Egyptian Informatics Journal (2021) **22**, 373–387

Cairo University

**Egyptian Informatics Journal**

www.elsevier.com/locate/eij
www.sciencedirect.com

FULL-LENGTH ARTICLE

# Enhancing cooperation in MANET using neighborhood compressive sensing model

**Mohammad Amir Khusru Akhtar** [a,*], **Gadadhar Sahoo** [b]

[a] *Department of Computer Science & Engineering, Cambridge Institute of Technology, Tatisilwai, Ranchi 835103, India*
[b] *Department of Computer Science & Engineering, Birla Institute of Technology, Mesra, Ranchi 835215, India*

Received 3 December 2015; revised 20 May 2016; accepted 19 June 2016
Available online 9 September 2016

**KEYWORDS**

Compressive sensing;
Neighborhood group;
Leader node;
Malicious node;
Neighborhood compressive sensing

**Abstract** This paper presents the use of Compressive Sensing (CS) in the reduction of resource consumption to minimize battery and bandwidth usage. It also focuses on how attacks and misbehavior can be nullified. The proposed Neighborhood Compressive Sensing (NCS) model compresses the neighborhood sparse data such as routing table updates, advertisement and trust information. It minimizes resource consumption because major computations are performed by the leader node. The use of compressive sensing gives the reduction in resource consumption because it reduces the amount of transmitting data in the network. It also prevents a network from unwanted advertisement and attacks because the neighborhood nodes do not accept the advertisements and updates directly, rather it uses leader node's processed information. The proposed NCS model is implemented in "GloMoSim" on top of the DSR protocol, resulting its effectiveness, as compared to the DSR protocol when the network is misconducting for its selfish needs. Simulation result shows that the proposed NCS model is outperformed DSR in terms of the energy consumption, network lifetime and packet dropping ratio. This work is the extended version of Reduction in Resource Consumption to enhance cooperation in MANET using Compressive Sensing (Akhtar and Sahoo, 2015) [68].



## 1. Introduction

Mobile ad hoc network (MANET) is an infrastructure-less, self-organized network in which a group of wireless devices (nodes) cooperate each other for its network operations. Unlike a wireless infrastructure network, an ad hoc network has certain characteristics such as lack of fixed infrastructure, self-organization, dynamic topology, multi-hop routing and energy constrained operation. An ad hoc network is a self-organized network because it does not involve any central authority or base station. Therefore, all ad hoc nodes need

*Abbreviations*: LN, leader node; BN, border node; RN, regular node; CS, Compressive Sensing; NG, neighborhood group; NCS, Neighborhood Compressive Sensing

* Corresponding author.
E-mail address: akru2008@gmail.com (M.A.K. Akhtar).

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

http://dx.doi.org/10.1016/j.eij.2016.06.007

to cooperate in network activities and must implement common functions for addressing, routing, power control, etc. Another key feature of an ad hoc network is the ability of a mobile node to move generously while still be connected to other mobile nodes and cooperate in network participation. As far as the communication is concerned, the sender could not communicate directly to the receiver due to the limited radio coverage. A connection is established without any base station and for only one session. To route packets, the devices discover their neighbors to form a network. If the target node is out of range then it is searched by flooding the network with broadcasts that are forwarded by every node. Thus, packets are transmitted through multiple hops to reach the destination. Because, nodes are moving around the network so routing protocols provide the stable connections. A mobile node normally operates with a limited battery power and reduced computational capability to minimize power consumption, because complex calculation and high communication will drain out the battery faster. So, a balance mechanism should be defined in order to use the low resource.

In spite of these complexities, it has a lot of applications such as in military war zones, disaster relief operations, mine site operations and other suitable domains where infrastructures are not available, impractical, or expensive.

These characteristics make the network complex compared to other infrastructure based networks. A lot of attack and misbehavior obstruct the growth and implementation. Existing models that guard on some threats still face other challenges. Designing a secure and reliable protocol that suits mass applications is still a challenge. The fact is that the protocol not only secures the network but it should provide reliability and throughput for which the MANET was actually designed.

A MANET is like a society in which nodes have the additional responsibilities of routing and forwarding. But, noncooperation is genuine for saving itself by reducing the resource consumption such as battery lifetime and other resources. To enforce correct functioning and a realistic model should be defined, so that misbehavior is nullified. That is why a reduction in resource consumption is required to enhance cooperation. The reduction is in terms of minimizing the routing activities by reducing the amount of transmitting data and reducing the burden of heavy computations. Thus, reduction saves battery lifetime and other resources resulting unethical behavior will be abridged. In Section 3.2 we have discussed how reduction in resource consumption is required to enhance cooperation in MANET. We have also discussed the meaning of misbehavior and why nodes misbehave.

This paper presents the use of Compressive Sensing (CS) [1,2] in the reduction of resource consumption to minimize battery and bandwidth usage. It also focuses on how attacks and misbehavior can be nullified. The proposed Neighborhood Compressive Sensing (NCS) model compresses the neighborhood sparse data such as routing table updates, advertisement and trust information. This gives a reduction in the amount of transmitting data. At first our model divides a MANET in terms of the neighborhood called neighborhood group (NG). In a neighborhood group we have a set of regular nodes, one or more border node(s) and one leader node. Regular nodes are responsible for compressing and forwarding the sparse data to the leader node. The leader node is responsible for the major computations. It joins all compressed data and reconstructs the original data as well as it checks the validity of the advertisement. The border node is a regular node with additional responsibility of passing the traffic to other neighborhood group. We have used the term neighborhood node to denote the regular or border node that belongs to a neighborhood group.

In the proposed NCS model nodes of the neighborhood group compress and forward the sparse data to the leader node. Finally, the leader node joins all neighborhood data and reconstructs the original data. The original data are broadcasted by the leader node in its neighborhood. This gives a reduction in resource consumption because major computations are performed by the leader node and only limited computations are performed by neighborhood nodes. Thus, it saves battery power of low processing devices because it compresses sparse data before transmission to reduce the amount of transmitting data. This gives a reduction in total energy consumption to prolong life of the network. It also prevents from attacks and misbehavior because individual nodes do not accept the advertisement and updates directly rather it uses leader node processed information.

The rest of the paper is organized as follows. Section 2 focuses on how compressive sensing is used for a mobile ad hoc network along with our motivation. In Section 3 we have discussed a detailed review on mitigation of misbehaving nodes, reduction in resource consumption to enhance cooperation and prior work on compressive sensing. Section 4 presents the proposed NCS model to enhance cooperation in MANET using compressive sensing (CS) technique. Experiments and result are given in Section 5. Finally, Section 6 concludes the paper.

## 2. Compressive sensing and motivation

### 2.1. Compressive sensing

Candès [1] and Donoho [2] proposed the new concept of signal sensing and compression called Compressive Sensing (CS). CS gained a wide acceptance in the recent years and applied in signal and image processing, pattern recognition, wireless communication, medical systems and analog-to-digital converters. In compressive sensing sampling and compression is done simultaneously and accurately. It compresses directly without involving intermediate steps of conventional compression techniques.

In the field of ad hoc network a set of sparse data can be compressed and forwarded to the leader node. The leader node uses projection to recover the actual data which reduces the amount of transmitting data in the network. The neighborhood nodes simply use leader node advertisements; thus, the proposed model prevents networks from several attacks (such as black hole and replay attacks) because wrong advertisements are not considered. It also declines the power consumption of neighborhood nodes because major computations are performed at the leader end. When we compare it with conventional routing methods all nodes are responsible for calculations, updates and forwarding. Thus, the battery of neighborhood nodes drains faster and leads to misbehave and noncooperation.

### 2.2. Prior work on compressive sensing

Compressive sensing is a new technique of signal sensing and compression, samples and compresses a signal simultaneously and reconstructs with high accuracy. Lots of work has been

proposed in the field of signal processing, pattern recognition and wireless communication to reduce the energy consumption and maximize the network lifetime. Here, we have discussed some of the prior work on compressive sensing.

Lee et al. [52] proposed a combined compressed sensing. It incorporates routing design with compressive sensing for energy efficient data gathering in sensor networks. In the Simulation results they have shown the effectiveness of the proposed combined technique in comparison with standard compressed sensing.

Chou et al. [53] proposed an adaptive algorithm based on the compressive sensing. This algorithm is used to gather information from WSNs in an energy efficient way.

Feizi et al. [54] demonstrated some applications of compressive sensing over networks. They make connection between compressive sensing and traditional information theoretic techniques for source coding and channel coding. They show the explicit trade-off between the rate and the decoding complexity.

Zhang et al. [55] proposed compressed neighbor discovery protocol that allows all nodes to concurrently discover their neighborhoods with a single frame of transmission, which is normally of a few thousand symbol epochs. This scheme is more efficient than conventional random-access discovery, because nodes have to retransmit lots of frames with random delays to effectively discovered.

For the reduction in energy consumption Xiong et al. [56] proposed a combined method by taking compressive sensing and network coding inner contact in WSN. This work enhances network lifetime by reducing total energy consumption.

Recently, for improving the performance of routing in wireless sensor network an adaptive and efficient technique based on compressive sensing (ECST) is proposed by Aziz et al. [57]. The proposed technique gives better results than the existing protocol in terms of the network lifetime and energy consumption. This paper inspired us to use compressive sensing in MANET.

### 2.3. Motivation

The motivation behind this work is to define some new way to tackle from several attacks and misbehavior by reducing the resource consumption and by centralizing the control. In a MANET we have mostly low battery power devices. These nodes have the dual responsibilities of routing and forwarding and in order to save itself noncooperation is genuine. Noncooperation is in terms of misbehavior or packet dropping attacks to reduce the resource consumption such as battery lifetime and other resources. That is why we want to minimize the battery usage so that these devices can survive more and cooperate in network activities. A device may be a personal computer (desktops/laptops) with wireless LAN cards, Personal Digital Assistants (PDA), Laptop, Palmtop or any other wireless or mobile devices. We have shown a MANET in Fig. 1 in which a set of devices is connected together to share information. The Laptop shown in Fig. 1 can be used as a leader node because it has the high computation capability and more battery power than low battery power devices such as mobile phones. In a battle zone the captain's Laptop can be taken as a leader node because it has high processing power and battery lifetime [3,4].

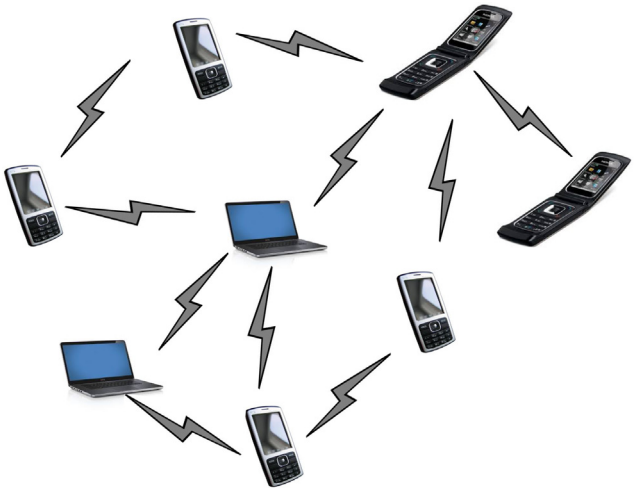

**Figure 1** A mobile ad hoc network.

We have used the compressive sensing in a neighborhood sparse domain. It compresses the neighborhood sparse data such as routing table updates and other advertisement and trust information. This saves battery power of low processing devices and protects the network from attacks and misbehavior because all advertisements and routing updates are under the care of leader nodes.

## 3. Literature review

In this section we have focused on mitigation of misbehaving nodes, reduction in resource consumption to enhance cooperation and prior work on compressive sensing.

### 3.1. Mitigation of misbehaving nodes

MANET is most susceptible to selfishness, that is why it needs some mechanisms to enhance cooperation [5]. Enforcing cooperation using complex techniques protects the network from attacks and misbehavior but consumes more battery power and bandwidth thus, reduces the life of the network. Our proposed model protects the network from attacks and misbehavior because it consumes less energy and bandwidth. Let us take a look on the existing mechanisms for the mitigation of misbehaving or selfish nodes. These mechanisms are categorized into two types the incentive based mechanisms and the reputation based mechanisms [6].

#### 3.1.1. Incentive-based mechanisms

The incentive based mechanisms discourage nodes to become selfish by assigning some sort of incentives or credits to nodes that cooperate in network activities. In this mechanism a successful forwarding is counted and senders are rewarded by giving virtual money or credits. The virtual money or credits are essential because to send its own packet also enough credits or currency are required. Several works for the detection of misbehavior using an incentive based mechanism are as follows.

The Packet Purse Model (PPM)/Packet Trade Model (PTM) [7] [8] is a two model concept. The first model (PPM) loads Nuglets for payment into the data packets before sending it to the intermediate nodes and intermediate nodes obtain more Nuglets than they deserve. In the PTM intermediate nodes trade packets are maintained on the basis of previous node, and finally the destination pays the price of the packets. The limitation of this model is that it needs a secure hardware to control nodes from tampering the amount of nuglets.

Anderegg and Eidenbenz proposed the ad hoc Vickrey-Clarke-Groves (VCG) [9] method in two phases. In the first Route Discovery phase destination nodes compute needed payments for intermediate nodes and intimate this to the source node or the central bank. The payment is performed in the second phase that is the Data Transmission phase. The limitation of ad hoc VCG is that nodes totally depend on the destination nodes report.

Sprite [10] uses Central Authorized Server (CCS) in which nodes have to send a receipt to CCS for every packet they forward and then CCS assigns credits to nodes according to the receipt. The limitation is in terms of scalability and message overhead.

In priority forwarding [11], it uses two layered forwarding concept: the Priced Priority forwarding and Free best-effort forwarding. But the limitation of this method is that it has packets forwarding problems.

Protocol independent Fairness Algorithm (PIFA) [12] is suitable for any available routing protocols. It uses a Credit Manager (CM) for maintaining the credit databases for nodes, bank stations or sink nodes. It has a weakness in terms of message processing overhead.

Buttayan and Hubaux [13] proposed the virtual currency, called nuglets for the detection of selfish nodes. This method increment a nuglet counter when nodes forward packets for others. If a node has to send its own packet, it requires enough credits because the system checks certain threshold value. If a node does not have enough credit it is not allowed to send packets. But this method needs tamper proof hardware to maintain the nuglets.

Fratkin et al. [14] introduced a software solution without involving the tamper resistant module. This method uses a trusted third party defined as the banker node in charge for payment consolidation and integrity.

Crowcroft et al. [15] proposed a pricing model in which every node updates its prices on the basis of bandwidth usage and power consumption.

Mok et al. proposed the Fee Arbitrated Incentive Architecture (FAIR) [16]. In this method the benefits and contribution of a node are measured and feedback schemes dynamically adjust the FAIR performance. On the basis of nodes participation in network activities benefits are decided. To send own packet nodes must cooperate in routing activities. This method uses energy, bandwidth and processor constraints for the optimization of performance.

Secure Incentive Protocol (SIP) [17] is a session-based approach proposed by Zhang et al. This method divides the function into three phases the Session initialization phase, the Data forwarding phase and the Rewarding phase. In this method a session initiator and a session responder are defined and they are charged for taking the services. All intermediate nodes gain credits on the basis of the number of packets successfully forwarded.

*3.1.2. Reputation-based mechanisms*

In the reputation-based mechanism some detection and punishment strategy is used for the mitigation of selfish nodes. These mechanisms maintain some sort of reputation system to identify and punish selfish nodes. In a MANET a node acts as a trustor as well as trustee. Due to its self organization reputation is defined on the basis of network participation seen by others. It is defined on the basis of the packet delivery ratio and other metrics. Lots of works have been proposed in the literature for the mitigation of misbehaving nodes using reputation based mechanism.

The first work on the detection of routing misbehavior was proposed by Marti et al. [18] named Watchdog and Pathrater. This base protocol for this mechanism is DSR [19] routing protocol. The Watchdog is responsible for neighbor monitoring and identifying malicious and selfish nodes. The Pathrater evaluates the reputation of nodes on a path and defines the route by isolating selfish nodes lying on the routing paths. But this mechanism rewards selfish nodes because there is no punishment for misbehaving. Another weakness is in terms of extra battery power consumption because each node has to frequently listen to the medium.

Buchegger et al. [20,21] proposed the CONFIDANT protocol that monitors the behavior of nodes, then calculates the reputation, and finally punish the identified misbehaving nodes. This protocol divides the work in four parts: a monitor, a reputation system, a trust manager and a path manager. The Monitor is in charge of watching the behavior information of neighboring nodes. The reputation system is accountable for calculating the reputation of nodes on the basis of direct and indirect observation. The trust manager is responsible to gather warning messages from friends. The path manager is used to manage routing by isolating selfish nodes. The limitation of this protocol is an inconsistent evaluation problem in which each node evaluates different evaluations for the same node and creates difficulty in identifying selfish nodes. Another problem is a location privilege because punishment is defined on the basis of packet drops not on the basis of network contribution. Thus, battery of nodes situated in the center of the network drain faster than the nodes lying on the periphery of the network.

Michiardi and Molva [22] proposed reputation measure to know a nodes contribution to a network. They classified reputation into three types: subjective, indirect and functional. The subjective reputation is computed on the basis of node's direct observation. The indirect reputation is computed based on the information provided by other nodes. Finally, in the functional reputation the subjective and indirect reputation is computed with respect to different functions. The functional reputation concentrates only on routing and packet forwarding function. After that is takes these reputations to aggregate a collaborative reputation.

Michiardi and Molva proposed the CORE [23] protocol for the mitigation of misbehavior. This model evaluate nodes on the basis of three reputations i.e., collaborative reputation. It maintains several reputation tables with a Watchdog mechanism at each node in the network. The Watchdog monitors the behavior of a node and the reputation tables are used to maintain the reputation values. The reputation is updated periodically, by direct and indirect listening. Thus the proposed model identifies the selfishness of a node or service requester and able to decide either to serve or to refuse the request.

Cooperation enhancement in MANETs (CineMA) [24] was presented in the literature that limits the number of packets forwarded by selfish nodes. The CineMA penalty scheme uses a similar penalty scheme as in CORE and CONFIDANT. It has three main modules the Watchdog module, a reputation system module, and an interface queue module. The Watchdog is responsible for system monitoring to collect information. A reputation system determines the level of cooperation on the basis of the number of packets received and the number of packets forwarded. Finally the interface queue module limits the amount of packets transmitted by selfish node. The key advantage of CineMA is that it degrades the sending rate of a selfish node.

The "TWOACK" mechanism [25,26] was proposed which is the substitute of the Watchdog mechanism that uses a network-layer acknowledgement-based scheme can be used with any source routing protocol. In this mechanism data packet has reached to the destination in two hops only. In the simulation study they have shown that if a network having 40 percent selfish nodes then the delivery throughput using TWOACK is 85–90%. The weakness of this method is that it requires additional transmissions i.e. TWOACK and consumes more energy than Watchdog mechanism.

Miranda and Rodrigues [27] proposed Friends & Foes to minimize misbehavior from a MANET. Friends receive services of the network and Foes are refused to serve by the nodes of MANET. The limitation of this method is that it has memory and message overhead.

Adams [28] suggested the Reputation Indexing Window (RIW) method in which emphasis is given on current feedback rather than old ones. This mechanism considers a node as selfish for a long time to build up a good reputation because of its impractical assumption.

In a work Hu et al. [29] suggested that nodes have to periodically broadcast status information of neighboring nodes in which it has to show the refusal of selfish nodes. The limitation of this mechanism is the high communication overhead.

Paul and Westhoff [30] suggested a security extension of the DSR protocol. It detects an attack in the routing process on the basis of neighbors observation and routing messages.

#### 3.1.3. Other reputation systems

The current status of reputation based systems is presented in the survey of trust and reputation management systems [31]. The limitation of these reputations based mechanisms is in terms of energy and other resource consumptions.

Several research works [13,32–37] show the usage of reputation value in the detection and exclusion of selfish node in MANET. These methods have limitation because of its stricter punishment strategy. These models isolate nodes from routing activity on the basis of lower reputation value, hence, reduce the total strength of nodes in the network. In view of the fact that a cooperative network is based on the nodes strength the network does not perform better.

A classification algorithm was proposed for the intrusion detection in MANET [38]. This is an innovative approach but not validated by real world data. Detection of selfish nodes is proposed in these methods [39,40] but still these algorithms consume more energy. A secure routing protocol is suggested by Li et al. with nodes selfishness resistance in MANETs; however, this protocol still consumes much energy [41].

Several trust management systems are proposed [42] and categorized into three types: in the first the centralized systems in which individual nodes cooperate with the system to manage the trust values. For a self organized network it is not practical. In the second category global trust calculation is performed for every node; however, the limitation is that it does not involve uncertainty. Finally, in the third category all nodes calculate and maintain the trust value by direct or indirect observation and suitable for a MANET. In this category we have a lot of existing protocols such as CONFIDANT [20,21], CORE [23], and OCEAN [32].

Josang et al. [43,44] developed algebra in support of assessing trust relations by using a triplet of belief, disbelief, and uncertainty in every trust statement. The limitation of this approach is that it fails since a user cannot allocate consistent value in each case.

Li and Wu [45] proposed the Certainty-Oriented Reputation System. It also uses a triplet $(b, d, u)$ to characterize a nodes opinion $(b, d, u) \in [0, 1]^3$: $b + d + u = 1$ where $b$, $d$, and $u$ denotes belief, disbelief, and uncertainty respectively. It uses $\alpha$ for successful forwarding and $\beta$ for unsuccessful forwarding. In case of a successful forwarding $\alpha$ is updated otherwise $\beta$ is updated. The triplet $(b, d, u)$ represents the nodes opinion and it is derived from Beta $(\alpha, \beta)$ which is the Bayesian inference that accepts two parameters $\alpha$ and $\beta$ for continuous modification as soon as new observations are made. But, the proposed work fails to express the core dimension of trust because it concentrates on belief and disbelief only.

### 3.2. Reduction enhances cooperation

Reduction in resource consumption surely enhances cooperation and minimizes misbehavior [6]. The reduction is in terms of minimizing the routing activities that save battery life and bandwidth, so that misbehavior can be controlled up to the maximum extent. To understand the fact let us discuss the meaning of misbehavior and why nodes misbehave.

A MANET is an autonomous body of mobile nodes or routers connected by wireless links. These networks work in a standalone fashion in which each node has dual responsibilities of forwarding and routing. As far as the wireless environment is concerned complex calculation and high communication will drain out the battery faster. In order to save its energy and bandwidth nodes drop packets of others [6]. When a node drops packet of others it is called misbehavior which degrades the efficiency of packet transfer, increases the packet delivery time, enhances the packet loss rate and creates network partitioning. Misbehavior further classifies into selfish and malicious. In selfish misbehavior a node drops packet of others due to its honest causes (i.e., to save battery life, to save bandwidth) encourages nodes to become selfish. Thus, energy and bandwidth are the genuine cause of misbehavior. On the other hand in the malicious attacks the attackers deploy wormhole and black hole attacks to drop packets of others. In this work, a node which drops packets of others is called a selfish node or misbehaving node or malicious node.

A lot of work is proposed in the literature to minimize total control traffic overhead using partitioning and subnetting. These works minimizes resource consumption, because they limit unnecessary broadcasts. Hence, nodes have fewer chances

for misbehaving and it is true also because they have enough energy to survive.

Chiang et al. [46] proposed a Partition Network Model to minimize the routing overhead using Mobile agents. This model enhances network cooperation by reducing routing overhead.

López et al. [47] proposed the subnetting concepts to reduce routing overhead. It divides a network into several subnets to reduce the unwanted packets in a network. By reducing the routing overhead it saves battery power thus enhance cooperation in MANET. This model uses an internet type structure to group nodes into subnets. But, subnetting concept is difficult to apply in MANET due to their dynamic and distributed nature. This paper introduces several open challenges such as subnet formation and address acquisition, mobility of nodes between subnets and the intra-subnet and inter-subnet routing.

Lots of efficient virtual subnet model for MANET were proposed in the literature [48–50]. These models enhance cooperation by minimizing overhead. But, these solutions are not appropriate for devices having low computation power. The limitation is that nodes in the subnet are authenticated using certificates which involve lots of computations.

Akhtar and Sahoo proposed a novel approach for securing an ad hoc network using the Friendly Group model [51]. It uses two Network Interface Cards (NICs) in the border node to partition a MANET into several friendly groups. This model reduces battery usage by reducing total control traffic overhead which enhances cooperation in MANET.

## 4. Proposed NCS model

### 4.1. Overview

This section presents the proposed model for the reduction in resource consumption using compressive sensing (CS) technique [1,2,58–60]. In a MANET we have heterogeneous devices having different storage, processing capability and battery lifetime. Processing of routing table updates and other advertisement consumes valuable resources (such as energy and bandwidth), which curtail the life of low battery power devices. That is why this model defines Neighborhood Compressive Sensing (NCS), so that the major computations are performed at leader end. Thus, it saves battery usage of low battery power devices as well as it prevents from attacks and misbehavior because all fake advertisements are identified using CS and correlated coefficients are treated. It identifies malicious attacks and misbehavior because the fake advertisement shows misclassified coefficients with abrupt and dissimilar values. In CS we check the sparse matrix in terms of zero and nonzero elements or in terms of similar and dissimilar coefficients. We have mostly zero elements and some are nonzero elements. Thus, the malicious advertisement can be easily identified using dissimilar coefficient or nonzero elements. But, the limitation of this technique is that if the network having a larger number of misbehaving nodes or attackers then it misclassifies the identity because we have large number of malicious data. Thus, we take action on regular or honest nodes because they are less in number. To handle this point we have considered the leader node reputation value as the basis for classification and validity of zero elements or matching coefficients. In this paper we are assuming mostly regular or honest nodes and a lesser number of malicious nodes in the network. The limitation will be considered for future work.

### 4.2. Mathematical background

Consider in an ad hoc network in which $K$ number of nodes are cooperating each other for its network operations. This work divides the network into $N$ number of NGs having $K_N$ number of nodes per NGs defined as

$$K_1 + K_2 + K_3 + \ldots + K_N = K$$

Let

$$d = [d_1, d_2, \ldots, d_N]^T$$

represent the data received by $N$ number of nodes in a neighborhood. The received data ($d$) are sparse in nature. Here, routing table updates and other advertisement are taken as sparse data because nodes belong to the same neighborhood group and neighborhood data are approximately same. This work assumes a less percentage of selfish nodes than regular nodes. The leader node coefficient is the basis of authenticity and sparsity because regular node coefficient is approximately same in the neighborhood. Hence, the leader node and regular nodes data are sparse in nature. Whereas malicious advertisement contain dissimilar coefficients and can be easily identified by leader node. Suppose that $\Psi$ denotes the domain which is an NXN orthonormal basis represented as

$$\Psi = \begin{bmatrix} \Psi_{11} & \Psi_{12} & \ldots & \Psi_{1N} \\ \Psi_{21} & \Psi_{22} & \ldots & \Psi_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ \Psi_{N1} & \Psi_{N2} & \vdots & \Psi_{NN} \end{bmatrix}$$

Then data **d** can be represented in $\Psi$ domain as

$$\begin{bmatrix} d_1 \\ d_2 \\ \vdots \\ d_N \end{bmatrix} = \begin{bmatrix} \Psi_{11} & \Psi_{12} & \ldots & \Psi_{1N} \\ \Psi_{21} & \Psi_{22} & \ldots & \Psi_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ \Psi_{N1} & \Psi_{N2} & \vdots & \Psi_{MN} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_N \end{bmatrix}$$

$$\text{i.e.,} \quad d = \Psi X \tag{1}$$

where

$$X = [x_1, x_2, \ldots, x_N]^T$$

are the obtained coefficients of **d** in domain $\Psi$.

### 4.3. Phases of the NCS model

In this work a MANET is logically divided into several neighborhood groups (NGs) on the basis of one hop distance. A neighborhood group consists of a set of regular nodes, one or more border node(s) and one leader node. Regular nodes are responsible for compressing and forwarding their sparse data to the leader node. The leader node is responsible for the major computations. It joins all compressed data and reconstructs the original data as well as checks the validity of the advertisement. The border node is a regular node with additional responsibility of passing the traffic to other neighborhood group. We have used the term neighborhood node

to denote a regular and border node that belongs to a neighborhood group. The leader node is taken to minimize battery usage of neighborhood nodes (low battery power devices) and to prevent a network from attacks and misbehavior. We have used DSR routing protocol [19] as the base protocol. Our model contains three phases i.e. the Neighborhood creation and leader selection phase, the Data compression and forwarding phase and the Data gathering, reconstruction and advertisement phase.

*4.3.1. Neighborhood creation and leader selection phase*

In this phase one or more neighborhood group(s) is defined on the basis of single hop neighbors or one hop distance. The one hop distance is computed on the basis of leader node and regular node locations as shown in Fig. 2a.

Let LN = $(x_1, y_1)$ and RN = $(x_2, y_2)$ then the Euclidean distance $d$ is computed using

$$d(\mathrm{LN}, \mathrm{RN}) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$

A node is in the coverage area of a NG if Euclidean distance is less than or equal to communication range. On the other hand when a RN is within the coverage of two or more NGs, then the minimum Euclidean distance is the basis for selecting a RN as a member for the NG. If two or more LNs are at the same distance from the RN, in that case the RN is added to any one of the NGs.

After that a leader node is elected for each neighborhood group on the basis of high computational power and battery lifetime. For example, in a battle zone a leader node could be a captain's laptop [3,4]. Figs. 2b and 2c shows the proposed diagram of the NCS model. Fig. 2b shows a neighborhood group in which nodes are at a distance of one hop and arranged in a grid pattern, where arrows indicate bidirectional flow. The center node acts as a leader node. The leader node could also be in the corner or periphery of the network. But, choosing a node at the center gives large geographical coverage. Here, this work employs only grid pattern, but nodes can be arranged in other patterns on the basis of one hop distance.

The complete network is shown in Fig. 2c in which 4 nodes act as leader nodes having high processing power and battery lifetime. For intergroup routing only relevant information is forwarded by border nodes. The border nodes can also be elected from the periphery of the neighborhood group. The selection of leader node and border node can be defined as per the requirement of the network and mobility. In this paper we are concentrating on data compression using compressive sensing to maximize the network lifetime and to prevent a network from attacks and misbehavior. We have not discussed the selection of leader node in this paper. To select a leader node we can use any of the existing algorithms [61,62]. We have used the "Elite Leader Finding Algorithm for MANETs" [61]. It elects a vice-coordinator and a group of elite nodes as cabinet that avoids frequent leader election in the event of leader crash or failure. It avoids the broadcast of messages, to a large extent, and uses multicast and eventually unicast in leader election.

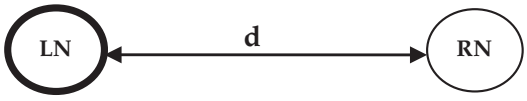


**Figure 2a** Euclidean distance ($d$) between LN and RN.

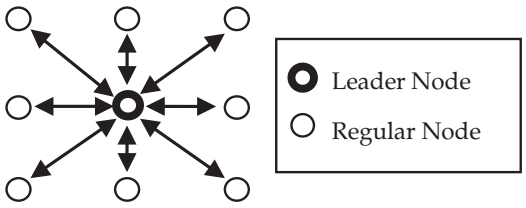


**Figure 2b** Neighborhood group.

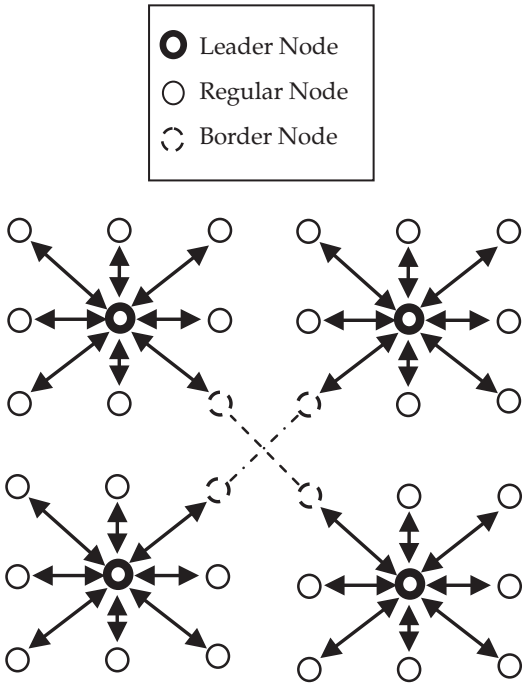


**Figure 2c** A MANET in NCS Model.

*4.3.2. Data compression and forwarding phase*

In this phase, neighborhood sparse data are compressed by neighborhood nodes individually and forwarded to the leader node instead of its direct use. Data means any type of advertisements or routing table updates.

For example, the reception and broadcast of hello message in a neighborhood are used to determine the network connectivity. A network having 4 NGs is shown in Fig. 2d. It shows that data within a NG is sparse or of the same coefficient. Tables 1 and 2 show the routing table of node $\mathrm{NG}_{1,1}$ which is sparse because, it has few large or dissimilar coefficients and many small or similar coefficients. The compression is performed by the all nodes of the neighborhood group individually. Here, sparse data denotes such type of data in which some of its coordinates having similar value and the rest having another value.

Let

$$d = [d_1, d_2, \ldots, d_N]^T$$

represent the data received by $N$ number of nodes in a neighborhood group. The compressed version $y$ can be defined for the data $\mathbf{d}$ through the measurement matrix $\mathbf{\Phi}$ as

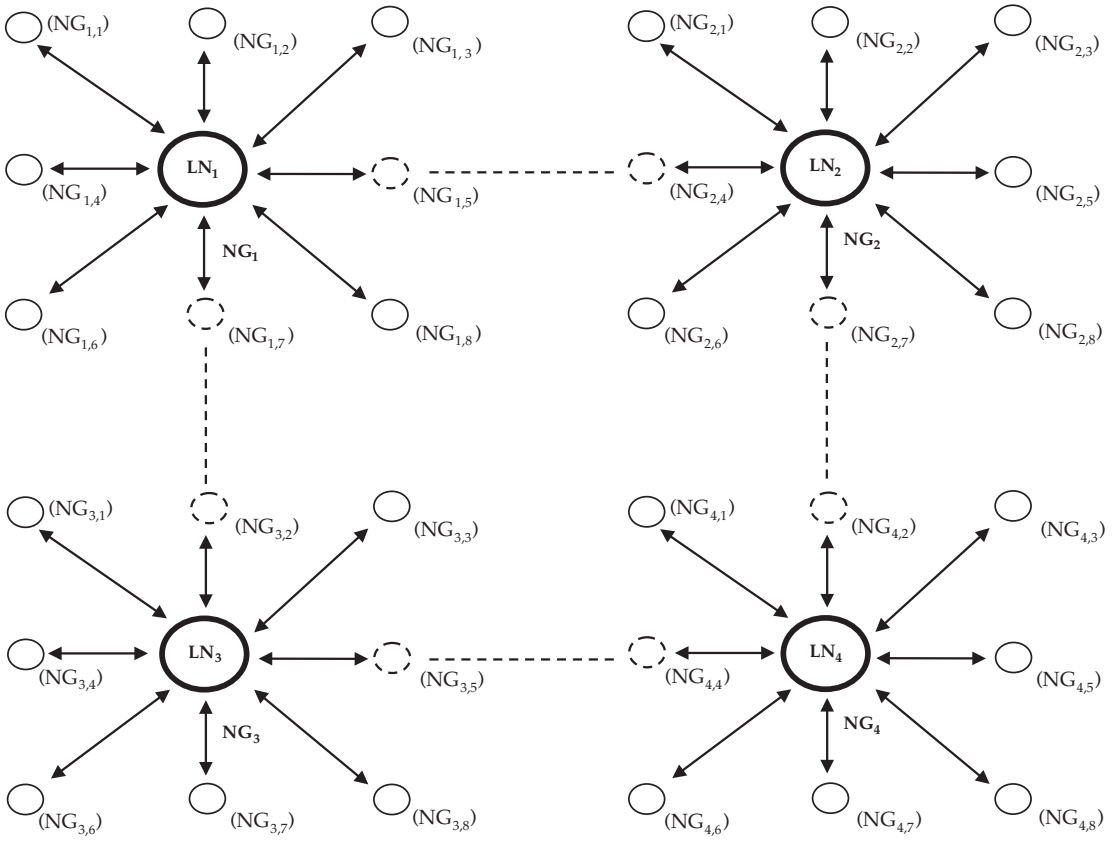


**Figure 2d** Hello message broadcast is sparse.

**Table 1** Hello message within the $NG_1$ for node $NG_{1,1}$.

| Dest | Next hop | Metric |
|---|---|---|
| $NG_{1,2}$ | $LN_1$ | 2 |
| $NG_{1,3}$ | $LN_1$ | 2 |
| $NG_{1,4}$ | $LN_1$ | 2 |
| $NG_{1,5}$ | $LN_1$ | 2 |
| $NG_{1,6}$ | $LN_1$ | 2 |
| $NG_{1,7}$ | $LN_1$ | 2 |
| $NG_{1,8}$ | $LN_1$ | 2 |

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_N \end{bmatrix} = \begin{bmatrix} \Phi_{11} & \Phi_{12} & \dots & \Phi_{1N} \\ \Phi_{21} & \Phi_{22} & \dots & \Phi_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ \Phi_{N1} & \Phi_{N2} & \vdots & \Phi_{MN} \end{bmatrix} \begin{bmatrix} d_1 \\ d_2 \\ \vdots \\ d_N \end{bmatrix}$$

or, we can write

$$y = \Phi d \tag{2}$$

where $\Phi$ is MXN random Gaussian or Bernoulli matrix with $M \ll N$.

On that basis, we can calculate the compressed version $y$ for every nodes of the neighborhood group. For example, the compressed version ($\mathbf{y_i}$) can be obtained for node$_i$ as

$$y_i = \sum_{j=1}^{n} \Phi_{ij} d_i$$

**Table 2** Hello message within the $NG_2$ for node $NG_{1,1}$.

| Dest | Next hop | Metric |
|---|---|---|
| $NG_{2,2}$ | $LN_1$ | 5 |
| $NG_{2,3}$ | $LN_1$ | 5 |
| $NG_{2,4}$ | $LN_1$ | 5 |
| $NG_{2,5}$ | $LN_1$ | 5 |
| $NG_{2,6}$ | $LN_1$ | 5 |
| $NG_{2,7}$ | $LN_1$ | 5 |
| $NG_{2,8}$ | $LN_1$ | 5 |

After compressing all nodes should forward their sparse data to the leader node.

*4.3.3. Data gathering, reconstruction and advertisement phase*

The leader node gathers neighborhood data and reconstructs the original data. After that it advertises the valid information in its neighborhood.

(a) Data gathering

The neighborhood data forwarded to the leader node are denoted as

$$y = (y_1 + y_2 + \ldots + y_N)$$

(b) Reconstruction using p-norm

Let us consider a vector

$$X = [x_1, x_2, \ldots, x_N]^T$$

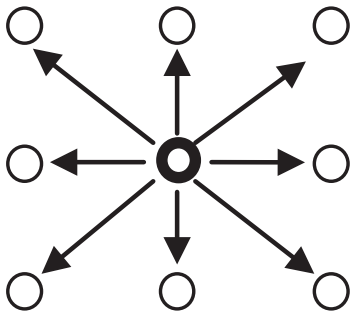

**Figure 3** Data advertisement by leader node.

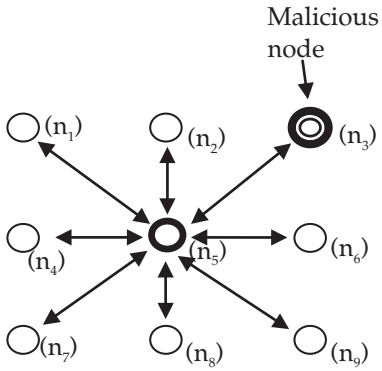


**Figure 4** Scenario description.

The p-norm of the vector is defined using

$$\|X\|_p = \sqrt[p]{\|x_1\|^p + \|x_2\|^p + \ldots + \|x_N\|^p}$$

Similarly the one norm can be obtained as

$$\|X\|_1 = \|x_1\| + \|x_2\| + \ldots + \|x_N\|$$

From "(1)," and "(2)," the leader node reconstructs the original data by solving the given L1-minimization problem.

$$\min \|X\|_{L1}$$

subject to

$$y = \Phi\Psi X$$

$$d = \Psi X$$

We have used the "Signal recovery from random measurements via orthogonal matching pursuit" algorithm [60] at the leader end to reconstruct the original data.

(c) Advertisement of valid information

The leader node after reconstruction advertises the valid information in its neighborhood as shown in Fig. 3, where arrows indicate data advertisement.

## 5. Experiments and results

### 5.1. Scenario description

To demonstrate the working of the proposed NCS model we have taken 9 nodes in which node $n_5$ is chosen as a leader node and node $n_3$ is defined as malicious node. The network is arranged in a grid pattern as shown in Fig. 4. The proposed model protects the MANET from threats and misbehavior as well as it reduces resource consumption. The detection of attacks and misbehavior is presented in Section 5.2 and reduction in resource consumption is discussed in Section 5.3.

### 5.2. Detection of attacks and misbehavior

The malicious advertisement gives wrong information to the network and thus nodes having false routes in the MANET. To check the validity of the advertisements neighborhood nodes forwards the Advertisement Check Request (ACREQ) compressed message to leader node as shown in Fig. 5a. The ACREQ message is denoted by a pair (node_number, data). The data forwarded by neighborhood nodes is '*i*' and malicious node is '*j*'. Arrows in the figure indicate transmission of ACREQ message from neighborhood nodes to leader node.

Fig. 5b shows the ACREP (Advertisement Check Reply) message broadcast by a leader node in its neighborhood after processing (joining and reconstructing) of the received compressed data. Arrows in the figure indicate ACREP advertisement.

The ACREQ information is sparse in nature because all neighborhood nodes are at a distance of one hop. The neighborhood node compresses these advertisements and forwards it to the leader node. The leader node gathers all neighborhood data and reconstructs the original data. The reconstruction is done using "Signal recovery from random measurements via orthogonal matching pursuit" algorithm [60]. Finally, it advertises the original data and identity of misbehaving nodes in its neighborhood.

The leader node receives all correlated data except the malicious nodes advertised fake or misclassified data. Thus, it identifies that malicious nodes have broadcasted wrong advertisements in the neighborhood. Now, we can punish the malicious node by isolating misbehaving from the routing path and discarding its messages by sending an alarm message in the neighborhood.

A neighborhood node forwards the node_number and compressed advertised data to leader node for checking the validity of the advertisement and to know the identity of the malicious nodes. The sparse data gathered by leader node can be represented as

$$y = (y_1 + y_2 + \ldots + y_N)$$

The data gathered by leader node is sparse in nature because all neighborhood nodes are at a distance of one hop. Thus malicious advertisements can be easily identified from

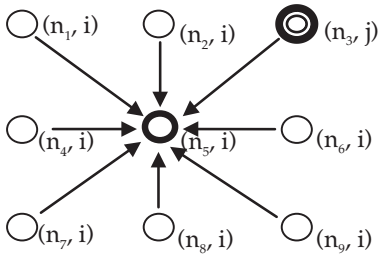


**Figure 5a** ACREQ message from neighborhood nodes.

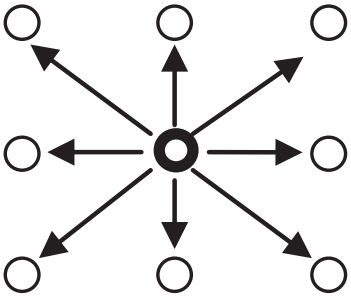

**Figure 5b** ACREP message advertisement by leader node.

the given matrix *S*. The data forwarded by neighborhood node is '*i*' and malicious node is '*j*' on the basis of its coefficient. This work assumes a less percentage of malicious nodes than regular nodes in a neighborhood. That is why the malicious advertisements contain dissimilar coefficients and can be easily identified by leader node. Matrix '*S*' shows that we have very little malicious advertisements. The '*j*' value in other nodes indicates that some neighborhood nodes received the advertisements of malicious nodes.

$$S = \begin{matrix} i \\ i \\ j \\ i \\ i \\ i \\ i \\ i \\ i \end{matrix} \begin{bmatrix} i & i & i & i & i & i & i & i \\ i & i & i & j & i & i & i & i \\ j & j & j & j & j & j & j & j \\ i & i & i & i & i & i & i & i \\ i & i & i & j & i & i & i & i \\ i & i & i & i & i & i & i & i \\ i & i & i & i & i & i & i & i \\ i & i & i & i & i & i & i & i \\ i & i & i & i & i & i & i & i \end{bmatrix}$$

Thus, the proposed model protects a network from unwanted advertisement and attacks because neighborhood nodes do not accept the advertisement and updates directly rather it uses its leader node processed information.

### 5.3. Reduction in resource consumption

In conventional routing methods all nodes are responsible for calculations, updates and forwarding. Thus, the battery of the neighborhood nodes drains faster and it leads to misbehave and noncooperation. Our proposed model declines the power consumption of neighborhood nodes because major computations are performed at the leader end. In routing table updates the battery usage of neighborhood nodes can be minimized by reducing the amount of transmitting data in the network using Compressive sensing. The leader node periodically broadcast RTREQ (Routing Table Request) message in its neighborhood to know the latest routes as shown in Fig. 6a, where arrows indicate RTREQ advertisement. After that neighborhood nodes compress and forward their routing table to the leader node using RTREP message as shown in Fig. 6b, where arrows indicate transmission of RTREP message from neighborhood nodes to leader node.

The leader node finally joins and reconstructs the routing table and broadcast the latest route in the neighborhood. The malicious advertisements can be easily identified from the matrix *S*. The data forwarded by neighborhood node is '*i*' and malicious node is '*j*' on the basis of its coefficient. Thus,

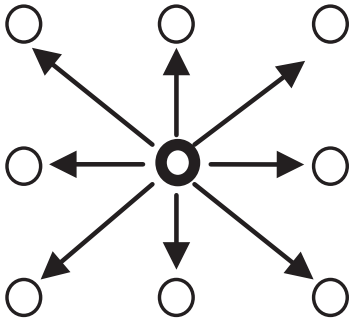

**Figure 6a** RTREQ message advertisement by leader node.

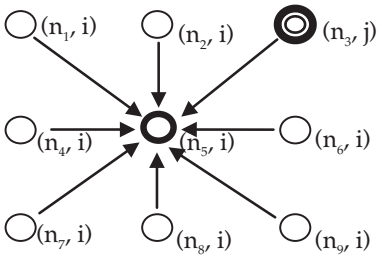


**Figure 6b** RTREP message from neighborhood nodes.

the malicious advertisements contain dissimilar coefficients and can be easily identified by leader node. This saves unwanted broadcast and minimizes the energy consumption of low battery power nodes.

The leader node gathers all RTREPs and the data are represented as

$$y = (y_1 + y_2 + \ldots + y_N)$$

After that the leader node reconstructs the original data using "Signal recovery from random measurements via orthogonal matching pursuit" algorithm [60]. Finally, the leader node broadcast the original data or latest route ($L_{\mathrm{ROUTE}}$) in its neighborhood as shown in Fig. 6c, where arrows indicate $L_{\mathrm{ROUTE}}$ advertisement.

The proposed model gives reductions in resource consumption because major computations are performed at leader end which saves battery power of low processing devices. It compresses sparse data before transmission thus, reduces the amount of transmitting data in the network. The energy consumption without CS ($E_{\mathrm{WCS}}$) and with CS using NCS model ($E_{\mathrm{Ncs}}$) is defined as

$$E_{\mathrm{WCS}} = E_T + E_P$$

$$E_{\mathrm{Ncs}} = E_{\mathrm{CT}} + E_{\mathrm{PCS}}$$

where

$E_T$: Energy consumption in transmission without CS
$E_{\mathrm{CT}}$: Energy consumption in transmission with CS
$E_{\mathrm{P}}$: Energy consumption in processing without CS
$E_{\mathrm{PCS}}$: Energy consumption in processing with CS

The ratio of $E_{\mathrm{T}}$ and $E_{\mathrm{CT}}$ is approximately 40:1.
The ratio of $E_{\mathrm{P}}$ and $E_{\mathrm{PCs}}$ is approximately 10:1.
Thus, our model reduces total energy consumption to prolong life of the network. In addition to that it protects a network from unwanted advertisement and

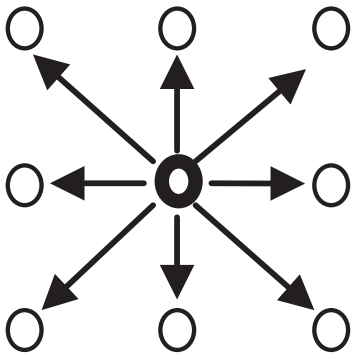

**Figure 6c** $L_{\mathrm{ROUTE}}$ advertisement by leader node.

attacks because neighborhood nodes do not accept the advertisement and updates directly rather it uses its leader node processed information.

### 5.4. Experimental result

We have used the Global Mobile Information System Simulator in our simulation [63,64]. The simulation parameters are listed in Table 3. In order to obtain the result we have analyzed several works [65–67].

Simulation result shows that the proposed NCS model is outperformed DSR in terms of the energy consumption network, lifetime and packet dropping ratio.

The NCS model defines packet delivery ratio (throughput) as the performance metric.

Packet Received Ratio (PRR) in ad hoc networks with and without NCS model.

We define PRR as follows:

PRR = (Total number of packets received successfully)/(Total number of packets sent)

If PRR is 1 it is the best case if it is less than 1 there is selfish activity.

#### 5.4.1. General analysis

In this section we present a simple analysis on best case, normal case and worst case view in terms of no of packet sent and received shown in Figs. 7a–7c respectively.

#### 5.4.2. Time taken to implement NCS model

Fig. 8 shows that PRR depends on the time to forward a packet from source to destination. The total time to forward a packet from source to destination can be computed as follows.

Without NCS Model total time to forward a packet is

$$TT = PFT + RDT$$

With NCS Model total time to forward a packet is

$$TT = NCT + PFT + RDT$$

where TT (Total time), NCT (NCS Clearance Time), PFT (Packet Forward Time), RDT (Route Discovery time).

**Table 3** Simulation parameters.

| Parameters | Values |
|---|---|
| SIMULATION-TIME | 15 M |
| TERRAIN-DIMENSIONS | (2000, 2000) |
| NUMBER-OF-NODES | 500 |
| NODE-PLACEMENT | Grid |
| MOBILITY RANDOM-WAYPOINT | |
| MOBILITY-WP-PAUSE | 30S |
| MOBILITY-WP-MIN-SPEED | 0 |
| MOBILITY-WP-MAX-SPEED | 5 |
| MOBILITY-POSITION-GRANULARITY | 0.5 |
| PROMISCUOUS-MODE | NO |
| ROUTING-PROTOCOL | DSR |
| PROPAGATION-LIMIT (dBm) | −111 |
| PROPAGATION-PATH LOSS | Two-ray |
| RADIO-FREQUENCY (Hz) | 2.40E + 09 |
| RADIO-TX-POWER (dBm) | 10 |
| RADIO-ANTENNA-GAIN (dBm) | 0 |
| RADIO-RX-SENSITIVITY (dBm) | −91 |
| RADIO-RX-THRESHOLD (dBm) | −81 |

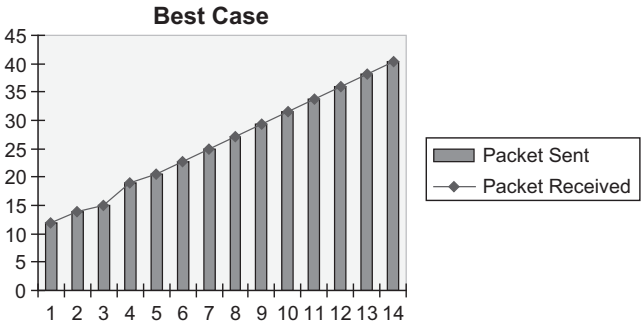


**Figure 7a** Best case.

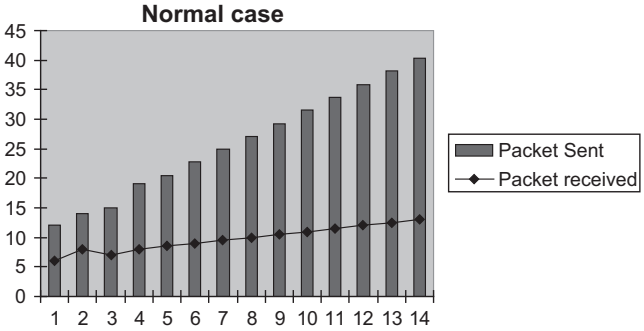


**Figure 7b** Normal case.

The NCT is the overhead that is required to enforce NCS to protect an ad hoc network from selfish node. Fig. 9a shows packet dropping status without using NCS model.

Fig. 9b shows graph shows packet dropping status with NCS Model.

Hence, NCS Model protect ad hoc network from selfish activity with some overhead.

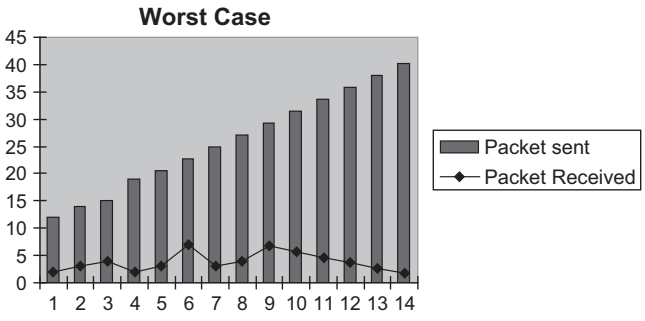


**Figure 7c** Worst case.

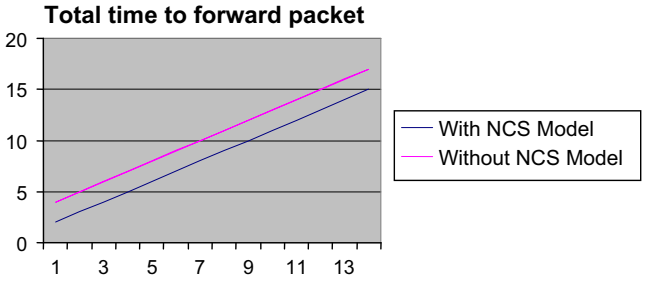


**Figure 8** Total time taken to forward packet.

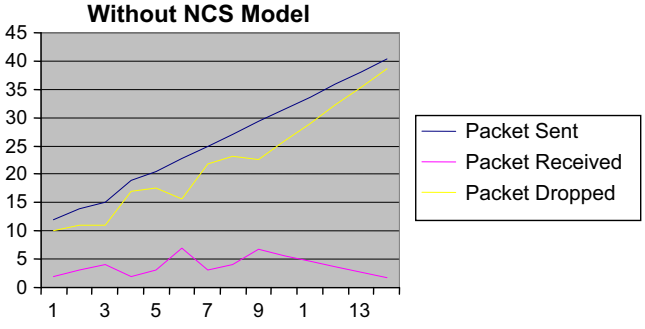


**Figure 9a** Without NCS Model.

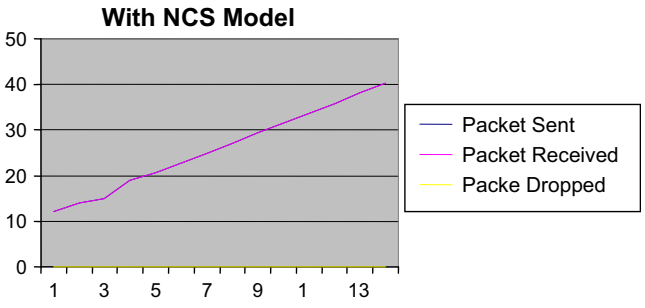


**Figure 9b** With NCS Model.

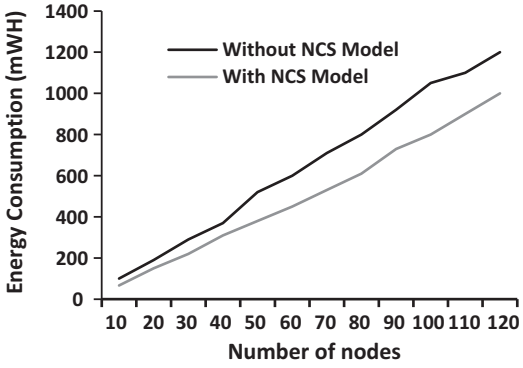


**Figure 10** Energy consumption.

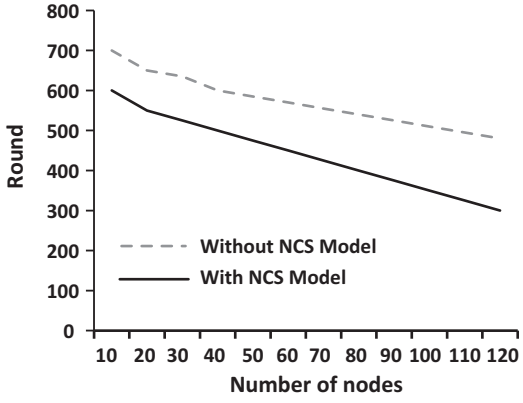


**Figure 11** Network lifetime as a function of number of sensor nodes.

*5.4.3. Energy consumption*

It compresses sparse data before transmission thus reduces the amount of transmitting data in the network. The energy consumption without NCS (EWCS) and with CS using NCS model (ENcs) is defined as

$$EWCS = ET + EP$$

$$ENcs = ECT + EPCS$$

where

ET: Energy consumption in transmission without CS
ECT: Energy consumption in transmission with CS
EP: Energy consumption in processing without CS
EPCS: Energy consumption in processing with CS
The ratio of ET and ECT is approximately 40:1.
The ratio of EP and EPCs is approximately 10:1.

The energy consumption of the proposed model is shown in Fig. 10. The average energy consumption is reduced from 30 mWH to 20 mWH using our proposed NCS model. It shows the reduction in energy consumption up to 33%.

Thus, the proposed model reduces total energy consumption to prolong life of the network.

*5.4.4. Network lifetime*

Moreover, Fig. 11 illustrates the effectiveness of NCS Model to prolong network lifetime than plain DSR.

Fig. 11 shows the comparison of network lifetime of plain DSR [19] and DSR with NCS Model. NCS Model offers improvements in network lifetime up to 20%.

## 6. Conclusion

Securing Ad-hoc network is today's major concern. A lot of attacks and misbehaves degrades the performance and reliability of Mobile Ad hoc network (MANET). This paper presents the use of Compressive Sensing (CS) in the reduction of resource consumption to minimize battery and bandwidth usage as well as it prevents from attacks and misbehavior. The proposed Neighborhood Compressive Sensing (NCS) model compresses the neighborhood sparse data such as routing table updates and other advertisement. Initially a MANET is divided in terms of the neighborhood called neighborhood group (NG). Sparse data are compressed by neighborhood node and then forwarded to the leader node. The leader node joins all neighborhood sparse data to reconstruct the original data and then broadcasts in its neighborhood. This gives a reduction in resource consumption because major computations are performed at the leader end which saves battery power of neighborhood nodes. It compresses sparse data before transmission thus reduces the amount of transmitting data in the network which saves the total energy consumption to prolong life of the network. It also prevents from attacks and misbehavior because individual nodes do not accept the advertisement and updates directly rather it uses leader node processed information. Simulation result shows that the proposed NCS model is outperformed DSR in terms of the energy consumption network, lifetime and packet dropping ratio. Hence, the proposed model enhances cooperation in MANET by reducing resource consumption.

## Acknowledgment

We would like to express our sincere gratitude to the Prof. (Dr.) Amitabh Bhattacharyya, Coordinator (TEQIP), Prof. (Dr.) S.K. Singh, Director and Prof. A. Usmani, HOD (CSE) of Cambridge Institute of Technology, Tatisilwai, Ranchi, who have always encouraged us in our research.

## References

[1] Candès E. Compressive sampling. In: Proceedings of international congress of mathematicians. Mathematical Society Publishing House; 2006. p. 1433–52.
[2] Donoho D. Compressed sensing. IEEE Trans Inf Theory 2006;52 ():1289–306.
[3] Saeed NH, Abbod MF, Al-Raweshidy HS. IMAN: an intelligent MANET routing system. In: 17th International conference on telecommunications.
[4] Saeed NH. Intelligent MANET optimisation system Ph.D. thesis. School of Engineering and Design, Electronic and Computer Engineering Department, Brunel University, Brunel University; 2011, February.
[5] Wang Y. Enhancing node cooperation in mobile wireless ad hoc networks with selfish nodes; 2008. http://uknowledge.uky.edu/gradschool_diss/602.
[6] Amornkul TA. On detection mechanisms and their performance for packet dropping attack in ad hoc networks. University of Pittsburgh; 2008.
[7] Buttyan L, Hubaux J. Enforcing service availability in mobile ad hoc WANs. In: The proceedings of IEEE/ACM MobiHOC workshop.
[8] Hubaux J, Buttyan L, et al. Toward mobile ad-hoc WANs: terminodes. Technical report. Lausanne: Swiss Federal Institute of Technology. Technical report no. DSC/2000/006; July 2000.
[9] Anderegg L, Eidenbenz S. Ad hoc-VCG: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents. In: Proceedings of ACM MobiCom. p. 245–59.
[10] Zhong S, Chen J, Yang YR. SPRITE: a simple, cheatproof, credit-based system for mobile ad-hoc networks. Proceedings of INFOCOM 03 2003:1987–97. April.
[11] Raghavan B, Snoeren AC. Priority forwarding in ad hoc networks with self-interested parties. In: Workshop on peer to peer systems, June.
[12] Yoo Y, Ahn S, Agrawal DP. A credit-payment scheme for packet forwarding fairness in mobile MANETs. In: The proceedings of IEEE ICC.
[13] Buttyan L, Hubaux J. Stimulating cooperation in self-organizing mobile ad hoc networks. ACM/Kluwer Mobile Networks Appl 2003;8(5).
[14] Fratkin E, Vijayaraghavan V, Liu Y, Gutierrez D, Li TM, Baker M. Participation incentives for ad hoc networks. http://www.stanford.edu/yl314/ape/paper.ps.
[15] Crowcroft FKJ, Gibbens R, Ostring S. Modelling incentives for collaboration in mobile ad hoc networks. In: Proceedings of workshop on modeling and optimization in mobile, ad hoc and wireless networks, ad hoc, and wireless networks (WiOpt'03), France, March.
[16] Mok A, Mistry B, Chung E, Li B. FAIR: fee arbitrated incentive architecture in wireless ad hoc networks. In: 10th IEEE real-time and embedded technology and applications symposium (RTAS'04). p. 38.
[17] Zhang Y, Lou W, Fang Y. SIP: a secure incentive protocol against selfishness in mobile ad hoc networks. IEEE wireless communications and networking conference (WCNC'04) 2004, March.
[18] Marti S, Giuli TJ, Lai K, Baker M. Mitigating routing misbehavior in mobile ad hoc networks. In: Proceedings of the 6th annual international conference on mobile computing and networking (ACM MobiCom 2000), New York, NY, USA. p. 255–65.
[19] Johnson D, Maltz D, Hu YC. The dynamic source routing protocol for mobile ad hoc networks (DSR). IEEE Internet Draft 2003. April.
[20] Buchegger S, Le-Boudec JY. Performance analysis of the CONFIDANT protocol (cooperation of nodes: fairness in dynamic ad-hoc networks). In: Proceedings of MobiHOC'02, June.
[21] Buchegger S, Le-Boudec JY. Nodes bearing grudges: towards routing security fairness and robustness in mobile ad hoc networks. In: Proceedings of EUROMICRO-PDP'02.
[22] Michiardi P, Molva R. Prevention of denial of service attacks and selfishness in mobile ad hoc networks. Research report RR-02-063; January 2002.
[23] Michiardi P, Molva R. CORE: a collaborative reputation mechanism to enforce cooperation in mobile ad-hoc networks. In: in CMS'2002, communication and multimedia security 2002 conference, Portoroz, Slovenia, September 26–27; 2002 [Also published in the book: Advanced Communications and Multimedia Security/Borka Jerman-Blazic & Tomaz Klobucar, editors, Kluwer Academic Publishers, ISBN 1-4020-7206-6, August 2002, 320p, August 2002].
[24] Frank M, Martini P, Plaggemeier M. CineMA: cooperation enhancement in MANETs. In: Proceedings of the 29th annual IEEE international conference on local computers networks (LCN'04).
[25] Wang Y, Singhal M. LSTOP: a light-weight scalable truthful routing protocol in manets with selfish nodes. In: Proceedings of

5th international conference of ad-hoc networks & wireless (AD HOC-NOW 2006), Ottawa, Canada. p. 280–93. August.
[26] Wang Y, Singhal M. On improving the efficiency of truthful routing in MANETs with selfish nodes. Pervasive Mobile Comput 2007;3(5):537–59, October [Elsevier].
[27] Miranda H, Rodrigues L. Friends and foes: preventing selfishness in open mobile ad hoc networks. In: ICDCSW'03.
[28] Adams WJ, Hadjichristofi GC, Davis IV NJ. Calculating a node's reputation in a mobile ad hoc network. In: Proc. IEEE Int'l performance computing and communications conference (IPCCC). p. 303–7.
[29] Hu Y, Perrig A, Johnson D. Ariadne: a secure on-demand routing protocol for ad hoc networks. In: Proceedings of the eighth annual international conference on mobile computing and networking. p. 12–23, September.
[30] Paul K, Westhoff D. Context aware detection of selfish nodes in DSR based ad-hoc networks. In: Proceedings of IEEE vehicular technology conference'02.
[31] Yu H, Shen Z, Miao C, Leung C, Niyato D. A survey of trust and reputation management systems in wireless communications. Proc IEEE 2010;98(10):1755–72, October.
[32] Bansal S, Baker M. Observation-based cooperation enforcement in ad hoc networks Technical report cs. NI/0307012. Stanford University; 2003.
[33] Akbani R, Korkmaz T. Enhancing role-based trust management with a reputation system for MANETs. URASIP J Wireless Commun Networking 2011;90, September.
[34] Wang F, Huang B, Yang LT. COSR: a reputation-based secure route protocol in MANET. EURASIP J Wireless Commun Networking 2010:1–11, January [Special issue on multimedia communications over next generation wireless networks archive Volume 2010].
[35] Zakhary SR, Radenkovic M. Reputation based security protocol for MANETs in highly mobile disconnection-prone environments. In: International conference on wireless on-demand network systems and services (WONS). p. 161–7, February.
[36] Buchegger S, Boudec JYL. Self-policing mobile ad hoc networks by reputation systems. IEEE Commun Mag 2005;43(7):101–7, July.
[37] Balasubramanian A, Ghosh J, Wang X. A reputation based scheme for stimulating cooperation in MANETs. In: Proceedings of the 19th international teletraffic congress, Beijing. August.
[38] Mitrokotsa A, Dimitrakakis C. Intrusion detection in MANET using classification algorithms: the effects of cost and model selection. Ad Hoc Netw 2012. http://dx.doi.org/10.1016/j.adhoc.2012.05.006.
[39] Orallo EH, Serrat MD, Cano JC, Calafate CMT, Manzoni P. Improving selfish node detection in MANETs using a collaborative watchdog. IEEE Commun Lett 2012;16(5):642–5.
[40] Orallo EH, Olmos MDS, Cano JC, Calafate CT, Manzoni P. Evaluation of collaborative selfish node detection in MANETS and DTNs. In: MSWiM '12 Proceedings of the 15th ACM international conference on modeling, analysis and simulation of wireless and mobile systems. p. 159–66.
[41] Li CT, Yang CC, Hwang MS. A secure routing protocol with node selfishness resistance in MANETs. Int J Mobile Commun 2012;10:103–18.
[42] Josang A, Ismail R, Boyd C. A survey of trust and reputation systems for online service provision. Decis Support Syst 2007;43():618–44.
[43] Josang A, Marsh S, Pope S. Exploring different types of trust propagation. Proc Int'l conf trust management 2006.
[44] Josang A, Pope S. Normalising the consensus operator for belief fusion. In: Proc int'l conf information processing and management of uncertainty, July.
[45] Li F, Wu J. Uncertainty modeling and reduction in MANETs. IEEE Trans Mob Comput 2010;9(7), July.
[46] Chiang T, Tsai HM, Huang YM. A partition network model for ad hoc networks. In: Wireless Mobile Comput Networking Commun. p. 467–72, WiMob'2005.
[47] López J, Barceló JM, Vidal JG. Subnet formation and address allocation approach for a routing with subnets scheme in MANETs. Wireless Syst Network Archit Next Generation Internet Lect Notes Comput Sci 2006;3883(2006):62–77. http://dx.doi.org/10.1007/11750673_6.
[48] Chowdhury MAH, Ikram M, Kim KH. Secure and survivable group communication over MANET using CRTDH based on a virtual subnet model. In: IEEE Asia-Pacific services computing conference.
[49] Chang CW, Yeh CH, Tsai CD. An efficient authentication protocol for virtual subnets on mobile ad hoc networks. In: International symposium on computer, communication, control and automation.
[50] Ankush A, Vilhekar, Jaidhar CD. Modified authentication protocol using elliptic curve cryptosystem for virtual subnets on mobile ad hoc networks. Wireless Commun Appl Lect Notes Inst Comput Sci Social Inf Telecommun Eng 2012;72:426–32.
[51] Akhtar MAK, Sahoo G. A novel methodology for securing ad hoc network by friendly group model. In: The fourth international conference on networks & communications (NetCoM), Chennai. Lecture notes in electrical engineering, vol. 131. Springer; 2013. p. 23–35. http://dx.doi.org/10.1007/978-1-4614-6154-8_3, January (Series ISSN 1876-1100).
[52] Lee S, Pattem S, Sathiamoorthy M, Krishnamachari B, Ortega A. Compressed sensing and routing in multi-hop networks CENG technical report. University of Southern California; 2009.
[53] Chou CT, Rana R, Hu W. Energy efficient information collection in wireless sensor networks using adaptive compressive sensing. In: IEEE 34th conference on local computer networks, 2009. LCN 2009. IEEE; 2009. p. 443–50.
[54] Feizi S, Medard M, Effros M. Compressive sensing over networks. In: 48th Annual allerton conference on communication, control, and computing (Allerton). IEEE; 2010. p. 1129–36.
[55] Zhang L, Luo J, Guo D. Neighbor discovery for wireless networks via compressed sensing. Perform Eval 2013;70(7):457–71.
[56] Xiong J, Zhao J, Xuan L. Research on the combining of compressed sensing and network coding in wireless sensor network. J Theor Appl Inf Technol 2013;47(3).
[57] Aziz A, Salim A, Osamy W. Adaptive and efficient compressive sensing based technique for routing in wireless sensor networks. In: The INTHITEN (INternet of THings and ITs ENablers) conference. St. Petersburg (Russia): The Bonch-Bruevich State University of Telecommunications (SUT); 2013.
[58] Zheng H, Wang X, Tian X, Xiao S. Data gathering with compressive sensing in wireless sensor networks: an in-network computation-perspective. http://iwct.sjtu.edu.cn/Personal/xwang8/paper/INFCOM2012_InNetworkComputation_techreport.pdf.
[59] Zheng H, Xiao S, Wang X, Tian X. Energy and latency analysis for in-network computation with compressive sensing in wireless sensor networks. In: Proceedings IEEE INFOCOM. IEEE; 2012. p. 2811–5.
[60] Tropp JA, Gilbert AC. Signal recovery from random measurements via orthogonal matching pursuit. IEEE Trans Inf Theor 2007;53(12):4655–66, December.
[61] Singh AK, Sharma S. Elite leader finding algorithm for MANETs. In: 10th International symposium on parallel and distributed computing (ISPDC). p. 125–32. http://dx.doi.org/10.1109/ISPDC.2011.27.
[62] Mohammed N, Otrok H, Wang L, Debbabi M, Bhattacharya P. Mechanism design-based secure leader election model for intrusion detection in MANET. IEEE transactions on dependable and secure computing 2011;8(1):89–103. http://dx.doi.org/10.1109/TDSC.2009.22.

[63] Bajaj L, Takai M, Ahuja R, Tang K, Bagrodia R, Gerla M. Glomosim: a scalable network simulation environment. UCLA Comput Sci Department Tech Rep 1999;990027:213.
[64] GloMoSim. Global mobile information system simulator. http://pcl.cs.ucla.edu/projects/glomosim/.
[65] Ganesh S, Amutha R. Efficient and secure routing protocol for wireless sensor networks through optimal power control and optimal handoff-based recovery mechanism. J Comput Networks Commun 2012;2012:8 Article ID: 971685.
[66] Ahvar E, Fathy M. Performance evaluation of routing protocols for high density ad hoc networks based on energy consumption by GlomoSim simulator, vol. 29. World Academy of Science, Engineering and Technology; 2007.
[67] Shoaib M, Jha NK, Verma N. A compressed-domain processor for seizure detection to simultaneously reduce computation and communication energy. In: Custom integrated circuits conference (CICC). IEEE; 2012. p. 1–4.
[68] Akhtar Md Amir Khusru, Sahoo G. Reduction in resource consumption to enhance cooperation in MANET using compressive sensing. In: Proceedings of 3rd international conference on advanced computing, networking and informatics. Smart innovation, systems and technologies, vol. 44. Springer; 2015. p. 169–83.

**Dr. Mohammad Amir Khusru Akhtar** is an Assistant Professor in the Department of Computer Science & Engineering, Cambridge Institute of Technology, Tatisilwai, Ranchi, Jharkhand, India. His research interest includes mobile ad-hoc network, parallel and distributed computing and cloud computing. He is the author of over 17 peer-reviewed publications. He received his Ph.D. from the Department of Computer Science & Engineering at Birla Institute of Technology, Mesra, Ranchi, India, in 2015. He received his M. Tech degree from the Department of Computer Science & Engineering at Birla Institute of Technology, Mesra, Ranchi, India, in 2009.

**Dr. G. Sahoo** received his M.Sc. in Mathematics from Utkal University in the year 1980 and Ph.D. in the Area of Computational Mathematics from Indian Institute of Technology, Kharagpur, in the year 1987. He has been associated with Birla Institute of Technology, Mesra, Ranchi, India, since 1988, and currently, he is working as a Professor and Head in the Department of Information Technology. His research interest includes theoretical computer science, parallel and distributed computing, cloud computing, evolutionary computing, information security, image processing and pattern recognition.