, **7**, 2070-2079. http://dx.doi.org/10.4236/cs.2016.78180

MANETs. Two standard specifications for track routing protocol were developed by this group, namely the reactive and proactive MANET protocols. Each node in a MANET is a computer acting as both a host and a router, having the job of forwarding the packets between two nodes which are not in direct communication with one another. Each MANET node requires a much smaller frequency spectrum that a node requires in an affixed infrastructure network [1].

A MANET is an autonomous collection of mobile user nodes communicating over wireless links, with a relative bandwidth constraint. Since the nodes are mobile, the network topology is more probable to unpredictable changes over time. A MANET is usually decentralized, *i.e.* all network activities including topology determination and message delivery, should be executed by the individual nodes themselves. Therefore, the routing functionality gets incorporated into the mobile nodes. **Figure 1** illustrates the infrastructure of nodes in MANET [2].

Mobile Ad hoc Network got outstanding success as well as tremendous attention due to certain characteristics such as self-maintenance and self-configuration. At early stages, researchers focused mostly on its user-friendly and mutual environment, however, many different problems came into being; security is one of the major issues since providing secure communication between different nodes in a mobile ad hoc network environment has become difficult. Finally, MANETs can be considered as an infrastructure less, multi-hop network with most importantly its self-organizing property [3] [4]. Due to its wireless and distributed environment, the system security becomes a challenging task for the designers. In the last few years, security problems in MANETs have attracted much attention, thereby making the researchers to focus on specific security areas, like intrusion detection and response, establishment of trust infrastructure and securing routing protocols.

Intrusion detection (ID) in MANETs is more complex and challenging than in fixed networks, because of the difficulty in collecting the audit data from the network, and applying ID techniques in detecting intrusions at a low rate of false positives and an effective response to intrusion. Certain features of MANETs create implementation and operational complexities, and such additional challenges for ID schemes in MANETs are as follows:

- Lack of concentration points during audit data collection and monitoring.
- The routing protocols in MANET necessitate cooperation of nodes to act as routers, thereby creating opportunity for attacks.
- Dynamic and unpredictable network topology due to mobility of nodes, making the process of intrusion detection complicated.
- Complex ID schemes due to the limited computational ability of most of the nodes.

Section 2 states the related works and discusses the conventional algorithms in detail. Section 3 proposes the clustering back-off duration algorithm for the detection of malicious nodes in the network, during cluster formation and Section 4 shows the results and their discussion in detail. Finally, Section 5 depicts conclusion.

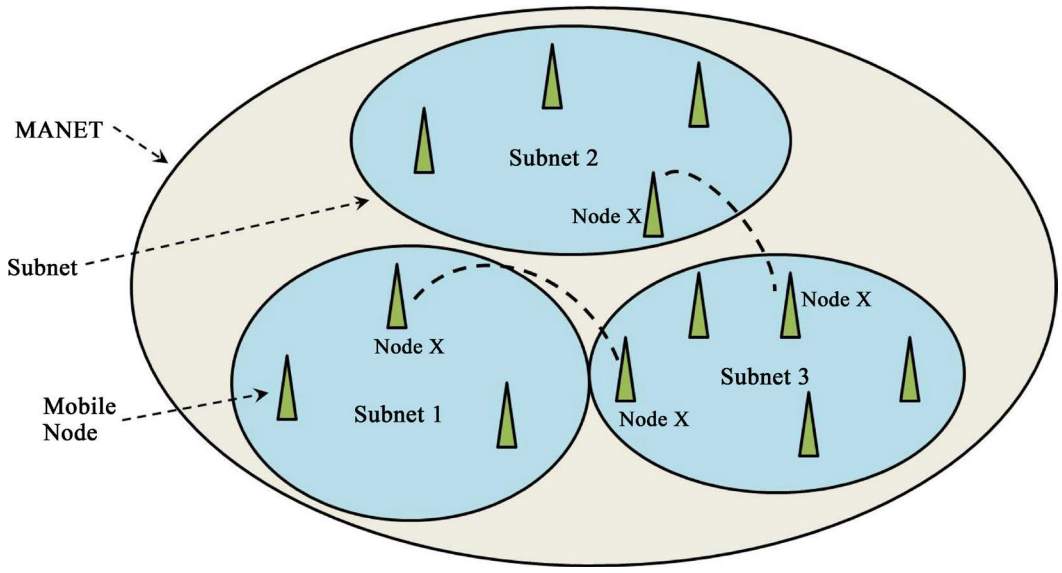


Figure 1. Interfacing nodes in MANET.

2. Literature Survey

Sandip Chakraborty *et al*. [4] developed an algorithm for Alleviating Hidden and Exposed Nodes in High-Throughput Wireless Mesh Networks. The authors achieved 28.50 mJ of energy consumption and 88.02% average packet delivery ratio to detect the hidden and exposed nodes in MANET environment. Jian-Ming Chang *et al*. [2] proposed a cooperative bait detection algorithm to detect the malicious nodes in MANET by preventing collaborative attacks. The authors attempted to resolve this issue by designing a dynamic source routing (DSR)-based routing mechanism, which is referred to as the cooperative bait detection scheme (CBDS), that integrates the advantages of both proactive and reactive defense architectures. Adnan *et al*. [3] developed an algorithm for trust based malicious node detection in MANET environment. The authors used Trust and reputation based approaches for global recognition in providing additional means of security for decision making in sensor and ad-hoc networks. The authors discussed in detail different type of node misbehaviors in MANET and WSN, bootstrapping mechanisms, trust evidence, trust computation and interactive decision making methods. Tselikis *et al*. [5] developed degree-based clustering algorithm for the nodes in MANET. This method was attack-resistant without imposing significant overhead to the clustering performance. The authors extended this clustering method with a cooperative consistent algorithm which integrated security into the clustering decision achieving attacker identification and classification. Yanqing Zeng *et al*. [1] proposed Cluster Header Election Scheme for intrusion detection in MANET. The authors provided a solution based on auction mechanism during CH election process. The methodology proposed in this work determined that all nodes in the network behave honestly to elect the least analysis cost nodes to handle the detection duty of the network.

Karunakaran and Thangaraj [6] have proposed service discovery architecture based on clustering. The authors selected the CH by allotting a combined weight value based on the factors Power Level, Connectivity and Stability, intended for wireless mobile ad hoc networks. The proposed method permitted switch over of the service discovery messages only among the cluster members. The proposed method in this paper considered the capabilities of the nodes for the distribution of workload. Su *et al*. [7] proposed an efficient cluster-based routing protocol which supports unidirectional network environments. In this approach, the node determined its own status by the exchange of cluster information with its neighbor nodes after updating the cluster information. The cluster head managed the degree of the node and the number of nodes in the proposed clustering algorithm. The authors reduced the cluster head formed by the pendent nodes and hence the efficiency of the cluster structure was improved. The proposed weight function required only status and degree of nodes. Bo Han and Weijia Jia [8] proposed an efficient clustering protocol for constructing virtual backbone of the nodes in MANET. The time complexity and message complexity of these algorithms were analyzed for suitability of the proposed scheme for the nodes in MANET. The authors observed that Area algorithm always outperforms the regardless of the size and density of the networks in terms of the size of network.

The conventional methodologies [1] [3] [5]-[8] discussed various techniques used for clustering the nodes in the network to detect the hidden nodes and analyzed the impact of hidden nodes on the performance of the network. Even though the methods are efficient, the performance of the network was degraded due to more number of hidden nodes in the network.

This paper proposes a new methodology to detect the hidden nodes in the network during clustering process. The main contribution of this paper is to detect the malicious or hidden nodes using backoff clustering approach and to increase the network performance with respect to the increase of packet delivery ratio and to decrease the latency and energy consumption.

3. Materials and Methods

3.1. Materials

The common simulation environment parameters used in this work are illustrated in **Table 1**. The initial values of these parameters are set during simulation process in Network simulator 2. The simulation environment uses two way ground and wireless channel between source and destination nodes. The omni directional antenna is used in order to transmit and receive data 360 degree around each node in the network environment. Total number of nodes in simulation environment is 100 and uses dynamic source routing protocol to route the packets from one node to another node in the network and the data rate is about 1 Mbps. The omni directional antenna is used in each node to send and receive the packets and the initial energy of each node in the network is assumed to have 1000 Joules.

Table 1. Simulation environment parameters.

Parameters	Type
Channel type	Wireless Channel
Radio-propagation model	Two Ray Ground
Antenna type	Omni directional Antenna
Max packet	300
Network interface type	Physical layer
Standard	IEEE 802.11b
Number of mobile nodes	100
Routing protocol	Dynamic Source Routing (DSR)
Initial energy in Joules	1000
Data Rate	1 Mbps
Area	1000 × 1000

3.2. Methods

All nodes in MANET are randomly deployed to monitor and to collect the data from the surrounding environment continuously. These collected data are then sent to the centralized node which is located in the remote area to monitor and control the nodes behaviour in MANET. Each node in MANET can be operated in any one of the following modes as slave and master. The slave mode collects the data and sends them to the master node [9]. The master node collects all the data's from various slave nodes and sends this details to other master node directly or through the intermediate other master nodes in MANET environment. The master node is otherwise called as Cluster Head (CH) and CH has high residual energy. In addition to this, the following assumptions are considered during node setup:

- All nodes have the same energy level initially.
- The distance between any two nodes is determined based on the received signal strength.
- All nodes including CH are freely moving from one location to another location.
- The link between any two nodes is assumed as symmetric such that the energy consumption from node 1 to node 2 is same as that of transmission from node 2 to node 1.

Consider a MANET having N number of nodes and each node being assigned with an Individual Identity (II). The identity is only used to identify the node and not based on the location and energy level. A cluster is a set of nodes and cluster head is located at the centre of the cluster. The cluster is organized as a concentric circular layers and each circular layer has a layer number starts from zero. The LN of the CH is zero. The layer close to the CH has the value of LN one and subsequently LN is assigned to each layer. A node in the outer layer has high LN.

Determination of Back-Off Duration

It is used to avoid the formation of too many clusters and cluster heads at an initial phase. The back-off duration (Ψ_i) of a node i is determined using Equation (1) as,

$$\Psi_i = \Psi_{\max}\left(1-\varepsilon*\left(\frac{E_{r-i}}{E_{\max}}\right)\right) \quad (1)$$

where, $\Psi_{\max}$ is the maximum back-off time; ε is an adjustment parameter ranging between 0 and 1; E_{r-i} is the residual energy and $E_{\max}$ is the maximum energy stored in a node *i*.

The node waits for a packet arrival till its back-off duration period vanishes to zero. If the packet is not received within this back-off duration, that node is considered as CH. The back-off duration will be low value when the node has larger residual energy. Therefore, a node with higher residual energy will have a higher probability of being a cluster head. It indicates that the CH should have maximum energy to transmit and receive the packets [10]. Now, CH will broadcast a message to its neighbour nodes of radius "*R*". This message consists of the II of the CH and number of layers (1) in the cluster.

The cluster radius (R) can be determined as,

$$R = \sqrt{w^2 + h^2} \tag{2}$$

where, w and h is the width and height of the sensing area, respectively.

The nodes which receive this message will operate as slave nodes, and not as a CH node.

The node which receives the packets will act as a cluster member for that particular CH. All the nodes are arranged in the concentric layers of the cluster, as earlier mentioned.

The following Equations are used to find the bounding (b_i) of i-th concentric layer of the cluster, where, $i = 1, 2, 3, \cdots, l$;

$$b_i = \begin{cases} 0, & \text{if } l \le 0 \\ b_{i-1}, & \text{else} \end{cases} \tag{3}$$

where, $b_{i\text{-}1}$ is the average distance between CH and cluster nodes at a i-1th layer and it is computed using the following Equation as,

$$\overline{b}_{k-1} = \sqrt{\frac{b_{k-1}^2 + b_{k-2}^2}{2}} \tag{4}$$

The Euclidean distance (ED) between each node within a cluster and cluster head is determined using the following Equation,

$$\mathrm{ED} = \sqrt{\left(x_2 - x_1\right)^2 - \left(y_2 - y_1\right)^2} \tag{5}$$

where, (x_1, x_2) represents the coordinates of the cluster head location and (y_1, y_2) represents the coordinates of the node within the cluster.

The cluster with its concentric layers is shown in **Figure 2**. The bound of layer 1 is represented by b_1, the bound of layer 2 is represented by b2 and so on. The bounding layer 1 is the bound value between CH and first concentric layer and bounding layer 2 is the bound value between CH and second concentric layer.

The CH broadcast a packet with time-to-live (TTL) to the nodes in the neighbour layer of its cluster. TTL specifies the number of hops that a message can travel to before it should be discarded. When a node in layer 1 receives a broadcast message containing a TTL value greater than zero; it rebroadcasts a packet with TTL value which is decremented by one [11]. The same process is repeated until the TTL value becomes zero. The nodes which have the TTL value greater than zero will become a member of that cluster. The clustering approach is illustrated in **Figure 3**.

Each CH in the cluster creates and maintains the cluster table. The cluster table consists of node number and the Euclidean distance between the cluster head (determined by Equation (5)) and 8-bit randomly generated

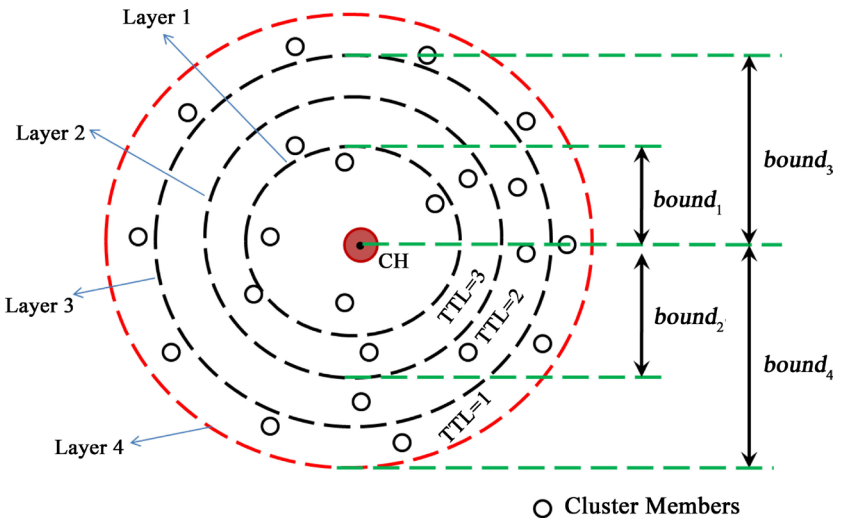


Figure 2. Layers in cluster.

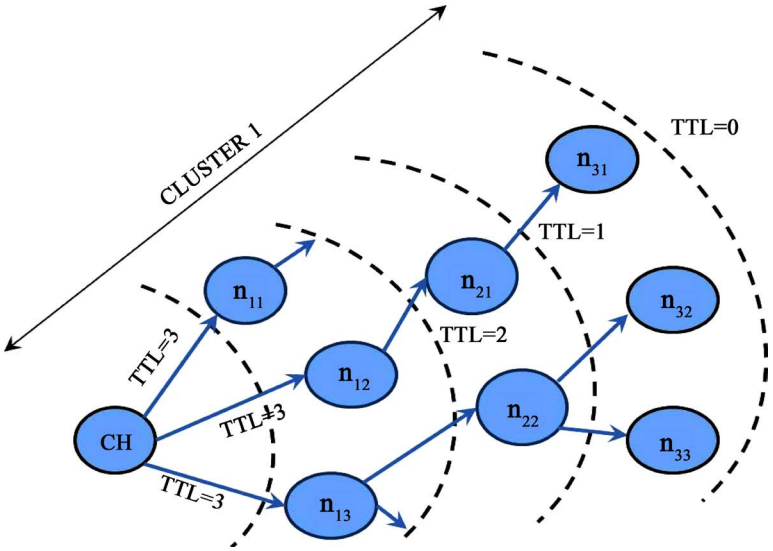
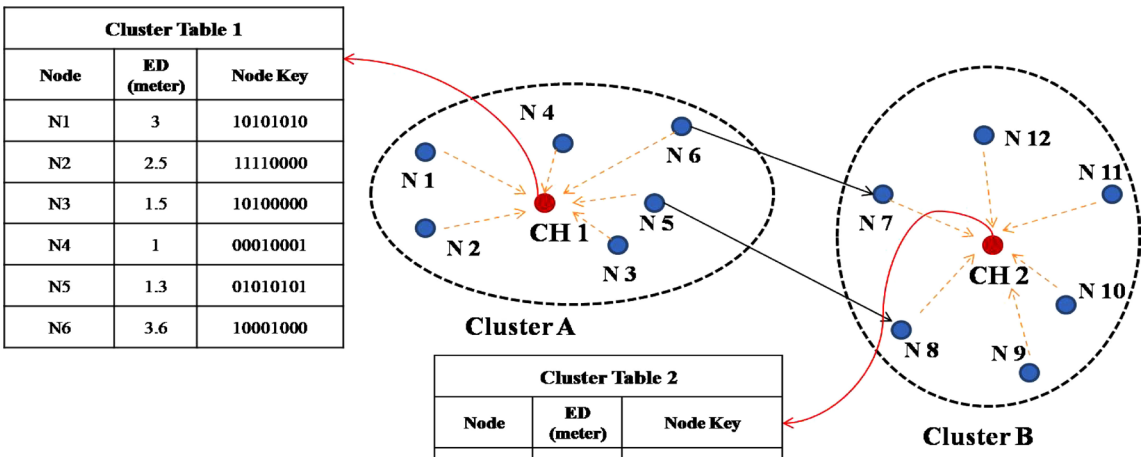


Figure 3. Clustering approach in MANET.



Cluster Table 1

Node	ED (meter)	Node Key
N1	3	10101010
N2	2.5	11110000
N3	1.5	10100000
N4	1	00010001
N5	1.3	01010101
N6	3.6	10001000

Cluster Table 2

Node	ED (meter)	Node Key
N7	3	10101011
N8	3.1	11110011
N9	1.8	10100011
N10	1	00010011
N11	2.8	01010000
N12	2.6	11111111

Figure 4. Proposed malicious node detection in MANET.

node key [10]. The CH also maintains the number of nodes in the cluster table. The nodes in the network are dynamic, *i.e.* each node in the network is moving to the other cluster of the network. Hence, the frequent updation in the cluster head is required to maintain the number of nodes within the cluster. **Figure 4** shows the proposed clustering methodology based malicious node detection system. The nodes in the network are grouped into 2 clusters namely A and B based on the energy level of the nodes. The CH is a node which has the highest energy level and also has the shortest distance to all of its surrounding nodes. Each CH maintains a cluster table to preserve the nodes flow within the network. For example, cluster A maintains Cluster **Table 1** and stores six neighbouring nodes details such as node name and its Euclidean distance with cluster head. This clustering table is dynamic due to the inflow and outflow of the nodes in the cluster. The cluster head 1 (CH1) additionally stores the number of nodes in the cluster table. The cluster head 1 in the cluster A initially sends the randomly

generated 8-bit cluster keys to all of its nodes inside the cluster A. Each node in the cluster A receives the cluster key and sends the message or information to the cluster head with this cluster key only. If there is presence of the malicious node in this cluster A, this hidden node will also receive the cluster key from the cluster head and starts transmitting the data to the cluster head. In this way, the cluster head determines the number of nodes within the cluster and matches this with the data available in the cluster table. If both are not same, then it will decide that the malicious node is present within this particular cluster. In this way, the malicious nodes are detected in MANET.

4. Results and Discussions

The proposed clustering based malicious nodes detection in MANET achieves higher performance in terms of the following performance evaluation parameters [2].

4.1. Packet Delivery Ratio (PDR)

It determines the percentage of packets correctly received at the destination node and it is defined as the ratio between the number of packets correctly received at the destination node and the total number of packets transmitted from the source node.

$$\text{FDR} = \frac{\text{number of packets correctly received}}{\text{total number of packets transmitted from the source node}} \times 100\% \quad (6)$$

The value of PDR lies between 0 and 100. Higher PDR indicates the performance of the MANET is high. In our experiment, number of malicious nodes are randomly generated and distributed among the nodes in MANET. The performance of the proposed system is analyzed in terms of PDR against number of malicious nodes and PDR values for different number of malicious nodes is depicted in **Figure 5**. The proposed method achieves 89.35% of PDR while the conventional methods Fatima Zohra *et al*. [10], Murad Abusubaih [11], Jian-Ming Chang *et al*. [2] and Sandip Chakraborty *et al*. [4] achieved PDR are 84.36%, 86.50%, 87.92% and 88.02%, respectively.

In some methodologies [2] [4] [11], PDR values are slightly higher than the proposed method at the case of 60% malicious nodes. However, the proposed method in this paper achieves higher average PDR than the conventional methods due to its robust and stability of the algorithm. The number of nodes between source and destination will increase the packet delivery ratio. Higher packet delivery ratio will decrease the error rate of the packets sent by source node in MANET environment. The packet delivery ratio will increase the system performance to the higher level.

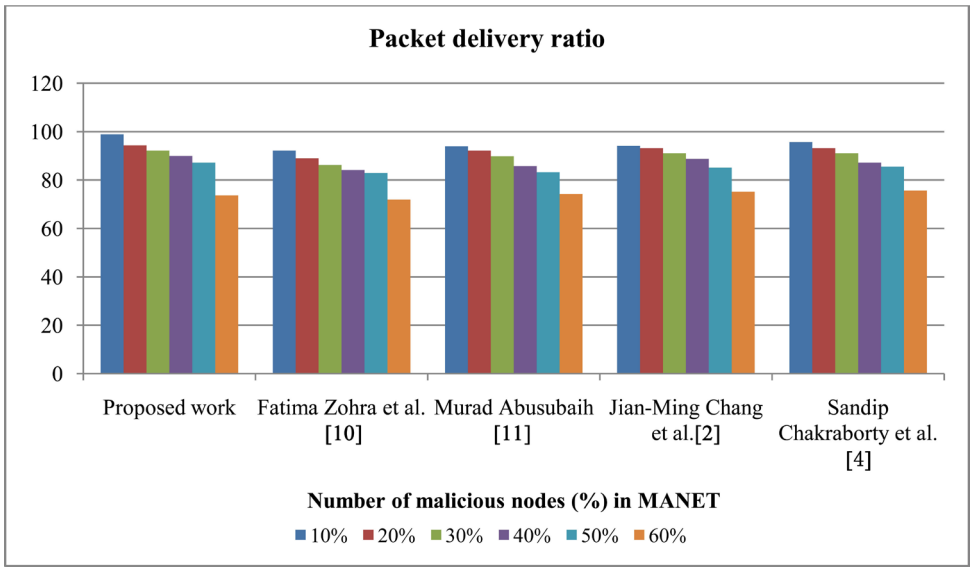


Figure 5. Performance analysis of proposed methodology in terms of packet delivery ratio.

4.2. Latency

It is defined as the total time taken to deliver the packet from source node to destination node in MANET environment. The latency is affected by malicious nodes due to the wastage of transmission through these nodes. It is estimated in milliseconds (ms). Lower latency indicates the performance of the MANET is high. The performance of the proposed system is analyzed in terms of latency against number of malicious nodes and latency values for different number of malicious nodes is depicted in **Figure 6**. The proposed method achieves 36.2 ms latency while the conventional methods Fatima Zohra *et al*. [10], Murad Abusubaih [11], Jian-Ming Chang *et al*. [2] and Sandip Chakraborty *et al*. [4] achieved latency are 37.47 ms, 36.98 ms, 37.49 ms and 37.40 ms, respectively.

4.3. Energy Consumption Model

The transmission of data between any two sensors nodes present within the cluster, consumes certain power [2]. The energy consumption for transmitting a data can be expressed as,

$$E_t = \left(E_{td} \times k\right) + \left(\gamma_{amp} \times d^{\alpha}\right) \tag{7}$$

where, k refers to the number of bits transmitted; α is a variable factor ranging from 1 to 5 between two consecutive sensor nodes based on their channel condition; γ_{amp} is the amplification coefficient relying on minimum bit error rate (BER); d is the distance between any two successive sensor nodes; E_{td} refers to the energy dissipation, expressed as

$$E_{td} = \frac{V_{cc} I_c}{b_{\text{rate}}} \tag{8}$$

where, V_{cc} and I_c denotes the voltage and current consumption of the sensor node, respectively; and b_{rate} is the baud rate or data transmission rate.

The consumed energy is directly proportional to the number of bits transmitted and distance between two consecutive sensor nodes.

Lower energy consumption indicates the performance of the MANET is high. It is measured in milli joules. The performance of the proposed system is analyzed in terms of energy consumption against number of malicious nodes and energy consumption values for different number of malicious nodes are illustrated in **Figure 7**. The proposed method achieves 26.91 mJ of energy consumption while the conventional methods Fatima Zohra *et al*. [10], Murad Abusubaih [11], Jian-Ming Chang *et al*. [2] and Sandip Chakraborty *et al*. [4] achieved energy consumption of 29.68 mJ, 29.3 mJ, 27.53 mJ and 28.50 mJ, respectively.

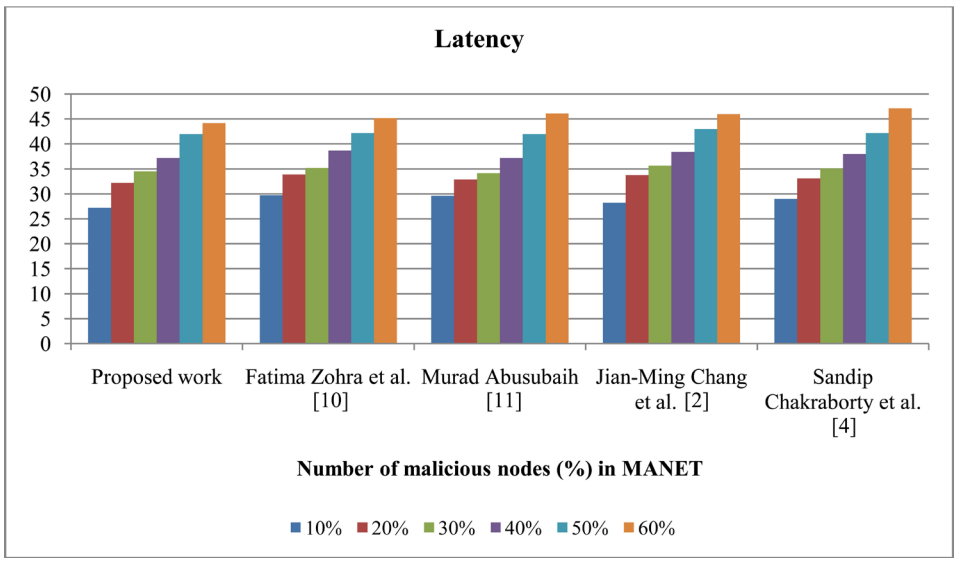


Figure 6. Performance analysis of proposed methodology in terms of latency.

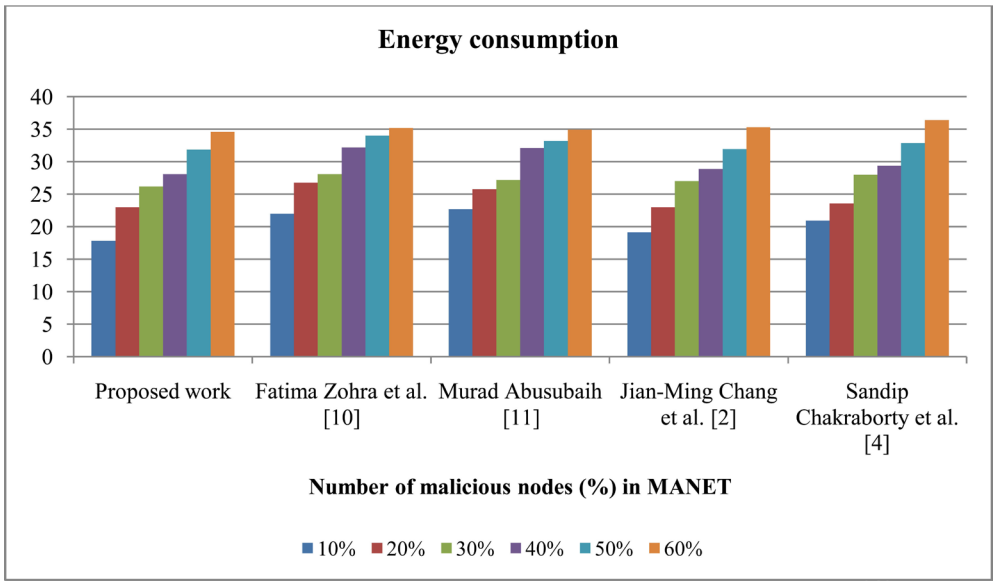


Figure 7. Performance analysis of proposed methodology in terms of energy consumption.

5. Conclusion

In this paper, a new efficient mechanism for the detection of malicious nodes in MANET is proposed. The nodes in MANET environment are grouped as cluster and based on this clustering approach, the malicious nodes are detected by cluster head. This method uses back-off duration to avoid the formation of too many clusters unnecessarily at the initial stage, which reduces the energy consumption. The simulation results reveal that the proposed cluster based malicious node detection outperforms the cooperative bait detection scheme (CBDS) [2] and opportunistic collision avoidance (OCA) method [4] in terms of packet delivery ratio, average latency and energy consumption. The proposed method achieves 89.35% of packet delivery ratio, 36.2 ms latency and 26.91 mJ of energy consumption. In future, this research work can be extended to detect and block the malicious nodes in MANET environment to increase the network performance.

References

[1] Zeng, Y.Q., Chen, Z.D., Qiao, C. and Xu, L. (2011) A Cluster Header Election Scheme Based on Auction Mechanism for Intrusion Detection in MANET. *International Conference on Network Computing and Information Security*, 433-437.

[2] Chang, J.-M., Tsou, P.-C., Woungang, I., Chao, H.-C. and Lai, C.-F. (2015) Defending against Collaborative Attacks by Malicious Nodes in MANETs: Cooperative Bait Detection Approach. *IEEE Systems Journal*, **9**, 619-621.

[3] Adnan, A., Kamalrulnizam, A., Muhammad Ibrahim, C., Khalid, H. and Abdul Waheed, K. (2014) A Survey on Trust Based Detection and Isolation of Malicious Nodes in Ad-Hoc and Sensor Networks. Frontiers of Computer Science, Higher Education Press and Springer-Verlag Berlin Heidelberg.

[4] Chakraborty, S., Nandi, S. and Chattopadhyay, S. (2016) Alleviating Hidden and Exposed Nodes in High-Throughput Wireless Mesh Networks. *IEEE Transactions on Wireless Communications*, **15**, 928-937. http://dx.doi.org/10.1109/TWC.2015.2480398

[5] Tselikis, C., Mitropoulos, S., Komninos, N. and Douligeris, C. (2012) Degree-Based Clustering Algorithms for Wireless Ad Hoc Networks Under Attack. *IEEE Communications Letters*, **16**, 619-621. http://dx.doi.org/10.1109/LCOMM.2012.031912.112484

[6] Karunakaran, S. and Thangaraj, P. (2011) A Cluster-Based Service Discovery Protocol for Mobile Ad-hoc Networks. *American Journal of Scientific Research*, **11**, 179-190.

[7] Su, Y.Y., Hwang, S.F. and Dow, C.R. (2008) An Efficient Cluster-Based Routing Algorithm in Ad Hoc Networks with Unidirectional Links. *Journal of Information Science and Engineering*, **24**, 1409-1428.

[8] Han, B. and Jia, W.J. (2007) Clustering Wireless Ad Hoc Networks with Weakly Connected Dominating Set. *Journal of Parallel and Distributed Computing*, **67**, 727-737. http://dx.doi.org/10.1016/j.jpdc.2007.03.001

[9] Cheng, C.-T., Tse, C.K. and Lau, F.C.M. (2011) A Clustering Algorithm for Wireless Sensor Networks Based on Social Insect Colonies. *IEEE Sensors Journal*, **11**, 711-721. http://dx.doi.org/10.1109/JSEN.2010.2063021

[10] Fatima Zohra, M., Maaza Zoulikha, M. and Said, K. (2011) Techniques of Detection of the Hidden Node in Wireless Ad Hoc Network. *Proceedings of the World Congress on Engineering*, **2**, 978-988.

[11] Abusubaih, M. (2011) A Combined Approach for Detecting Hidden Nodes in 802.11 Wireless LANs. Annals of Telecommunications. *Annales des Telecommunications*, **66**, 635-642.