An Efficient En-Route Filtering Technique based on Partial Key Distribution with Modified Lee Sphere region and Modified Bloom Filter

1Sibi Amaran, 2Dr. R. Madhan Mohan, Dr.R.Jebakumar
1Research Scholar, Department of Computer Science and Engineering, Annamalai University.
2Associate Professor, Department of Computer Science and Engineering, Annamalai University.
3Associate Professor, Department of CSE, SRM Institute of Science and Technology, Kattankulathur.
sibi.amaran@gmail.com, madhanmohan_mithu@yahoo.com, jebakumr@srmist.edu.in

Abstract

Wireless sensor network (WSN) becomes highly vulnerable to report fabrication attacks where the compromised nodes can be utilized by an adversary to flood the network with bogus/false reports. En-route filtering technique is commonly employed to identify and filter false reports from WSN. Several state of art en-route filtering techniques is probability based where the nodes in every cell distribute the shared keys with a predefined probability with middle nodes. Therefore, forwarded reports are confirmed in a probabilistic way by intermittent nodes due to the fact that the false reports can be travelled over numerous hops before being dropped. This paper presents a novel En-Route Filtering Technique based on Partial Key Distribution System with combinatorial design (PPDS-CD) model for WSN. The presented PPDS-CD model aims to reduce the key storage overhead in cluster heads (CHs) while providing effective resiliency over compromised nodes in WSN. The presented model utilizes Modified Lee Sphere region and Modified Bloom Filter for the effective selection of nodes in the en-route filtering process. In order to validate the supremacy of the PPDS-CD model, a series of experiments were performed and the results are highlighted under several aspects. The obtained simulation outcome ensured the effectual performance of the PPDS-CD model over the other compared methods.

Keywords: Wireless sensor networks, Clustering, Combinatorial method, En-route filtering, Partial key distribution

1. Introduction

Wireless Sensor Networks (WSNs) are developed progressively owing to its technical improvements in Microelectromechanical Systems (MEMS) [1]. Since WSNs is cost-effective, compact, and greater density features, it is applied in various applications. But, the extensive...
utilization needs appropriate solution for the security threats. One of the major threats is referred to be false report injection intrusion and results in data loss, unwanted power dispersion, and so on. The compromised node produces a negative report regarding the fictional event and sends it to sink node or base station (BS), exhaustion of node's power on the path. Moreover, the false alarms are accelerated for the missed events to the user. En-route filtering approaches as well as dynamic en-route filtering (DEF) and commutative cipher-based EF (CCEF) are used to provide better security to extend the system duration. Actually, DEF applies the hill-climbing scheme for key dissemination for earlier prediction of false report intrusions. The legitimate report is ensured by multiple nodes of keys and secret keys from global keys. As DEF applies maximum keys in key chain model, it is highly difficult for huge-size WSNs. Besides, CCEF depends upon the expansive public key structure.

Mostly, EF methods same constraints are observed in the fixed path routing which does not adopt the system lifespan in the model and fixed responses of various attacks. For instance, the shortest path or greedy routing results in fixed path routing named Greedy Perimeter-based Stateless Routing (GPSR). Here, the major constraints are resolved by the presented energy-aware dynamic routing and alternate one is catered using pre-deterministic key distribution. Such models are used for training the newly developed technology so that dynamic response of network and attacks could be reduced. Dynamic path routing acts as the tool for eliminating the energy-hole problem or hot spot issues; however, it provides several paths as well as Load Balancing (LB). Unfortunately, sensor networks from the hot spot hole as the power consumption are maximum when compared with distant nodes. Then, the network partition is performed as communication among diverse portions are interrupted in the system. Hence, energy-hole problem tends in network breaking which can be eliminated using dynamic path routing. The DEF [2] applies the hill-climbing method for key distribution and resolves the attacks to preserve the energy in significant manner. Every node sends the key to forwarding node and the transmitting nodes define the keys once the reports are sent and enable the forwarding node(s) to verify the reports. It uses the broadcasting hierarchy of wireless systems to defend against Denial of Service (DoS) attacks as well as multipath routing to counter topology modifications. DEF is capable of solving the insufficient memory when compared to alternate methods.

Numerous state of art en-route filtering techniques is probability based where the nodes in every cell distribute the shared keys with a predefined probability with middle nodes. Therefore, forwarded reports are confirmed in a probabilistic way by intermittent nodes due to
the fact that the false reports can be traveled over numerous hops before being dropped. This paper presents a novel En-Route Filtering Technique based on Partial Key Distribution System with combinatorial design (PPDS-CD) model for WSN. The presented PPDS-CD model aims to reduce the key storage overhead in cluster heads (CHs) as providing effective resiliency over compromised nodes in WSN. The presented model utilizes Modified Lee Sphere region and Modified Bloom Filter for the effective selection of nodes in the en-route filtering process. In order to validate the supremacy of the PPDS-CD model, a series of experiments were performed and the results are highlighted under several aspects.

2. Related works

Statistical EF (SEF) [3] is the first approach used for predicting invented reports. Moreover, global key pool is divided into non-overlapping blocks. The event predicting node produces a Message Authentication Code (MAC) by applying the recorded keys. Event prediction nodes select a center of stimulus (CoS) node for collecting and consolidating the attained prediction outcomes to generate a report with corresponding MACs. False reports accomplished at sink node might be predicted as BS is composed of shared keys. SEF has minimum filtering ability and fails to overcome impersonating intrusions. The CCEF conserves the power by earlier prediction. But it also experiences few constraints namely, fix path routing, not assuming Residual Energy (RE), and allocate the prediction ability. Underlying fixed path routing does not consider energy-aware; thus, it projects adverse impacts on network duration.

Secure ticket-based EF (STEF) [4] employs tickets provided by BS for report validation. It is performed similarly to SEF and DEF. The interleave hop-by-hop authentication (IHA) model depends upon the fixed path routing that experiences the constraints of CCEF. It requires interleaved upper and lower correlations among the sensor nodes to distribute sensor details. Because of the frequent changes and unreliable behavior of WSNs when it is impossible to gain defined routes. In addition, the associations require global awareness which is complicated and expensive for energy-scarce problem. A node in Bandwidth-Efficient Cooperative Authentication (BECAN) [5] method needs determined number of neighbors for authorization. It distributes the authorization keys of EF to the sensor nodes in a path. Bit compression is applied for bandwidth conservation. BECAN is not applicable to identify false routing data and defined dropping intrusions. In addition, newly deployed scheme is not suitable to counter selective dropping as well as false routing data with limited demerits derived from previous models.
Generally, Greedy perimeter-based stateless routing (GPSR) is utilized in EF approach which is elegant and effective. But the routing technology is developed for ad hoc networks which do not perform well in the network. It has elected a forwarding node between the candidate nodes nearby the sink node. In [6], projected multipath routing to reduce the enhancements in network security like eavesdropping and modification attacks. It is productive and defends these kinds of intrusions. In addition, LB has been presented with the help of opportunistic routing [7]. To determine the power consumption, first-order radio scheme has been applied [8]. Furthermore, the variables applied in the performance validation of first-order radio model derived from the previous approach. The reasonable energy-to-noise ratio is projected in [9]. In [10], maximum efforts were taken for enhancing the system duration by using the routing approaches. However, there is a requirement for extending the network lifespan in security approaches and eliminate routing to expand the network duration. From [11], the recent state of research is reviewed in WSNs.

In [12], prediction and countermeasures against Distributed DoS (DDoS) attacks in WSNs has been presented. These attacks drain the power; however, it causes data loss inside the system. It is used for predicting new messages and resist over attacks. Attacks and measures in sensor networks are defined in [13]. Then, in [14] EF techniques in WSNs are applied. Traditionally, it has revealed that unbalanced communication overhead in static sink-relied networks which results in hot spot problem [15]. These issues reduce the performance and mitigate the network duration. As a result, the final outcomes are composed of Mica2. Sensor clocks are synchronized by the application of synchronization elements in the energy-efficient time synchronization protocol (ETSP). Sensor nodes predict the position by using the localization unit.

3. The Proposed PPDS-CD Model

This section develops a novel PPDS-CD model which reduces the key storage burden in CH while exhibiting better resiliency over the compromised nodes in WSN. The detailed working of the PPDS-CD model is discussed in the succeeding subsections.

3.1. Assumptions

Assume that CHs and sensor nodes are incorporated by an opponent. If the adversary compromises a sensor node, then the details are collected in it are known by adversary. Then,
the accomplished data, intruder could change or modify the actual data and create a false packet. In addition, few other assumptions are given below.

- In this model, the shared sensor network with \( M \) sensor nodes for newly developed approach and classified as equal-sized cells with the help of modified Lee Sphere region. A cell contains \( m \) sensor nodes and BS is also available to validate the reports completely.
- A cell is composed of 2 divisions namely, normal sensor and CH nodes.
- For the newly developed approach, 3 CH is assumed to be in a cell. Additionally, there are 3 kinds of key sets namely, Type1, Type2, Type3 are produced from diverse sources. The key values are offered to CH present in different key sets. Therefore, CH communicates with same type of CHs in the entire system.
- CHs could be aware of the geographical position using localization method or in-built GPS. It is capable of resolving the position errors as the middle portion of the home cell.
- Any event is predicted using multiple sensor nodes. The sensor nodes that examine the event, produce a report and forward it to CHs. Followed by, CHs transmits the finishing report to BS by multi-hop path.
- Reports validation and transmission are processed by the CHs in WSN.
- The sensor nodes as well as CHs has individual IDs.

### 3.2. Partial Key Pre-distribution Scheme based on Combinatorial Method:

The integration of \((\alpha, \beta)\), in which \(\alpha\) defines group of elements and \(\beta\) denotes the collective subsets of \(\alpha\), named blocks \([\beta = \{y : y \subseteq \alpha\}]\). A Partially Balanced Incomplete Block Design (PBIBD) along with \(m\) associated classes \((\vartheta, \mu, \delta, \gamma, \tau)\) are defined the model that satisfies the given constraints [16]:

- \(|\alpha| = \vartheta, |\beta| = \mu\),
- The count of elements in every subset \(\beta\) is accurately \(\gamma\),
- The variety of \(\alpha\) exists in \(\delta\) blocks,
- Pair of varieties in \(\alpha\) is projected in \(\tau\) blocks of \(\beta\).

While \(\vartheta = \mu\), PBIBD is named as symmetric PBIBD which is implied as SPBIBD \((\vartheta, \gamma, \tau)\)
The difference set \((\vartheta, \gamma, \tau) \mod \vartheta\) is illustrated as set \(\omega = \{\omega_1, \omega_2, ..., \omega_{\gamma}\}\), where \(\omega_{\gamma}\) computes the exclusive element of \(\varphi_{\vartheta}\), where the element \(\omega\) is available and \(\omega \neq 0\) is represented as \(\omega = \omega_i - \omega_j \mod \vartheta\) accurately \(\tau\) ways. Followed by, blocks for symmetric model \((\vartheta, \gamma, \tau)\) could be attained using \(\omega, \omega + 1, \omega + 2, ..., \omega + (\vartheta + 1) \mod \vartheta\). For instance, the module \((7,3,1)\) is generated for symmetric design, difference set \(\{1,2,4\}\) could be employed. The final blocks would be \(\{1,2,4\}, \{2,3,5\}, \{3,4,6\}, \{4,5,7\}, \{5,6,1\}, \{6,7,2\}, \{7,1,3\}\). A multiplier \(\chi\) of applied difference set \((\omega)\) for \((\vartheta, \gamma, \tau)\) in Abelian set \((\psi, +)\) meets the gives features:

- \(m\) denotes the prime value in which \(\gcd(m, \vartheta) = 1\).
- \(m > \tau\) is projected by that \(\gamma - \tau = 0 \mod m\).

**Algorithm 1: Block Generation using Symmetric Design**

<table>
<thead>
<tr>
<th>Input: Symmetric design ((\vartheta, \gamma, \tau)) in which (\tau = 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output: (\gamma^2 + \gamma + 1) blocks of keys, a block is composed of (\gamma + 1) keys and 2 blocks have applied a shared key</td>
</tr>
<tr>
<td>Step 1: Identify Multiplier (a) for different group.</td>
</tr>
<tr>
<td>Step 2: Estimate the orbits by mapping (x \rightarrow ax \mod \vartheta)</td>
</tr>
<tr>
<td>Step 3: Identify difference set ({\omega_1, \omega_2, ..., \omega_{\gamma+1}}) of (\gamma + 1) length by the orbits.</td>
</tr>
<tr>
<td>Step 4: for (j = 1) to ((\gamma^2 + \gamma + 1)) do</td>
</tr>
<tr>
<td>Step 5: Block (j = {d_1, d_2, ..., d_{\gamma+1}})</td>
</tr>
<tr>
<td>Step 6: for (i = 1) to ((\gamma + 1)) do</td>
</tr>
<tr>
<td>Step 7: ({\omega_i = (\omega_i + 1) \mod (\gamma^2 + \gamma + 1)})</td>
</tr>
<tr>
<td>Step 8: end for</td>
</tr>
<tr>
<td>Step 9: end for</td>
</tr>
</tbody>
</table>

### 3.3. Modified Lee Sphere region

Here, the lee sphere applied for a selected lee distance \((\rho)\), is composed of adjacent cells where at-most \(\rho\) distance is accessed from the selected cell. In order to estimate the distance amongst 2 cells, addition of horizontal and vertical distance might be estimated. Consider every cell as a sensor node, which selects the neighboring nodes proficiency.
3.4. Modified Bloom Filter (MBF)

Here, MBF technique is used for the selection of cells (i.e., nodes) for en-route filtering process. In last decades, Bloom Filter was assumed to be a well-known and effective data structure applied for validating the membership which means that the element selection process is performed using bloom filter which identifies the existence of elements in a previous set. Basically, MBF demands set $S = s_1, s_2, s_3 \ldots, s_y$, a string of size $f$-bits as well as $t$ independent hash functions ($H_1, H_2, \ldots H_t$). Moreover, input for the data structure is represented as set $S = s_1, s_2, s_3 \ldots, s_y$, the size $f$-bits as well as $t$ independent hash functions ($H_1, H_2, \ldots H_t$). An item $(s_i)$ with hash function ($H_i$) makes a hash value and maps them from the range of $\{0,1,2, \ldots f-1\}$ equally, in which $\{0,1,2, \ldots f-1\}$ demonstrates the bits available in $f$-string. A bit of $f$-bit string is predetermined as 0 initially. $\forall s_i \in S$ are the hash values emanated by hash functions ($H_i$) to fix the respective values as 1 in $f$-bit string.

In order to validate the membership of specific element $s'$ from the given set $S$, the hash values are produced with the help of hash functions. Next, the hash values are related to accurate values of $f$-bit string. When the values are previously marked as 1, $s'$ is meant to be derived from $S$ and even if the single value is 0 then it is not accessible in $S$.

3.5. Processes involved in En-route Filtering

The CD-PEFS is comprised of initialization of sensor nodes and CHs. Furthermore, the process of report generation as well as EF models are described in the following.

3.5.1. Deployment

In this state, network controller is used for selecting the measure of parameters $T$ and $t$, in which $T$ implies the authorization to generate valuable reports and $t$ indicates the number of accurate endorsements needed for effective report validation. Also, network controller has emanated 4 master secret keys ($K_m, P^1_m, P^2_m, P^3_m$), a large prime value $P$ as well as hash function $H(\cdot)$.

3.5.2. Initialization of sensor nodes

The network controller allocates the master secret keys ($K_m, P^1_m, P^2_m, P^3_m$) to all sensor nodes. Also, the value of, $H(\cdot)$, position of sensor node ($x_{loc}$) as well as center portion of home cell ($x_c, y_c$) to all the sensor nodes. First, the secret key $K_x$ is evaluated by a sensor node $x$ and
integrate the master secret key $K_m$ along with location $(x_{loc})$. Next, sub-master key $(p^i_m)$ is evaluated by unification of $p^i_m$ with position of home cell. Afterward, the secret key $(p^i_x)$ is determined by applying the secret key and location of sub-master. $p^i_x$ is a secret key applied to secure the communication of CH.

**3.5.3. Initialization of cluster heads**

Here, network controller has adopted a master key $K_m$ and $p^i_m$ (Type 1, Type 2, Type 3 CHs are declared to $p^1_m$, $p^2_m$, $p^3_m$, correspondingly to the CHs in a cell. Moreover, a CH is allocated as T and $(x_c, y_c)$. A CH applies the master key $K_m$ for accomplishing exclusive secret key $X_i$ and expressed as:

$$X_i = H(K_m|C_{loc})$$

In which $C_{loc}$ defines the CH location. The secret key saves the communication between BS and CH. Also, CH estimates the sub-master secret key under the application of $P^i_m$ as:

$$P_{sm} = H(p^i_m|(x_c,y_c))$$

Where $(x_c, y_c)$ indicates the position of a home cell. It is applied for securing the inter-cell transmission in a home cell. The authenticated and secured reports are generated by allocating the CH with the help of combinatorial model. To allocate the combinatorial method relied on key-set generation. While generating the key-sets by symmetric design, minimum prime value $k$ is applied and represented as $C \leq k^2 + k + 1$, in which $C$ is overall CHs of specific class. Next, symmetric method is deployed as $(k^2 + k + 1, k + 1, 1)$. In particular, multiplier$(a)$ for different set of symmetric design $(v, k, \lambda)$ is found in Abelian set $(Z_v, +)$. Followed by, multiplier is applied to gain the orbits of Abelian set $(Z_v, +)$. By using appropriate orbits, the difference set of size $k + 1$ has been generated. Consequently, the key-sets are emanated by applying the difference set. Moreover, the information about block generation with difference set is attained. Besides, produced key-sets are allocated to CHs specifically. Diverse key-pools have been applied for accomplishing key-sets for various classes of CHs.

**3.5.4. Report generation**

The $2T$ sensor nodes from a node predict an event that generates the report. Once the report generation is completed, the candidate sensor nodes retrieve the secret share $M_\chi$ of report $M$ with the help of pre-determined threshold $(t, T)$ LSSS as provided in Eq. (3).
Here, $M_x$ is derived by univariate polynomial of degree $(t - 1)$ across definite field $GF(P)(GF(.))$ means the finite Galois field by $X_x$ and $P_i$, in which $p_i$ defines the complete division of $M$ so that $0 \leq i < t$ is accomplished. The $t$ and $P$ are previously loaded attributes. A sensor node produces the confidential share so that a BS makes use of endorsement. Then, the $2T$ sensor nodes encrypt the report $M$ by applying $P_x^i$ and expressed as shown below:

$$M_{enr}^i = E_{P_x^i}(M)$$

Every sensor nodes forward the tuple $\{M_x, x, M_{enr}^i\}$ to 3 CHs, in which $x$ defines the ID of a sensor node. Also, CH selects a $T$ tuples from $2T$ tuples so that a CH selects diverse tuples. CHs make sure of this by distributing the IDs of candidate sensor nodes.

When the tuples are received from $T$ sensor nodes, CHs validates the efficacy of the report, event’s position, and location of sensor nodes by forwarding the tuple. Sensor nodes in a tuple generation should be evolved from the same cell, otherwise, the report is lost by CH. First, CH produces a MAC for message $M$ by applying unique secret key with BS $(X_i)$ as $MAC_{X_i}(M)$ (in which $i$ defines the ID of CHs) and forwards it to alternate CHs in similar cell. While acquiring the MAC from one or more CHs, a CH begins to prepare the final report while participating in report production. Next, contribution of CHs is used in generating MAC $(MAC_i)$ for report $M$ with the $k' + 1$ keys. At last, CHs offers consequent report of the $\{M_1, M_2, ..., M_T, ID_1, ID_2, ..., ID_T, MAC_1, MAC_2, ..., MAC_{k'+1}, ID_{k_1}, ID_{k_2}, ..., ID_{k'+1}, MAC_{X_1}, MAC_{X_2}\}$, where $\{M_1, M_2, ..., M_T\}$ indicates the secret shares, $\{ID_1, ID_2, ..., ID_T\}$ defines the ID of involved sensor node, $\{MAC_1, MAC_2, ..., MAC_{k'+1}\}$ depicts the MACs produced by keys from key-set, $ID_{k_i}$ implies the IDs of keys employed to make MACs and $MAC_{X_1}, MAC_{X_2}$ demonstrates MACs forwarded by 2 CHs in similar cell.

3.5.5. Shared key discovery

CD-PEFS applies a symmetric model for generating the key-sets to make sure that a pair of key-sets are comprised of single key. In addition, forwarding report is comprised of key indexes applied by CHs for MAC generation. Thus, a shared key from 2 CHs is attained by relating the key indexes in a report with previously saved in CHs.
3.5.6. En-route filtering and sink verification

In EF model, forwarding CH verifies the authentication of a report when it can be allocated with a key-set in initialization phase. When the CH does not have the key-set, afterward it forwards the report to consecutive hop. Else, it validates the general key applied for MAC generation linked with report. When a common key is identified, CH validates the MAC transmitted with a report by reforming MAC with the help of general key. In case of a mismatch, the report is lost, otherwise, it is relayed to next hop. BS performs 2-way authentication for a received report. At the first state, it validates the report for effective share \(M_x\) and checks the affinity of home cell to participate sensor nodes. It is repeated by MACs \(MAC_i\) validation. Furthermore, BS validates the accuracy of \(MAC_{X_1}, MAC_{X_2}\). If MACs \(MAC_{X_1}\) or \(MAC_{X_2}\) is considered to be accurate, BS recovers \(M\) from \(M_x\). It is repeated by identifying the result to \(t\)-variable linear function to gain \(p_i\), in which \(i = [0, t - 1]\) in Eq. (3) and achieves \(M\).

4. Performance Validation

This section validates the performance of the PPDS-CD technique in terms of different aspects. The proposed model is simulated using MATLAB R2014a. In addition, the results are investigated under varying number of compromised CHs and cell count. The parameter settings involved in the experimentation process is tabulated in Table 1.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of sensor nodes</td>
<td>10005</td>
</tr>
<tr>
<td>Total no. of cells</td>
<td>667</td>
</tr>
<tr>
<td>Total sensor nodes in every cell</td>
<td>15</td>
</tr>
<tr>
<td>Cell size</td>
<td>50×50m²</td>
</tr>
<tr>
<td>CHs in every cell</td>
<td>3</td>
</tr>
<tr>
<td>Transmission range of sensor nodes</td>
<td>25m</td>
</tr>
<tr>
<td>Transmission range of CHs</td>
<td>50m</td>
</tr>
<tr>
<td>(T, t)</td>
<td>5, 4</td>
</tr>
<tr>
<td>Size of report</td>
<td>36 Bytes</td>
</tr>
<tr>
<td>Size of MAC</td>
<td>4 Bytes</td>
</tr>
</tbody>
</table>
4.1. Results Analysis in terms of Fraction of Cells Disconnected

Fig. 1 investigates the results analysis of the presented PPDS-CD model with other existing methods [17, 18] in terms of fraction of cells disconnected over the total number of cells of 200. Besides, the methods devised by Mitra et al. and Alok et al. have portrayed ineffective outcomes over the compared methods. Besides, the methods developed by Bag and Bag & Roy models have demonstrated competitive performance. But the figure has shown that only minimal fraction of cells disconnected by the presented PPDS-CD model compared to other existing methods.

![Total Number of Cells (200)](image)

Fig. 1. Result analysis of PPDS-CD model in terms of cells disconnected on 200

For instance, under the presence of 50 compromised CHs, the proposed PPDS-CD model has reached a minimum of 0.02 fraction of cells disconnected whereas the other methods such as...
Mitra et al., Bag and Roy, Bag, and Alok et al. methods have shown reduced results with the 0.085, 0.085, 0.065, and 0.05 respectively. Likewise, under the existence of 150 compromised CHs, the presented PPDS-CD model has reached a minimum of 0.32 fraction of cells disconnected while the other methods such as Mitra et al., Bag and Roy, Bag, and Alok et al. methods have shown limited results with the 0.492, 0.476, 0.432, and 0.39 correspondingly. Simultaneously, under the application of 300 compromised CHs, the proposed PPDS-CD model has attained a minimum of 0.8 fractions of cells disconnected and the other methods such as Mitra et al., Bag and Roy, Bag, and Alok et al. models have depicted reduced results with the 0.951, 0.947, 0.9, and 0.831 respectively.

\[ \text{Fraction of Cells Disconnected} \]

![Total Number of Cells (800)](image)

**Fig. 2.** Result analysis of PPDS-CD model terms of cells disconnected on 800

Fig. 2 examines the results analysis of the proposed PPDS-CD model with other existing methods terms of fraction of cells disconnected over the total count of cells of 800. Besides, the methods devised by Mitra et al. and Alok et al. have depicted ineffective outcomes over the compared methods. Besides, the methods deployed by Bag and Bag & Roy models have demonstrated competitive performance. However, the figure has shown that the only minimal fraction of cells disconnected by the established PPDS-CD model compared to other existing methods. For instance, under the application of 50 compromised CHs, the proposed PPDS-CD
The model has reached the least value of 0.019 fractions of cells disconnected whereas the other methods such as Mitra et al., Bag and Roy, Bag, and Alok et al. approaches have shown reduced results with the 0.083, 0.083, 0.061, and 0.056 respectively. Similarly, under the presence of 150 compromised CHs, the proposed PPDS-CD model has obtained to a minimum of 0.37 fraction of cells disconnected whereas the other schemes like Mitra et al., Bag and Roy, Bag, and Alok et al. methods have exhibited reduced results with the 0.42, 0.4, 0.392, and 0.35 respectively. At the same time, under the presence of 400 compromised CHs, the proposed PPDS-CD model has attained a minimum of 0.78 fractions of cells disconnected whereas the other methods such as Mitra et al., Bag and Roy, Bag, and Alok et al. methods have shown lower results with the 0.907, 0.9, 0.888, and 0.801 respectively.

**Fig. 3.** Result analysis of PPDS-CD model in terms of cells disconnected on 1400

Fig. 3 inspects the results analysis of the presented PPDS-CD model with other existing methods by means of fraction of cells disconnected over the total number of cells of 1400. Besides, the models introduced by Mitra et al. and Alok et al. have portrayed ineffective outcomes over the compared methods. On the other hand, the methods developed by Bag and Bag & Roy models have demonstrated competing performance. However, the figure portrayed
that the only minimal fraction of cells disconnected by the projected PPDS-CD model compared to other existing methods. For instance, under the existence of 50 compromised CHs, the proposed PPDS-CD model has accomplished a minimum of 0.362 fractions of cells disconnected while the other methods such as Mitra et al., Bag and Roy, Bag, and Alok et al. methods have showcased minimum results with the 0.426, 0.4, 0.38, and 0.356 respectively. Likewise, under the presence of 200 compromised CHs, the proposed PPDS-CD model has reached a reduced 0.7 fraction of cells disconnected whereas the other methods such as Mitra et al., Bag and Roy, Bag, and Alok et al. models have shown reduced results with the 0.85, 0.841, 0.8, and 0.735 respectively. Meantime, under the presence of 400 compromised CHs, the proposed PPDS-CD model has achieved a minimum of 0.73 fractions of cells disconnected whereas the other methods such as Mitra et al., Bag and Roy, Bag, and Alok et al. methods have shown minimal results with the 0.9, 0.895, 0.871, and 0.79 correspondingly.

4.2. Results Analysis interms of Fraction of Links Broken

Fig. 4 scrutinizes the results analysis of the presented PPDS-CD model with other existing methods by means of fraction of link broken over the total number of cells of 200. Besides, the methods devised by Mitra et al. and Alok et al. have demonstrated poor results over the related models. Followed by, the methods implied by Bag and Bag & Roy models have depicted competing performance. However, the figure has shown that the only minimal fraction of link broken by the presented PPDS-CD model related to other previous methods. For instance, under the presence of 10 compromised CHs, the proposed PPDS-CD model has achieved a minimum of 0.03 fraction of link broken while the other methods such as Mitra et al., Bag and Roy, Bag, and Alok et al. methods have shown low results with the 0.095, 0.09, 0.071, and 0.052 respectively. Likewise, under the application of 40 compromised CHs, the proposed PPDS-CD model has accomplished a minimum of 0.22 fraction of link broken whereas the other methods such as Mitra et al., Bag and Roy, Bag, and Alok et al. technologies have depicted reduced results with the 0.332, 0.316, 0.292, and 0.253 respectively. Simultaneously, under the existence of 80 compromised CHs, the proposed PPDS-CD model has reached a minimum of 0.5 fractions of link broken while the other methods such as Mitra et al., Bag and Roy, Bag, and Alok et al. methods have illustrated reduced results with the 0.8, 0.714, 0.654, and 0.617 respectively.
Fig. 4. Result analysis of PPDS-CD model interms of link broken on 200

Fig. 5 investigates the results analysis of the presented PPDS-CD model with other former models interms of fraction of link broken over the total number of cells of 800. Besides, the methods devised by Mitra et al. and Alok et al. have portrayed ineffective outcomes over the compared methods. Next, the methods developed by Bag and Bag & Roy models have depicted competing performance. Therefore, the figure showed that only minimal fraction of link broken by the newly developed PPDS-CD method compared to other classical technologies. For sample, under the existence of 10 compromised CHs, the proposed PPDS-CD model has reached a minimum of 0.01 fraction of link broken whereas the other methods such as Mitra et al., Bag and Roy, Bag, and Alok et al. schemes have shown reduced results with the 0.065, 0.056, 0.031, and 0.02 respectively. In line with this, under the presence of 40 compromised CHs, the proposed PPDS-CD model has attained a minimum of 0.19 fraction of link broken whereas the other frameworks like Mitra et al., Bag and Roy, Bag, and Alok et al. methods have shown reduced results with the 0.3, 0.381, 0.369, and 0.212 correspondingly. Simultaneously, under the presence of 80 compromised CHs, the projected PPDS-CD model has achieved a minimum of 0.476 fractions of link broken while the other methods such as
Mitra et al., Bag and Roy, Bag, and Alok et al. methods have represented minimum results with the 0.771, 0.69, 0.627, and 0.59 respectively.

**Fig. 5.** Result analysis of PPDS-CD model in terms of link broken on 800

Fig. 6 investigates the results analysis of the projected PPDS-CD model with other previous methods in terms of fraction of link broken over the total number of cells of 1400. Besides, the methods devised by Mitra et al. and Alok et al. have implied poor outcomes over the compared methods. Besides, the models deployed by Bag and Bag & Roy models have demonstrated competitive performance. However, the figure illustrated that the only minimal fraction of link broken by the presented PPDS-CD model related to conventional approaches. For sample, under the existence of 10 compromised CHs, the proposed PPDS-CD model has reached a minimum of 0.01 fraction of link broken while the other methods such as Mitra et al., Bag and Roy, Bag, and Alok et al. methods have shown minimum results with the 0.055, 0.041, 0.029, and 0.011 respectively.
Likewise, under the application of 40 compromised CHs, the proposed PPDS-CD model has attained minimum of 0.07 fraction of link broken and the other methods such as Mitra et al., Bag and Roy, Bag, and Alok et al. technologies have depicted reduced results with the 0.29, 0.271, 0.249, and 0.2 respectively. At the same time, under the existence of 80 compromised CHs, the presented PPDS-CD model has reached a minimum of 0.35 fraction of link broken whereas the other models such as Mitra et al., Bag and Roy, Bag, and Alok et al. methods have indicated limited results with the 0.75, 0.679, 0.617, and 0.578 respectively.

5. Conclusion

This paper has presented an efficient PPDS-CD technique for WSN. The presented PPDS-CD model intends to the minimization of the key storage overhead in CHs while providing effective resiliency over compromised nodes in WSN. The presented model utilizes the Modified Lee Sphere region and MBF technique for the effective selection of nodes in the en-route filtering process. In order to validate the supremacy of the PPDS-CD model, a series of experiments were performed and the results are highlighted under several aspects. The obtained simulation
outcome ensured the effectual performance of the PPDS-CD model over the other compared methods. Therefore, the presented model is found to be effective over the other compared methods. In future, the performance of the PPDS-CD model can be improved by the use of different clustering algorithms.

References


