Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.035499
Article

Real-Time Data Transmission with Data Carrier Support Value in Neighbor Strategic Collection in WSN

S. Ponnarasi[1,*] and T. Rajendran[2]

[1]Department of Computer Science, Periyar University, Salem, Tamil Nadu, 636011, India
[2]Department of Computer Science, Government Arts & Science College, Kangeyam, Tamil Nadu, 638108, India
*Corresponding Author: S. Ponnarasi. Email: sponnarasi2022@gmail.com
Received: 23 August 2022; Accepted: 15 November 2022

Abstract: An efficient trust-aware secure routing and network strategy-based data collection scheme is presented in this paper to enhance the performance and security of wireless sensor networks during data collection. The method first discovers the routes between the data sensors and the sink node. Several factors are considered for each sensor node along the route, including energy, number of neighbours, previous transmissions, and energy depletion ratio. Considering all these variables, the Sink Reachable Support Measure and the Secure Communication Support Measure, the method evaluates two distinct measures. The method calculates the data carrier support value using these two metrics. A single route is chosen to collect data based on the value of data carrier support. It has contributed to the design of Secure Communication Support (SCS) Estimation. This has been measured according to the strategy of each hop of the route. The suggested method improves the security and efficacy of data collection in wireless sensor networks. The second stage uses the two-fish approach to build a trust model for secure data transfer. A simulation exercise was conducted to evaluate the effectiveness of the suggested framework. Metrics, including PDR, end-to-end latency, and average residual energy, were assessed for the proposed model. The efficiency of the suggested route design serves as evidence for the average residual energy for the proposed framework.

Keywords: Data carrier support; data collection; neighbor strategy; secure routing; wireless sensor network

1 Introduction

Modern society has run over the support of information technology which supports access to various services in different domains. Among them, the Wireless Sensor Network (WSN) is identified as a key entity supporting multiple services' entry. In general, the WSN is framed with the support of several sensor nodes with limited power or energy and a Transceiver capable of communicating with the other sensor nodes located within its own transmission range. This encourages cooperative transmission to be performed between the source as well as the destination to achieve any data

transmission. Such suitable transmission is performed by adapting a routing protocol to support data communication [1].

The sensor nodes are geographically distributed throughout the network, and the location of the sink node and the data sensors would be at different diagonals of the grid. To perform data collection, data packets are transmitted through the intermediate node. The presence of malicious nodes in the route would involve various threats like eavesdropping, modification, and many more. To achieve higher performance in data transmission, it is significant to consider security parameters [2].

Secure routing is performed in several ways, either by data or route levels. The data level security is approached by adapting some encryption standards. In this approach, the data present in the packet has been encrypted using some secret keys, which are decrypted by the destination node. Route-level security is enforced in the routing scheme. This paper presents a route-level security scheme to support data collection performance in WSN.

Data collection is retrieving data from data sensors where the data is available. The WSN has been used for several purposes. For example, the Warfield environment uses WSN to collect data from different battlefield locations to get information related to many constraints like troop position, requirements, etc. They would use any routing protocol to achieve this, but malicious nodes would leak the same information to the enemy troops. This encourages the enforcement of secure routing in data collection. WSNs play a critical role in establishing networks and facilitating numerous services for smart cities because of their low cost, rapid deployment, and self-organized qualities. In the context of smart city environments, ubiquitous sensor nodes collect physical data about urban environments and manage public or private infrastructure. As a result, many smart city studies have been conducted using WSN technologies. WSN often connects via a multi-hop path due to its limited radio communication range. A routing protocol model that defines data forwarding and transmission path is a necessary procedure to consider in this scenario since it will directly impact WSN performance, such as network lifetime, PDR, and end-to-end packet delay.

The neighbor strategy has been identified as the more supporting factor in choosing a data forwarder. For example, consider route R, which comprises K number of intermediate nodes. Each node would have a different energy, number of transmissions, number of neighbors, etc. Considering all this, you can measure the trust of any intermediate node and data collection; support influenced by the intermediate node can be measured. This research presents a novel data collection and secure routing technique by considering all these factors.

Researchers have focused much attention on the issue of how to implement reliable and efficient data transfer, which is where routing protocols come in. Routing models developed using traditional protocols may not be well suited to network security since they often assume that all sensor nodes are trustworthy and the network is not under attack. If this is correct, then improving routing security is crucial to ensuring that networks perform as intended.

The contributions of this work are as follows,

- To design Secure Communication Support (SCS) Estimation, this has been measured according to the strategy of each hop of the route.
- It is important to consider at least two-hop neighbor information to prevent insecure route selection from estimating a trustworthy value.
- A data classification should be used to implement the encryption methods and schemes.
- Classifying the data into various levels of confidentiality is essential.

2 Related Works

Several algorithms are available for secure routing and data collection in WSN. This section presents a set of techniques related to the issue. The authors [3] present a secure routing algorithm that combines k means clustering and ant lion optimization algorithms. Clustering is performed with K means, and ant lion optimizer is used for route selection. The method uses multi-curve Elliptic curve cryptographic routing (MALOKSER), which encodes the data and routes toward secure routing.

The authors [4] propose an effective Enhanced Fuzzy C Means and Adaptive TDMA Scheduling (ECATS) approach as a protocol to facilitate network communication. So that data packets are delivered to the mobile sink promptly. We introduce the revolutionary protocol known as Neural Elliptic Galois (NEG) cryptography for effective data security. Additionally, for improved safety, location privacy is taken into mind. To handle data aggregation among several nodes in the network, cluster heads (CH) are chosen based on energy. This paper introduces a hybridization of TDMA-based Ant Lion Optimization scheduling for optimal CH selection and improved energy efficiency. The authors [5] discuss a secure routing protocol that uses an energy parameter named EOSR. It measures the trust value for various nodes. Based on the trust measure, the technique chooses a route. The trust value is calculated according to the route length and energy.

The authors [6] propose a secure routing protocol that combines the LEACH algorithm with a crypto scheme. The HCBS algorithm uses ECC to perform encryption to support higher performance in routing. The authors [7] proposed a trusted routing algorithm that is described as suitable for different networks. The method uses the multi-flow data topology (MDT) approach, which is ideal for mitigating various attacks. The energy parameter of sensor nodes has been used with the combination of nodes' location to measure the nodes' trust. The authors [8] proposed a link quality-based secure routing algorithm with K means clustering. The nodes are grouped according to the energy values using K means clustering, and the fitness of the route has been evaluated with link quality. The node selection is performed according to the fitness and route selection is performed.

The authors [9] survey different secure routing protocols for WSNs. Also, various security issues have been discussed regarding secure data communication in a network. The authors [10] analyze different secure routing approaches and propose novel algorithms considering the energy and resiliency toward attack. Based on these two, the node's fitness has been verified to perform secure routing. The authors [11] present a TESRP (Trust and Energy-aware Secure Routing Protocol) that performs route selection according to hop count, energy, and trust value. According to the features mentioned above, route selection is performed. The authors [12] propose a data collection algorithm for a virtual grid environment. The sensor nodes can discover a minimum route for data transmission toward the sink node.

The authors [13] propose that the network nodes are grouped under region-specific, where a selection of CH is performed with the base station and mobile nodes. This reduces the time complexity to provide more lifetimes. The authors [14] review various routing protocols to collect big data in large-scale WSN networks. The authors [15] define the routing as enforced with the Hamilton loop and PEGASIS approach. The local optimization is performed by inserting a mobile agent into the network in an optimal location with the support of the Hamilton loop. The mobile agent collects and transfers data in the network toward the sink. The authors [16] propose a data collection algorithm for a client-server model is presented. The nodes are grouped under various clusters. Node under a cluster transmits data to the cluster head according to a sending threshold informed to the sink node. CH, in turn, receives data and sends it to the sink node. However, the selection of CH is performed based on energy.

The authors [17] proposed that redundancy problems are considered to perform data collection. The method monitors packets received and evaluates their lifetime before being transmitted to the next hop. If the time value is expired, it will not be transferred to the other node or sink. In recent years, there has been enhanced effort in research on routing protocols due to the developing trend in the security field [18]. SAODV [19] is an AODV security enhancement that protects against routing threats. All routing messages in SAODV are digitally signed to ensure data integrity and authenticity. Intermediate nodes cannot send RREP in this circumstance because the destination node signs the RREP message. Although SAODV introduces a double signature solution to address this issue, it will undoubtedly raise the strain on intermediary nodes. To counteract SAODV's deleterious effects, Cerri and Ghioni created the A-SAODV protocol [20].

On the other hand, the preceding suggestions are security enhancements of existing ad hoc routing protocols incompatible with resource-constrained WSNs. In WSNs, SAR is a safe routing technique that can find the shortest path with the appropriate security properties [21]. The source node sets the route's desired security level. Routing packets can only be decrypted by nodes with the same security level and encryption keys. SAR can provide data confidentiality to some extent, but the cryptographic primitives built on it have a considerable encryption overhead, limiting its appeal for WSN applications [22]. Work [23] developed a new cross-layer statistic called anticipated forwarding counter (EFW) for reliable routing in wireless networks. The EFW can encourage node collaboration while also addressing the issue of selfish conduct.

In WSNs, [24] presents a Bayesian game strategy for preventing DoS attacks. Then, a secure routing protocol is provided by merging the Bayesian technique with the LEACH protocol. These routing protocols are designed to address a specific attack, which is insufficient to assure network security. The nodes in some proposed systems [25] are expected to collaborate while following a common routing protocol. On the other hand, the smartness of nodes is highly frequent in ad hoc and IoT networks. As a result, this component must be handled carefully while creating an energy-efficient plan for these networks. Many methods adjust a routing protocol [26], sleep behavior, coordination method, data aggregation method [27], hop division, cluster divisions, and so on to focus on the specific contribution of every node to energy efficiency. The nodes may intelligently coordinate with one another based on the status of each node. The nature of node deployment also substantially impacts the network's performance and lifespan. In such networks, energy efficiency solutions should take advantage of the density or redundancy of nodes [28]. There is enough room in a WSN-based IoT network to consider as many parameters as feasible while creating an energy-efficient routing. All approaches suffer to gain higher performance in safe routing and data collecting in WSN. Some of the issues have been uncovered by examining the works above of literature. As long as a node seems to be or forwards traffic connected with an instance, it may belong to any instance. Nodes in this scenario must thus be active both during the period allocated to its traffic and throughout the active time allotted to the other instances in which they participate. According to the literature review, the lack of a trusted routing channel between nodes means that the current approaches are still open to routing attacks. The trustworthy routing path is frequently statically found and used for transmission in many existing methods. Nodes in a statically discovered trustworthy path could eventually behave maliciously and aid a routing attack. Therefore, a safe routing strategy is required, one that dynamically determines the trusted path and disregards the involvement of hostile nodes in data transfer. The suggested approach should also guarantee a tamper-proof system and a moderate time complexity required in determining the trusted path

3 Neighbor Strategic Real-Time Trust Aware Routing and Data Collection

The proposed neighbor strategic real-time secure routing and data collection algorithm discovers the routes available [29–32]. Route discovery is performed by using a broadcast mechanism. For the route identified, the technique collects information related to sensor nodes. The method estimates various route selection and data collection measures according to the strategy obtained. The exact method is presented in this section.

3.1 Collection System

The architecture of the proposed neighbor strategic secure routing technique is represented in Fig. 1. The functional components of the system have been explained in detail in this section.

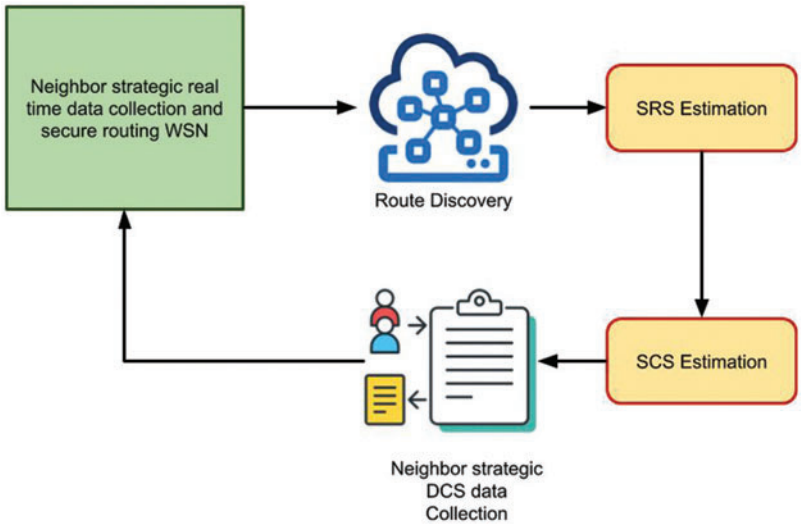

Figure 1: Architecture of proposed neighbor strategic secure routing and data

3.2 Route Discovery

The routes have been identified between the data sensor and the sink node by discovering the routes. The method generates the NS-RREQ message to perform route discovery, which contains the source and destination details. The generated packet has been broadcast in-network, and the neighbor receives the packet. If there is an entry for the destination node in the neighbor table, the neighbor generates the NN-RREP packet toward the source node. Otherwise, the packet has been forwarded to the data sensor. Finally, a set of nodes with the entry for the destination node then node produces an NS-RREP packet and tags information related to the number of neighbors, number of transmissions involved, energy, and so on. The sink node receives NS-RREP messages and extracts the route and other features to update the strategic table.

3.3 Uplink Training

Users broadcast pilot symbols in the uplink, and every BS then evaluates its users' channels. Consider that users from various cells send the same pilots simultaneously, with a one-to-one pilot reuse factor. A K $\times$ τ matrix ΦH gives pilot signals of K users with orthogonality property $\overline{\Phi}^{H}\Phi = \tau\overline{\mathbf{I}}_{K}$, ($K \leq \tau$).

Received pilot symbols at BS i are given by an M × τ matrix $\mathbf{Y}_i$ as Eq. (1),

$$\mathbf{Y}_i = \sum_{l=1}^{L} \sqrt{q}\mathbf{G}_{il}\Phi^H + \mathbf{N}_i \tag{1}$$

for evaluation of channel $\mathbf{g}_{ilk}$at BS i, a sufficient statistic is an Eq. (2)

$$\mathbf{z}_{ik} = \frac{1}{\sqrt{q\tau}}\mathbf{Y}_i\phi_k = \sum_{l=1}^{L} \mathbf{g}_{ilk} + \mathcal{CN}\left(\mathbf{0}, \frac{1}{\tau q}\mathbf{I}_M\right) \tag{2}$$

We have $\mathbf{z}_{ik} \sim \mathcal{CN}(\mathbf{0}_M, \zeta_{ik}\mathbf{I}_M)$ where Eq. (3)

$$\zeta_{ik} \triangleq \sum_{l=1}^{L} \beta_{ilk} + \frac{1}{\tau q} \tag{3}$$

3.4 Uplink Data Transmission

Because this article is based on multiplexing pilot assignments, each cell uses the same pilot sequences given to each user. $\Phi = (\varphi_1, \varphi_2, \ldots, \varphi_k, \ldots, \varphi_K)^T$ T indicates k × τ dimensional pilot sequence matrix allocated to all K users in cell i. τ is pilot sequence length, which agrees with orthogonality between pilots, $\Phi\Phi^H = I_K \cdot I_K$ is a $K \times K$ K dimension unit matrix. Finally, pilot $\mathbf{Y}_i^p$ received by BS in cell i is represented by Eq. (4),

$$\mathbf{Y}_i^p = \sqrt{P_p}\sum_{j=1}^{L}\sum_{k=1}^{K} \mathrm{h}_{jki}\varphi_k + \mathrm{N}_i^p \tag{4}$$

The received signal corresponding is written as Eq. (5),

$$\hat{r}_n = \sqrt{p_u}\hat{\mathrm{a}}_n^H \mathrm{g}_n x_n + \sqrt{p_u}\sum_{i=1,i\neq n}^{N} \hat{\mathrm{a}}_n^H \mathrm{g}_i x_i + \hat{\mathrm{a}}_n^H \mathrm{n} \tag{5}$$

Considering BS performs ZF detection, the interference term in the denominator is given as Eq. (6)

$$\hat{\mathrm{a}}_n^H \mathrm{g}_i = \left[\frac{\hat{\mathrm{g}}_n}{\hat{\mathrm{g}}_n^H \hat{\mathrm{g}}_n}\right]^H \mathrm{g}_i = \frac{\hat{\mathrm{g}}_n^H \mathrm{g}_i}{\hat{\mathrm{g}}_n^H \hat{\mathrm{g}}_n}$$

$$\overline{\mathbf{Y}}_i\mathbf{g}_{iik} + \left(\left(\mathrm{g}_n^{\mathrm{NLOS}}\right)^H \mathrm{g}_i^{\mathrm{NLOS}} + \sum_{\substack{j\in\psi_m \\ j\neq n}} \left(\mathrm{g}_j^{\mathrm{NLOS}}\right)^H \left(\mathrm{g}_i^{\mathrm{LOS}} + \mathrm{g}_i^{\mathrm{NLOS}}\right) + \left(1/\sqrt{p_p}\,\mathrm{N}_n\right)^H \mathrm{g}_i^{\mathrm{LOS}} + 1/\sqrt{p_p}\,(\mathrm{N}_n)^H \mathrm{g}_i^{\mathrm{NLOS}}\right) \tag{6}$$

We define the LOS interference $I_{ni} \triangleq \left(\mathrm{g}_n^{\mathrm{NLOS}}\right)^H \mathrm{g}_i^{\mathrm{NLOS}}$ given in Eq. (7)

$$\mathrm{g}_i^{\mathrm{LOS}} = \Omega_{ni}\left[1 + \ldots + e^{j(M-1)d\theta_{mi}}\right] \tag{7}$$

Using the property of the sum of exponentials, it is given by Eq. (8)

$$(\mathrm{g}_n^{\mathrm{LOS}})^H \mathrm{g}_i^{\mathrm{LOS}} = \Omega_{ni} \frac{e^{jMd\theta_{ni}} - 1}{e^{jd\theta_{ni}} - 1} = \Omega_{ni} \frac{-e^{-j\frac{\mu}{2}d\theta_{ni}}(-e^{-j\frac{\mu}{2}d\theta_{ni}} - e^{j\frac{M}{2}d\theta_{ni}})}{-e^{-j\frac{j}{2}d\theta_{ni}}(-e^{j\frac{\mu}{2}d\theta_{ni}} - e^{-j\frac{2}{2}d\theta_{ni}})}$$

$$= \Omega_{ni} \left[\frac{\sin\frac{(Md\theta_{mi})}{2}}{\sin\frac{(d\theta_{mi})}{2}} \right] e^{jd\theta_{mi}\frac{(M-1)}{2}}$$

$$\frac{1}{M}\grave{\mathrm{g}}_n^H \grave{\mathrm{g}}_n = \frac{1}{M}\left(\mathrm{g}_n^{\mathrm{Los}} + \mathrm{g}_n^{\mathrm{NLOs}} + \sum\nolimits_{\substack{j\in\mathcal{E}_m \\ j\neq n}} \mathrm{g}_j^{\mathrm{NL.os}} + \frac{1}{\sqrt{p_p}}\mathrm{N}_n \right)^H$$

$$\times \left(\mathrm{g}_n^{\mathrm{LOS}} + \mathrm{g}_n^{\mathrm{NLos}} + \sum\nolimits_{\substack{j\in\mathcal{W} \\ j\neq n}} \mathrm{g}_j^{\mathrm{NLLos}} + \frac{1}{\sqrt{p_p}}\mathrm{N}_n \right), \tag{8}$$

$$\frac{1}{M}\mathbf{h}_i^H \mathbf{h}_j = \begin{cases} 1, \forall i = j \\ 0, \text{otherwise.} \end{cases}$$

Using this property in Eq. (9),

$$\frac{1}{M}\grave{\mathrm{g}}_n^H \grave{\mathrm{g}}_n \xrightarrow{a.s} \beta_n + \sum\nolimits_{\substack{\in\mathbb{W}_m \\ j\neq n}} \frac{\beta_j}{1+K_j} + \frac{1}{p_p}$$

$$|I_{ni}|^2 = \frac{\Omega_{ni}^2}{M^2\left(\beta_n + \sum_{j\in W_m}\frac{\beta_j}{1+K_j} + \frac{1}{p_p}\right)^2}\left[\frac{\sin\left(\frac{Md\theta_{ni}}{2}\right)}{\sin\left(\frac{d\theta_m}{2}\right)}\right]^2 \tag{9}$$

The proposed channel estimator is given by Eq. (10)

$$\hat{\mathbf{g}}_{iik}^{\mathrm{prop}} = M\beta_{iik}\frac{\mathbf{z}_{ik}}{||\mathbf{z}_{ik}||^2} \tag{10}$$

Its MSE represented by $\eta_{ik}^{\mathrm{prop}} \triangleq \frac{1}{M}\mathbb{E}\left\{||\hat{\mathbf{g}}_{iik}^{\mathrm{prop}} - \mathbf{g}_{iik}||^2\right\}$ is shown by Eq. (11)

$$\eta_{ik}^{\mathrm{prop}} = \frac{M}{M-1}\frac{\beta_{iik}^2}{\zeta_{ik}} + \beta_{iik} - 2\beta_{iik}\theta_{ik}$$

$$\text{where } \theta_{ik} = \int_0^1\int_{-1}^1 \frac{\kappa_{ik}^2(1-t) + \kappa_{ik}w\sqrt{t(1-t)}}{\kappa_{ik}^2(1-t) + 2\kappa_{ik}w\sqrt{t(1-t)} + t} f_T(t) f_W(w)\, dwdt \tag{11}$$

with $k_{ik} \triangleq \sqrt{\frac{\beta_{iik}}{\zeta_{iik}-\beta_{iik}}}$, and $f_T(t)$ and $f_W(w)$ are givien by Eq. (12)

$$f_T(t) = \frac{\Gamma(2M)}{(\Gamma(M))^2}(t(1-t))^{M-1}, 0 < t < 1 \tag{12}$$

$$f_W(w) = \frac{M}{\pi}B\left(\frac{1}{2}, M\right)\left(1-w^2\right)^{M-\frac{1}{2}}, |w| < 1. \tag{13}$$

Algorithm:

Input: Neighbor Table Nt, Route Table Rt, Data sensor List Dsl.
Output: Route Table Rt, Neighbor Strategic Table Nst
Start
Read Data sensor list Dsl.
For each data sensor, ds from Dsl
Generate NS-RREQ packet = {*SourceID* = *sink, Destination* = *ds*}
Broadcast NS-RREQ in the network.
The neighbor receives the NS-RREQ packet.
If $\int_{i=1}^{size(NT)} NT\,(i)\,.ID == DestinationID$ *then*
Generate NS-RREP message with energy, no transmission involved, and no neighbors.
NS-RREP = {*e, nti, nn*}
Send to sink node
Else
Forward NS-RREQ to neighbors.
End
While timer runs
Receive NS-RREP packet.
Extract route and for each node
Extract energy, number of transmissions, and number of neighbors.
Add to the neighbor strategic table.
$NSt = \sum (stragy \in Nst) \cup \{NodeID, e, Nti, nn\}$
Add route to the routeing table.
$RT = \sum (Route \in Rt) \cup R$
Do
Stop

Above discussed algorithm shows how the list of routes is identified and added to the strategic table and route table. Identified routes have been used to perform data transmission in WSN. To investigate routing challenges in WSNs, we use a graph model. The collection of vertices V in a weighted directed graph (V, E, ω) represents sensor nodes in a network. $E \subseteq V \times V$ is an edge set that indicates node relationships. The weighted label ω represents metrics for measuring links or pathways. We take node I as the issuer and node j as the target for each $(i, j) \in E$. A path p from V1 to Vn is given by (V1, Vn) $\triangleq$ (V1, V2,..., Vn). The trust model performs trust derivation, computation, and application. We use a watchdog as the cornerstone of detection techniques in this paper. Every sensor node keeps an eye on its neighbors' actions and determines how trustworthy they are. The detection results are especially used in the computation of proof of trust. The trust value of node j for node I is represented by (i, j). Evaluating device is node I, and the evaluated device is node j in our model. An arbitrary node's trust t comprises direct trust dt and indirect trust it. A random node's trust t comprises direct trust dt and indirect trust [33–36].

3.5 Sink Reachable Support (SRS) Estimation

Data collection performance depends on the reachability between the sink and the data sensor node. It is important to consider reaching any data sensor and reaching the sink node to deliver the data. In any route identified, there will be several intermediate sensor nodes available. However, the

energy constraints will vary, and after some time, the energy of any sensor node will be very poor. So, it is important to consider energy and how long sensor nodes will be available to forward the data packet. It has been measured based on the SRS [37–41]. It has been measured according to the energy, transmission performed, depletion ratio, and number of neighbors. If a sensor node has as many neighbors, even if the sensor is dead, the communication can be continued through its neighbors. The sink reachability support (SRS) measure has been estimated according to the abovementioned factors.

H[kj] also signifies the N[k] × M[j] channel coefficients matrix from the j th transmitter to the k th receiver and is considered to have i.i.d. complex Gaussian random variables selected from a continuous distribution. Furthermore, H has been identified as a transmitter. Finally received signal vector at receiver k after ZF interference is given by $\overline{\boldsymbol{Y}}^{[k]} = \boldsymbol{U}^{[k]}\boldsymbol{Y}^{[k]} = \boldsymbol{U}^{[k]}\left(\sum_{j=1}^{K}\boldsymbol{H}^{[k)]}\boldsymbol{V}^{[/]}\boldsymbol{S}^{[1]} + \boldsymbol{W}^{[k]}\right), k \in \kappa$

Let $\alpha = R \parallel \mathbf{d} \parallel_{\infty}, \beta = \alpha/(\alpha - 1)$. by Eq. (14)

$$\mu = \underset{i\in\{0,\ldots,4\}}{max}\left\{\mathbb{E}\left\{(\parallel \mathrm{x} \parallel_2 + \beta)^{i}(\parallel \mathbf{h} \parallel_2 - \beta)^{4-i}\right\}\right\}. \tag{14}$$

Consider that μ is finite. Then, for all $\varepsilon > 0$ and by Eq. (15)

$$|\mathcal{Z}| \geq 8\mu\left(\alpha^{l+1} + 1\right)^{4}/\varepsilon^{2} \tag{15}$$

From Eq. (16)

$$\mathbf{P}\left(\underset{\theta\in\Theta_R}{sup}\left|J_{\mathcal{Z}}(\mathbf{f}_\theta) - J(\mathbf{f}_\theta)\right| > \varepsilon\right) \leq 4\mathbf{P}\left(\underset{\theta\in\Theta_R}{sup}\left|J^{\circ}_{\mathcal{Z}}(\mathbf{f}_\theta)\right| > \frac{\varepsilon}{4}\right) \tag{16}$$

where $\mathbf{P}$ indicates training sample distribution in $\mathcal{Z}$ and $J^{\circ}_{\mathcal{Z}}(\mathbf{f}_\theta) = 1/|\mathcal{Z}|\sum_{m=1}^{|\mathcal{Z}|}\omega_m||\mathbf{f}_\theta(\mathbf{x}_m) - \mathbf{h}_m||_2^2$ with {w1, ... wz} a Rademacher sequence. From Eq. (17)

$$\mathrm{If}\mathbf{P}\left(\left|J_{\mathcal{Z}}(\mathbf{f}_\theta) - J(\mathbf{f}_\theta)\right| > \frac{\varepsilon}{2}\right) \leq \frac{1}{2} \tag{17}$$

for all $\boldsymbol{\theta} \in \Theta R$

Let $\sigma^2(\mathbf{f}_\theta)$ be the variance of $||\mathbf{f}_\theta(X) - h||_2^2$ so, by Eq. (18)

$$\mathbf{P}\left(\left|J_{\mathcal{Z}}(\mathbf{f}_\theta) - J(\mathbf{f}_\theta)\right| \geq \frac{\varepsilon}{2}\right) \leq \frac{4\sigma^2(\mathbf{f}_\theta)}{|\mathcal{Z}|\,\varepsilon^2} \tag{18}$$

for all $\boldsymbol{\theta} \in \Theta R$. Specifically, $\sigma^2(\mathbf{f}_\theta)$ satisfies by Eq. (19)

$$\begin{aligned}\sigma^2(\mathbf{f}_\theta) &= E\left\{||\mathbf{f}_\theta(\mathbf{x}) - \mathbf{h}||_2^4\right\} - J(\mathbf{f}_\theta)^2 \leq E\left\{||\mathbf{f}_\theta(\mathbf{x}) - \mathbf{h}||_2^4\right\}\\ &\leq E\left\{\left(||\mathbf{f}_\theta(\mathbf{x})||_2^2 + 2||\mathbf{f}_\theta(\mathbf{x})||_2 \parallel \mathbf{h} \parallel_2 + \parallel \mathbf{h}\parallel_2^2\right)^2\right\}\\ &= E\left\{(||\mathbf{f}_\theta(\mathrm{x})||_2 + \parallel \mathbf{h} \parallel_2)^4\right\}\end{aligned} \tag{19}$$

Consider that the input space of $\mathbf{f}\boldsymbol{\theta}(\mathbf{x})$ follows partition by Eq. (20). Utilizing cluster inequality gives,

$$||\mathrm{f}_\theta(\mathrm{x})||_2 = ||\mathbf{W}_{\mathcal{X}_k}\mathrm{x} + \mathbf{b}_{\mathcal{X}_k}||_2 \leq ||\mathbf{W}_{\mathcal{X}_k}||_2 \parallel \mathbf{x} \parallel_2 + ||\mathbf{b}_{\mathcal{X}_k}||_2 \tag{20}$$

For $x \in \mathcal{X}_k$ Moreover, $||\mathbf{W}_{\mathcal{X}_k}||_2$ *and* $||\ \mathbf{b}_{\mathcal{X}_k}||_2$ are upper bounded by Eq. (21),

$$\begin{aligned} ||\mathbf{W}_{\mathcal{X}_k}||_2 &= ||\prod_{i=0}^{l} \widetilde{\mathbf{W}}_i||_2 = ||\prod_{i=0}^{l} \mathbf{w}_i \mathbf{\Lambda}_i||_2 \\ &\leq \prod_{i=0}^{l} ||\mathbf{w}_i \mathbf{\Lambda}_i||_2 \leq \prod_{i=0}^{l} ||\mathbf{w}_i||_2 \end{aligned} \tag{21}$$

And by Eq. (22)

$$\begin{aligned} \|\mathbf{b}_{\mathcal{X}_k}\| &= \left\| \sum_{i=0}^{l-1} \left(\prod_{j=0}^{i} \tilde{\mathrm{W}}_{l-j} \right) \mathbf{b}_{l-1-i} + \mathbf{b}_l \right\|_2 \\ &\leq \sum_{i=0}^{l-1} \left\| \prod_{j=0}^{i} \tilde{\mathrm{W}}_{l-j} \right\|_2 \|\mathbf{b}_{l-1-i}\|_2 + \|\mathbf{b}_l\|_2 \\ &\leq \sum_{i=0}^{l-1} \left(\prod_{j=0}^{i} \|\mathrm{W}_{l-j}\|_2 \right) \|\mathbf{b}_{l-1-i}\|_2 + \|\mathbf{b}_l\|_2 \end{aligned} \tag{22}$$

Note that $||\mathbf{W}_i||_2 \leq R \parallel \mathbf{d} \parallel_\infty = \alpha$ and $||\mathbf{b}_i||_2 \leq \alpha, \alpha$ *for* $i \in \{0, 1, ..l\}$ Replacing these bounds into (11) and (12) yields by Eq. (23)

$$||\mathbf{W}_{\mathcal{X}_k}||_2 \leq \alpha^{l+1} \tag{23}$$

And by Eq. (24)

$$||\mathbf{b}_{\mathcal{X}_k}||_2 \leq \left(\sum_{i=0}^{l-1} \alpha^{i+1} \right) \alpha + \alpha = \frac{\alpha^{l+2} - \alpha}{\alpha - 1} \leq \beta \left(\alpha^{l+1} - 1 \right) \tag{24}$$

From (24)–(26), $\parallel \mathbf{f}(\mathrm{x}) \parallel_2$ is further given by

$$\parallel \mathbf{f}(\mathrm{x}) \parallel_2 \leq \alpha^{l+1} (\parallel \mathrm{x} \parallel_2 + \beta) - \beta \tag{25}$$

Merging (24) and (25),

$$\begin{aligned} \sigma^2(f) &\leq E\left\{ \left(\alpha^{l+1} (\parallel \mathbf{x} \parallel_2 + \beta) + \parallel \mathbf{h} \parallel_2 - \beta \right)^4 \right\} \\ &= \sum_{i=0}^{4} \binom{4}{i} \alpha^{i(l+1)} E\left\{ (\parallel \mathbf{x} \parallel_2 + \beta)^i (\parallel \mathbf{h} \parallel_2 - \beta)^{4-i} \right\} \\ &\leq \mu \left(\alpha^{l+1} + 1 \right)^4 \end{aligned} \tag{26}$$

$|\mathcal{Z}| \geq 8\mu \left(\alpha^{l+1} + 1 \right)^4 / \varepsilon^2$ condition for the cluster formation is satisfied. The set of indices of K Tx–Rx pairs are denoted by K = 1, . . . , K. On K, clustering is a partition. Let A stand for the sum of all potential clustering for K.

Then, by eq., define A = A (1), . . . , A(NA) as the resulting clusters for each clustering A ∈ A, where A(m) is mth cluster, and NA is the number of clusters (27)

$$\begin{aligned} &\mathcal{A}(m) \subseteq \mathcal{K}, \forall m \\ &\mathcal{A}(m) \cap \mathcal{A}(n) = \emptyset, m \neq n \\ &\cap_{m=1}^{N_A} \mathcal{A}(m) = \mathcal{K}. \end{aligned} \tag{27}$$

Let mj be the index of the cluster that includes jth Tx–Rx pair, i.e., mj = n, where j ∈ A(n) is the number of Tx–Rx pairs (n). Eq. (28) is used to express the received signal at the jth receiver

$$\mathbf{y}_j = \sqrt{\rho_{jj}}\mathbf{H}_{jj}\mathbf{v}_j s_j + \underbrace{\sum_{i\in\mathcal{A}(m_j)\setminus\{j\}} \sqrt{\rho_{ji}}\mathbf{H}_{ji}\mathbf{v}_i s_i}_{\text{intercluster interference}} + \underbrace{\sum_{k\notin\mathcal{A}(m_j)} \sqrt{\rho_{jk}\mathbf{H}_{jk}\mathbf{v}_k s_k}}_{\text{intercluster interference}} + \mathbf{z}_j. \tag{28}$$

Assume that the jth receiver's equalizer is $u_j \in C^{N\times 1}$, where $||u_j|| = 1$. Eq. (29) gives the feasible rate for the jth Tx–Rx pair

$$R_j = \log_2\left(1 + \frac{\rho_{jj}P_j\left|\mathbf{u}_j^H\mathbf{H}_{jj}\mathbf{v}_j\right|^2}{1 + I_j^{\text{intra}} + I_j^{\text{inter}}}\right) \tag{29}$$

where $I_j^{\text{intra}} = \sum_{i\in\mathcal{A}(m_j)\setminus\{j\}} \rho_{ji}P_i\left|\mathbf{u}_j^H\mathbf{H}_{ji}\mathbf{v}_i\right|^2$ and $I_j^{\text{inter}} = \sum_{k\notin\mathcal{A}(m_j)} \rho_{jk}P_k\left|\mathbf{u}_j^H\mathbf{H}_{jk}\mathbf{v}_k\right|^2$ indicates degradation caused by intra as well as intercluster interference. Only interference from transmitters of Tx–Rx pairs in A(mj) is aligned and canceled at the jth receiver by Eq. (30)

$$\left\{\mathbf{u}_j^H\mathbf{H}_{ji}\mathbf{v}_i = 0, i \in A\left(m_j\right)\setminus\{j\}\ \forall j \in \{1,\ldots,K\}\right. \tag{30}$$

Algorithm:

Input: Route R, Node Strategic Table Nst
Output: SRS
Start
  Read route R.
  Read strategic table NSt.
  Identify a list of sensor nodes available in route R.
  Slist = $\sum$ *Sensors* ∈ *R*
  For each sensor s
    Extract energy E = $\int_{i=1}^{size(NSt)} Nst(i).\ E$ *where* $Nst(i).\ NodeID = s$
    Extract Nti = $\int_{i=1}^{size(NSt)} Nst(i).\ Nti$ *where* $Nst(i).\ NodeID = s$//transmission involved
    Extract Nn = $\int_{i=1}^{size(NSt)} Nst(i).\ Nn$ *where* $Nst(i).\ NodeID = s$//no of neighbors
    Compute energy depletion ratio Edr = $(InitialEnergy - E)/Nti$
    Compute SRS = $\left(\frac{Nti}{TotalTimestamp} \times Edr\right) \times \left(\sum_{i=1}^{size(Slist)} Slist\,(i)\,.Nn/size\,(Slist)\right)$
  End
  Compute cumulative value for SRS = $\sum_{i=1}^{size(Slist)} SRS/size\,(Slist)$
Stop

Above discussed technique represents how reachability supports any route given. It has been measured according to the different factors mentioned above. The estimated SRS value has been used for route selection.

3.6 Secure Communication Support (SCS) Estimation

The SCS measure has represented the support of any route toward secure communication. It has been measured according to the strategy of each hop of the route. Each node would have been involved in several transmissions. If the intermediate node is a malicious one, the packet may be dropped or modified, which makes the communication fail so that the same packet would be retransmitted through another route. The sink node would maintain this, and based on that, and the SCS measure can be computed.

Algorithm:

Input: Node Strategic Table NSt, Route R
Output: SCS
Start
Read Nst, R.
Identify the hops of R as $\mathrm{Hl} = \sum Sensors \in R$
For each hop h
Extract energy $\mathrm{E} = \int_{i=1}^{size(NSt)} Nst(i).\ E\ where\ Nst(i).\ NodeID = h$
Extract $\mathrm{Nti} = \int_{i=1}^{size(NSt)} Nst(i).\ Nti\ where\ Nst(i).\ NodeID = h$//transmission involved
If $(Nti \times \mu) > (InitialEnergy - E)$ then
$\mathrm{SCS} = 0$
Return
Else
$\mathrm{SCS} = \sum SCS\,(h-1) \cup (No\ of\ retransmission/Nti)$
End
End
Compute cumulative $\mathrm{SCS} = \dfrac{\sum_{i=1}^{size(Hl)} SCS\,(Hl\,(i))}{Size\,(Hl)}$
Stop

The technique above represents how secure communication support is measured toward route selection. The method evaluates communication support measures for any route based on the retransmission frequency of transmission through the hop or route identified. Based on the value of SCS only, the route selection is performed.

3.7 Neighbor Strategic DCS Data Collection

The neighbor strategic secure routing and data collection algorithm start with route discovery on each data sensor available. The technique evaluates reachable sink support (SRS) and secure communication support (SCR) for every route identified. The SRS is measured to identify the possibility of reaching the sink, whereas the SCR is measured to gauge the trust of the route to perform secure data transmission. Using the value of SCR and SRS, the technique evaluates the Data carrier Support (DCS) value. Based on the value of DCS, the approach identifies the optimal route to perform data collection.

Algorithm:

Input: Route Table RT, Strategic Table Nst, Data sensor table DST.
Output: Optimal Route R.
Start
Read route table RT and strategic table Nst, DST.
Identify a list of data sensors Dsl = $\sum Datasensors \in DST$
For each data sensor d
RT = Route Discovery (sink, d)
For each route r
SRS = estimate sink reachable support®
SCS = estimate secure communication support®
Compute DCS = SRS × SCS
Route R = $\int_{i=1}^{size(RT)} Max\,(RT\,(i))$
Perform data collection through R.
End
Stop

Above discussed technique represents how reachable sink and secure communication support have been measured to evaluate communication support. Based on the value of DCS, a single route is identified to perform data collection.

4 Results and Discussion

The proposed neighbor strategic real-time secure data collection has been implemented and evaluated for its performance. The protocol is hard coded in network simulator NS2, and implementation of the algorithm has been calculated under various simulation conditions. The result obtained by technique is compared with the result of other techniques. A Comparison of Throughput is shown in Table 1.

Table 1: Comparison of throughput

Throughput performance			
Time in s	FAEM in %	NPBNS in %	NSSR in %
10	13	19	36
20	26	34	48
30	42	49	67
40	68	72	81
50	82	91	96

The performance on throughput has been measured for the algorithms at different simulation times and compared with other results. The Proposed NSSR technique has obtained higher throughput performance at all simulation periods than other methods.

Various techniques attain throughput performance is measured and compared with the results of other techniques. Comparison result has been presented in Fig. 2, and debits the NSSR approach has achieved noticeable throughput growth than previous methods.

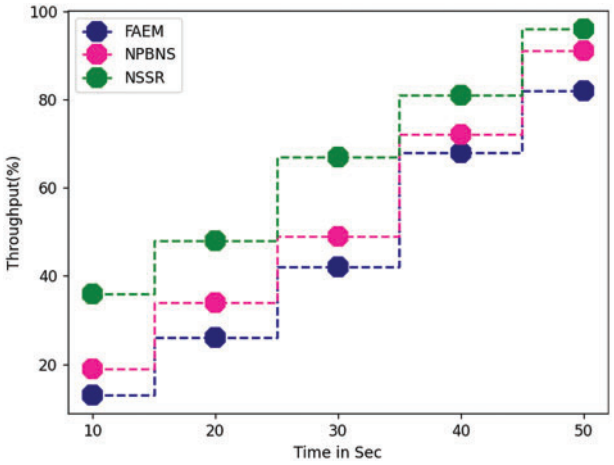

Figure 2: Performances on throughput

The PDR produced by various algorithms is measured according to the number of packets sent and received. PDR performance is measured and compared with other techniques' results.

The result of the packet delivery ratio is measured as well as compared in Table 2. The Result shows that the proposed NSSR method has produced higher PDR than other techniques.

Table 2: Performance on packet delivery ratio

Packet delivery ratio			
Time in s	FAEM in %	NPBNS in %	NSSR in %
10	19	23	34
20	36	45	56
30	49	61	72
40	58	78	86
50	73	86	97

The performance of PDR is measured as well as compared with the results of other techniques. Comparison has been presented in Fig. 3, representing that the NPBNS algorithm has achieved higher PDR than other techniques.

The latency is the measure that represents the time taken to transmit a packet between any source as well as the destination. It has been measured based on the total time taken for the specific number of packets.

The latency produced by different methods is measured and presented in Table 3. The proposed NSSR algorithm has produced less latency than other techniques.

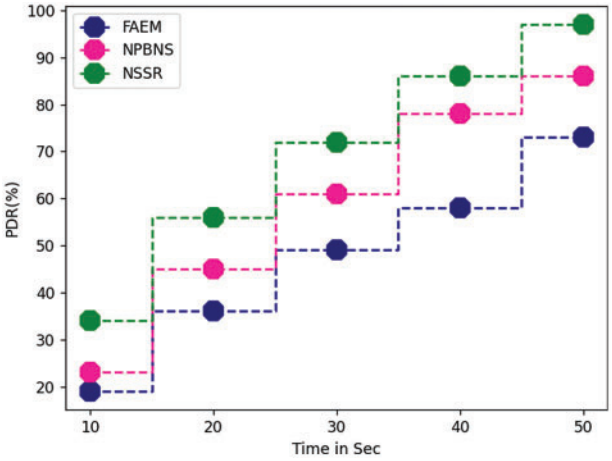

Figure 3: Performance on PDR

Table 3: Comparison of packet delay

Latency in seconds			
The rate of sending Packets/s	FAEM in s	NPBNS in s	NSSR in s
4	4.5	3.0	1.8
8	6.8	5.4	2.9
16	7.2	6.5	4.3
32	8.9	7.1	5.9
64	9.4	8.9	6.4

Fig. 4 represents the packet delay ratio produced by various techniques, and NSSR techniques have produced less latency value than other techniques. The nodes are initially placed in a certain building area to sense various data forms. In each building, about 20 sensor nodes were installed. The sink's location coordinates are (4, 4) and the server's (4, 1). The intercommunication range of these deployed nodes is then used to construct grids. Fig. 2 depicts the grid created using the intercommunication range. The nodes that make up the grid are referred to as grid members. One node was chosen as a grid organizer from each grid. For a set amount of time, the elected grid organizer serves as the leader. The sailfish optimization algorithm selects the grid organizer based on two important parameters: distance and residual energy. The previous graphic shows the grid organizer selection in each grid. The grid organizer is the node in each grid that is highlighted in green. The grid organizer receives the sensed information from each grid member. The data must then be sent from the grid organizer to the sink. The source grid organizer chooses its neighbour grid organizer using the relay-node selection technique to execute this function.

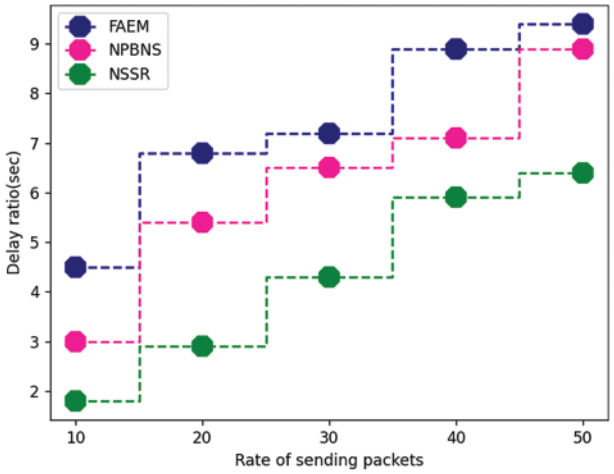

Figure 4: Packet delay ratio of different methods

Open issues- the trust-aware secure routing protocol in WSN still face the following major challenges:

- Identifying potentially harmful nodes in a short amount of time: It is possible that much information will be lost if the rogue nodes are not swiftly identified and removed from the network.
- Methods for protecting the network against simultaneous routing attacks: However well the network is protected, it will still be vulnerable to serious threats if it can only fight off a subset of the many possible network assaults.
- How to lessen the network's electrical supply load: Longevity in operation is a primary concern for WSNs, and one of its primary functions is reducing energy consumption.

5 Conclusion

This research presents an efficient neighbor strategic real-time trust-based secure routing and data collection algorithm. The route level security has been enforced by choosing a route according to the secure communication support (SCS). It is measured based on the previous transmission behavior of various intermediate nodes available in any route. Similarly, data collection performance is enforced by choosing a route with maximum reachability to the sink node. It has been selected based on the sink reachability support (SRS) measure. Combining both measures, the method estimates the data collection support (DCS) value using a route with maximum DCS. The proposed algorithm enhances the performance of route selection and secure data collection. Performance produced by the NSSR algorithm is comparatively higher than other methods. The remaining energy of a sensor node, the distance of sensor nodes from BS, the density of other surrounding sensor nodes around potential CH, and the trust levels of nodes to send data to the next hop are all parameters to consider. To ensure that CHs are distributed evenly across the WSN area, a condition requires a minimum separation distance between them. In inter-cluster communication, a threshold-based data transmission method is utilized, as well as a multi-hop routing strategy in which only CHs closer to BS broadcast their information directly to BS, reducing the amount of energy squandered by CHs further away from BS. Simulation results indicate that networks employed with the proposed method perform well in dealing with various routing-targeting or trust-targeting attacks. Additionally, in case malicious attackers are

appearing on an established secure route, the routing maintenance method has a higher speed of route update than contrast models.

Acknowledgement: The authors would like to thank the R&D department of Periyar University, Salem, for supporting this work.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] G. Dhand and S. S. Tyagi, "SMEER: Secure multi-tier energy-efficient routing protocol for hierarchical wireless sensor networks," *Wireless Personal Communications*, vol. 105, pp. 17–35, 2019.
[2] V. Kavidha and S. Ananthakumaran, "Novel energy-efficient secure routing protocol for wireless sensor networks with Mobile sinks," *Peer-to-Peer Network Applications*, vol. 12, pp. 881–892, 2019.
[3] T. Yang, X. Xiangyang, L. Peng, L. Tonghui and P. Leina, "A secure routing of wireless sensor networks based on trust evaluation model," *Procedia Computer Science*, vol. 131, pp. 1156–1163, 2018.
[4] F. Mezrag, S. Bitam and A. Mellouk, "Secure routing in cluster-based wireless sensor networks," in *GLOBECOM 2017-2017 IEEE Global Communications Conf.*, Singapore, pp. 1–6, 2017.
[5] B. Patil and R. Kadam, "A novel approach to secure routing protocols in wsn," in *2018 2nd Int. Conf. on Inventive Systems and Control*, Coimbatore, India, pp. 1094–1097, 2018.
[6] S. Karthick, S. P. Sankar and Y. P. A. Teen, "Trust-distrust protocol for secure routing in self-organizing networks," in *2018 Int. Conf. on Emerging Trends and Innovations in Engineering and Technological Research*, Ernakulam, India, pp. 1–8, 2018.
[7] A. M. E. Semary and M. M. A. Azim, "New trends in secure routing protocols for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 9, no. 5, pp. 1–16, 2013.
[8] F. Ishmanov and Y. B. Zikria, "Trust mechanisms to secure routing in wireless sensor networks: Current state of the research and open research issues," *Journal of Sensors*, vol. 2017, no. 1, pp. 1–16, 2017.
[9] A. Ahmed, K. A. Bakar, M. I. Channa and A. W. Khan, "A secure routing protocol with trust and energy awareness for wireless sensor network," *Mobile Networks and Applications*, vol. 21, pp. 272–285, 2016.
[10] K. B. P. Rao, B. Ravi and P. K. Kumari, "Efficient data collection for wireless sensor network using virtual grid-based clustering," *International Journal of Computer Applications*, vol. 159, no. 1, pp. 0975–8887, 2017.
[11] R. Kaur and D. Kumar, "Region based clustering for data collection in WSN," *International Journal of Computer Techniques*, vol. 16, no. 5, pp. 6913–6919, 2017.
[12] D. boum, A. Christian, A. A. A. Ari, A. M. Gueroui, A. Mohamadou *et al.,* "Big data collection in large-scale wireless sensor networks," *Sensors 18*, no. 12, pp. 4474, 2018.
[13] J. Wang, X. Gu, W. Liu and A. kumar, "An empower hamilton loop based data collection algorithm with mobile agent for WSNs," *Human-centric Computing and Information Sciences*, vol. 9, no. 1, pp. 18, 2019.
[14] V. Saranya, S. Shankar and K. Chidambaresan, "Energy efficient data collection algorithm for mobile wireless sensor network," *Wireless Personal Communications*, vol. 105, pp. 219–232, 2019.
[15] N. A. M. Alduais, J. Abdullah, A. Jamil and L. Audah, "An efficient data collection and dissemination for IoT based WSN," in *2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conf. (IEMCON)*, Vancouver, BC, Canada, pp. 1–6, 2016.
[16] S. M. Mujeeb, R. P. Sam and K. Madhavi, "Adaptive EHTARA: An energy-efficient and trust aware secure routing algorithm for big data classification in IoT network," *Wireless Personal Communications*, vol. 121, no. 1, pp. 621–646, 2021.

[17] M. Kumar, P. Mukherjee, K. Verma, S. Verma and D. B. Rawat, "Improved deep convolutional neural network based malicious node detection and energy-efficient data transmission in wireless sensor networks," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 5, pp. 3272–3281, 2021.
[18] N. Mittal, S. Singh, U. Singh and R. Salgotra, "Trust-aware energy-efficient stable clustering approach using fuzzy type-2 Cuckoo search optimization algorithm for wireless sensor networks," *Wireless Networks*, vol. 27, no. 1, pp. 151–174, 2021.
[19] K. S. Kumar and P. Vimala, "Energy efficient routing protocol using exponentially-ant lion whale optimization algorithm in wireless sensor networks," *Computer Networks*, vol. 197, pp. 108250, 2021.
[20] T. Khan and K. Singh, "TASRP: A trust aware secure routing protocol for wireless sensor networks," *International Journal of Innovative Computing and Applications*, vol. 12, no. 2–3, pp. 108–122, 2021.
[21] U. Meena and P. Sharma, "Secret dynamic key authentication and decision trust secure routing framework for internet of things based WSN," *Wireless Personal Communications*, vol. 125, no. 2, pp. 1753–1781, 2022.
[22] W. Fang, W. Zhang, W. Yang, W. Gao, Y. Yang *et al.,* "Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks," *Digital Communications and Networks*, vol. 7, no. 4, pp. 470–478, 2021.
[23] H. Hu, Y. Han, H. Wang, M. Yao and C. Wang, "Trust-aware secure routing protocol for wireless sensor networks," *Electronics and Telecommunications Research Institute Journal*, vol. 43, no. 4, pp. 674–683, 2021.
[24] R. R. Devi and T. Sethukarasi, "Develop trust-based energy routing protocol for energy efficient with secure transmission," *Wireless Personal Communications*, vol. 123, no. 3, pp. 2835–2862, 2021.
[25] S. V. N. S. Kumar, Y. Palanichamy, M. Selvi, S. Ganapathy, A. Kannan *et al.,* "Energy efficient secured k means based unequal fuzzy clustering algorithm for efficient reprogramming in wireless sensor networks," *Wireless Networks*, vol. 27, no. 6, pp. 3873–3894, 2021.
[26] S. G. Selvan and I. M. Lakshmi, "An energy efficient trust-based routing scheme using hybrid particle swarm optimization for wireless sensor-based healthcare networks," *Journal of Medical Imaging and Health Informatics*, vol. 11, no. 12, pp. 3096–3102, 2021.
[27] M. Selvi, S. V. N. Santhosh Kumar, S. Ganapathy, A. Ayyanar, H. K. Nehemiah *et al.,* "An energy efficient clustered gravitational and fuzzy based routing algorithm in wsns," *Wireless Personal Communications*, vol. 116, no. 1, pp. 61–90, 2021.
[28] T. Khan, K. Singh, M. H. Hasan, K. Ahmad, G. T. Reddy *et al.,* "ETERS: A comprehensive energy aware trust-based efficient routing scheme for adversarial wsns," *Future Generation Computer Systems*, vol. 125, pp. 921–943, 2021.
[29] N. Veeraiah and B. T. Krishna, "Intrusion detection based on piecewise fuzzy c-means clustering and fuzzy Naïve Bayes rule," *Multimedia Research*, vol. 1, no. 1, pp. 27–32, 2018.
[30] N. Veeraiah and B. T. Krishna, "Trust-aware fuzzyclus-fuzzy nb: Intrusion detection scheme based on fuzzy clustering and Bayesian rule," *Wireless Networks*, vol. 25, pp. 4021–4035, 2019.
[31] N. Veeraiah and B. T. Krishna, "Selfish node detection idsm based approach using individual master cluster node," in *2018 2nd Int. Conf. on Inventive Systems and Control (ICISC)*, Coimbatore, India, pp. 427–431, 2018.
[32] K. Pradeep and N. Veeraiah, "VLSI implemetation of euler number computation and stereo vision concept for cordic based image registration," in *2021 10th IEEE Int. Conf. on Communication Systems and Network Technologies (CSNT)*, Bhopal, India, pp. 269–272, 2021.
[33] N. Veeraiah, O. I. Khalaf, C. V. P. R. Prasad, Y. Alotaibi, A. Alsufyani *et al.,* "Trust aware secure energy efficient hybrid protocol for manet," *IEEE Access*, vol. 9, pp. 120996–121005, 2021.
[34] U. Srilakshmi, S. A. Alghamdi, V. A. Vuyyuru, N. Veeraiah and Y. Alotaibi, "A secure optimization routing algorithm for mobile ad hoc networks," *IEEE Access*, vol. 10, pp. 14260–14269, 2022.
[35] U. Sri Lakshmi, N. Veeraiah, Y. Alotaibi, S. A. Alghamdi, O. I. Khalaf *et al.,* "An improved hybrid secure multipath routing protocol for manet," *IEEE Access*, vol. 9, pp. 163043–163053, 2021.

[36] D. Anuradha, N. Subramani, O. Khalaf, Y. Alotaibi, S. Alghamdi *et al.,* "Chaotic search-and-rescue-optimization-based multi-hop data transmission protocol for underwater wireless sensor networks," *Sensors*, vol. 22, no. 2867, 2022.
[37] P. Mohan, N. Subramani, Y. Alotaibi, S. Alghamdi, O. I. Khalaf *et al.,*" "Improved metaheuristics-based clustering with multihop routing protocol for underwater wireless sensor networks," *Sensors*, vol. 22, no. 4, pp. 1618, 2022.
[38] N. Subramani, P. Mohan, Y. Alotaibi, S. Alghamdi and O. I. Khalaf, "An efficient metaheuristic-based clustering with routing protocol for underwater wireless sensor networks," *Sensors*, vol. 22, pp. 415, 2022.
[39] S. Bharany, S. Sharma, S. Badotra, O. I. Khalaf, Y. Alotaibi *et al.,* "Energy-efficient clustering scheme for flying ad-hoc networks using an optimized leach protocol," *Energies*, vol. 14, no. 19, pp. 6016, 2021.
[40] S. Sennan, K. Gopalan, Y. Alotaibi, D. Pandey and S. Alghamdi, "EACR-LEACH: Energy-aware cluster-based routing protocol for wsn based IoT," *Computers, Materials & Continua*, vol. 72, no. 2, pp. 2159–2174, 2022.
[41] P. Kollapudi, S. Alghamdi, N. Veeraiah, Y. Alotaibi, S. Thotakura *et al.,* "A new method for scene classification from the remote sensing images," *CMC-Computers, Materials & Continua*, vol. 72, no. 1, pp. 1339–1355, 2022.