RESEARCH ARTICLE

Region Based Secured Data Transmission Protocol for Wireless Sensor Network

Ashok Kumar R
Department of Computer Science, SRMV College of Arts and Science, Coimbatore, Tamil Nadu, India.
ashsha.90@gmail.com

R. Kannan
Department of Computer Science, SRMV College of Arts and Science, Coimbatore, Tamil Nadu, India.
ramadosskannan@gmail.com

Received: 07 July 2022 / Revised: 29 August 2022 / Accepted: 08 September 2022 / Published: 30 October 2022

Abstract – Outlier detection based on region is a very useful safety strategy for wireless sensor networks with a high number of scattered nodes. Developing a more effective outlier detection system in WSNs can ensure that data packets are successfully transmitted without loss or corruption. The Evolutionary Game-based Secured Clustering Protocol (EGSCP) has been created for the existing system. Those research approaches, however, failed to discover outlier activities when area leaders behave as malevolent nodes or are compromised by hackers. This is addressed in this work by introducing a novel mechanism for the reliable detection of outlier behaviors, namely Region-Based Secured Data Transmission Protocol (RSDTP). The proposed research approach ensures private rule sharing by introducing the Privacy position-aware Routing in Wireless Sensor Networks (WSNs) which use group public keys of intra-region leaders to create group signatures that are shared by all members of the region which also makes it impossible to know exact positions of area members. Thus, sharing private rules can be guaranteed while using group signatures. This study leverages Enhanced Adaptive Acknowledgment, which checks for the existence of hostile nodes before rule sharing, to enable secure rule sharing. This would take place during intraregional leaders' rule-sharing sessions. To optimize memory storage and address bandwidths/memory concerns, the rule set aggregations are executed in this study following secure rule set transfers between intra and inter-region leaders. NS2 simulations have been used for evaluations of the proposed Region-Based Secured Data Transmission Protocol (RSDTP) approach for attaining effective non-hazardous, safe, and reliable data transport processes.

Index Terms – Outlier Detection Based on Region, Data Transmission, Wireless Sensor Networks, Acknowledgment, Data Aggregation, Privacy, Memory Overhead.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are made up of a very large number of sensor nodes, each of which is outfitted with wireless transceivers, low-power micro - controllers, energy sources, and a wide variety of sensors [1]. WSNs have a broad range of potential applications, including those in the research, professional, commercial, and even military spheres, amongst others. These requests may be seen in individual areas, as well as in business, industry, and the army. However, the sensor observes obtained from sensor nodes often have poor data integrity and dependability because of the restricted capabilities of sensor nodes in terms of energy, storage, processing power, and bandwidth, as well as the harshness of the deploying environment [2,3]. The use of sensor data of poor quality in any data analysis and decision-making process reduces the likelihood of achieving accurate and up-to-the-minute situational understanding. The identification of outliers is one approach that may be used to solve the problem of poor-quality sensor data. In additional, the identification of outliers may assist in the diagnosis of the health state of WSNs as well as the identification of environmental events (such as forest fires, air pollution, and other similar occurrences) [4,5,6]. Therefore, it is of the utmost importance to discover an outlier sensing method for WSNs that is both effective and efficient. This technique should be able to recognize outliers with a greater correctness and a low false alarm rate, while also satisfying the constraints in terms of memory and computational complexity [7]. "The readings that greatly vary from the regular pattern of detected data" [8] is one way to describe outliers in wireless sensor networks (WSNs).

Outlier detection is more difficult in sensor networks than in traditional networks [9]. Where network traffic is concentrated in wired or LAN/WAN networks [10, 11], a gateway is present, and an Outlier Detection System can be established. In ad hoc networks, there is no such thing as a convenient location. In ad-hoc networks, a node with a significant number of surrounding nodes within communication range provides an option for IDS installation [12]. They should be numerous because they must cover all network participants, and these participants must communicate with one another to convey local outlier-related information [13]. It is challenging to locate such nodes and allow them to communicate effectively [14]. To make matters worse, the nodes are sensors, and the network topology can vary frequently: the complex process of setting up outlier detection architecture may have to be repeated [15].

The association of an outlier Detection System with WSNs are efficient means of identifying attacks in WSNs when they occur [16]. IDSs (intrusion detection systems) are a set of combinatorial approaches for detecting logical attacks in secure WSNs [17]. The framework identifies attacks by analyzing each packet that enters the environment and continually observing network activity [18]. There are two approaches to implementing outlier detection systems: in a controlled setting with numerous SNs, or in a single SN (sensor nodes) [19]. It just monitors incoming traffic on that specific node in the latter situation. As needed, these SNs can actively warn their neighbors of outlier information [20]. The research contribution deals with the ODSs (outlier detection systems) for WSN environments and ensures secure and dependable data connections. This effort seeks to protect the privacy of SNs by concealing their direct position sharing. By implementing the acknowledgment verification phase, the erroneous hostile activity identification is also precisely identified, ensuring optimal and trustworthy encoding. All of this is accomplished by RSDTP (Region Based Secured Data Transmission Protocol), which securely performs data transfers while maintaining privacy limitations.

The research approach has the following general structure: The outlier detection system and its significance in ensuring safe data transfer have been broadly described in this section. Depending on their manner of operation, Section 2 delves further into several similar research methodologies that aim to accomplish outlier prevention. An in-depth discussion of the suggested research methodology is provided in Section 3, along with relevant examples, explanations, and flow diagrams. Using information from the NS2 simulation environment, Section 4 gives an experimental assessment of the recommended study methodology. Finally, in section 5, the results and conclusions of the investigation procedure are discussed.

2. RELATED WORKS

To reduce network energy usage, Srivastava et al. [21] proposed rate-based congestion controls based on clustered routing. To prolong network lives in lengthy simulation periods, the rate control strategy lowered end-to-end latencies. Their proposed hybrid K-means and Greedy best first search methods clustered nodes followed by firefly optimizations for higher PDRs (packet delivery ratios). The packets were transmitted with the highest throughputs by the use of routing based on ACOs (Ant Colony Optimizations). To ensure consistency in QoS (Quality of Services) including dependability, congestion controls, energy efficiencies, and end-to-end latencies, Kalnoor et al. [22] protected routing protocols in conjunction with IDSs, and guaranteed QoS is not compromised in WSNs. The study examined several routing strategies based on QoS for enhancing overall network performances.

The communicating nodes were monitored by Thangaramya et al. [23] using a fuzzy temporal rule-based cluster-based routing approach that incorporated outlier identifications and trust models. The study's secured routing proposed fuzzy temporal rule-and distance-based outlier identifications to assess and identify hostile nodes from other nodes within network clusters.

Jan et al [24] priority-based application-specific latency management by considering node mobility and heterogeneities for identifying congestions. The study’s suggested approach used novel queue schedules for ensuring coverage integrities and additional resource usage by faraway nodes effectively. The objective of the work was to guard WSNs against Sybil attacks while conserving their energies.

In this work, Kalidoss et al. [25] created a unique routing protocol named Protocol for Secured Energy-Efficient Routing that is Aware of Quality of Service. This protocol, which is based on trust and energy modeling, makes an effort to enhance WSN security while simultaneously making the most efficient use of available energy. Authentications and key-based security are used in the work that is being suggested, which results in the assignment of trust ratings. In addition, direct, indirect, and total trust ratings are calculated to further enhance the security of communication.

TERP (Trust and Energy Aware Routing Protocol) was introduced by Ahmed et al. [26]. Their proposed protocol used distributed trust paradigm to identify and isolate bad nodes where composite routing algorithms decided on routes by considering trusts, residual energies, and hop count of nearby nodes. The study's versatile routing helped in distributing energies using reliable nodes while data transmissions occurred over shorter links. Additionally, TERP detected connectivity breaks smartly, obviating the requirement for pointless route searches.

TA-EEAs (Trust Assisted- Energy Efficient Aggregations) was introduced by Latha et al. [27] for improving overall aggregation precisions while placing only slight restrictions on neighbor dependability and aggregations. TA-EEAs employed a three-step process to ensure perfect transmissions, which included duty cycle-based energy conservations, trusted neighbor selections, and proactive reduction of congestions. The network lifetimes were increased with lesser control overheads by reducing node energy consumption.

A reliable, secure, and energy-efficient routing solution for WSNs was presented by Beheshtiasl et al. [28]. The study assessed trust values of routes using fuzzy logic along with determinations of shortest paths from sources to destinations. Their recommended methodology also used fuzzy logic to evaluate trusts models and optimal MDS-MAP (multidimensional scaling-map) routing strategy where TC-BACs (Trust and Centrality Degree Based Access Controls) and TARFs (Trust-Aware Routing Frameworks) along with the suggested technique were compared.

Dhand et al. [29] provided Using Spherical grid-based MALOKSER (multi-curve Elliptic curve cryptographic routing) and Ant Lion optimizations inside K-means for clustering, it is possible to efficiently cluster data and send secure data packets to the base station in a timely manner. Our study seeks to improve wireless network communication systems' energy efficiency and network security. Combining elliptic curve encryption with spherical grid multi-tier routing provides an additional layer of security for data transmission. This is accomplished by encrypting communications using two distinct keys and moving packets in a spherical manner.

AlFarraj et al. [30] suggested AF-TNSs (activation function-based trustworthy neighbor selections) enabling WSNs that are limited in their resources, to improve their network's safety. To preserve the neighbors' trustworthiness, AF-TNSs worked in two stages: Energy-limited, additive metric-based node assessment. Random Tran sigmoid function divides trusted and untrusted nodes to maintain network performance, simplifying AF decision-making.

In [31], a unique Data Aggregation Protocol Model (DAPM) helps Wireless Sensor-based Communication Networks save energy and serve clients' communication demands. By aggregating data at relay nodes, large wireless sensor networks may reduce transmission power and energy consumption (that is, merging incomplete outcomes throughout work system). Wireless Sensor Networks demand safe information transport and regular routing support to nodes. This research aims to build a novel protocol to transmit data packets to destination without flaws throughout the communication route. The proposed DAPM allows wireless networks to perform flaw-free communications in a satisfactory manner. Computations and trials prove the proposed protocol design's efficiency. The recommended Wireless Sensor Network protocol beats existing secure protocols in security, cost, and energy use.

In [32] the best method to handle secure communications in WSNs is suggested in this study using the efficient particle-based spider monkey optimization (P-SMO) algorithm. In order to build the routing path based on the selected cluster heads, the network is modeled and the effective learning automata-based cell clustering algorithm (ELACCA) is used to select the cluster heads (CHs). In order to construct a safe routing path, the suggested P-SMO algorithm takes into account variables including energy consumption, latency, stability component, and confidence. Particle swarm optimization (PSO) and spider monkey optimization (SMO) are combined in the suggested P-SMO technique to efficiently determine the optimum pathways.

As a result, the application of game theory to the process of designing the routing protocol for WSNs is a preferable strategy. Because of the one-of-a-kind characteristics of WSNs, game theory has the potential to be regarded as an appealing and reliable solution for the design of a routing protocol that, in the long run, can result in a network that is pragmatic and nimble. Game theory can be applied to the examination of system processes in self-organizing and decentralized networks thanks to the players' ability to behave rationally in the game. The application of game theory to the design of routing protocols for wireless sensor networks (WSNs) has already been done in a number of completed works, and these protocols promise to have superior effectiveness to many established protocols in terms of end-to-end delay, network lifetime, packet delivery ratio, energy efficiency, and route establishment time. In this study, Region Based Secured Data Transmission Protocol (RSDTP) for effective outlier detection system is proposed for the purpose of dependable identification of outlier behaviours with improved outcomes. This system is formulated on region based secured data transmission approach.

3. REGION BASED SECURED DATA TRANSMISSION PROTOCOL (RSDTP) FOR EFFECTIVE OUTLIER DETECTION SYSTEM

Due to its ability to detect anomalous behavior detecting outliers using a region-based approach is useful when there are many nodes in the network systems are the most focused and widely utilized techniques in the WSNs environment. The effectiveness of region-based outlier identification, however, may be compromised in the face of the greatest level of malicious node activity. The capacity of regional leaders to identify outliers would be impacted by the compromising of genuine nodes more likely to be area leaders. Sensor node privacy is considerably more important in the WSNs environment and must be prioritized for identification of WSN nodes that is both precise and effective.

In the method of research that has been suggested for the accurate identification of abnormal activities, the Region Based Secured Data Transmission Protocol (RSDTP) For Effective Outlier Detection System is introduced. By incorporating private position awareness, the proposed research approach ensures private rule sharing. Routing in WSNs in which all region members create a group signature using the intra-region leader's public key. As a result, the precise location of area members is unavailable. This organizational signature may be utilized to guarantee the exchange of confidential rules. Enhanced Adaptive Acknowledgement is utilized in this work to allow safe rules distribution, which verifies the existence of unfriendly nodes prior to rule sharing. This discussion would take place within the regulation session that would involve leadership. Within the scope of this study, regulation set aggregating is conducted with the goal of optimizing memory storage following the safe transfer of a rule set from based on inter leaders to inter-region leaders. Figure 1 depicts the general architecture of the proposed research technique.

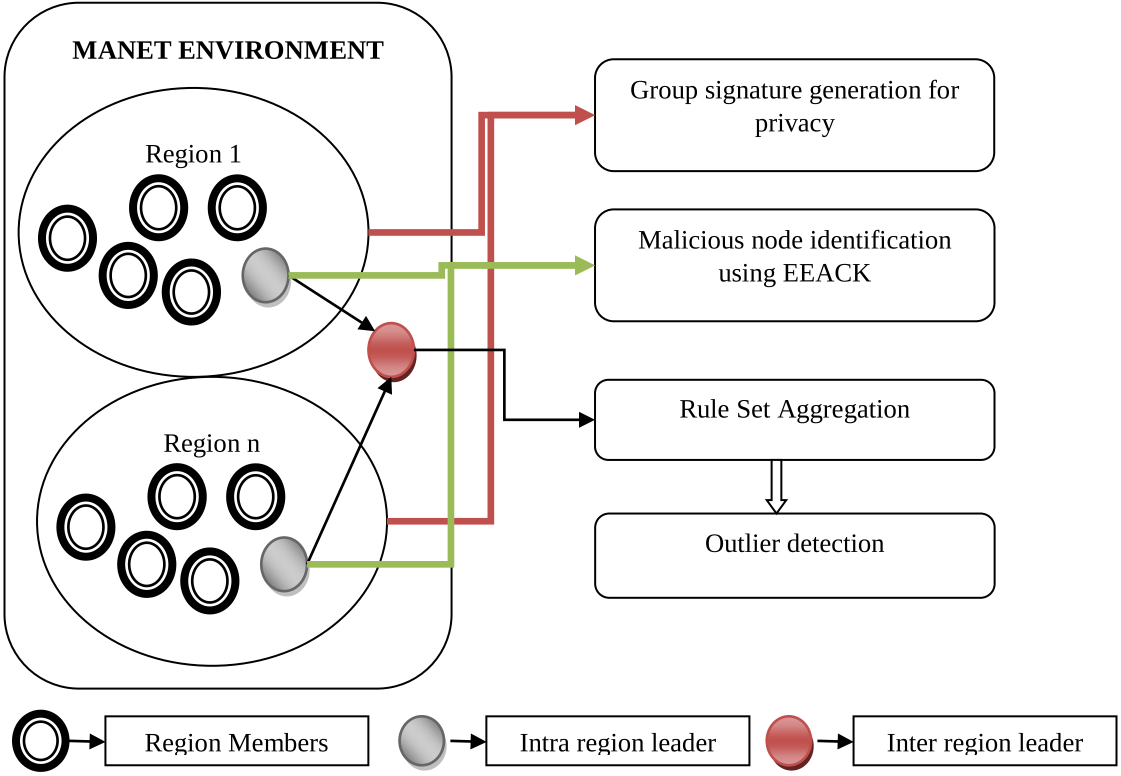

Figure 1 Overall Architecture of Proposed Work

Figure 1 depicts a possible outlier identification architecture. The WSNs environment would be separated into different regions in this effort, and then outlier activity would be discovered using a rule set. The following are the processing steps of the suggested research method:

- Selection of intraregional and interregional leaders
- Using ALARM, create a group signature to privately share rules.
- Sharing rules from intraregional leaders to interregional leaders and detecting malicious node presence via EEACK
- Aggregation of Rule Sets in the Interregional Leader
- Identification of outlier activity using the incoming aggregated rule set

3.1. Region Leader Selection

In the outlier detection system, region leader selection is particularly significant since region leaders serve as the richness of resources and the number of neighboring nodes. These measures are mostly dependent on the gateway via which outlier activity detection is accomplished. This work identifies intra/inter-region leaders where intra-region leaders collect traffic rules from members of regions and forward them to inter-regional leaders. Inter-regional leaders aggregate traffic regulations and compare them with knowledge base rules to determine the presence of outliers. Various criteria for selecting area leaders in WSNs have been proposed including:

(1) The highest degree, in which SNs with the most neighboring nodes are chosen as regional leaders. This approach has low rates of region leader interchanges with small inputs as throughputs get distributed amongst cluster members.

(2) Peak-id, where the region leader is assigned to the SNs with the smallest or largest id the issue with this strategy is that it favors SNs with peak ids.

(3) Node weight is an included measure for determining a node's suitability as a regional leader. It is able to take into consideration a wide variety of criteria, including the characteristics of the grouping. As a result, it is reasonable to take them into consideration when

determining whether or not a node is qualified to play the role of a header by modifying the weights assigned to a number of metrics according to a number of different hypotheses.

The aforementioned three limitations are taken into account while electing intraregional leaders and the interregional leader is chosen from the intraregional leaders depending on the degree of centrality.

3.2. Group Signature Generation

Using the server to detect anomalous activity, some SNs may need to protect their private information. For example, in a military situation, while transmitting critical information with servers, soldiers' positions must be concealed to minimize threats. Traditional data communication protocols, on the other hand, need the sharing of source and destination addresses for proper communication. This is addressed in this research technique by proposing the group signature concept, in which region members from the same region generate group signatures by disguising identifying details with group public key, so ensuring leaking position information. In the event that the membership of a region needs to be verified, the group manager can disassemble the group signature and inspect the node. Position information, avoiding self-violation. The intraregional leader would serve as a group member in this project.

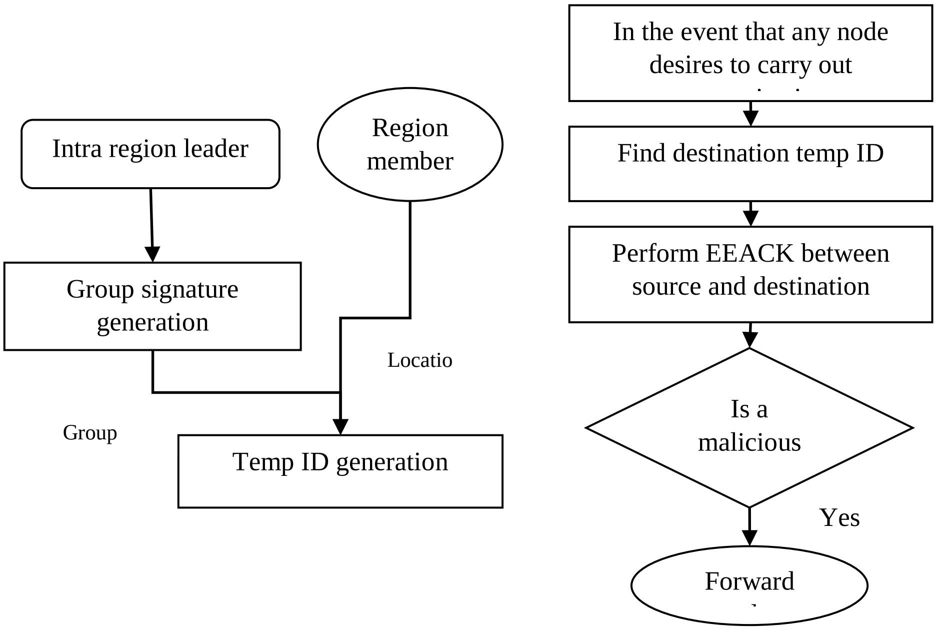
Intra region leader
Region member
Group signature generation
Locatio
Group
Temp ID generation
In the event that any node desires to carry out
Find destination temp ID
Perform EEACK between source and destination
Is a malicious
Yes
Forward

Figure 2.a. Group Signatures are used to Conceal Identities

Figure 2.b. Rule Set Sharing

Figure 2 Protection of Confidentiality via the Production of Group Signatures

Group signatures are comparable to conventional public key signatures, except that they include more privacy safeguards. Members of large, active groups can sign messages using the group signatures method by the creation of group signatures which can be validated with copies of constant-size group public keys. Legitimate group signatures are attested to the signer's membership in groups. Nevertheless, it is computationally challenging to distinguish between two valid group signatures produced by the same (or several) group members. In addition, if group signatures are contested, GMs (Group Managers) which are special entities can examine signatures and determine actual signers. This critical feature is called Escrowed privacy. Thus, group signatures are excellent fits for WSN environments. SNs can routinely sign their current locations (link-states) without worrying about being followed because numerous group signatures cannot be linked. Simultaneous verifications of group signatures are also possible. The following steps are followed in creating group signatures:

a. GMs create foundational group signature schemes and include all authorized SNs into groups. Participant nodes create exclusive private keys (members) during this stage that is not shared for creating legitimate group signatures. Additionally, corresponding public keys (PK members) are generated; however, only GMs can view these keys. Common group public keys (PKGMs), needed to validate group signatures are also taught to members. GMs are in charge of offline forensics, examining any disputed group signatures, and identifying legitimate signers in case of disputes.

b. Depending on specific group signature systems, GMs may also manage future memberships for new members as well as revoke existing members. However, it is envisaged that memberships are fixed in the majority of envisioned WSN situations, allowing all joins to be completed in bulk before deployments. Furthermore, it would need real-time propagations of updated information on revocations of legitimate nodes.

c. SNs broadcast PAMs (Position Announcement Messages) which contain information on their position (GPS coordinates), time stamps, temporary public keys (PK-TMPs), and computed group signatures. PAMs in WSNs may experience flooding.

d. SNs check group signatures and time stamps after receiving new PAMs to ensure that they are not repeated. SNs broadcast PAMs to their neighbors if both of these requirements are satisfied. SNS build geographical maps of the WSN and node connection graphs after gathering all current PAMs.

e. SNs first determine if there is another node at the desired place before attempting to connect with it (or near) that location.

f. If this is the situation, it employs the EEACK mechanism to look for any participation from malicious nodes source-to-destination TmpID.

g. If a viable route is discovered, a notification is delivered to the current pseudonym of the destination (TmpID). This message is encrypted using a session key and a symmetric cipher. The destination's most recent PAM's current public key is then used to encrypt the session key (PK-TMP). The session key is initially recovered when the message reaches its intended recipient, and it is then used to decode the remaining data.

Figure 2 presents an overview of the process that underlies the formation of group signatures for the purpose of protecting users' discretion. The process flow for privacy preservations achieved with group signatures is shown in Figure 2. The communication channel routes are secured and kept clear of hostile nodes mainly due to the employment of EEACK module and explained in the following subsections.

3.3. Malicious Node Identification

The rule set must be sent to the integration leader after obtaining the temp ID for each region member to validate the presence of outlier behavior. Any hacked or malicious node found among the route path nodes has the potential to contaminate the data sent and must be identified and avoided. This is accomplished by using the EEACK strategy in this work. Three of the Watchdog scheme's six shortcomings—false misbehaviors, restricted transmission powers, and receiver collisions—are addressed by EAACK. ACK, secure ACK (S-ACK), and misbehavior report authentication make up the three main parts of EAACK (MRA). We added a 2-b header to EAACK to identify packet kinds in multiple methods. The DSR header has 6 b reserved, according to the Internet draught of DSR. To differentiate between various types of packets, we employ two of the six bits in EAACK.

ACK: In ACK mode, the intra-region leader S delivers Pad1 of an ACK data packet to the intercultural leader D first. If all intermediary nodes across the channel connecting nodes S and D are cooperating and node D gets Pad1, node D is required to send back an ACK acknowledgement packet Pak1 along the same path but in reverse order. If node S gets Pak1 within a definite amount of time, the packet transmission from node S to node D is successful. Without this, node S will enter S-ACK mode and broadcast an S-ACK data packet in order to search for errant nodes in the route.

S-ACK: The three subsequent nodes (F1, F2, and F3) work together in S-ACK mode to find network nodes that are acting improperly. The S-ACK data packet known as Psad1 was transferred from node F1 to node F2. After that, node F2 forwards the message to node F3. It is necessary for node F3, the third node in this trio of nodes, to send node F2 an S-ACK acknowledgment packet, or Psak1, as soon as it receives Psad1. Psak1 is delivered to node F1 after passing via node F2. If node F1 does not receive this acknowledgement packet within a certain length of time, then nodes F2 and F3 are considered to be malevolent. In addition to this, the node F1 will generate a report of inappropriate activity, which will then be sent to the source node S.

MRA: The primary purpose of the MRA approach is to determine whether or not the claimed lost packets were really delivered to the destination nodes by means of an alternative channel. The MRA mode is initiated by the source node conducting a search inside its local knowledge base for an alternate path leading to the destination node. In the event that there isn't already a route, the source node will initiate a DSR routing request in order to locate another one. Multiple paths between two nodes are common in WSNs due to their design. We may avoid the misbehaving reporting node by taking an alternate path to the target.

The target node checks its local knowledge base to see whether the requested packet was delivered. It is safe to assume that this report of fraudulent misbehavior is already in existence and that its author is a malevolent person if it has already been received. Otherwise, the report about the misbehavior is seen as accurate and credible. Because of the

MRA methodology, EAACK may identify malicious nodes even when there are false reports of misbehavior is shown in Algorithm 1.

Pseudo Code for Intra region nodes	Pseudo Code for Inter region nodes
INPUT: Set of activities	INPUT: Set of activities
OUTPUT: True positive detection rate	OUTPUT: True positive detection rate
Start the process	Start the process
Send data between nodes IF (node is the destination)	Send data between nodes IF (node is the destination)
Receive ACK from destination	Receive ACK from destination
ELSE	ELSE
Wait for the ACK before TTL expires	Wait for the ACK before TTL expires
Is ACK receive on time?	Is ACK receive on time?
YES: Node behavior is normal	YES: Node behavior is normal
NO: Enters into S-ACK	NO: Enters into S-ACK
Is S-ACK receive on time?	Is S-ACK receive on time?
YES: Node behavior is normal	YES: Node behavior is normal
NO: Enters into MRA	NO: Enters into MRA
MRA deploys alternate shortest path	MRA deploys alternate shortest path
Is ACK received?	Is ACK received?
YES: Authentication is applied	YES: Authentication is applied
NO: Node is suspected as malicious	NO: Node is suspected as malicious
END IF	END IF
Store node behavior in local rule set	Store node behavior in local rule set
Match the node behavior with the knowledge base	Match the node behavior with the knowledge base
Advertise node behavior to neighbour rule set	Advertise node behavior to neighbour rule set
End the process	Repeat
	Send local audit traces to intrazone node using IDMEF
	UNTIL
	Aggregation algorithm is applied
	Compare the aggregated rule set with knowledge base
	If (knowledge base matches aggregated rule set)
	Node is marked as malicious
	ELSE
	Node is not marked as malicious
	END IF
	End the process

Algorithm 1 Pseudo Code for Intra Region Nodes & Pseudo Code for Inter Region Nodes

The accompanying pseudo code shows how to quickly share rule sets. After exchanging rules from one region to another, rule set aggregation should be performed to ensure accurate outlier activity detection. This procedure is detailed in the following section.

3.4. Rule Set Aggregation

In aggregation techniques, local IDSs are widely utilized. Existing aggregation methods frequently rely on accurate data from local IDSs and are initiated by the receipt of local alerts. In contrast to other instances, ours runs the aggregation procedure often to lighten the computational burden on the gateway nodes. Gateway nodes do nothing if they haven't received any local alerts in the preceding interval. Additionally, our aggregation technique does not depend on the correctness of the data supplied by neighborhood IDSs. The gateway node mostly uses the information below.

The similarity in categorization: The MIDMEF classification field provides this information and indicates the name of the assault. In our situation, it ought to read "Routing Disruption."

The similarity in time: It is possible to get data on time via the usage of the MIDMEF entities Detect Time and Create Time. When an attack takes place, it is specified by the Detect Time, and when it is discovered, it is indicated by the Create Time. A local alert is disregarded if the time difference between the Create Time of an alert that was just received in your area and the gateway node's current time exceeds a certain limit.

Source similarity: It indicates potential attack sources.

Source similarity is the basic foundation of the suggested aggregation strategy. If a node has a viable path to the destination and gets an RREQ (Routing REQuest) packet during the ordinary routing discovery phase, it will respond with an RREP (Routing REPly) packet. If the network topology were random, the distribution of source addresses inside these RREP packets would be uniform over a specific amount of time. Generally speaking, no major bias exists for a particular source address.

The local broadcast data is combined by the gateway nodes, who also calculate the dispersion of source addresses over time. The probability from a certain node must surpass a predetermined threshold P for that address to be recognized as the attacker's to distinguish it from the regular nodes as an attacker. It is vital to note that an attacker cannot change its IP address frequently to send out false messages. Otherwise, its neighbors will quickly detect it. The accuracy of P is essential to the efficiency of our aggregating method. In theory, P is influenced by factors such as attack intensity, attack time, network structure, and so on. If P is set too low, the gateway nodes will have a higher chance of detecting the attack and will be able to do so sooner if they are able to recognize it. On the other side, a low P value will result in a large percentage of false positives being reported. In contrast, the gateway nodes may face a high percentage of false positives if P is set too high. However, there will also be a decrease in the detection rate.

4. RESULTS AND DISCUSSION

The NS-2 simulator is used to evaluate the functionality of the proposed region-based secure data transmission protocol (RSDTP). In our simulations, there is a network comprised of one hundred nodes that are strewn about in a square that is one hundred meters on each side. There are two types of nodes that appear in the experiments: nodes that behave themselves and nodes that act maliciously. Malware nodes have the potential to execute denial of service threats in experimental scenarios. The BS has an endless supply of energy. For one period, there is a cap of 10% placed on the number of area leaders who may be elected. The characteristics of the intended RSDTP are compared to those of the already existing Secure Clustering Scheme with Cloud based Trust Evaluation method (SCCT), Taylor Kernel Fuzzy C-Means Clustering (TKFCC) protocol, and Evolutionary Game based Secure Clustering Protocol (EGSCP) systems. The values that were chosen for the simulation parameters utilized in this research are shown in Table 1. The RSDTP model's performance was assessed using metrics including delivery ratios, detection rates, false alarm and positive rates, connection change rates, and mean times to alarm.

Table 1 Simulation Parameters

Simulation Parameters	Values
Channel	Wireless Channel
Mac	802.11
Antenna Type	Omni antenna
Initial Energy	100 joules
Traffic type	CBR
Agent	UDP
Simulation Area	100x100 meters
Number of nodes	100

4.1. Energy Consumption

The amount of energy that is used is an important presenting statistic for sensor networks. The less energy utilized, the longer the network lifespan, and it validates that the security pattern does not deplete the networks at the time when attacks are being detected.

Table 2 Energy Consumption Comparison Values

Time(Seconds)	Energy consumption(mJ)			
	SCCT	TKFCC	EGSCP	RSDTP
10	97	96.5	95	92
20	93	92	90	88
30	87	85	83	80
40	86	84	81	79
50	81	79	77	75

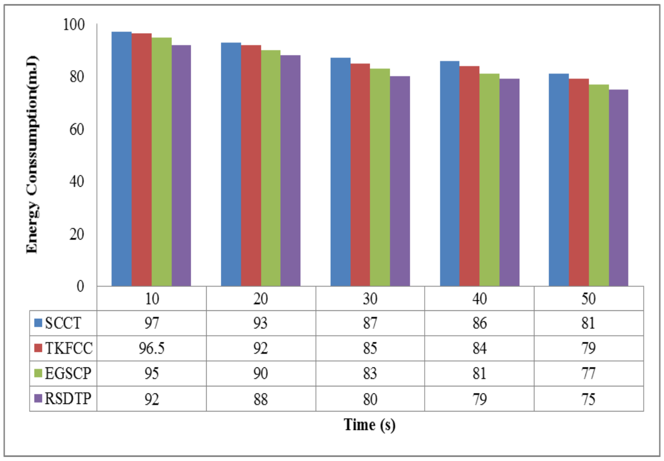

Figure 3 Energy Consumption (mJ) Vs Time

Table 2 and Figure 3 depicts the evaluation of the methods such as SCCT, TKFCC, EGSCP and proposed RSDTP in terms of energy consumption. According to the graphical evaluation, the proposed RSDTP approach provides a better indication in secured packet transfer while consuming lesser energy. For the time period of 50 s, the amount of energy that is consumed by the proposed RSDTP model is 75 mJ that is much lesser when compared to existing methods such as SCCT (81 mJ), TKFCC (79 mJ) and EGSCP (77 mJ). It is clearly indicated that the proposed RSDTP approach outperforms the other existing techniques taken for comparison. This performance improvement of the proposed approach is mainly due to the region based approach formulated by the RSDTP technique.

4.2. Delay

An important component of the planning and operation of a computer network or a telecommunication system is the ability to report the amount of time it takes for one byte of data to travel from one node or endpoint to another across the network. It is measured in either whole seconds or fractions of whole seconds. The experimental analysis of the data for proposed tactic in relation to the delay parameter is shown in Figure 4 and Table 3.

Table 3 Delay Comparison Values

Time (Seconds)	Delay (ms)			
	SCCT	TKFCC	EGSCP	RSDTP
10	0.15	0.08	0.05	0.015
20	0.21	0.11	0.06	0.04
30	0.32	0.15	0.11	0.09
40	0.40	0.21	0.15	0.12
50	0.50	0.30	0.23	0.17

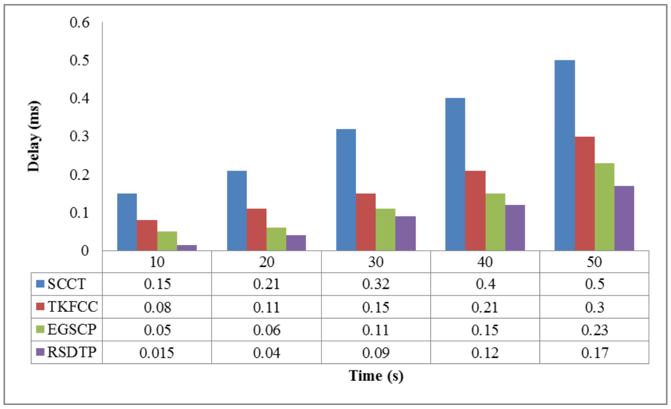

Figure 4 Delay Comparison

Table 3 and Figure 4 depict the evaluation of existing techniques such as SCCT, TKFCC, EGSCP and the proposed RSDTP technique in terms of delay. According to the graph, the proposed RSDTP provides a better indication in secured packet transfer with lesser delay. For the time period of 50 seconds, the delay attained by the proposed RSDTP model is greatly reduced with 0.17 ms when compared other existing techniques attaining higher delay comparatively. For example, SCCT attained 0.50 ms, TKFCC attained 0.30 ms and EGSCP attained 0.23 ms. The proposed system has 66%, 43.333%, and 26.08% lesser delay when compared to SCCT, TKFCC, and EGSCP methods for 50 seconds respectively. This is mainly because of the group signature generation, proposed RSDTP work has lesser delay for data transmission between nodes.

4.3. Delivery Ratio

The percentage of delivered packets to all packets sent is known as the delivery ratio. The percentage of packets that are sent to a destination above what the transmitter supplies in terms of packets. In terms of delivery ratio, Figure 5 compares the proposed technique with earlier research methodologies.

Table 4 Delivery Ratio Comparison Values

Time (Seconds)	Delivery ratio (%)			
	SCCT	TKFCC	EGSCP	RSDTP
10	75	82	88.5	90.3
20	79	83	89.5	91
30	82	85	90	92.4
40	86	88	91.2	93.7
50	88	90	92	94

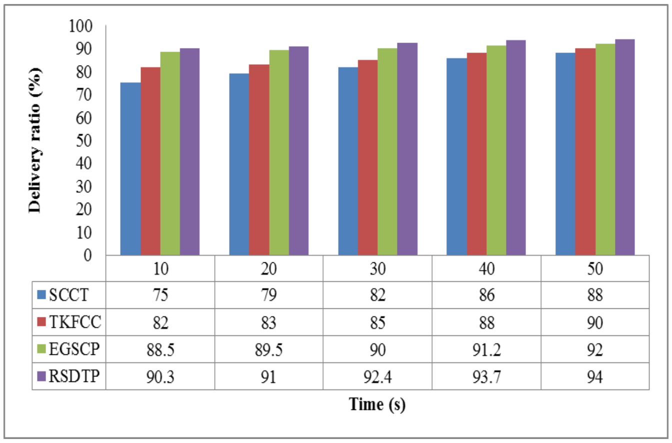

Figure 5 Delivery Ratio Comparison

This experimental evaluation confirms that the proposed RSDTP method of study that has been offered has a good chance of ensuring effective routing with an improved delivery ratio, hence increasing the number of packets that can be transmitted. Table 4 and Figure 5 confirm that the proposed research approach produces the best results in terms of delivery ratio. For the time period of 50 seconds, the Delivery Ratio attained by the proposed RSDTP model is 94% that is better than the delivery ratio attained by the existing approaches SCCT (88%), TKFCC (90%) and EGSCP (92%). The proposed system has 6%, 4%, and 2% higher delivery ratio when compared to the existing methods such as SCCT, TKFCC, and EGSCP methods for a time period of 50 seconds respectively. The higher delivery ratio of the proposed work is due to the fact that an enhanced adaptive acknowledgment is generated between the sources and destination.

4.4. Network Lifetime

The length of time that a Wireless Sensor Network is capable of functioning normally is referred to as its network lifespan. One of the definitions of network lifetime that is utilized quite frequently is the point in time at which the first network node expends more effort than is required to transfer a packet. This is due to the fact that the network might be deprived of certain functionality in the event that a node is lost.

Table 5 Network Lifetime Comparison Values

Time (Seconds)	Network lifetime (s)			
	SCCT	TKFCC	EGSCP	RSDTP
10	79	87.25	94.55	95.3
20	82	89.5	94.53	95
30	86	91.50	94.3	94.4
40	89	92.10	93.8	94.1
50	91	93	93.6	93.8

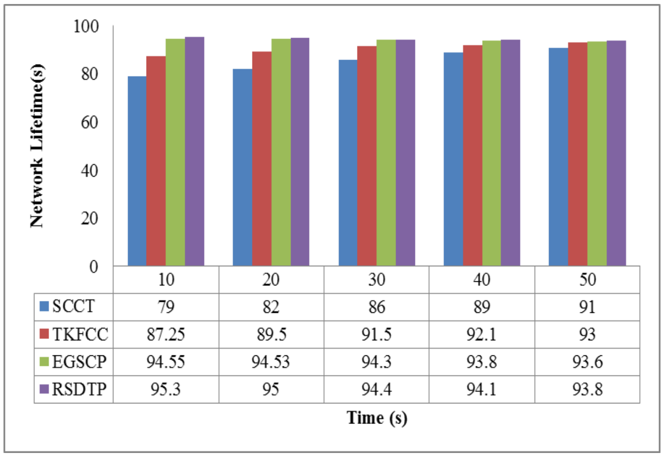

Figure 6 Network Lifetime Comparison

Table 5 and Figure 6 confirm that the approach to study that has been described is likely to assure effective packet transfer with no failures during execution. For the time period of 50 s, the network lifetime of the proposed work attained higher network lifetime of 93.8 seconds. Alternatively, the other existing techniques such as SCCT, TKFCC and EGSCP attained lesser network lifetime of 91 s, 93 s and 93.6 s respectively. The proposed system has 2.80%, 0.80%, and 0.20% higher network lifetime when compared to SCCT, TKFCC, and EGSCP methods for a period of 50 s respectively. The main reason for the better network lifetime of the proposed model is the deployment of an identification of outlier activity using the incoming aggregated rule set.

4.5. Throughput

Throughput in networking refers to the quantity of information that can be moved from one location to another within a certain length of time.

Table 6 and Figure 7 confirm that the throughput Comparison of the proposed and existing research method tends to ensure successful packet transmission with no failures during execution. For the time period of 50 seconds, the throughput is effectively increased using proposed RSDTP model by 156 Kbps when compared to existing techniques taken for comparison SCCT (128 Kbps), TKFCC (140 Kbps), and EGSCP (150 Kbps). The proposed RSDTP model attained 17.94%, 10.25%, and 3.84% higher throughput when compared to SCCT, TKFCC, and EGSCP methods for 50 period seconds respectively. Since the proposed work used the private rule sharing using group signatures, the network throughput is increased comparatively.

Table 6 Throughput Comparison Values

Time (s)	Throughput (kbps)			
	SCCT	TKFCC	EGSCP	RSDTP
10	90	105	118	126
20	95	111	121	132
30	102	120	127	141
40	120	132	147	152
50	128	140	150	156

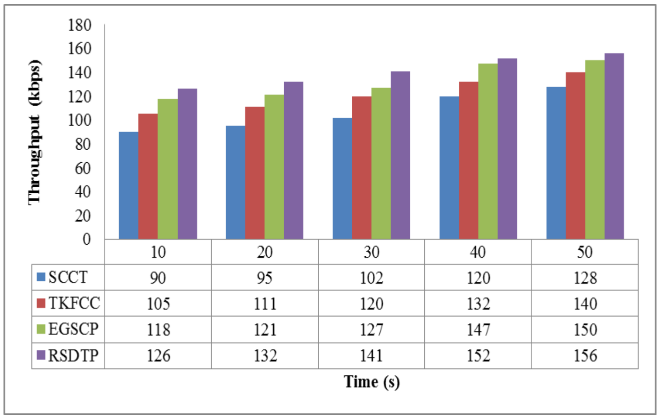

Figure 7 Throughput Comparison

5. CONCLUSION

The Region-Based Secured Data Transmission Protocol (RSDTP) is used in the proposed research project for the precise identification of anomalous behavior. By using Private Position Aware Routing in WSNs, where group signatures are created by all region members using the group public key supplied by the intra-region leader, private rule sharing is ensured in the suggested research approach. As a result, it is impossible to give members of the region their exact location. Private rule sharing may be safeguarded using these group signatures. Secure rule sharing is made possible in this study by the use of Enhanced Adaptive Acknowledgement, which verifies that there are adversarial nodes present before rule sharing. This discussion would take place at the conference of domestic and regional leaders dedicated to rule-sharing. In order to make the most of the available memory space, this research performs rule set aggregate while securely transmitting rule sets from inter-regional leadership. The NS2 simulation environment is used to fully evaluate the proposed technique RSDTP, showing that it is capable of ensuring the secure and reliable conveyance of data values that does not include the involvement of potentially harmful actions.

REFERE NCES

[1] Tomić I., Mccann J.A. A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols. IEEE Int. Things J. 2017;4:1910–1923.

[2] Rawat P., Singh K.D., Chaouchi H., Bonnin J.M. Wireless sensor networks: a survey on recent developments and potential synergies. J. Supercomput. 2014;68:1–48.

[3] Zhang Z., Mehmood A., Shu L., Huo Z., Zhang Y., Mukherjee M. A survey on Fault Diagnosis in Wireless Sensor Networks. IEEE 2016;6:11349–11364.

[4] Qiu T., Qiao R., Wu D.O. EABS: An Event-Aware Backpressure Scheduling Scheme for Emergency Internet of Things. IEEE Trans. Mob. Comput. 2018;17:72–84.\

[5] Qiu T., Chen N., Li K., Atiquzzaman M., Zhao W. How can heterogeneous Internet of Things build our future: A survey. IEEE Commun. Surv. Tutorials. 2018;20:2011–2027.

[6] Qiu T., Zheng K., Song H., Han M., Kantarci B. A local-optimization emergency scheduling scheme with self-recovery for smart grid. IEEE Trans. Ind. Inf. 2017;13:3195–3205.

[7] Dhurgadevi M., Devi P.M. An Analysis of Energy Efficiency Improvement through Wireless Energy Transfer in Wireless Sensor Network. Wirel. Pers. Commun. 2018;98:3377–3391.

[8] Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey. ACM Comput. Surv. 2009;41:1–58. doi: 10.1145/1541880.1541882.

[9] Butun, I., Morgera, S. D., &Sankar, R. (2014). A survey of intrusion detection systems in wireless sensor networks. IEEEcommunications surveys & tutorials, 16(1), 266-282.

[10] Chow, P., Rhee, W., Tehrani, A. M., &Goldburg, M. (2016). U.S. Patent No. 9,369,370. Washington, DC: U.S. Patent and Trademark Office.

[11] Kenkre, P. S., Pai, A., &Colaco, L. (2015). Real-time intrusion detection and prevention system. In Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014 (pp. 405-411). Springer, Cham.

[12] Krishnan, D. (2015). A distributed self-adaptive Intrusion Detection System for Mobile Ad-hoc Networks using tamper evident mobile agents. Procedia Computer Science, 46, 1203-1208.

[13] Ahmadifard, N., Nabizadeh, H., &Abbaspour, M. (2014). ISEFF: An ID-based scalable and efficient distributed file sharing technique in vehicular ad hoc networks. Wireless personal communications, 75(2), 821-841.

[14] Hadded, M., Muhlethaler, P., Laouiti, A., Zagrouba, R., &Saidane, L. A. (2015). TDMA-based MAC protocols for vehicular ad hoc networks: a survey, qualitative analysis, and open research issues. IEEE Communications Surveys & Tutorials, 17(4), 2461-2492.

[15] Sharma, S. K., Kumar, R., Gangwar, A., &Pakhre, K. (2014). Routing protocols and security issues in MANET: A survey. International Journal of Emerging Technology and Advanced Engineering,(IJETAE), 4(4), 918-924.

[16] Shaikh, F., & Parekh, C. (2017). A Review Paper on Intrusion Detection System in MANETs.

[17] Lin, W. C., Ke, S. W., & Tsai, C. F. (2015). CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. Knowledge-based systems, 78, 13-21.

[18] Athavale, N., Deshpande, S., Chaudhary, V., Chavan, J., &Barde, S. S. (2017). Framework for Threat Analysis and Attack Modelling of Network Security Protocols. International Journal of Synthetic Emotions (IJSE), 8(2), 62-75.

[19] Gai, K., Qiu, M., Tao, L., & Zhu, Y. (2016). Intrusion detection techniques for mobile cloud computing in heterogeneous 5G. Security and Communication Networks, 9(16), 3049-3058.

[20] Mehrotra, A., Saxena, A., &Tolani, M. (2014). Performance comparison of different routing protocols for traffic monitoring application. International Journal of Computer Applications, 92(4).

[21] Srivastava, V., Tripathi, S., & Singh, K. (2020). Energy efficient optimized rate based congestion control routing in wireless sensor network. Journal of Ambient Intelligence and Humanized Computing, 11(3), 1325-1338.

[22] Kalnoor, G., &Agarkhed, J. (2016, March). QoS based multipath routing for intrusion detection of sinkhole attack in wireless sensor networks. In 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT) (pp. 1-6). IEEE.

[23] Thangaramya, K., Kulothungan, K., Gandhi, S. I., Selvi, M., Kumar, S. S., &Arputharaj, K. (2020). Intelligent fuzzy rule-based approach with outlier detection for secured routing in WSN. Soft Computing, 24(21), 16483-16497.

[24] Jan, M. A. (2016). Energy-efficient routing and secure communication in wireless sensor networks (Doctoral dissertation).

[25] Kalidoss, T., Rajasekaran, L., Kanagasabai, K., Sannasi, G., & Kannan, A. (2020). QoS aware trust based routing algorithm for wireless sensor networks. Wireless Personal Communications, 110(4), 1637-1658.

[26] Ahmed, A., Bakar, K. A., Channa, M. I., Haseeb, K., & Khan, A. W. (2016). A trust aware routing protocol for energy constrained wireless sensor network. Telecommunication Systems, 61(1), 123-140.

[27] Latha, A., Prasanna, S., Hemalatha, S., &Sivakumar, B. (2019). A harmonized trust assisted energy efficient data aggregation scheme for distributed sensor networks. Cognitive Systems Research, 56, 14-22.

[28] Beheshtiasl, A., &Ghaffari, A. (2019). Secure and trust-aware routing scheme in wireless sensor networks. Wireless Personal Communications, 107(4), 1799-1814.

[29] Dhand, G., &Tyagi, S. S. (2019). SMEER: secure multi-tier energy efficient routing protocol for hierarchical wireless sensor networks. Wireless Personal Communications, 105(1), 17-35.

[30] AlFarraj, O., AlZubi, A., &Tolba, A. (2018). Trust-based neighbor selection using activation function for secure routing in wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 1-11.

[31] V. Nagaraju, N. J. Kumar, A. M. Ali, T. B. R. Bapu and N. Partheeban, "Efficient Data Transmission Scheme using Modified Wireless Communication Protocol Design," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), 2022, pp. 1-7, doi: 10.1109/ACCAI53970.2022.9752622.

[32] Khot, P. S., &Naik, U. L. (2022). Cellular automata-based optimised routing for secure data transmission in wireless sensor networks. Journal of Experimental & Theoretical Artificial Intelligence, 34(3), 431-449.

Authors

Ashok Kumar R, Research Scholar, SRMV College of Arts and Science, Coimbatore. His research interests include Network Security and Big Data.

R. Kannan, Associate Professor, SRMV College of Arts and Science, Coimbatore. His specialization is Network Security, and his area of interest is, Artificial Intelligence, Pattern Recognition, Machine Learning and Deep Learning.

How to cite this article:

Ashok Kumar R, R. Kannan, “Region Based Secured Data Transmission Protocol for Wireless Sensor Network”, International Journal of Computer Networks and Applications (IJCNA), 9(5), PP: 533-544, 2022, DOI: 10.22247/ijcna/2022/215914.