Wireless Networks (2019) 25:2697–2721
https://doi.org/10.1007/s11276-019-01988-7

E^2SR^2: An acknowledgement-based mobile sink routing protocol with rechargeable sensors for wireless sensor networks

Bharat Bhushan[1] · Gadadhar Sahoo[1]

Published online: 12 April 2019

Abstract
The advances in hardware manufacturing technologies and wireless communications enabled the evolution of tiny, multi-functional, low-power and resource constrained sensor nodes (SNs) for wireless sensor networks (WSNs). SNs located in sinks vicinity, deplete their batteries quickly because of concentrated data traffic near the sink, leaving the data reporting wrecked and disrupted. In order to mitigate this problem, mobile sinks are introduced that provide uniform energy consumption and load balanced data delivery through the sensor network. However, advertising the mobile sinks position information brings forth additional overhead in terms of energy wastage. Recently, an energy-efficient distributed mobile sink routing protocol named ring routing has been proposed aiming to mitigate the introduced overhead. In this present work, we propose an Energy Efficient Secured Ring Routing (E^2SR^2) protocol which is an enhancement of existing ring routing protocol [62] that considers rechargeable sensors to be deployed in the sensing region and employs Maximum Capacity Path (MCP), a dynamic load balanced routing scheme for load balancing and prolonging the networks lifetime. Furthermore, we use 2ACK scheme that serves as an efficient mechanism for detecting the routing misbehaviour and simultaneously enhance the security. Finally, the proposed protocol was simulated by varying the sink speed for similar node deployments and the results obtained confirm that the proposed E^2SR^2 achieves improved performance than the existing protocols such as LBDD (Line Based Data Dissemination), rail road and ring routing.

Keywords Security · Attacks · Vulnerabilities · LBDD · Rail road · Ring routing · Mobile sinks · Data dissemination

1 Introduction

Energy efficiency and security are the two most crucial issues in wireless sensor networks (WSNs) majorly because of the limited battery supply to the sensor nodes (SNs) and open broadcast nature of the medium. WSNs must be in operable condition for an adequately longer period without any human intervention as battery replacement of these SNs demands considerable effort [1, 2]. Packet forwarding approach in traditional WSNs is converge-cast in nature and results in more data traffic in the sink's vicinity. Therefore, nodes residing in the sink's vicinity deplete their energy earlier than normal nodes. This leads to the problem of energy hole creation thereby causing topology disruptions and sensing coverage area reduction. These may also lead to sink isolation and hindered sensor data delivery [3, 4]. Therefore, mobile sink concept is introduced that balances the traffic distribution as well as deals with constrained network resources [5]. Furthermore, mobile sinks are more challenging to compromise in comparison to the static sinks. This is because sensitive information retrieval and sink destruction requires the attacker to firstly locate and then chase down the mobile sink carrier. Furthermore, network connectivity also gets enhanced with the use of mobile sinks as these can even access the isolated network portions in order to retrieve data [6, 7]. These isolated network portions remain inaccessible in case of static sink nodes. Apart from these merits, sink mobility also brings forth the issue of sink localization that requires advertisement of the frequently

✉ Bharat Bhushan
bharat_bhushan1989@yahoo.com

Gadadhar Sahoo
gsahoo@bitmesra.ac.in

[1] Department of Computer Science and Engineering, Birla Institute of Technology, Mesra, Jharkhand 835215, India

varying sink position [8]. Therefore, an effective sink mobility routing strategy must avoid high latencies especially in case of time-critical applications, where freshness of data determines its validity [9, 10].

A typical example of sink mobility is the WSNs deployed in forest fire detection systems that incorporate numerous SNs for humidity or temperature reporting. Habitat monitoring is another application area of mobile sink. It employs a robot designated to perform the function of mobile sink that gathers data from distant located sensors in a large field [11]. Also, sensors employing mobile sinks monitor as well as detect the enemy vehicle or enemy troops movement and unmanned aerial vehicles (UAV) in the case of battlefield scenario [12]. Sink mobility is shown in Fig. 1 in which the sink gets relocated from its original position to a new position.

The advertisement of sink position to the entire network is the major problem for any mobile sink routing protocols. Flooding is the simplest and easiest solution proposed to address this issue. However, this introduces high overhead because of frequently happening broadcasting communications that causes increased energy consumption. Battery powered sensors is a solution to this energy consumption and lifetime issue. However, it is not desirable to have such sensors for long-term applications. Therefore, energy harvesting technologies needs to be incorporated with the sensors to enable the perpetual operations where every sensor is capable of harvesting energy from the surroundings and storing it in the battery [13]. Mostly researchers have considered static sink nodes along with rechargeable sensor nodes (RSNs) which is not that advantageous as the amount of energy harvested is limited for static sinks. This leads to declined network performance and unbalanced traffic distribution [14]. Therefore, energy harvesting technologies must be incorporated in mobile sink data dissemination protocols such as ring routing protocol [15, 16].

Further, the malicious adversary can access the entire network from a distant location and place their own nodes into the distributed and uncontrolled environment [17]. Also, as the battery power is a major concern for WSNs, a selfish node may attempt to benefit from normal nodes but deny sharing its own resource [18]. Protecting of sensitive data being sent through the wireless medium in presence of various attacks as well as maintaining security principles such as confidentiality, integrity, authentication and non-repudiation is a challenging task [19–24]. The existing ring routing protocol did not consider the security aspect of WSNs. This again is an important issue that motivates us to design an energy efficient and secured mobile sink routing protocol that also considers rechargeable sensors.

In this paper, an Energy Efficient Secured Ring Routing (E^2SR^2) protocol is proposed to incorporate the two above cited aspects: Energy harvesting and Security. The main purpose of the work is to enhance the existing ring routing protocol discussed in [62] by considering rechargeable sensors and incorporating energy harvesting technologies. The proposed Energy Efficient Secure Ring Routing (E^2SR^2) protocol employs Maximum Capacity Path (MCP), a dynamic load balanced routing scheme for load balancing and prolonging the networks lifetime. Furthermore, we use 2ACK scheme that serves as an efficient mechanism for detecting the routing misbehaviour and simultaneously enhance the security. Novelty of the proposed work lies in the fact that rechargeable sensors and energy harvesting technologies have not been incorporated in the ring routing protocol to the best our knowledge. Apart from this we also consider the enhancement of the security. The major contribution of this paper is summarized as follows.

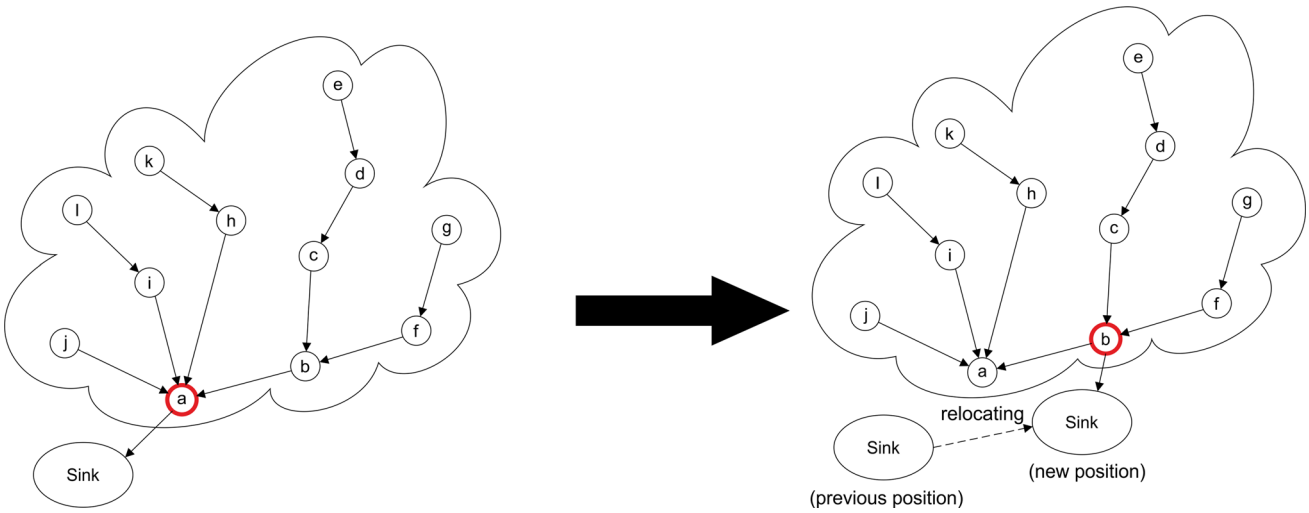

Fig. 1 Sink mobility

1. Security aspect of hierarchical routing protocol with mobile sinks is addressed from a different angle. A specialised attack model is constructed that is comprised of blackhole attack, grey-hole attack and identity attack. The performance of existing data dissemination protocols such as LBDD, rail road and ring routing under the constructed attack model is analysed.
2. A novel hierarchical protocol with mobile sink named E^2SR^2 is proposed. It is targeted for large scale WSNs with a mobile sink and numerous stationary nodes.
3. E^2SR^2 supports a virtual ring structure that facilitates easy delivery of fresh sink positions to the ring. The ring nodes are capable of switching their roles with the regular nodes owing to such structure. This mitigates the hotspot problem, one of the most serious issue involving mobile sinks.
4. The proposed E^2SR^2 protocol considers rechargeable sensors and incorporates energy harvesting technologies in ring routing, an existing data dissemination protocol.
5. In order to prolong the networks lifetime and achieve load balancing, E^2SR^2 employs Maximum Capacity Path (MCP), a dynamic load balanced routing scheme.
6. E^2SR^2 use 2ACK scheme that serves as an efficient mechanism for routing misbehaviour detection and also mitigates the adverse effect of several prominent attacks in WSNs.

The remainder of the paper is organised as follows. Section 2 presents the literature review on various hierarchical routing protocols that employs mobile sink. The existing routing protocols including LBDD, rail road and ring routing chosen for comparison with the developed E^2SR^2 protocol is elaborated in Sect. 3. Attack model under consideration is elaborated in Sect. 4. Section 5 presents the proposed E^2SR^2 protocol. Section 6 highlights the experimental setup along with the considered simulation parameter values. The obtained results are detailed and elaborated in Sect. 7 followed by conclusion and open future research challenges in the field of routing security in WSNs in Sect. 8.

2 Related work

In recent years, several research works have addressed numerous issues that indirectly or directly influence our investigation. Few of the most relevant works among them are highlighted in this section covering subjects related to hierarchical mobile sink routing protocols, load balanced routing and energy harvesting techniques in WSNs.

2.1 Hierarchical mobile sink routing protocols

Many routing techniques have been proposed in order to overcome the problems of WSNs with mobile sinks. Hierarchical mobile sink routing mitigates the load of network wide sink position advertisement by establishment of hierarchy among nodes thereby assigning varied roles to various nodes. SNs present in the overlay forms the higher tier whereas remaining nodes account for the low tier. Initially the former obtains the position of the sink and then later on the low tier nodes queries them. Therefore, for a hierarchical approach to be successful, easily reachable structure needs to be employed and countermeasures needs to be proposed against hotspot problems. Another approach is a non-hierarchical routing that employs mechanisms like overhearing, flooding or exploiting geometric properties for advertising the sinks position [25, 26]. The most influential hierarchical routing protocols based on sink mobility are reviewed in the section below.

Zhang et al. [27] proposed Two-Tier Data Dissemination (TTDD), a flooding-based approach, where every SNs possessing the data forms a rectangular grid and makes itself the crossing point of the grid. The employed grid structure reduces the overall communication overhead that might be caused due to the location updates. Kweon et al. [28] proposed Grid-Based Energy-Efficient Routing (GBEER) scheme in which the data requests and data announcements are propagated in different manner. The data announcements are propagated in horizontal direction whereas the data requests are propagated along the shared grid in vertical direction. Erman et al. [29] proposed a honeycomb tessellation based virtual infrastructure, a hexagonal grid structure that provides a shorter sink and data advertisement routes in comparison to the rectangular grids. Lin et al. [30] proposed Hierarchical Cluster-based Data Dissemination (HCDD) protocol that used clustering techniques instead of grid strategy for determining the high-tier nodes. The higher-level structure is formed by the cluster heads (CHs) that are responsible for accumulation of the global information. Valois et al. [31] proposed a Dynamic Directed Backbone (DDB) that consists of high-tier structured backbone. It comprises of two types of nodes, namely the gateway and the leader nodes. The sink is connected to the backbone which is responsible for data dissemination. In case the nodes in the backbone structure switches its role with the normal nodes, there is relatively less overhead as it requires only the immediate neighbours to be informed. Li et al. [32] proposed Grid-based Directed Diffusion method (GDD) in which small clusters are formed on the basis of virtual grids set up in accordance with the routing fidelity. The entire network is subdivided into several virtual grids with the grid header leading the

responsibility of broadcasting interest message. This reduces the broadcast overhead resulting in decreased energy consumption as well as delay. Xing et al. [33] proposed Minimum Energy Rendezvous Planning (MERP) protocol for data collection using mobile sink in an efficient manner. It selects a set of nodes responsible for buffering the source data and uploading them to the sink using single-hop routing. Vecchio et al. [34] proposed density-based data dissemination Protocol (DEEP) protocol that reduces storage as well as the communication overhead. It uses probabilistic flooding or random walk approach for propagation of data packets from the source. Kim et al. [35] proposed Virtual Line-based Data Dissemination (VLDD) for reliable data dissemination. VLDD shows both type of mobility for data dissemination namely the group mobility in which the mobile sink groups use collective moving technique in order to change the group region and individual mobility in which the sink moves individually within the group region.

The above discussed routing protocols are compared in terms of their merits and demerits in Table 1.

2.2 Load balanced and energy efficient routing

In order to conserve the battery power of nodes and balance the overall energy consumption in a sensor network, designing an energy efficient routing scheme is needed. Li et al. [36] proposed Enhanced Dynamic Source Routing (EDSR) that employs Route Maintenance based-on Energy Threshold (RMET) and Route request Delay Transmit (RRDT). RMET evenly distributes the energy consumption among nodes and RRDT prevents the selection of low residual energy nodes for the purpose of routing. On the basis of residual battery capacity, EDSR achieves balanced energy consumption thereby enhancing the networks lifetime. Collotta et al. [37] proposed dynamic load balancing technique for industrial WSNs that counters the unbalanced load caused due to fluctuating channel characteristics and mobile nodes. LEACH [38] divides its operational time into several rounds and the nodes are elected as CHs in every round on the basis of a predefined criteria. In [39], Li et al. proposed to regulate the time length for every round in order to enhance the throughput and lifetime of the network. The time length of every round is increased to decrease the overhead in the set-up phase. However, this increase in time length leads to increased energy consumption of CHs thereby decreasing the networks lifetime. Collotta et al. [40] proposed a distributed load balancing scheme that distributes network load among all stations for industrial IEEE 802.11 wireless networks. Li et al. [41] proposed Blind Cooperative Communications (BCC) that allows cooperation among nodes for achieving spatial

Table 1 Comparison of various routing protocols

Routing protocols	Merits	Demerits
TTDD [27]	It divides the entire deployed area into grids therefore enabling the queries to be resolved by the grids. This reduces the communication overhead in comparison to flooding-based approach	The performance of TTDD falls dramatically for applications such as large-scale networks as it increases the overheads involved in the construction and maintenance of the grid overlay
GBEER [28]	TTDD involves huge overhead in construction of separate grid for each source node which is eliminated by GBEER	SNs that reside on the grids in GBEER are more prone to become hotspots
HexDD [29]	It reduces the redundant data propagation by preventing the propagation of such queries from the sink to the entire grid	HexDD faces the problem of hotspots
HCDD [30]	It does not involve construction and maintenance of an infrastructure for every source node thereby saves the communication overhead	This leads to decreased network lifetime
DDB [31]	It incurs minimal overhead in case of change in the backbone structure for avoiding hotspots	This introduces redundancy in the sink data queries
MERP [33]	It achieves a trade-off between the data latency and energy efficiency	It consumes more energy therefore nodes die out early
DEEP [34]	It does not rely on the location information of the SNs. These make it suitable for real-world applications	In case of larger networks, DEEP shows scalability issues
VLDD [35]	It shows decreased energy consumption as it reduces the number of hops counts between the VLS and the sink by proper selection of next-hop nodes	In case of increase in the radius size, the distance between the VLS and the sink also slowly increases thereby decreasing the packet delivery ratio (PDR)

diversity gains in a multi-hop wireless network. In [42] Li et al. proposed to enhance the energy efficiency and system capacity by jointly optimizing the serving range and positions of relay nodes in the cellular networks. Collotta et al. [43] proposed dual fuzzy controller-based approach that dynamically regulate the transmission power and sleeping time to improve the power consumption of the network. Collotta et al. [44] proposed Bluetooth Home Energy Management Scheme (BluHEMS) that addresses the impact of high-power loads during peak hours and standby appliances on the power consumption charges. BluHEMS efficiently reduces the peak load demand thereby reducing the overall power consumption charges. In [45], Li et al. proposed Cooperative Spectrum Sharing with Energy-save (CSSE) to enhance the spectrum efficiency while maintaining the communication QoS by cooperatively sharing the spectrum. A two level Stackelberg game theory is employed for transaction between multiple relaying secondary transmitters (STs) and the primary transmitters (PT) where the STs are the followers and the PTs are the leaders. Collotta et al. [46] proposed fuzzy-based data fusion schemes for clustered WSNs to reduce the overall energy consumption of the network.

2.3 Energy harvesting routing approaches

Recently, issues of unbalanced traffic distribution and inadequate network resources in WSNs is efficiently being solved by employing mobile sink. Thus, optimal data gathering with mobile sinks has drawn huge research interests. For rechargeable WSNs, data gathering problem needs to be designed in distributed and online manner. Hence most data gathering techniques designed for battery powered WSNs with mobile sink is not feasible for rechargeable WSNs with mobile sink [47–49]. Chen et al. [50] considered the problem of network utility maximization and developed a low complexity routing and energy allocation scheme. Guo et al. [51] proposed a distributed algorithm to fine-tune routing, link scheduling and data rates on the basis of current energy replenishing state of nodes. In [52], Zhao et al. proposed a framework to jointly optimize data gathering and mobile energy replenishment. Andrea et al. [53] proposed a global power management scheme based on a joint transmission power control and duty-cycle optimization for energy harvesting WSN. In [54], authors proposed piezoelectric nanogenerator based energy harvesting technology to supply power to nanosensors that cannot be charged using conventional energy harvesters. Ting et al. [55] considered both energy efficient sensing as well as routing in unreliable energy harvesting WSNs. In [56], authors proposed energy aware opportunistic routing scheme for large scale WSNs. In [57], authors proposed to use receiver-initiated communication capable of regulating the active and sleep periods by introducing an energy threshold policy. This resulted in decreased duty-cycle and balanced energy harvesting ability and energy consumption by each node in the network. Several works related to data gathering optimization considered uncontrolled harvested energy. Ren et al. [58, 59] proposed an online distributed solution as well as an offline algorithm for maximizing data collection using single hop data transmission for rechargeable sensor networks employing mobile sink. However, this results in limited network performance due to use of one-hop data transmission. Thus, the proposed E^2SR^2 considers the problem of data collection with multi-hop data transmission for improvement in data gathering performance.

3 Existing data dissemination protocol

In this section we explore three existing area-based data dissemination routing protocols that employs mobile sink. LBDD [60], Railroad [61] and Ring routing [62] are the data dissemination techniques that are chosen for the comparative analysis with the proposed protocol. These protocols are the most efficient as compared to the above discussed protocols since they alleviate the problems of hotspots by utilizing its huge areas and distributing the load over various nodes. Considering the advantages of these protocols, they are the right candidate for performance comparison with the proposed E^2SR^2. These protocols are explored in the section below.

3.1 LBDD

The entire sensor field is divided into two portions with the help of virtual vertical line of width w. The line is again split into equal sized groups of size g. The scalability issue and the hotspot problem are the two problems that are addressed by these parameters. In order to ease the access for all the nodes, the line is placed at the central portion of the field. The nodes are categorized into two types. The *inline nodes* that lie within the boundary of the wide line and the remaining nodes are *ordinary nodes*. The wide line serves as a rendezvous region for lookup as well as data storage. The LBDD protocol works under several assumptions. Firstly, every node is aware of its geographic location or the network boundaries. Secondly, GPS or any other virtual coordinate system are used for finding the SNs position. LBDD operates basically in two steps. First is the *data dissemination step* in which data generated from any general SN is transmitted to the closest inline node. Second is the *data collection step* in which the sinks query the line for retrieving any specific data. It uses two different data

storage schemes in order to ease the data lookup process. Under high traffic loads, there is an abrupt increase in congestion therefore there is a need of fine-tuning the value of g and w in the first step. The second step involves group leader election and periodic replication.

Why LBDD? It lowers the data dissemination cost due to existence of huge virtual infrastructure that facilitates the distribution of communication load amongst the nodes placed in the rendezvous area. In order to mitigate the hotspot problem, the line needs to be wide enough. A wider line leads to increased energy consumption due to flooding in large networks. Due to these reasons LBDD is a strong candidate for comparison with the proposed E^2SR^2 protocol [60].

3.2 Railroad

Railroad exploits the networks geographical shape and constructs a single rail in the network placed at a convenient position making it easy for every node to access the rail. Railroad using this rail, implements an energy-efficient and scalable data dissemination protocol considering dynamic conditions having several mobile observers and targets. A globally unique virtual infrastructure called rail consists of *rail nodes*. Whenever an event is generated by the source, the corresponding metadata is sent to the closest located station and every node in the station are called *platform nodes*. The four phases involved in railroad are rail construction, event notification, querying and data delivery phase. These phases are described in the section below. The process of rail construction is carried out only during the network setup phase. This can be done by adopting a central server but this solution is not feasible for large WSNs because of scalability issue. Therefore, a completely distributed construction algorithm is required where every node is aware of its distance from the centre as well as the nearest boundary node distance. Whenever an event is detected by nodes, it stores the sensed data and informs the rail via notification message including the metadata such as event summary and its location. Information is retrieved by the sink by sending queries. Once the query notification message is received, the source needs to send relevant data message towards the sink [61].

Hot spot complexity In few data centric storages, majority of messages converge towards a few home nodes. Therefore, in order to prevent the home nodes from getting exhausted, several replicas of the home nodes are prepared. This replica technique reduces the huge burden on the home nodes however the replication cost as well as the total energy consumption is always an added overhead. In railroad, every event summaries and queries are sent to the rail and a wide rail is designed to enhance the lifetime of the network. This prevents very few rail nodes to fall victim to the hot spot problem. The complexity of the hotspot messages of railroad (H_{Rail}) can be estimated as [61].

$$H_{Rail} = \frac{S}{N_R}\left[\left(rp_cN_{ST} + up_qN_{RT}\right) \times Req + \left(up_qN_{RT} + rp_c + rp_q\right) \times S\right] \quad (1)$$

where N_{ST}, N_{RT}, and N_R represents the total number of platform nodes at any station, number of nodes in which query faces single tour and the number of rail nodes respectively. Req denotes the energy requirement for receiving one-bit data while S represents the energy requirement for transmitting one-bit data. r represents the number of events and u represents the number of queries for every event. p_c, p_d and p_q represents the number of control messages, data reply messages and query messages respectively. In case of data centric storage, the complexity of the hot spot message of the home nodes $(H_{DataCentric})$ can be estimated as [61].

$$H_{DataCentric} = \left[rp_d + \frac{1}{\gamma}up_q\right] \times Req + \left[\frac{1}{\gamma}rp_d\right] \times S \quad (2)$$

where γ represents the total number of nodes including the home nodes in a replica set. Number of replicas is equal to $(\gamma - 1)$ in a home node. If γ is equal to 1, then it can be inferred that there are no replicas and only one single home node exists.

Why railroad? Railroad is chosen for comparison with our proposed protocol because of its strength in terms of extending networks lifetime as well as reducing the energy consumption. Also, railroad overcomes the issues of hot spot and thereby prevents the rail from forming a bottleneck.

3.3 Ring routing

Ring routing divides the SNs into three categories namely *anchor nodes, ring nodes* and the *regular nodes*. It works on the following basics: (1) sink position is advertised to the ring (2) sink position is obtained by regular nodes from the ring (3) nodes that disseminate their data with the help of anchor nodes serves as an intermediate link connecting sink and the network [63, 64]. The coordinates of the centre point of the network needs to be known by all SNs and is encapsulated by the ring structure at all times. Various phases of ring routing protocol is described in the section below.

3.3.1 Ring construction

Once the WSN is deployed, the ring construction mechanism initiates. Firstly, the initial ring radius is specified. Greedy approach is used for selecting the ring nodes and to complete the closed loop. If the closed loop is not formed, the ring node selection is repeated with a different set of neighbours. If still the ring cannot be formed, then the value of the ring radius is changed. The initial process of ring construction is energy efficient and straight-forward therefore does not require any centralized decision entity.

3.3.2 Sink position advertisement

Once there is change in the position of the sink, it selects a different set of anchor nodes (ANs) that are primarily responsible for managing the communication between the normal nodes and the sink. Initially the closest node that possess highest SNR value is chosen by the sink and then the sink broadcasts the selection packet. The sink selects new ANs before leaving the communication range of the previous AN and informs the previous AN about the MAC address and the position of the new AN. Old AN has the information about the location of the new AN, therefore, it relays any data towards to the new AN whereas, the new AN directly relays data towards the sink. This process is "*follow-up mechanism*". Once the source node receives the location information of the current AN, it sends the data to the sink via geographic forwarding thereby completing the process of data dissemination. During this phase, location information and the MAC address of the newly selected ANs is delivered to the ring. The new AN sends ANPI packet towards the centre of the ring. The ring node upon receiving these packets share this information to its anti-clockwise and clock-wise ring neighbours. This enables all the ring nodes to be aware of MAC address and the position of the new AN, thereby completing the sink position advertisement to the entire ring.

3.3.3 Determining the position of the sink from the ring and data dissemination

Any node possessing data, needs to obtain the location of ANs before transmitting its data towards the sink. Ring stores the fresh location of these ANs which can be retrieved using the ANPI packets. Source nodes send ANPIREQ packet to the ring. The ring nodes upon receiving the ANPIREQ, transmits them towards the source which contains the current position of the ANs. A node gets the position of ANs, once it receives ANPIREP to its ANPIREQ. In case the data is received by the old AN which has already changed its role, the follow-up mechanism is initiated and the data is disseminated to the new AN [62].

3.3.4 Ring change

Ring nodes need to handle more traffic and therefore must switch roles with the normal nodes periodically. This switching of roles could be done periodically or could be triggered by the battery threshold. Every ring is independent in switching roles with the normal nodes. During the ring change process, two property needs to be preserved namely *network centre encapsulation property* and *the closed loop property.* In order to preserve these, a geometric check needs to be done after the ring candidates' election. The ring node informs their new role to the ring candidates by broadcasting ring change packets [62].

4 Attack model

WSNs is susceptible to several types of attacks. These can be categorized into internal and external attack. Attackers in external attack does not have control over the nodes and they eavesdrop on the information or inject data in order to disrupt the normal network operation. Attackers in internal attack captures the node and therefore can launch wide range of attacks. In this work, we consider the attack model that comprise of blackhole attack, grey-hole attack and identity attack. The effect of these attacks on the performance of various routing protocols are evaluated later in the paper. The considered attack model is elaborated below.

4.1 Blackhole attack

It is a type of denial of service attack where a malicious node advertise itself as the most optimal path to the destination. With the propagation of this message, increased amount of traffic gets directed towards this malicious node. A typical blackhole attack involves two routing packets: Route Reply (RREP packets) and Route Request (RREQ packets). The broadcasted RREQ packets holds the destination address of all network nodes. Upon receiving such packets, nodes respond directly to the original sender using RREP. The attackers upon receiving RREQ, replies immediately to the source node with RREP claiming to possess the most optimal route to the destination. Furthermore, the source node also receives the blackholes RREP before the original correct RREP packets. Therefore, source sends data packets by selecting the first RREP packet and discards the subsequently received RREP packets. This leads to packet dropping thereby degrading

Table 2 Attack model of blackhole attack

1. **Initialisation**
2. SN → Sensor Node
3. N → Network size
4. BS → Base station
5. CH → Cluster Head
6. x → integer such that [0 < x < (N − 1)]
7. **BEGIN**
8. ∀ SN_i, 0 < i ≤ N, Compute random r_{SN} and T (SN_i),
9. **if** (r_{SN} < T (SN_i)) **then**
10. SN_i = Cluster Head
11. **else**
12. SN_i = Cluster Member
13. **end**
14. ∀ CH_j, j ∈ Cluster heads list
15. CH_j broadcasts (ADV_CH) advertisement messages
16. Few cluster members(x) join CH_j
17. CH_j generates TDMA schedule
18. Cluster members send packets within the TDMA time slot to CH_j
19. **if** CH_j = malicious node **then**
20. Drop all the packets
21. **else**
22. Aggregated data is sent to BS
23. **END**

Table 3 Attack model of grey-hole attack

1. **Initialisation**
2. N → Network size
3. CH → Cluster Head
4. BS → Base station
5. N → Sensor Node
6. x → integer such that [0 < x < (N − 1)]
7. **BEGIN**
8. ∀ SN_i, 0 < i < N, Compute random r_{SN} and T (SN_i),
9. **if** (r_{SN} < T (SN_i)) **then**
10. SN_i = Cluster Head
11. **else**
12. SN_i = Cluster Member
13. **end**
14. ∀ CH_j, j ∈ Cluster heads list
15. CH_j broadcasts (ADV_CH) advertisement messages
16. Few cluster members(x) join CH_j
17. CH_j generates TDMA schedule
18. Cluster members send packets within the TDMA time slot to CH_j
19. **if** CH_j = malicious node
20. Drop selected packets randomly
21. **else**
22. Aggregated data is sent to BS
23. **END**

the overall networks performance [65, 66]. Table 2 presents the attack model of blackhole attack.

4.2 Grey-hole attack

It is an advanced version of blackhole attack that fools the monitoring system and the source by employing partial data forwarding. The adversary in such attack participates in the route discovery phase and updates the routing table. This attack makes a distant situated source node to consider the attacker to be its next hop neighbour. The malicious node captures all the incoming packets and drops them on a random basis. This mechanism makes the attack detection difficult, as sometimes random packets may also be dropped by normal nodes due to network overhead or congestion. Typically, it can be implemented in two phases: In the initial phase, vulnerabilities associated with the routing protocols are exploited in order to update the source routing table. This phase diverts the data route towards the attacker rather than normal route. In the second phase, interrupted packets are dropped in some probability by the attacker [67, 68]. Table 3 presents the attack model of grey hole attack.

4.3 Identity attack

This attack facilitates a malicious user in the network to hijack application requests. In identity attack, malicious nodes forge many identities in order to trick the network. These obtain several identities and behave like independent nodes in the network. Due to multiple identities, adversary can defeat the routing mechanisms that use disjoint paths. One node can participate only once in activities such as polling and reputation calculation but the fraud node can participate for several number of times thereby can win the voting. Whenever a legal node distributes a certain task among other network nodes, the adversary node executes the assigned task alone utilizing multiple identities and delays the result. The network performance is significantly reduced by defeating fault-tolerant and group-based voting schemes such as distributed storage, redundancy mechanism and multipath routing [69, 70]. Table 4 presents the attack model of identity attack.

Table 4 Attack model of identity attack

1. **Initialisation**
2. N → Network size
3. CH → Cluster Head
4. BS → Base station
5. SN → Sensor Node
6. x → integer such that [0 < x < (N − 1)]
7. **BEGIN**
8. ∀ SN_i, 0 < i < N, Compute random r_{SN} and T (SN_i),
9. **if** (r_{SN} < T (SN_i)) **then**
10. SN_i = Cluster Head
11. **else**
12. SN_i = Cluster Member
13. **end**
14. ∀ CH_j, j ε Cluster heads list
15. CH_j broadcasts (ADV_CH) advertisement messages
16. Few cluster members (x) join CH_j
17. **if** CH_j = malicious node **then**
18. CH_j performs attack using a TDMA schedule and provides all nodes with the same time slot for sending data
19. **else**
20. CH_j generates normal TDMA schedule
21. **end**
22. Few Cluster members send packets to CH_j within the TDMA time slot
23. Aggregated data is sent to BS by CH_j
24. **END**

5 Proposed model

In this paper, a novel E^2SR^2 protocol for WSNs with rechargeable sensors and mobile sink is proposed. SNs in mobile sink hierarchical routing protocols needs to transmit the sensed data to the mobile sink for further processing consuming some extra energy in the process. Battery powered SNs are not suitable for long-term applications therefore sensors needs to be powered with energy harvesting technologies thereby enabling perpetual operations. In this work, we enhance the existing ring routing protocol [62] by incorporating our proposed energy consumption and data transmission model that considers rechargeable and energy harvesting sensors [71]. The proposed E^2SR^2 uses MCP that allows to alter the routing path after every round on the basis of the residual energy of the nodes in the routing path thereby resulting in balanced load for all SNs and enhancing the networks lifetime [72, 73]. In presence of the above presented attack model, there is a significant decrease in the performance of existing data dissemination protocols. Therefore, in order to enhance the security of the proposed protocol, 2ACK scheme is used [66, 74]. 2ACK is a network layer approach for detecting and mitigating the effects of misbehaving links and is implemented as an add-on to the ring routing protocol. These enhancement modules are detailed in the section below.

Assumptions Several Ideal Constraints (ICs) are utilized in order to simplify the experimental calculations. These ICs are listed below.

IC1 All SNs have knowledge of their own position. This information about the position of the nodes according to deployment area is based on local or global geographic coordinate system.
IC2 All SNs must have knowledge of their neighbour. This can be obtained using neighbour discovery protocol for enabling the greedy geographic routing.
IC3 The coordinates of the network centre must be known by every SNs and must be encapsulated by a ring structure at all times. This allows easy access to ring by the sink as well as the regular nodes.
IC4 Event generation probability over the network can be random or uniform.
IC5 SNs can alter its transmission range by varying the data transmission path and also their transmission power.

The following Table 5 lists the abbreviations used in this paper.

5.1 Optimal data gathering and recharging module

E^2SR^2 considers energy harvesting sensors as the battery powered sensors are not suitable for long-term applications. We consider Rechargeable Sensor Nodes (RSNs) consisting of N rechargeable sensors and a mobile sink deployed in the sensing area. Due to limited analysis and data pre-processing ability of sensors, these transmit the sensed data directly or in multi-hop fashion to the mobile sink. Every sensor consumes constant energy, E_i^s, in sensing its environment periodically. The total amount of data that one sensor sends indicates the monitoring performance of the network therefore better monitoring performance is indicated by increased data reporting. The proposed energy consumption model and the data transmission model of E^2SR^2 is detailed in the section below.

5.1.1 Energy consumption model

Sink movement is assumed to be along a predefined straight path in order to collect the sensed data periodically from all sensors. We consider rechargeable sensors that are powered by rechargeable batteries and solar cell. Generally, the solar energy harvesting cycle is of one day. In this work, we consider one day as any single period. Let Kth period denoted as K be divided into T slots. Let tth *slot* be

Table 5 List of abbreviations

Abbreviations or notations	Meaning or description
$B_i^{initial}$	Initial energy content of the sensor node i
$B_i^{capacity}$	Battery capacity of the sensor node i
$\rho_i(t)$	Energy harvested or collected at time slot t by sensor i
$P_i(t)$	Energy consumed at time slot t by sensor i
$B_i(t)$	Energy content of the sensor i at time slot t
$E_{ij}^{transmission}$	Energy consumed by sensor i in directly transmitting data to its one hop neighbour j
$E_{ij}^{threshold}(t)$	Threshold for the energy consumed by sensor node i in directly transmitting data to its one hop neighbour j at time slot t
$E_{is}^{transmission}$	Energy consumed by sensor i in successfully transmitting data to the sink s
$d_{ik}(t)$	Euclidean distance between the two sensors i and k
α	The path loss exponent
β	Distance-independent term
μ	Distance-dependent term
N	Number of nodes
$N_{density}$	Density of nodes
N_{TC}	Number of nodes lying within the transmission circle
R	Transmission range of nodes
H	Average hop counts between the source and the destination
L	The average progress in every hop
p_r	The probability of routes having a minimum of one misbehaving node
p_m	Probability of the routers to misbehave
$F(r)$	The probability that all the N_{Tc} nodes resides within the distance r from the centre
$f(r)$	Progress probability density function

denoted as t such that $t = 1, 2, 3, 4, \ldots T$. Denoting battery capacity of the ith sensor node by B_i, its capacity which is assumed to be large enough so as to store all the harvested energy can satisfy the condition

$$B_i^{capacity} \geq B_i^{initial} + \sum_{t=1}^{T} \rho_i(t) \tag{3}$$

The energy content of the battery at time slot $(t + 1)$ for sensor i can be estimated as $B_i(t + 1)$.

$$B_i(t+1) = B_i(t) + \rho_i(t) - P_i(t) \tag{4}$$

Energy consumed in transmission of one-unit data from sensor i to sensor j located at one hop distance at time slot t can be estimated as

$$E_{ij}^{threshold}(t) = \beta + \mu\big(d_{ij}(t)\big)^{\alpha} \tag{5}$$

where α represents the path loss exponent (for free space radio communication value of α varies such that $2 \leq \alpha \leq 4$), β represents distance-independent term and μ represents distance-dependent term. The euclidian distance between the next hop j and sensor i is represented by $d_{ij}(t)$. Equation 5 proves $E_{ij}^{threshold}(t)$ to be an increasing function of $d_{ij}(t)$. It is assumed that the energy consumed during transmission of data is constant in one period [75]. Also, in order to successfully transmit one-unit data to sensor j located at next hop directly, sensor i must satisfy $E_{ij}^{transmission} \geq E_{ij}^{threshold}(t)$. Since the Euclidean distance between the two sensors i and k are fixed, the threshold for the energy consumed during transmission, $E_{ik}^{threshold}$, is constant and can be estimated as

$$E_{ik}^{threshold} = \beta + \mu(d_{ik}(t))^{\alpha} \tag{6}$$

Because of sink movement, the Euclidean distance between the sink s and the sensor i, $(d_{is}(t))$, changes with slot t. Therefore, the threshold for the energy consumption during transmission also varies for varied time slots and can be estimated as

$$E_{is}^{threshold}(t) = \beta + \mu(d_{is}(t))^{\alpha} \tag{7}$$

Let $\underline{t_i}$ represent the earliest time slot after which the sensor i is capable of transmitting data to the sink and $\overline{t_i}$ represent the latest time slot after which sensor i is no longer capable of transmitting data to the sink.

Theorem 1 *For a given value of energy consumed during transmission $E_{is}^{transmission}$, in one slot, sensor i is capable of successfully transmitting data to sink s, only during slot t' where $t' \in [\underline{t_i}, \overline{t_i}]$.*

Proof Using Eq. 7, the maximum Euclidean distance between the sensor i and the sink node s can be estimated as

$$d_{is}^{max} = \left(\frac{E_{is}^{transmission} - \beta}{\mu}\right)^{\frac{1}{\alpha}} \tag{8}$$

Consider, sensor i to be the centre and d_{is}^{max} to be the radius of the circle. There are only two crossover points found between the straight road and the circle as shown in Fig. 2. Cross over points of the corresponding slots are denoted by $\underline{t_i}$ and $\overline{t_i}$. There exist three possible cases for the values of $\underline{t_i}$ and $\overline{t_i}$:

- Case 1: If $d_{is}^{max} < h_i$ then $\underline{t_i} = \overline{t_i} = \Theta$
- Case 2: If $d_{is}^{max} = h_i$ then $\underline{t_i} = \overline{t_i}$
- Case 3: If $d_{is}^{max} > h_i$ then $\underline{t_i} < \overline{t_i}$

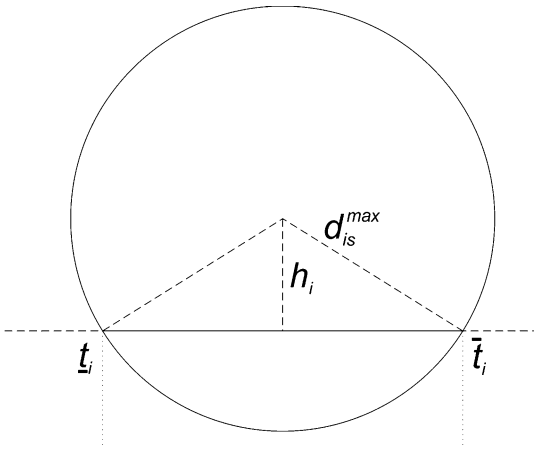

Fig. 2 Optimal data gathering and rechargeable module

where h_i represents the vertical distance between the straight road and the sensor i and Θ represents the null set. Therefore, sensor i is capable of sending data directly to the mobile sink s only if $d_{is}^{max} \geq h_i$.

Assume $y(t)$ to be an increasing function of t. Let $(y(t), 0)$ represent the mobile sink position at slot t and (y_i, h_i) represent the sensor position. Here y_i is constant and its value ranges between $y(1)$ and y_T such that $y(1) < y_i < y_T$. The euclidian distance between the sensor i and the sink s can be estimated as

$$d_{is}(t) = \sqrt{(y(t) - y_i)^2 + (0 - h_i)^2} \tag{9}$$

Equation 9 shows two inferences listed as follows.

- *Inference 1* $d_{is}(t)$ is a descending function of t if $y(1) \leq y_i$ and
- *Inference 2* $d_{is}(t)$ is a ascending function of t if $y_i \leq y_T$.

Therefore, $d_{is}(t') > d_{is}^{max}$ if $t' \langle \underline{t_i}$ *or* $t' \rangle \overline{t_i}$ and $d_{is}(t') \leq d_{is}^{max}$ if $t' \in [\underline{t_i}, \overline{t_i}]$. At any time slot t', data transmission to the mobile sink for any sensor is possible only if the Euclidean distance $d_{is}(t')$, satisfies $d_{is}(t') \leq d_{is}^{max}$ that is only possible if $t' \in [\underline{t_i}, \overline{t_i}]$.

Let $\theta_{is}(E_{is}^{tr})$ represent the upper bound on the number of slots possible between $\underline{t_i}$ *and* $\overline{t_i}$. Therefore, we have

$$\theta_{is}(E_{is}^{tr}) = \left[(\overline{t_i} - \underline{t_i}) + 1\right] \tag{10}$$

Relationship between d_{is}^{max} and $\theta_{is}(E_{is}^{tr})$ can be obtained using Fig. 2. From Fig. 2, using Pythagoras theorem, we have

$$\theta_{is}(E_{is}^{tr}) \times v = 2 \times \sqrt{(d_{is}^{max})^2 - (h_i)^2} \tag{11}$$

Equation 11 can be rewritten as

$$\theta_{is}(E_{is}^{tr}) = \left\lceil \frac{2 \times \sqrt{(d_{is}^{max})^2 - (h_i)^2}}{v} \right\rceil \tag{12}$$

The underlying MAC layer using TDMA eliminates the existence of any kind of signal interference. This work considers only the energy consumption for receiving, transmitting and sensing as these activities accounts for the maximum energy usage [48, 76].

5.1.2 Data transmission model

Sometimes the nodes may be located far from the straight path in such scenarios, significant energy may get wasted in direct data transmission to the mobile sink. In E^2SR^2, nodes located closer to the straight path, act as relay nodes and forward the sensed data thereby improving the overall networks performance. For network topology establishment, consider the vertical distance h_i and h_k. Let d_{ik} represent the Euclidean distance between the sensor i and k, whereas $h_i(h_k)$ represent the distance between the straight path and sensor i.

---

if $(h_i > h_k$ *and* $h_i > d_{ik})$
  $k \in O(i)$
else
  $k! \in O(i)$

---

where $k \in O(i)$ is the logical link that is established for transmission of data via sensor k serving as next-hop to forward data from sensor i to mobile sink s. The total energy consumed by any sensor i at a given slot t cannot exceed the sum of energy that sensor i has collected at time slot t and the reserved energy of the battery. Therefore, in any time slot t', the total energy consumed by the sensor i must always be less than the aggregated value of collected and the initial energy [71, 77].

5.2 Energy efficient load balancing module (MCP)

In this work, the WSN and residual energy of the SNs is modelled using a capacity graph $G = (V, E)$, where set E represent all the direct communications possible between the nodes and set V represent set of all SNs. Let, r represents the residual energy of each sensor, $r : V \rightarrow R^+$. s represents the sink as it possesses infinite energy or is assumed to be equipped with extremely huge capacity battery in comparison to that of the SNs. The values associated with different nodes represent the current

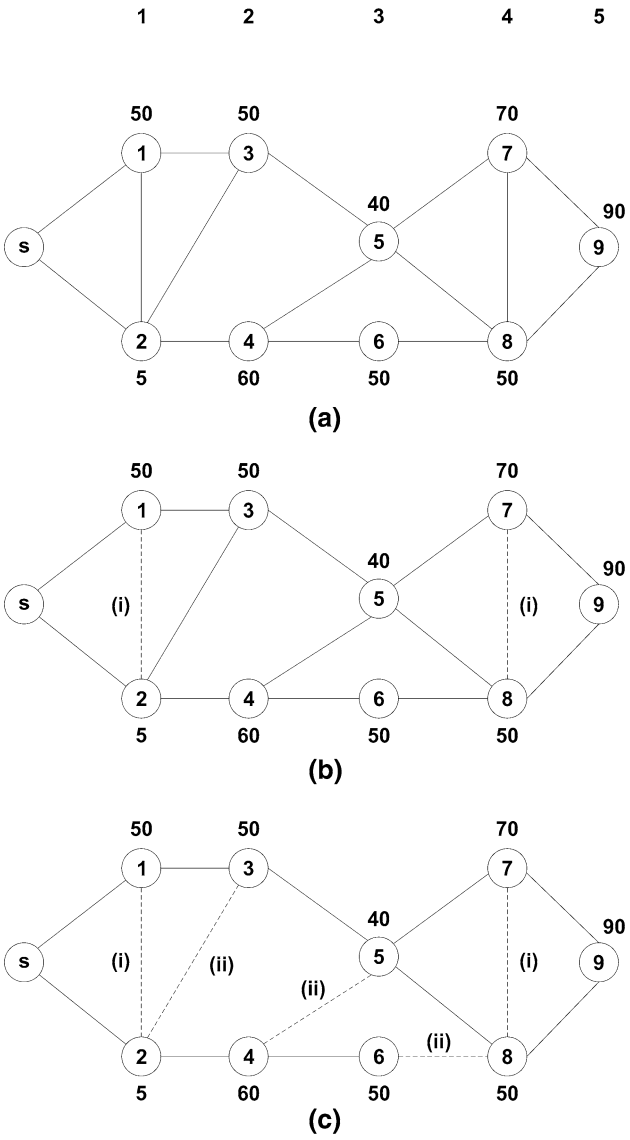

Fig. 3 Energy efficient load balancing module

residual energy of that particular node [73]. This module consists of three phases detailed in the section below.

Phase 1 A layered network, N is obtained after layering the graph G: let, L_v denote the shortest distance path length between v (any sensor node, $v \in V$) and sink node s. In Fig. 3(a), the shortest distance path length to node s from node 7 and node 8 is equal ($L_7 = L_8 = 4$). This layered network can thus be obtained from the graph G by elimination of edges $(u, v) \in Es.t.L_u = L_v$. The layered network can be obtained as follows. Initially, the sink s sets its $L_s = 0$ and all the other nodes sets its $L_u \leftarrow N_1$ such that $(N_1 > N)$. Sink broadcasts poll messages (with L_s as hop count values) to neighbours periodically. Node u upon receiving such poll messages from node v, extracts the value of L (hop count value) and conduct the following comparisons.

1. If $L > L_u - 1$, node u does no action.
2. If $L = L_u - 1$, in-bound link is established from u to v.
3. If $L < L_u - 1$, Priority to be given to source nodes and simultaneously avoid sending data to other nodes, in-bound link is established from u to v, node u sets $L_u = L + 1$ and poll message is broadcasted again to the neighbours with a new hop count value, L_u.

As shown in Fig. 3(a), $L_7 = L_8 = 4$ and $L_1 = L_2 = 1$, edges (h, g) *and* (a, b) is eliminated from G. Now the obtained layered network, N, is a directed graph obtained from G such that the directed edge (u, v) from node u to v follows $L_u - L_v = 1$ for all the remaining edges after elimination of $(u, v) \in V$. The resulting network obtained from G in Fig. 3(a) is shown by Fig. 3(b).

Phase 2 The maximum capacity path is determined for every sensor node: Assume P_{us} to be the path from node u to mobile sink s and $c(P_{us})$ be the minimum residual energy in path P_{us} such that $P_{us} = u, u_1, \ldots u_l, s$ and $c(P_{us}) = \min\{r(u), r(u_1), \ldots r(u_l)\}$. P^*_{us} is the maximum capacity path from sensor u to s amongst every possible path and this forms the message routing path. Figure 3(c) shows the maximum capacity path that is obtained from the layered graph of Fig. 3(b).

Phase 3 Routing is performed and finally the residual energy of the nodes is updated. Now if the sensor u has sensed some data or detected any abnormal event, it reports to the sink s by relaying data packets via maximum capacity path. After the message is successfully relayed to the sink, the residual energy level of every node that comes in the path is updated.

In our proposed E^2SR^2, the above three phases are repeated again and again for every transmission round until any one of the nodes dies or drains all its energy out.

5.2.1 Time complexity analysis

The two major steps of MCP is the construction of layered network and the determination of maximum capacity paths. During the construction of layered network, the determination of shortest path from node u to sink s takes $O(n^2)$ operations. The determination of maximum capacity paths involves $O(n)$ operations. Therefore, the overall time complexity of MCP is $(O(n^2) + O(n)) = O(n^2)$. The following Table 6 presents the pseudocode of MCP Scheme.

5.3 ACK scheme

Why 2ACK? 2ACK is a network layer approach for detecting and mitigating the adverse effects of misbehaving

Table 6 Pseudocode of MCP Scheme

Maximum Capacity Path Algorithm (MCP)
Input
V → Sensor nodes
E → Edges
C → Capacity of nodes
r → Residual energy of nodes
Output
Maximum Capacity Path
1. Initialisation:
2. N → Number of nodes
3. $c(P_{us})$ → minimum residual energy
4. P^*_{us} → The maximum capacity path from sensor u to s
5. BEGIN
6. $s \leftarrow i$ /*select s randomly, $i \in N$ */
7. Set $l_s \leftarrow 0$
8. Set $l_u \leftarrow N_1$ /* $(N_1 > N)$*/
9. while true do
10. Broadcast polling message
11. if polling message is received then
12. Extract l_v from polling message
13. end
14. if $(l_v > l_u - 1)$ then
15. Node u does nothing
16. end
17. if $(l_v = l_u - 1)$ then
18. Node u builds in-bound link to node v $(u \rightarrow v)$
19. end
20. if $(l_v < l_u - 1)$ then
21. Priority to be given to source nodes and simultaneously avoid sending data to other nodes
22. Node u builds in-bound link to node v $(u \rightarrow v)$
23. Set $l_u = l_v + 1$
24. Rebroadcast polling message with hop count value l_u
25. end
26. end
27. Obtain layered network N $suchthat L_u - L_v = 1$ for all the remaining edges
28. Allocate the edge capacity $r : V \rightarrow R^+$
29. Perform binary search to find maximum values $c(P_{us})$ of the minimum residual energy fraction for which there is a path P from u to s.
30. Return P^*_{us}
31. Change the weight of every remaining edge (u, v)
32. END

links. Several protocols such as TCP use end-to-end acknowledgement policy (ACK) for detecting malicious nodes or routing misbehaviour [78]. The out of order packets are acknowledged using selective acknowledgement (SACK) policy. 2ACK scheme is capable of detecting the malicious nodes that refuse to forward data packets even after agreeing to do so whereas the SACK and ACK measures the usefulness of the current route in order to take appropriate action [79, 80]. Also, the 2ACK does not rely on end-to end acknowledgement and efficiently handles as well as mitigates the misbehaving nodes impact. In this scheme, an event is passed to the reputation system (RS) and based on the frequency of the event, RS decides the rating of suspicious node [81]. If this rating becomes intolerable, the path manager takes control and controls the routing cache accordingly. The trust manager sends warning messages to other nodes using alarm messages. Also, the receiving node sends acknowledgement only for a small fraction of received packets therefore the employed 2ACK scheme leads to reduced routing overhead.

In this paper, 2ACK is implemented as an add-on to the existing ring routing protocol. Suppose the three consecutive nodes N_1, N_2, N_3 lie along a route in the form of a *triplet*. In general, N_1 sends packet to N_2 which forwards it to N_3. Even in absence of misbehaving nodes, there exists an ambiguity in N_1 as it has no knowledge about the successful reception of packet by N_3. The presence of misbehaving nodes deteriorates such problem even further in WSNs. In 2ACK scheme, an explicit acknowledgement is sent to N_1 by N_3 in the direction opposite to the routing path in order to notify the successful reception of packets. In $[N_1 \rightarrow N_2 \rightarrow N_3]triplet$, the node that serves as the receiver of the 2ACK packets is *observing node* (N_1) and N_3 serves as 2ACK *packet sender* as shown in Fig. 4. The observing nodes maintains a data structure corresponding to $[N_2 \rightarrow N_3]$ and increments the countervalue for the forwarded data packets (C_{pkts}) simultaneously. At N_1 every node stays on the list for τ s where τ represents the 2ACK reception timeout. If the 2ACK packet arrives before the timeout, ID is removed from the list and the counter value C_{mis} is incremented. Node N_1 observes the links behaviour for a specified time period, T_{obs} and then calculates the ratio, R_{mis}, where $\left[R_{mis} = \frac{C_{mis}}{C_{pkts}}\right]$. If $R_{mis} > threshold$, the link is labelled as malicious or suspicious and N_1 broadcasts misbehaviour report. All the nodes that receive such report labels the link as suspicious and avoids using them during its own data transfer [82, 83]. Table 7 presents the Pseudocode of 2ACK scheme.

Assume h to be the average hop count in a route, then there exists $(h-1)$ routers in the path. If the probability of these routers to misbehave is denoted by p_m, then the probability of routes having a minimum of one malicious node can be estimated as

$$p_r = 1 - (1 - p_m)^{h-1} \tag{13}$$

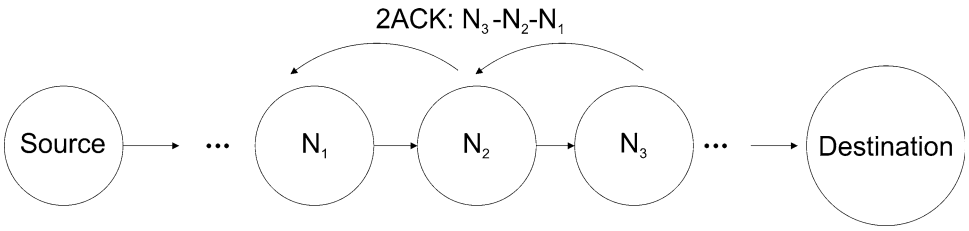

Fig. 4 2ACK scheme

For estimating the value of p_r, $\left[h = \frac{d}{l}\right]$, where d is the distance between source and destination and l is the average progress in every hop.

Theorem 2 *Considering a transmission circle, the probability that all the N_{Tc} nodes resides within the distance r from the centre can be calculated as*

$$F(r) = \frac{r^{2N_{Tc}}}{R^{2N_{Tc}}}$$

Proof Consider a network area of size $[X \times Y]$, then the node density, $N_{density}$, can be estimated as

$$N_{density} = \frac{N}{X \times Y} \tag{14}$$

Therefore, the number of nodes lying within the transmission circle of radius 'r' can be calculated as

$$N_{Tc} = N_{density} \times \pi r^2 \tag{15}$$

Using Eqs. 14 and 15, we have

$$N_{Tc} = \frac{N}{X \times Y} \times \pi r^2 \tag{16}$$

The probability that all the N_{Tc} nodes resides within the distance r from the centre can be estimated as $F(r)$. Therefore,

$$F(r) = p(All\ N_{Tc}\ resides\ within\ radius\ r)$$

$$= [p(1\ node\ resides\ within\ radius\ r)]^{N_{Tc}}$$

$$= \left[\frac{\pi r^2}{\pi R^2}\right]^{N_{Tc}}$$

$$F(r) = \frac{r^{2N_{Tc}}}{R^{2N_{Tc}}} \tag{17}$$

Theorem 3 *If the average distance between the source and destination is estimated as $d \approx \frac{\sqrt{X^2+Y^2}}{2}$, then the expected hop counts between the source and the destination can be estimated as*

$$h \approx \frac{(2N_{Tc}+1) \cdot \sqrt{X^2+Y^2}}{4N_{Tc}R}$$

Proof The progress probability density function, $f(r)$, can be estimated as

$$f(r) = \frac{\partial}{\partial x} F(r) = \frac{2N_{Tc} \cdot r^{2N_{Tc}-1}}{R^{2N_{Tc}}} \tag{18}$$

Therefore, the average progress can be calculated by estimating the value of r w.r.t. $f(r)$ as given below.

$$l = \int_0^R r f(r) dr = \frac{2N_{Tc} \cdot R}{2N_{Tc}+1} \tag{19}$$

Thus, the expected hop counts between the source and the destination can be estimated as

$$h \approx \frac{d}{l} \approx \frac{\sqrt{X^2+Y^2}}{2l} \tag{20}$$

Hence, using Eqs. 19 and 20, we have

$$h \approx \frac{(2N_{Tc}+1) \cdot \sqrt{X^2+Y^2}}{4N_{Tc}R} \tag{21}$$

Theorem 4 *If the probability of the routers to misbehave is p_m then the probability of routes having a minimum of one misbehaving node can be estimated as*

$$p_r = \left[1 - (1-p_m)^{\left[\frac{(2N_{Tc}+1)\cdot\sqrt{X^2+Y^2}}{4N_{Tc}R}\right]-1}\right]$$

Proof Based on Eq. 19, when $N_{Tc} = 0$, there is no progress and $l = 0$. When $N_{Tc} = 1$, the progress is till the location of the only node from the centre therefore, $l = \frac{2}{3}R$. If the value of N_{Tc} becomes large, then the progress approaches R. Assuming the average progress in one hop to be free from the average progress made in any of the earlier hops, the probability of routes having a minimum of one misbehaving node can be calculated using Eq. 13. In Eq. 13, putting the value of h from the Eq. 21, the probability of routes having a minimum of one misbehaving node can be estimated as

$$p_r = \left[1 - (1-p_m)^{\left[\frac{(2N_{Tc}+1)\cdot\sqrt{X^2+Y^2}}{4N_{Tc}R}\right]-1}\right] \tag{22}$$

6 Experimental setup and simulation parameters

In this section, numerical experiments are conducted for verifying the performance of the proposed E^2SR^2 in comparison to existing data dissemination protocols. For

Table 7 Pseudocode of 2ACK Scheme

2ACK sender (N_3)

BEGIN
Publish h_n
$C_{ack} \leftarrow 0, C_{pkt} \leftarrow 0, i \leftarrow n$
while *true* **do**
  if $packet_{data}$ is successfully received **then**
    $C_{pkt}++$
    if $\left[\frac{C_{ack}}{C_{pkt}} < R_{ack}\right]$ **then**
      acknowledge the data packets by sending *2ACK packets*
      $C_{ack}++, i—$
      end
  end
END

2ACK receiver (N_1)

BEGIN
while *true* **do**
  if h_n is received from the sender of 2ACK **then**
    record $h_n, i \leftarrow n$
  end
end
while *true* **do**
  select T_{start}
  while $(T_{current} < T_{start} + T_{observation})$
    if ($packet_{data}$ is forwarded) **then**
      Add data ID to the LIST
      $C_{pkts}++$
      Setup timer τ
  end
  if ($packet_{2ACK}$ is received) **then**
    Search 2ACK ID from the LIST
    if (found) **then**
      $LIST \leftarrow LIST - ID$
      Clear timer
    end
  end
    if (*timeout*) **then**
    $LIST \leftarrow LIST - ID$
    $C_{miss}++$
    end
  end
  if $\left[\frac{C_{miss}}{C_{pkt}} > R_{miss}\right]$ **then**
    Link misbehaviour report generated
  end
END

performance evaluation of the proposed E^2SR^2, extensive simulations are conducted using NS2, a network simulation platform. Here we considered a topology of 100–120 nodes deployed randomly in a rectangular WSN region of 1350×1100 m^2. We considered flat grid topology powered by omni antenna and two ray ground propagation model. Ad hoc routing strategy is considered with 802.11 MAC support. In order to prove the efficiency of the developed routing protocol in terms of security, a specialized attack model is developed. The performance of the considered existing as well as proposed data dissemination protocols is measured in presence of the considered attack model. Tests are conducted using plane coordinates consisting of mobile as well as static nodes. One single sink node roam in the entire network consistently and in order to support the claim of our research, the performance of these routing protocols is measured in terms of varying sink speeds. Table 8 presents the details of the simulation parameters considered.

Table 8 Simulation parameters considered for the experiment

Simulation parameters	Considered values
Coverage area	1350×1100 m^2
Simulation period	50 ms
Buffer size	25 packets
Size of data packets	20 bytes
Antenna type	Omni-antenna
Propagation type	Two-ray ground propagation model
Routing	Ad-hoc
MAC type	802.11
Width of rail in railroad	100 m
Width of line in LBDD	100 m
Sink speed	1–5 km/h
No. of nodes	100–120
Attacks	Blackhole, grey-hole and identity attack
No of malicious nodes	5–8
Agent type	UDP
Traffic type	CBR
Queue type	Drop-Tail
Initial energy	100 J
Receiving energy	1.0 J
Transmission energy	1.5 J

7 Results and discussions

7.1 Energy

Energy is the premiere resource in WSNs as SNs are energy constrained. SNs consume varied amount of energy during different phases like transmission phase, reception

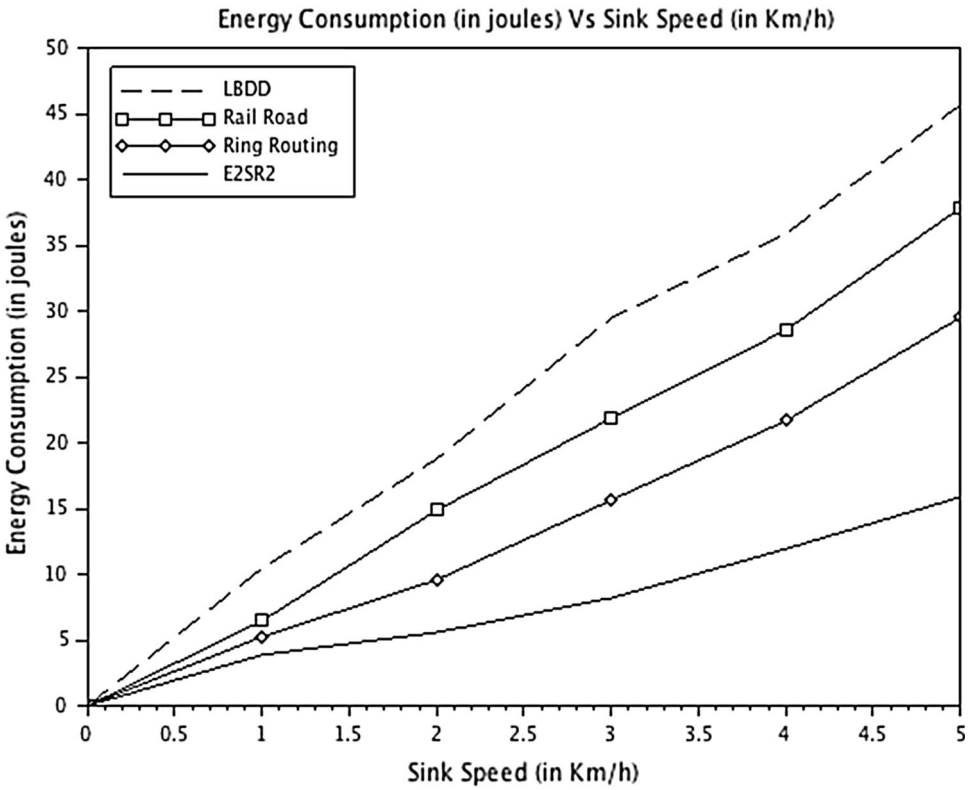

Fig. 5 Comparison of energy consumption for various schemes with varying sink speeds

phase, sleeping phase and idle waiting phase. Energy consumption during these phases are collectively considered for the experiment and performance evaluation. Figure 5, shows the variation of energy consumption with varying sink speed. LBDD shows maximum energy consumption followed by rail road and ring routing. In case of LBDD, increased sink speed leads to elevated rate of change of anchor nodes thereby resulting in increased broadcast message transmissions. This elevates the overall networks energy consumption. The number of broadcasts is limited in railroad as the broadcasts are confined only to the localized stations along the rail. The position information of the AN is shared using unicast strategy along the rail. Due to this reason rail road shows improved performance than LBDD for higher values of sink speed. The proposed E^2SR^2 incurs minimum energy consumption for all sink speeds. As the distance between the sink and the sensor node decreases, there is a decrease in consumption of transmission energy for the nodes. In order to do so, nodes select routing schemes on the basis of mobile sinks location. E^2SR^2 is capable of changing its transmission range by adjusting the data transmission path or its transmitting power. Figure 6, shows the energy efficiency of the considered routing protocols and it can be noticed that the LBDD shows worst performance and the proposed E^2SR^2 performs best amongst all others in terms of energy efficiency for varying sink speeds.

7.2 Average delay

Another metric that effects the performance of the WSNs is the delay incurred in data reporting process. For several time critical applications of WSNs such as military investigations and heath care monitoring, freshness of data directly relates to the data validity. This is because transmitting data to an outdated sink may cause these sinks to disseminate data via some other paths influenced by the follow-up mechanism. Figure 7, shows the comparison of average delay of various schemes with varying sink speeds. LBDD incurs maximum delay followed by rail road and ring routing schemes. The proposed E^2SR^2 shows least delay in comparison to all other schemes. Even if the delay associated with the proposed mechanism is close to other schemes in comparison, it is in reasonable limits in order to support time-critical applications, energy consumption performance of the proposed routing scheme is favoured.

7.3 Lifetime of network

WSNs performance is directly proportional to its lifetime. Lifetime can be defined as the time at which any SN in the network dies out because of battery depletion. It is the time interval from network activation until the area being monitored by k working nodes, have number of nodes below a threshold limit in working condition. Death of

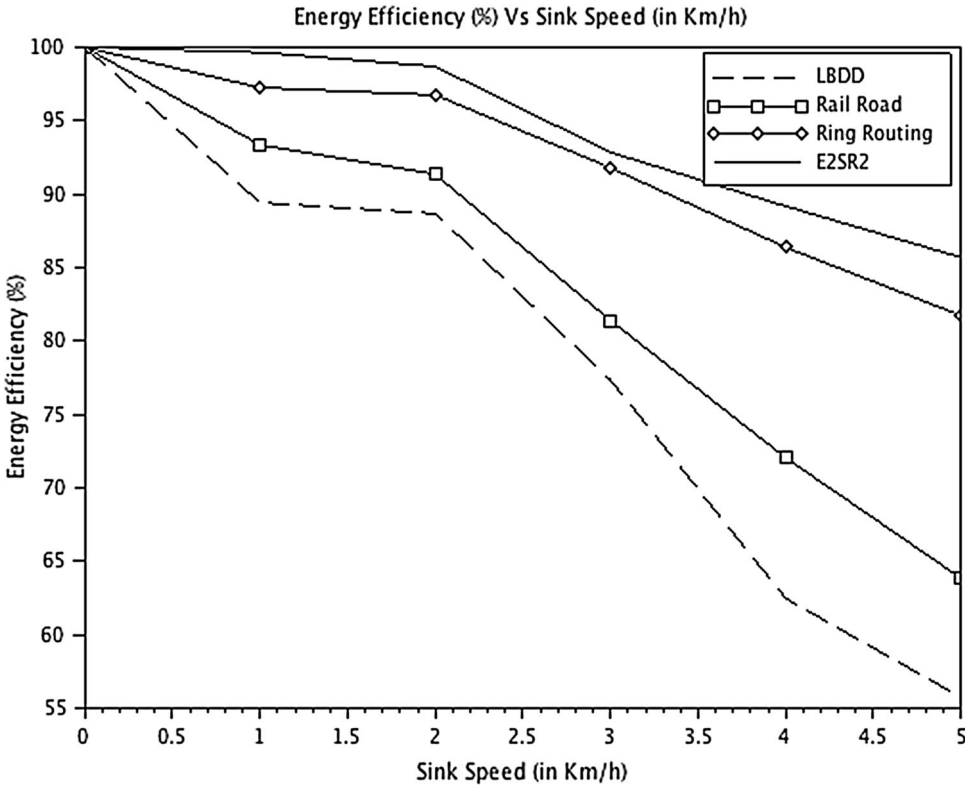

Fig. 6 Comparison of energy efficiency of various schemes with varying sink speeds

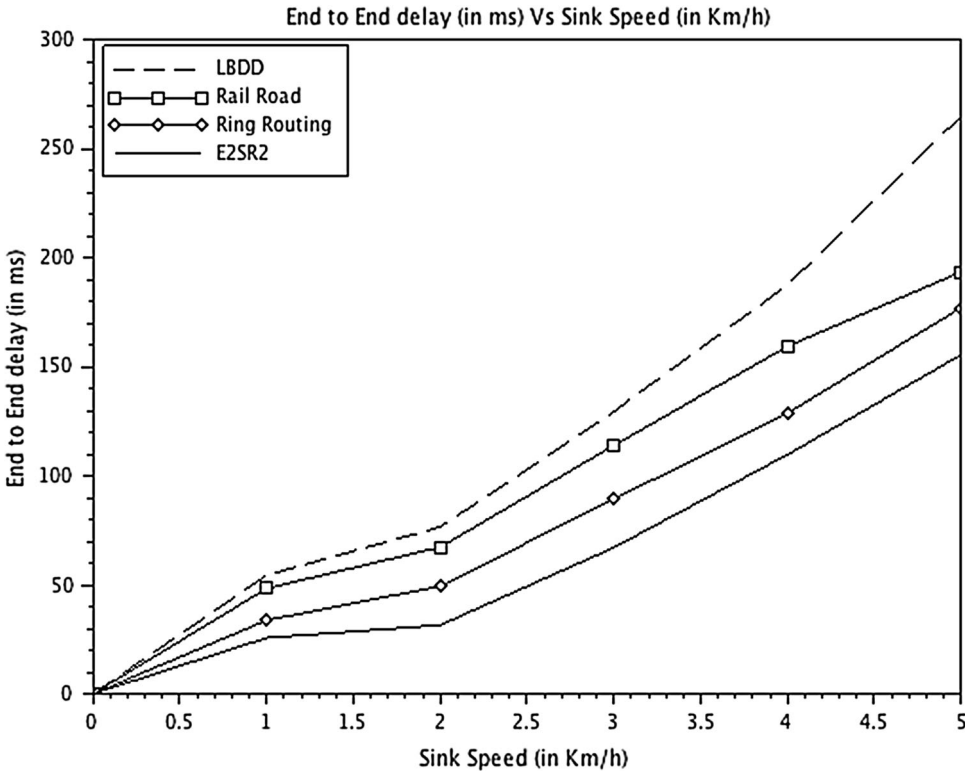

Fig. 7 Comparison of average delay involved in various schemes with varying sink speeds

even a single node may lead to topology disruption and disconnectedness among various network portions. The criticality of this issue depends on the position of the dying nodes. However, mobile sinks mitigate the impact of such problems as the mobile sink visits even the disconnected network areas, it therefore provides enhanced performance

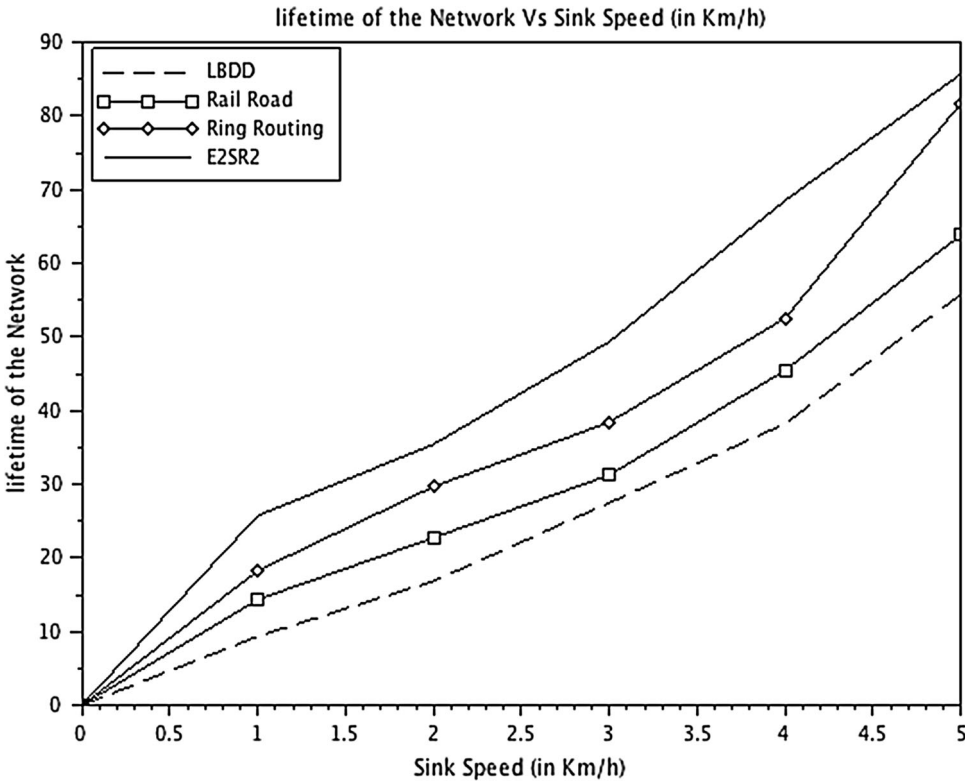

Fig. 8 Comparison of lifetime of the network of various schemes with varying sink speeds

in terms of data delivery and reliability. Figure 8, shows the comparison of lifetime of the network of various schemes with varying sink speeds. LBDD shows worst lifetime performance due to non-uniformity in degree of energy consumption that might be caused by the inability of the line nodes to handle heavy traffic. Performance of railroad is impeded significantly for larger networks because of station building mechanism. With an increase in number of nodes and consequent increase in number of generated packets, there is a need to build more stations and issue more broadcasts. The proposed E^2SR^2 enhances lifetime of the network in comparison to other protocols under comparison. Railroad employs a response/request mechanism similar to the proposed routing scheme; however, the second-tier structure broadcasts is not completely eliminated thereby enabling the proposed scheme to perform outstandingly well in terms of network lifetime.

7.4 Routing overhead

Overhead associated with the routing protocols is generally responsible for the overall network traffic therefore a routing strategy imposing high overhead is likely to result in increased delays. Figure 9, shows the routing overheads associated with the considered protocols. LBDD shows maximum routing overhead followed by rail road and ring routing. The proposed E^2SR^2 protocol proves to be most efficient in terms of routing overhead. This is because it uses 2ACK scheme. 2ACK experiences maximum routing overhead when the value of R_{ack} approaches unity mainly because of increased number of 2ACK packets being transmitted in the network. The routing overhead also decreases with a decrease in the value of R_{ack}. Therefore, the value of R_{ack} can be used to tune the routing overhead of the network.

7.5 Packet delivery ratio

Figure 10 shows the comparison of packets generated in various schemes with varying sink speeds. LBDD, rail road and ring routing shows almost equivalent number of packets generated. E^2SR^2 shows much higher number of packets generated in comparison to other existing protocols. Figure 11 shows the comparison of the number of packets received by the receiver in various schemes under consideration. LBDD shows least numbers of packets received followed by rail road and ring routing. E^2SR^2 shows much higher number of packets received in comparison to other existing protocols. This is because railroad and LBDD use large load distribution structures. Structure change mechanism is employed by the ring routing protocol for similar performance. For every triplet set in E^2SR^2, 2ACK transmission takes place via fixed predefined

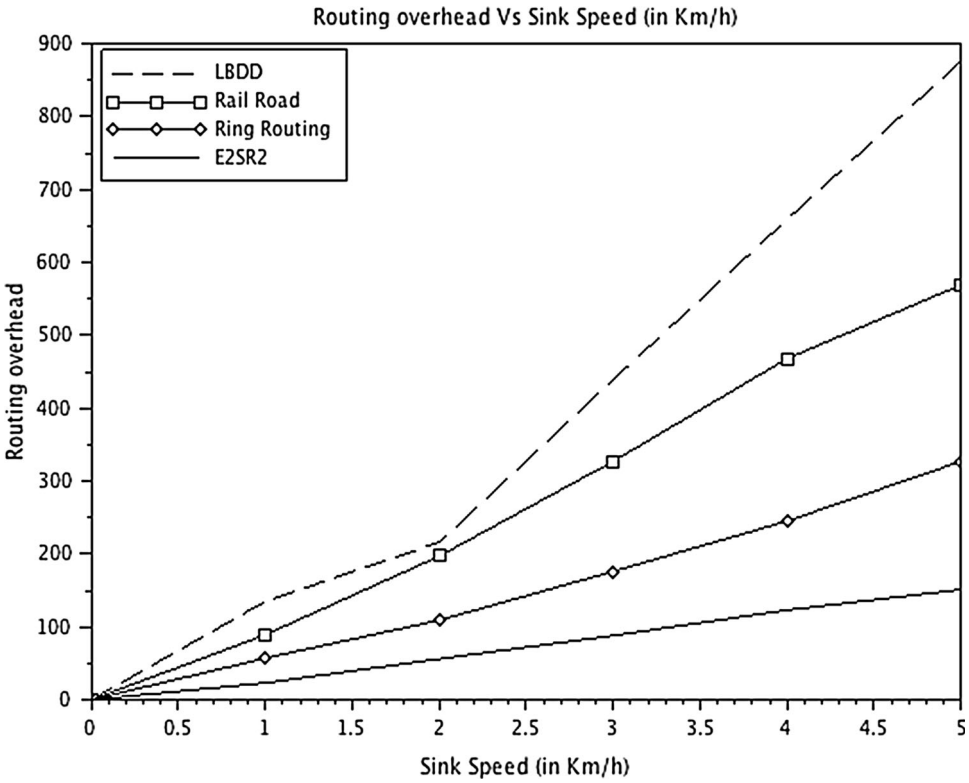

Fig. 9 Comparison of routing overhead of various schemes with varying sink speeds

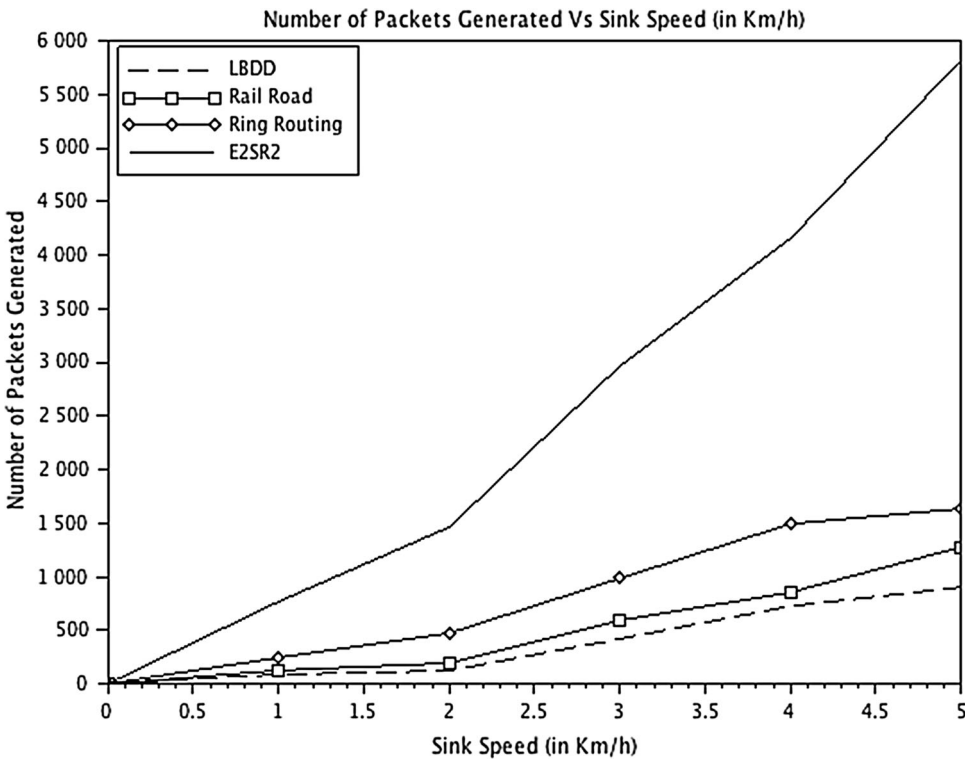

Fig. 10 Comparison of packets generated in various schemes with varying sink speeds

route between three nodes of 2 hops in the direction opposite to the data traffic route. This detects the malicious node that refuses to forward the packets even after agreeing to do so. Therefore, the proposed scheme results in increased number of generated as well as received packets. Figure 12 shows the average PDR of the network. PDR is

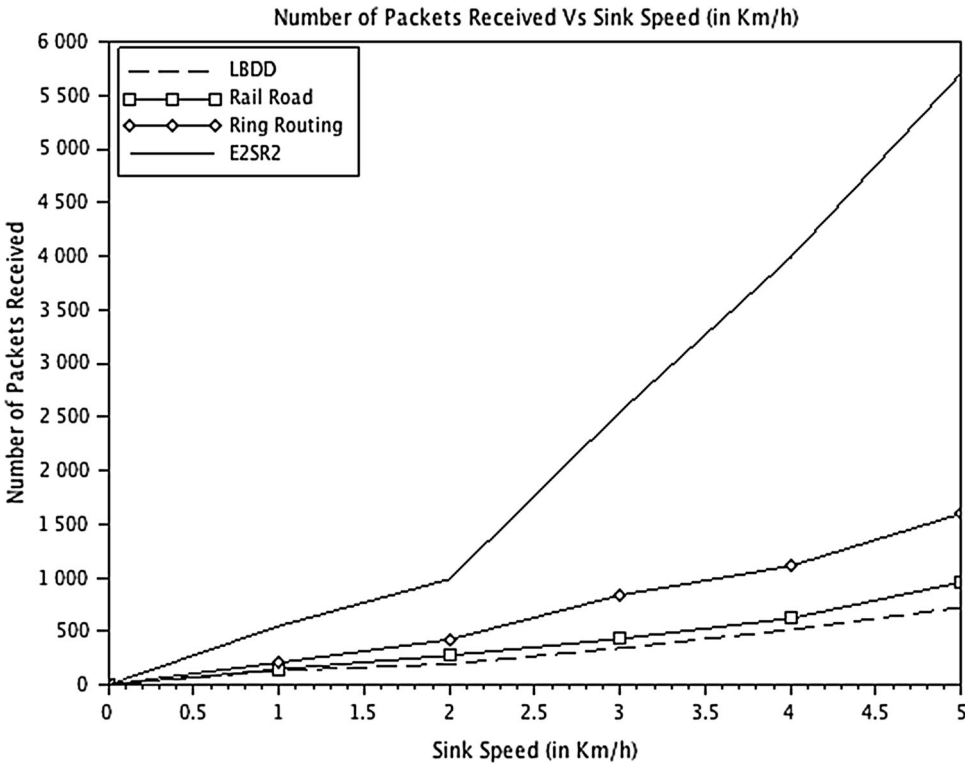

Fig. 11 Comparison of packets received in various schemes with varying sink speeds

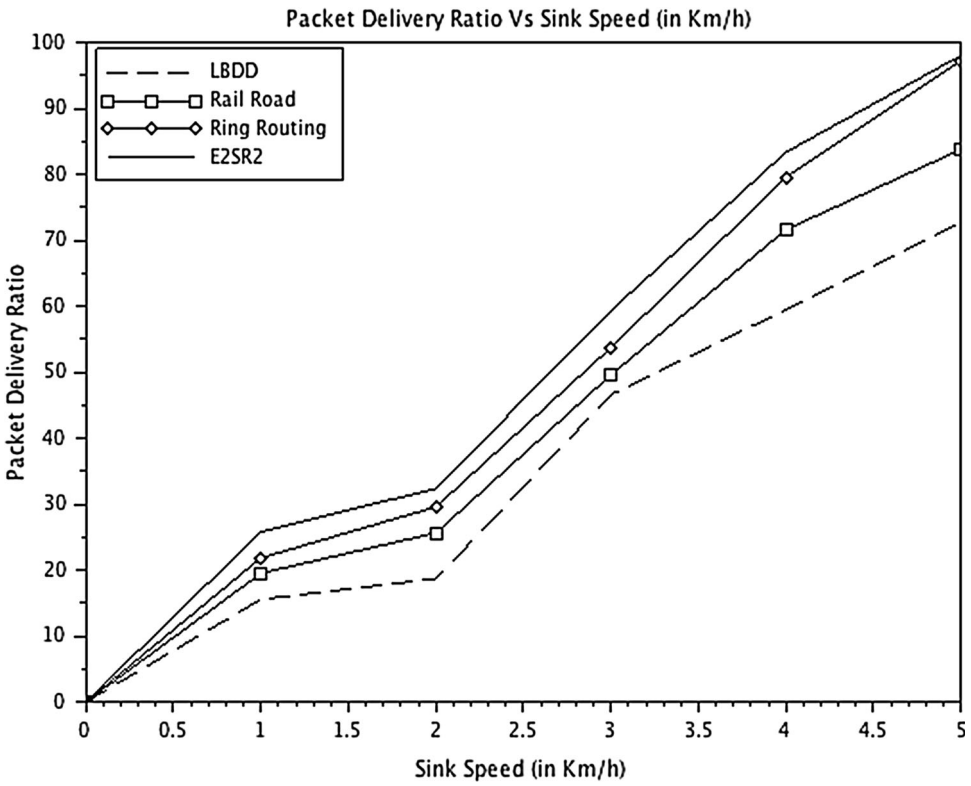

Fig. 12 Comparison of PDR of various schemes with varying sink speeds

the ratio of number of packets received by the receiver to the number of packets generated by the source. LBDD shows least PDR followed by railroad and ring routing. E^2SR^2 shows highest PDR as the impact of attack is limited thereby causing limited packet loss. The advantage or the performance difference of the proposed routing

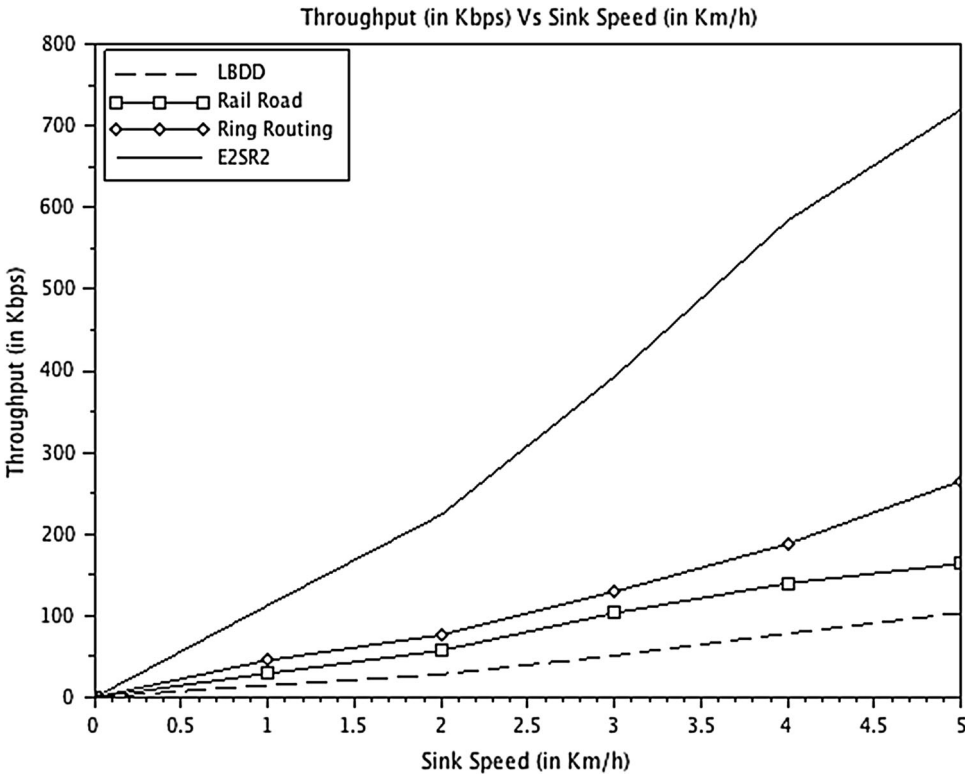

Fig. 13 Comparison of throughput of various schemes with varying sink speeds

scheme compared to its rivals LBDD, railroad and ring routing is not only because of its geometric structure but also due to the combined effect of the 2ACK security scheme and energy efficient load balancing model that addresses the problems of security, redundancy, overhead, energy depletion and traffic congestion observed in its counterparts.

7.6 Throughput

Figure 13 shows the comparison of throughput of various schemes. LBDD yields least throughput followed by rail road and ring routing. E^2SR^2 shows best performance in comparison to all the other three protocols in terms of the overall network throughput.

7.7 Packet loss

Figure 14, shows the comparison of number of packet loss for various protocols in consideration. LBDD is noticed to be the most vulnerable to attacks as it shows maximum packet loss followed by rail road and ring routing. E^2SR^2 shows least number of packets being lost during data transmission. The advantages of the proposed E^2SR^2 scheme compared to its rivals LBDD, railroad and ring routing is due to the effect of the 2ACK security scheme discussed further.

7.7.1 Security: 2ACK

The 2ACK scheme distinguishes the temporary link failures and the link misbehaviours by observing the 2ACK packets reception over a time period, T_{obs}. Since link misbehaviour lasts longer as compared to the temporary link failures, 2ACK scheme is capable of distinguishing link behaviour and temporary link failures. The additional overhead due to 2ACK packets transmission can be controlled by the controlling the parameter value of acknowledgement ratio, R_{ack}, at the sender of the 2ACK packet. Controlling the value of R_{ack} in the 2ACK scheme provides a tuning mechanism to tune the routing overhead by enabling the acknowledgement of only a fraction of packets.

Partial data forwarding A malicious node may partially forward data packets and cheat the monitoring system by forwarding only a fraction of packets. 2ACK scheme is capable of detecting such malicious behaviour using the triplet $N_1 \rightarrow N_2 \rightarrow N_3$. Assume N_2 to be a malicious node that receives N_D packets from N_1 and forwards only a small fraction of it, N_{frac}, to N_3. N_3 received only $N_{frac} \cdot N_D$ packets so only $R_{ack} \cdot N_{frac} \cdot N_D$ packets are acknowledged by the 2ACK packets from N_3. Therefore, for launching a successful attack, adversary needs to make sure that $1 - R_{ack} \cdot N_{frac} < R_{miss}$. This enables the 2ACK scheme to effectively guard against the considered attack model.

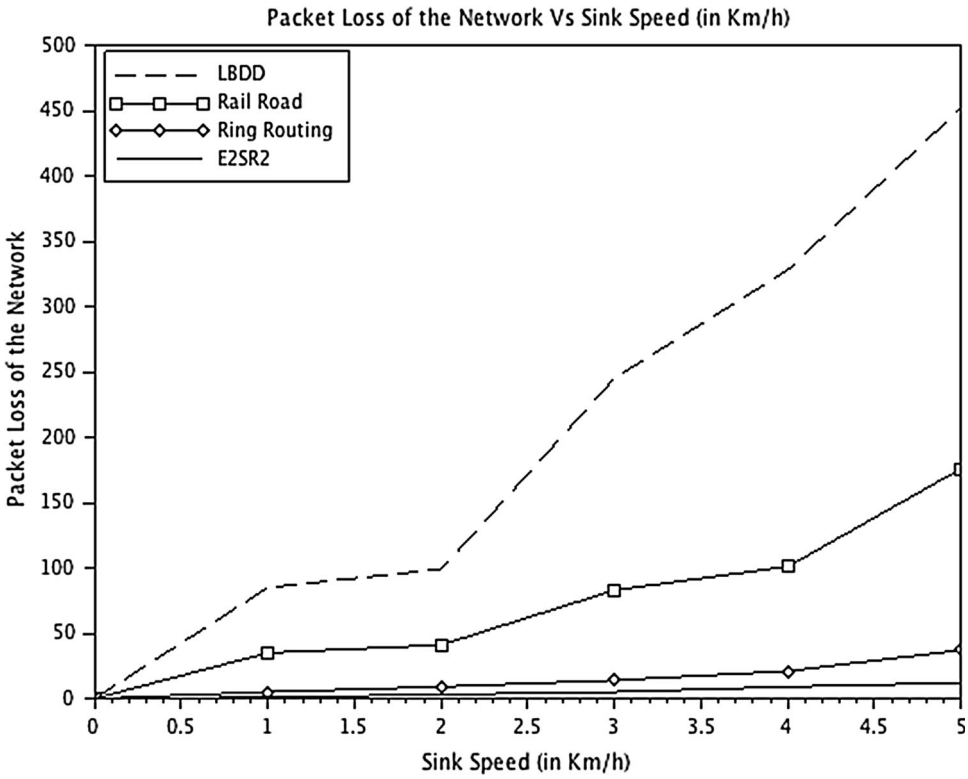

Fig. 14 Comparison of packet loss in various schemes with varying sink speeds

8 Conclusion and future works

WSNs have been an active research area over the recent past because of their potentially widespread areas of applications such as civilian and military communications, environment monitoring, health care monitoring, forest fire detection, and so on. Such networks depend heavily on the cooperation among its members in order to perform the networking operations. In this work, we propose E^2SR^2, a mobile sink routing protocol that facilitates rechargeable sensors to be deployed in the sensing region considering both the disadvantages and limitations of the existing protocols in the literature. E^2SR^2 is an enhancement of existing ring routing protocol that considers rechargeable sensors and energy harvesting technologies to enable perpetual operations. E^2SR^2 employs MCP, an energy efficient dynamic load balancing scheme to prolong the networks lifetime. Furthermore, the performance degradation of the network under the considered attack model is investigated. The considered existing ring routing protocol is susceptible to the attack model and therefore we also propose to enhance the security aspect of ring routing protocol. E^2SR^2 use 2ACK scheme that is based on 2-hop acknowledgement packet which the receiver of the next-hop link sends back. The used 2ACK scheme also overcome the issues of limited transmission powers, receiver collisions or ambiguous collisions and is used as an add-on scheme to the ring routing protocol.

Finally, the proposed protocol was simulated by varying the sink speed for similar node deployments and the results obtained confirm that the proposed E^2SR^2 achieves improved performance than the existing protocols such as LBDD (Line Based Data Dissemination), rail road and ring routing. E^2SR^2 is proved to be the most secure, energy efficient and network lifetime extending protocol. Also, the delays associated with the proposed protocol is within the reasonable limits therefore making it suitable for time-critical scenarios.

- In our future work, we want to enhance the ring routing so as to make it capable of supporting multiple mobile sinks. In the current scenario, ring routing can operate with multiple mobile sinks by broadcasting ANPIREP packets using the sinks located near the source. Though this approach supports multiple sinks but does not reap all the benefits associated with mobile sinks use. Thus, we propose to modify and extend the ring routing so that it can operate using multiple mobile sinks.
- As WSNs is vulnerable to wide range of attacks, in our future work, we want to design even more secure mechanism to counter all the possible type of attacks in WSNs.

References

1. Khan, I., Belqasmi, F., Glitho, R., Crespi, N., Morrow, M., & Polakos, P. (2016). Wireless sensor network virtualization: A survey. *IEEE Communications Surveys & Tutorials, 18*(1), 553–576. https://doi.org/10.1109/comst.2015.2412971.
2. Mehrabi, A., & Kim, K. (2017). General framework for network throughput maximization in sink-based energy harvesting wireless sensor networks. *IEEE Transactions on Mobile Computing, 16*(7), 1881–1896. https://doi.org/10.1109/tmc.2016.2607716.
3. Kumar, N., & Dash, D. (2018). Mobile data sink-based time-constrained data collection from mobile sensors: A heuristic approach. *IET Wireless Sensor Systems, 8*(3), 129–135. https://doi.org/10.1049/iet-wss.2017.0106.
4. Khan, A. W., Bangash, J. I., Ahmed, A., & Abdullah, A. H. (2017). QDVGDD: Query-driven virtual grid based data dissemination for wireless sensor networks using single mobile sink. *Wireless Networks*. https://doi.org/10.1007/s11276-017-1552-8.
5. Wen, W., Zhao, S., Shang, C., & Chang, C. (2018). EAPC: Energy-aware path construction for data collection using mobile sink in wireless sensor networks. *IEEE Sensors Journal, 18*(2), 890–901. https://doi.org/10.1109/jsen.2017.2773119.
6. Zhou, Z., Du, C., Shu, L., Hancke, G., Niu, J., & Ning, H. (2016). An energy-balanced heuristic for mobile sink scheduling in hybrid WSNs. *IEEE Transactions on Industrial Informatics, 12*(1), 28–40. https://doi.org/10.1109/tii.2015.2489160.
7. Dobslaw, F., Zhang, T., & Gidlund, M. (2016). End-to-end reliability-aware scheduling for wireless sensor networks. *IEEE Transactions on Industrial Informatics, 12*(2), 758–767. https://doi.org/10.1109/tii.2014.2382335.
8. Francesco, M. D., Das, S. K., & Anastasi, G. (2011). Data collection in wireless sensor networks with mobile elements. *ACM Transactions on Sensor Networks, 8*(1), 1–31. https://doi.org/10.1145/1993042.1993049.
9. Liang, W., Luo, J., & Xu, X. (2010). Prolonging network lifetime via a controlled mobile sink in wireless sensor networks. In *2010 IEEE global telecommunications conference GLOBECOM 2010*. https://doi.org/10.1109/glocom.2010.5683095.
10. Rao, J., & Biswas, S. (2010). Network-assisted sink navigation for distributed data gathering: Stability and delay-energy tradeoffs. *Computer Communications, 33*(2), 160–175. https://doi.org/10.1016/j.comcom.2009.08.009.
11. Grammalidis, N., Cetin, E., Dimitropoulos, K., Tsalakanidou, F., Kose, K., Gunay, O., et al. (2011). A multisensor network for the protection of cultural heritage. In *19th European signal processing conference (EUSIPCO2011), special session on signal processing for disaster management and prevention, 2011*.
12. Yun, Y., & Xia, Y. (2010). Maximizing the lifetime of wireless sensor networks with mobile sink in delay-tolerant applications. *IEEE Transactions on Mobile Computing, 9*(9), 1308–1318. https://doi.org/10.1109/tmc.2010.76.
13. He, S., Chen, J., Jiang, F., Yau, D. K., Xing, G., & Sun, Y. (2013). Energy provisioning in wireless rechargeable sensor networks. *IEEE Transactions on Mobile Computing, 12*(10), 1931–1942. https://doi.org/10.1109/tmc.2012.161.
14. Liu, R., Fan, K., Zheng, Z., & Sinha, P. (2011). Perpetual and fair data collection for environmental energy harvesting sensor networks. *IEEE/ACM Transactions on Networking, 19*(4), 947–960. https://doi.org/10.1109/tnet.2010.2091280.
15. Mao, Z., Koksal, C. E., & Shroff, N. B. (2012). Near optimal power and rate control of multi-hop sensor networks with energy replenishment: Basic limitations with finite energy and data storage. *IEEE Transactions on Automatic Control, 57*(4), 815–829. https://doi.org/10.1109/tac.2011.2166310.
16. Ren, X., Liang, W., & Xu, W. (2013). Use of a mobile sink for maximizing data collection in energy harvesting sensor networks. In *2013 42nd International conference on parallel processing*. https://doi.org/10.1109/icpp.2013.53.
17. Wu, J., Ota, K., Dong, M., & Li, C. (2016). A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities. *IEEE Access, 4*, 416–424. https://doi.org/10.1109/access.2016.2517321.
18. Pu, C., & Lim, S. (2018). A light-weight countermeasure to forwarding misbehavior in wireless sensor networks: Design, analysis, and evaluation. *IEEE Systems Journal, 12*(1), 834–842. https://doi.org/10.1109/jsyst.2016.2535730.
19. Hsueh, C., Wen, C., & Ouyang, Y. (2015). A secure scheme against power exhausting attacks in hierarchical wireless sensor networks. *IEEE Sensors Journal, 15*(6), 3590–3602. https://doi.org/10.1109/jsen.2015.2395442.
20. Tan, L., & Tang, S. (2017). Energy harvesting wireless sensor node with temporal death: Novel models and analyses. *IEEE/ACM Transactions on Networking, 25*(2), 896–909. https://doi.org/10.1109/tnet.2016.2607229.
21. Cao, B., Ge, Y., Kim, C. W., Feng, G., Tan, H. P., & Li, Y. (2013). An experimental study for inter-user interference mitigation in wireless body sensor networks. *IEEE Sensors Journal, 13*(10), 3585–3595. https://doi.org/10.1109/jsen.2013.2267053.
22. Li, Y., Huang, Q., & Huang, W. (2011). A cooperative retransmission strategy for error-prone wireless networks. In *2011 Eighth international conference on wireless and optical communications networks*. https://doi.org/10.1109/wocn.2011.5872934.
23. Wang, L., Zhao, W., Li, Y., Qu, Y., Liu, Z., & Chen, Q. (2008). Sleep-supported and cone-based topology control method for wireless sensor networks. In *2008 IEEE international conference on networking, sensing and control*. https://doi.org/10.1109/icnsc.2008.4525447.
24. Sharma, V., You, I., Pau, G., Collotta, M., Lim, J., & Kim, J. (2018). LoRaWAN-based energy-efficient surveillance by Drones for intelligent transportation systems. *Energies, 11*(3), 573. https://doi.org/10.3390/en11030573.
25. Liu, X., Zhao, H., Yang, X., & Li, X. (2013). SinkTrail: A proactive data reporting protocol for wireless sensor networks. *IEEE Transactions on Computers, 62*(1), 151–162. https://doi.org/10.1109/tc.2011.207.
26. Hawbani, A., Wang, X., Kuhlani, H., Karmoshi, S., Ghoul, R., Sharabi, Y., et al. (2017). Sink-oriented tree based data dissemination protocol for mobile sinks wireless sensor networks. *Wireless Networks, 24*(7), 2723–2734. https://doi.org/10.1007/s11276-017-1497-y.
27. Luo, H., Ye, F., Cheng, J., Lu, S., & Zhang, L. (2005). TTDD: Two-tier data dissemination in large-scale wireless sensor networks. *Wireless Networks, 11*(1–2), 161–175. https://doi.org/10.1007/s11276-004-4753-x.
28. Kweon, K., Ghim, H., Hong, J., & Yoon, H. (2009). Grid-based energy-efficient routing from multiple sources to multiple mobile sinks in wireless sensor networks. In *2009 4th International symposium on wireless pervasive computing*. https://doi.org/10.1109/iswpc.2009.4800585.
29. Erman, A. T., Dilo, A., & Havinga, P. (2012). A virtual infrastructure based on honeycomb tessellation for data dissemination in multi-sink mobile wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking*. https://doi.org/10.1186/1687-1499-2012-17.
30. Lin, C., Chou, P., & Chou, C. (2006). HCDD. In *Proceeding of the 2006 international conference on communications and mobile computing—IWCMC 06*. https://doi.org/10.1145/1143549.1143787.

31. Lu, J., & Valois, F. (2007). On the data dissemination in WSNs. In *Third IEEE international conference on wireless and mobile computing, networking and communications (WiMob 2007)*. https://doi.org/10.1109/wimob.2007.4390852.
32. Li, Y., Xiong, S., Chen, Q., & Fang, F. (2007). Grid-based directed diffusion for wireless sensor networks. In *2007 Second international conference on communications and networking in China*. https://doi.org/10.1109/chinacom.2007.4469508.
33. Xing, G., Wang, T., Xie, Z., & Jia, W. (2007). Rendezvous planning in mobility-assisted wireless sensor networks. In *28th IEEE international real-time systems symposium (RTSS 2007)*. https://doi.org/10.1109/rtss.2007.44.
34. Vecchio, M., Viana, A. C., Ziviani, A., & Friedman, R. (2010). DEEP: Density-based proactive data dissemination protocol for wireless sensor networks with uncontrolled sink mobility. *Computer Communications, 33*(8), 929–939. https://doi.org/10.1016/j.comcom.2010.01.003.
35. Mo, H., Lee, E., Park, S., & Kim, S. (2013). Virtual line-based data dissemination for mobile sink groups in wireless sensor networks. *IEEE Communications Letters, 17*(9), 1864–1867. https://doi.org/10.1109/lcomm.2013.072913.131354.
36. Hu, L., Li, Y., Chen, Q., Liu, J., & Long, K. (2007). A new energy-aware routing protocol for wireless sensor networks. In *2007 International conference on wireless communications, networking and mobile computing*. https://doi.org/10.1109/wicom.2007.609.
37. Collotta, M., Bello, L. L., Toscano, E., & Mirabella, O. (2010). Dynamic load balancing techniques for flexible wireless industrial networks. In *IECON 2010—36th annual conference on IEEE Industrial Electronics Society*. https://doi.org/10.1109/iecon.2010.5675489.
38. Hu, J., Jin, Y., & Dou, L. (2008). A time-based cluster-head selection algorithm for LEACH. In *IEEE Symposium on computers and communications*, 2008, pp. 1172–1176.
39. Li, Y., Yu, N., Zhang, W., Zhao, W., You, X., & Daneshmand, M. (2011). Enhancing the performance of LEACH protocol in wireless sensor networks. In *2011 IEEE conference on computer communications workshops (INFOCOM WKSHPS)*. https://doi.org/10.1109/infcomw.2011.5928813.
40. Collotta, M., Pau, G., Salerno, V. M., & Scata, G. (2012). A distributed load balancing approach for industrial IEEE 802.11 wireless networks. In *Proceedings of 2012 IEEE 17th international conference on emerging technologies & factory automation (ETFA 2012)*. https://doi.org/10.1109/etfa.2012.6489583.
41. Li, Y., Zhang, Z., Wang, C., Zhao, W., & Chen, H. (2013). Blind cooperative communications for multihop ad hoc wireless networks. *IEEE Transactions on Vehicular Technology, 62*(7), 3110–3122. https://doi.org/10.1109/tvt.2013.2256475.
42. Li, Y., Zhu, X., Liao, C., Wang, C., & Cao, B. (2015). Energy efficiency maximization by jointly optimizing the positions and serving range of relay stations in cellular networks. *IEEE Transactions on Vehicular Technology, 64*(6), 2551–2560. https://doi.org/10.1109/tvt.2014.2342236.
43. Collotta, M., Scata, G., Tirrito, S., Ferrero, R., & Rebaudengo, M. (2014). A parallel fuzzy scheme to improve power consumption management in Wireless Sensor Networks. In Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA). https://doi.org/10.1109/etfa.2014.7005363.
44. Collotta, M., & Pau, G. (2015). A novel energy management approach for smart homes using bluetooth low energy. *IEEE Journal on Selected Areas in Communications, 33*(12), 2988–2996. https://doi.org/10.1109/jsac.2015.2481203.
45. Li, Y., Li, Y., Cao, B., Daneshmand, M., & Zhang, W. (2015). Cooperative spectrum sharing with energy-save in cognitive radio networks. In *2015 IEEE global communications conference (GLOBECOM)*. https://doi.org/10.1109/glocom.2015.7417201.
46. Collotta, M., Pau, G., & Bobovich, A. V. (2017). A fuzzy data fusion solution to enhance the QoS and the energy consumption in Wireless Sensor Networks. *Wireless Communications and Mobile Computing, 2017,* 1–10. https://doi.org/10.1155/2017/3418284.
47. Chakrabarti, A., Sabharwal, A., & Aazhang, B. (2006). Communication power optimization in a sensor network with a path-constrained mobile observer. *ACM Transactions on Sensor Networks (TOSN), 2*(3), 297–324.
48. Gao, S., Zhang, H., & Das, S. K. (2011). Efficient data collection in wireless sensor networks with path-constrained mobile sinks. *IEEE Transactions on Mobile Computing, 10*(4), 592–608. https://doi.org/10.1109/tmc.2010.193.
49. Guo, S., & Yang, Y. (2012). A distributed optimal framework for mobile data gathering with concurrent data uploading in wireless sensor networks. In *Proceedings of IEEE INFOCOM* (pp. 1305–1313). IEEE.
50. Chen, S., Sinha, P., Shroff, N. B., & Joo, C. (2014). A simple asymptotically optimal energy allocation and routing scheme in rechargeable sensor networks. *IEEE/ACM Transactions on Networking, 22*(4), 1325–1336.
51. Guo, S., Wang, C., & Yang, Y. (2014). Joint mobile data gathering and energy provisioning in wireless rechargeable sensor networks. *IEEE Transactions on Mobile Computing, 99*(1), 1.
52. Zhao, M., Li, J., & Yang, Y. (2014). A framework of joint mobile energy replenishmentanddatagatheringinwirelessrechargeable-sensornetworks. *IEEE Transactions on Mobile Computing, 13*(12), 2689–2705.
53. Castagnetti, A., Pegatoquet, A., Le, T. N., & Auguin, M. (2014). A joint duty-cycle and transmission power management for energy harvesting WSN. *IEEE Transactions on Industrial Informatics, 10*(2), 928–936. https://doi.org/10.1109/tii.2014.2306327.
54. Anisi, M. H., Abdul-Salaam, G., Idris, M. Y., Wahab, A. W., & Ahmedy, I. (2015). Energy harvesting and battery power based routing in wireless sensor networks. *Wireless Networks, 23*(1), 249–266. https://doi.org/10.1007/s11276-015-1150-6.
55. Lu, T., Liu, G., & Chang, S. (2016). Energy-efficient data sensing and routing in unreliable energy-harvesting wireless sensor network. *Wireless Networks, 24*(2), 611–625. https://doi.org/10.1007/s11276-016-1360-6.
56. Shafieirad, H., Adve, R. S., & Shahbazpanahi, S. (2018). Max-SNR opportunistic routing for large-scale energy harvesting sensor networks. *IEEE Transactions on Green Communications and Networking, 2*(2), 506–516. https://doi.org/10.1109/tgcn.2018.2789783.
57. Bengheni, A., Didi, F., & Bambrik, I. (2018). EEM-EHWSN: Enhanced energy management scheme in energy harvesting wireless sensor networks. *Wireless Networks*. https://doi.org/10.1007/s11276-018-1701-8.
58. Ren, X., Liang, W., & Xu, W. (2013). Use of a mobile sink for maximizing data collection in energy harvesting sensor networks. In *Proceedings of ICPP* (pp. 439–448). IEEE.
59. Ren, X., Xu, W., & Liang, W. (2014). Data collection maximization in renewable sensor networks via time-slot scheduling. *IEEE Transactions on Computing, 64,* 1.
60. Hamida, E. B., & Chelius, G. (2008). A line-based data dissemination protocol for wireless sensor networks with mobile sink. In *2008 IEEE international conference on communications*. https://doi.org/10.1109/icc.2008.420.
61. Shin, J., Kim, J., Park, K., & Park, D. (2005). Railroad. In *Proceedings of the 2nd ACM international workshop on performance evaluation of wireless ad hoc, sensor, and ubiquitous networks—PE-WASUN 05*. https://doi.org/10.1145/1089803.1089982.
62. Tunca, C., Isik, S., Donmez, M. Y., & Ersoy, C. (2015). Ring routing: An energy-efficient routing protocol for Wireless Sensor Networks with a mobile sink. *IEEE Transactions on Mobile*

Computing, 14(9), 1947–1960. https://doi.org/10.1109/tmc.2014.2366776.
63. Niculescu, D. (2004). Positioning in ad hoc sensor networks. *IEEE Network, 18*(4), 24–29. https://doi.org/10.1109/mnet.2004.1316758.
64. Gopakumar, A., & Jacob, L. (2008). Localization in wireless sensor networks using particle swarm optimization. In *IET conference on wireless, mobile and multimedia networks*. https://doi.org/10.1049/cp:20080185.
65. Pham, T. N., & Yeo, C. K. (2016). Detecting colluding blackhole and greyhole attacks in delay tolerant networks. *IEEE Transactions on Mobile Computing, 15*(5), 1116–1129. https://doi.org/10.1109/tmc.2015.2456895.
66. Chang, J., Tsou, P., Woungang, I., Chao, H., & Lai, C. (2015). Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. *IEEE Systems Journal, 9*(1), 65–75. https://doi.org/10.1109/jsyst.2013.2296197.
67. Schweitzer, N., Stulman, A., Margalit, R. D., & Shabtai, A. (2017). Contradiction based gray-hole attack minimization for ad-hoc networks. *IEEE Transactions on Mobile Computing, 16*(8), 2174–2183. https://doi.org/10.1109/tmc.2016.2622707.
68. Pal, S., Sikdar, B., & Chow, J. H. (2018). An online mechanism for detection of gray-hole attacks on PMU data. *IEEE Transactions on Smart Grid, 9*(4), 2498–2507. https://doi.org/10.1109/tsg.2016.2614327.
69. Chen, Y., Yang, J., Trappe, W., & Martin, R. P. (2010). Detecting and localizing identity-based attacks in Wireless and Sensor Networks. *IEEE Transactions on Vehicular Technology, 59*(5), 2418–2434. https://doi.org/10.1109/tvt.2010.2044904.
70. Sun, C., Liu, J., Xu, X., & Ma, J. (2017). A privacy-preserving mutual authentication resisting DoS attacks in VANETs. *IEEE Access, 5,* 24012–24022. https://doi.org/10.1109/access.2017.2768499.
71. Mehrabi, A., & Kim, K. (2016). Maximizing data collection throughput on a path in energy harvesting sensor networks using a mobile sink. *IEEE Transactions on Mobile Computing, 15*(3), 690–704. https://doi.org/10.1109/tmc.2015.2424430.
72. Wang, C., Shih, J., Pan, B., & Wu, T. (2014). A network lifetime enhancement method for sink relocation and its analysis in Wireless Sensor Networks. *IEEE Sensors Journal, 14*(6), 1932–1943. https://doi.org/10.1109/jsen.2014.2306429.
73. Vadivazhagu, P., & Selvam, P. (2015). Network lifetime enhancement method for sink relocation and packet drop detection in wireless sensor networks. In *2015 International conference on communications and signal processing (ICCSP)*. https://doi.org/10.1109/iccsp.2015.7322534.
74. Liu, K., Deng, J., Varshney, P. K., & Balakrishnan, K. (2007). An acknowledgment-based approach for the detection of routing misbehavior in MANETs. *IEEE Transactions on Mobile Computing, 6*(5), 536–550. https://doi.org/10.1109/tmc.2007.1036.
75. Shi, Y., & Hou, Y. T. (2012). Some fundamental results on base station movement problem for wireless sensor networks. *IEEE/ACM Transactions on Networking, 20*(4), 1054–1067. https://doi.org/10.1109/tnet.2011.2171990.
76. Orihuela, L., Gomez-Estern, F., & Rubio, F. R. (2014). Scheduled communication in sensor networks. *IEEE Transactions on Control Systems Technology, 22*(2), 801–808. https://doi.org/10.1109/tcst.2013.2262999.
77. Liu, J., Xiong, K., Fan, P., & Zhong, Z. (2017). RF energy harvesting wireless powered sensor networks for smart cities. *IEEE Access, 5,* 9348–9358. https://doi.org/10.1109/access.2017.2703847.
78. Saha, S., Nandi, S., Verma, R., Sengupta, S., Singh, K., Sinha, V., et al. (2016). Design of efficient lightweight strategies to combat DoS attack in delay tolerant network routing. *Wireless Networks, 24*(1), 173–194. https://doi.org/10.1007/s11276-016-1320-1.
79. Heydari, V., & Yoo, S. (2015). E2EACK: An end-to-end acknowledgment-based scheme against collusion black hole and slander attacks in MANETs. *Wireless Networks, 22*(7), 2259–2273. https://doi.org/10.1007/s11276-015-1098-6.
80. Kumar, V. A., & Das, D. (2014). Data enriched SACK: A novel acknowledgement generation scheme for secure SCTP. *IEEE Communications Letters, 18*(12), 2109–2112. https://doi.org/10.1109/lcomm.2014.2367109.
81. Pu, C., Lim, S., Chae, J., & Jung, B. (2017). Active detection in mitigating routing misbehavior for MANETs. *Wireless Networks*. https://doi.org/10.1007/s11276-017-1621-z.
82. Anand, A., Aggarwal, H., & Rani, R. (2016). Partially distributed dynamic model for secure and reliable routing in mobile ad hoc networks. *Journal of Communications and Networks, 18*(6), 938–947. https://doi.org/10.1109/jcn.2016.000128.
83. Yin, D., Shen, Y., & Liu, C. (2017). Attribute couplet attacks and privacy preservation in social networks. *IEEE Access, 5,* 25295–25305. https://doi.org/10.1109/access.2017.2769090.

Bharat Bhushan received the B.Tech. degree in computer science and engineering from SHIATS, Allahabad, India in 2012, and the M.Tech. degree in information security from Birla Institute of Technology, Mesra, Jharkhand, India in 2015, and is currently working towards the Ph.D. degree at Birla Institute of Technology, Mesra, Jharkhand, India. From 2012 through 2013, he worked as a network engineer at HCL Infosystems Ltd., Noida, India. He is IEEE student member. His research interests include the security and attacks in wireless sensor networks, performance analysis of wireless sensor network communications and security in networking systems.

Gadadhar Sahoo received his Ph.D. degree from IIT Kharagpur. He is currently working as professor (Department of Computer Science and Engineering) of Birla Institute of Technology, Mesra, Jharkhand, India. He has teaching and research experience of 30 years with Birla Institute of Technology, Mesra, Jharkhand, India. His research interests includes Soft Computing, Clustering, Cloud Computing, Cryptography, BioInformatics and security in wireless sensor networks.