International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/59 Volume 12, Issue 6, November – December (2025)

RESEARCH ARTICLE

Secure Routing Through Trust Evaluation for Aggregator Node in Hierarchical Wireless Sensor Networks (WSN)

N. Shantha Kumar
Department of Computer Science and Engineering, K R Pet Krishna Government Engineering College, K.R.Pet, Mandya, Karnataka, India.
✉ shanth86309@gmail.com

Hareesh. K
Department of Computer Science and Engineering, K R Pet Krishna Government Engineering College, K.R.Pet, Mandya, Karnataka, India.
hareeshk.gec@gmail.com

Received: 06 August 2025 / Revised: 07 November 2025 / Accepted: 12 December 2025 / Published: 30 December 2025

Abstract – Wireless Sensor Networks (WSN), offer cost efficient solutions to monitor physical tasks and has become popular and widely used in real-time monitoring applications to exchange digital data with physical things or devices. Integration of WSN into IoT (Internet of Things) offers game changing solutions and technical improvements can further lead to deliver real time data effectively. However, WSN are restricted to limited resources and their working environment and communication characteristics faces security threats. Nodes are exposed to different types of attacks, including unauthorized information access and malicious activities. These vulnerabilities degrade network performance and reduce node trustworthiness. Therefore, it is imperative for nodes to detect threats early and mitigate compromised nodes. Security measures based on cryptography are designed to shield sensor nodes against WSN attacks and operate in safe environment. However, cryptographic operations devour more resources and not appropriate to administer misbehaving attacks. To cope with different activities and behaviour of malicious nodes, trust-based model offers feasible solution to detect and isolate attacker nodes. As a part of this paper, we propose light weighted reputation-based trust aware routing scheme (LRTARS) to defend against malicious activities during routing, especially internal attacks. LRTARS is designed through trust model evaluating direct and indirect trust value. The proposed scheme chooses secure cluster head (CH) and establishes secure multihop routes towards base station (BS) through inter and intra cluster communication. To avoid communication congestion, LRTARS computes channel busy ratio at MAC and assigns secure channel for reliable data transmissions.

Index Terms – Attacks, Cluster, Misbehaviour, Trust, Lightweighted, Congestion, Secure.

1. INTRODUCTION

Wireless Sensor Networks (WSNS) has made significant contributions in research and innovation expansion. WSN have been majorly implemented in various useful important fields, including the defence, healthcare, smart cities, and environmental monitoring [1-3]. Sample WSN is shown in Figure 1. Nodes in the network access common resources like bandwidth and node queues which are limited and restricted resources. When node has some data to be sent it tries to access channel, the packet gets queued in nodes temporary cache. In large scale network, multiple nodes try to access channel simultaneously which may lead to collision and packet drop. If the drop ratio is more than the specified limit, then the network is said to be congested therefore it is necessary to detect and alleviate congestion to improve overall network Quality of Service (QoS) parameters. It is required to know the status of the channel to avoid data collision. The channel busy ratio parameter can be integrated for capturing the channel status until the node finds channel busy with a certain interval of time.

WSN assisted IoT endures the possibility to serve number of application fields such as significant data-powered applications and 5G networks [4-6]. Without any human aide, WSN can withstand harsh weather conditions and operate independently over extended period of time. As shown in Figure 1, WSN comprises of small, battery-operated sensor nodes that are self-configured. The energy and resources available to sensors are limited. These data-centric nodes are in tasked for gathering applicable data in the target region and relaying it, either single-hop or multi-hop, to the data

RESEARCH ARTICLE

collection node known as base station (BS) or sink. The sink or BS receives the collected data from the sensor nodes [7-8]. Nodes consume more energy due to their constantly sensing and sending data. To balance nodes energy, hierarchical clustering techniques offers advantages in terms of scalability and energy efficiency, and substitutes for network energy harvesting to overcome energy issues. Using data aggregation, clustering algorithms effectively balance node energy. The well-known cluster-based routing technique known as low energy adaptive clustering hierarchy (LEACH) and its variants, including i-LEACH, Centralized-LEACH, and Threshold-LEACH, have subsequently seen further development [9-11]. Deployment of nodes in harsh environment and unattended area makes susceptible to internal and external attacks [12-13].

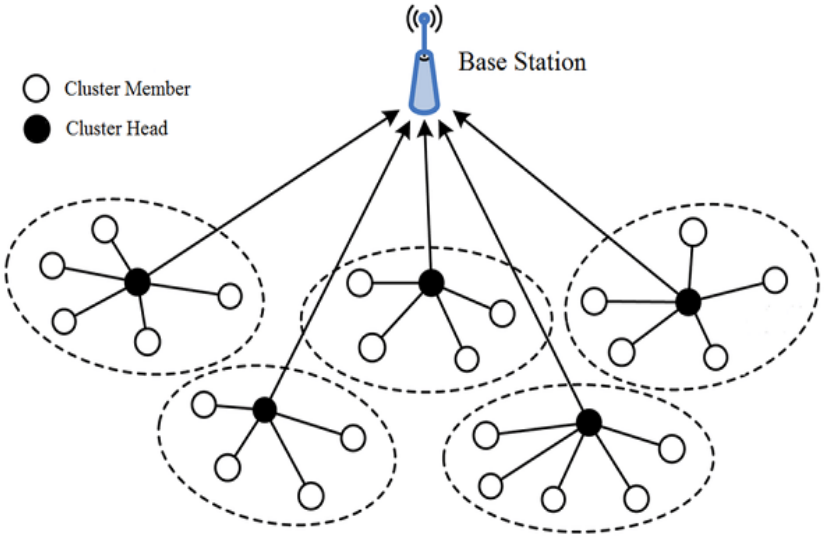

Figure 1 WSN Cluster

To ensure secure routing of WSN, many authors proposed cryptography-based authentication and verifying routing protocols. Cryptographic based secure mechanism involves complex operations and sophisticated calculations during key generation, authentication and verification, which incurs higher computational overhead and consumes more resources. However, cryptographic based secure routing protocols do not deal with internal attacks.

Trust aware or reputation-based routing mechanism have been potentially verified to be effective in defending against internal misbehaviour attacks in WSN [14-18]. Trust routing schemes anticipate the behaviour of node moment depending on its previous historical conducts. Nodes trust values are built through quantifying its behaviour, higher the trust value the node is believed to be in good behaviour and trustworthy.

However, conventional trust aware model schemes suffer some drawbacks such as trust value calculation whenever node is revoked, not being fast enough to compute trust value to identify malicious node due to complex operations, more information resulting congestion and fail to secure against too many attacks.

Also do not considering multi attributes such as energy balance, optimal CH selection and channel condition to avoid data collision as a part of this paper, we recommend light weighted reputation-based trust aware routing scheme (LRTARS) to defend against malicious activities during routing, especially internal attacks.

1.1. Main Objectives

- To design energy efficient cluster-based routing through evaluating trust to determine the next forwarder.
- To ensure energy balance among the nodes, existing LEACH is modified for optimal CH selection considering energy parameters with trust value.
- Integration of Channel busy ratio at MAC layer for congestion free and secure data transmission through channel during retransmissions for the lost packets.

1.2. Contributions

- LRTARS provides resource aware adaptive routing by integrating lightweighted trust scheme through computing nodes direct and indirect trust scores or value, which can defend against common attacks.
- Channel busy ratio and several trust metrics are computed and better decisions are made to achieve network performance.
- Modification of existing LEACH for choosing optimal cluster head (CH) considering energy and trust parameters to prolong network lifetime.

RESEARCH ARTICLE

1.3. Problem Statement

WSNs are susceptible to different kinds of threats due to their deployment in hostile environments and left unattended by human. Attacks are classified as external and internal attacks. Cryptography based security mechanism enables WSN to function securely through authentication and verification process. However, such cryptography mechanism cannot defense against internal attacks. In internal attacks, node establishes fake ID, misbehaves with authentic node leading to degraded network performance and reduces node trustworthiness. Thus, it is imperative to establish trust between nodes in WSN, which comprises of multitude sensor nodes and data aggregator nodes or CH that aggregate the sensed data. In order to guarantee secure routing and avoid misbehaving of node in WSN, it is necessary for the node to be aware of behaviour moment of the next node based on the trust model through quantifying its historical behaviours. Therefore, this motivates us to propose light weighted trust aware scheme to defend against internal attacks and also reduce the computational overhead compared to cryptographic schemes.

The rest of the paper is planned as follows: the related works are provided in section 2, the proposed LRTARS are defined in section 3, and the configuration of simulation and metrics of performance are discussed in section 4. Section 5 concludes with conclusion and future potential improvements.

2. RELATED WORKS

Due to WSN limited resources, their deployment and environmental conditions and secure communication author in [19] presented trust and energy aware routing method using adaptive genetic algorithm to mitigate routing attacks in addition to minimize energy consumption. The secure performance of nodes is evaluated using filtering mechanism, volatilization and adaptive penalty factors. The comprehensive trust score or value is constructed based on these factors. Secure CH is chosen based to dynamic variations in threshold energy value and trust scores. Genetic algorithm computes the shortest and selects energy efficient routes towards BS using fitness function along with the higher trust value nodes. Simulation results show, this routing scheme efficiently resist common blackhole attacks in network layer and delivers higher packet ratio. However, this method exploits higher computational overhead during multihop communication during mutation and crossover operators resulting higher resources. In [20], author proposed trust based dynamic network security model for wireless sensor network. In this model, the inclusive value of trust is computed considering the dynamic changes in node according to trust degree and network topology structure. This model adapts and reacts to the network changes using adaptive dynamic adjustment method as well as the direct trust value of the nodes are evaluated based on its behaviour within the transmission range. Comprehensive trust values are evaluated based on energy consumption, trust value recommendation of high trust nodes. Finally, the misbehaving nodes are detected and mitigated according to their trust credibility which ensures secure, dynamic and reliable network operations. Due to topology changes, network experiences communication failures which results in higher routing overhead. In [21], energy and trust aware opportunity routing scheme (ETOR) was presented by author to mitigate misbehaviour nodes. ETOR functions in two phases. Initially, trustworthy secured nodes are determined through energy fitness, trust value, connectivity range and QoS parameters. The opportunistic routing is accomplished by choosing secure and energy efficient nodes. ETOR adapts reactive routing and discovers optimal multipath routes considering traffic load and distance to deliver higher packet ratio. K-means algorithm is used for cluster formation and CH selection, and ETOR performance demonstrates energy efficiency, defense against suspicious nodes, and enhancement of PDR, communication overhead and throughput metrics. However, this scheme selects CH based on energy fitness and is limited to defend against specific routing attack. In [22], author proposed mechanism to detect and isolate Denial of Service (DoS) and Man-in-the-Middle (MITM) for hierarchical cluster-based routing using LEACH. The goal is to determine secure routes through optimal CH's through defending attacker nodes. Cryptographic function such as secure hash function SHA-256 and real time message content validation (RMCV) is used to authenticate valid nodes for secure communication. Experimental results show robustness in detection and mitigating attacker node against vulnerabilities. Due to complex cryptographic operations, this scheme suffers from higher computational overhead and consumes higher resources. In [23], author proposed trust management scheme for hierarchical cluster based WSN using fuzzy logic. This scheme aims to secure and minimise the communication overhead and memory during intra and inter cluster communication. Sensor nodes trust value calculation is computed at every level of hierarchy. This scheme records the trust between cluster members (CM) of same cluster, between CH and CM and between CH and BS. Direct trust calculation is evaluated on the history of previous real time behaviour and credit-based evaluation. The control factors are used to reduce biasness of trust value and credit points helps to increase the accuracy of trust value. The experience point or the previous behaviour of the node is provided by the reputation of the sensor node. Fuzzy based decision helps to distinguish between good and malicious nodes and makes appropriate decision for secure routing between CH to CH and CH to BS. Simulation results show the overall decrease in communication overhead and better decision making for delivering higher packet ratio. However, this scheme is restricted to small scale WSN cluster and experiences higher delay. In [24], author proposed cluster-based routing by

RESEARCH ARTICLE

employing trust index through optimized CH to achieve secure communication and improved network lifetime. CH's are selected based on trust metrics such as energy backup, trust degree, packet delivery rate and packet consistency. The trust degree of node should be greater; nodes with least degree are restricted to join particular CH, thus reducing the likelihood of network being attacked. The trust index is build based on the nodes trust degree and influences the CH to choose secure routes by referring trust index in order to assure integrity and reliability. Multiple alternate potential paths are chosen by the most trustworthy nodes. This scheme delivers higher packet ratio through defending malicious node and improves network lifetime. However, this scheme does not provide robust trust evaluation. In [25], author proposed secure trust-based energy efficient routing to defend against common attacks in WSN. This routing scheme aims to resist multiple attacks such as blackhole, sinkhole, and wormhole attacks through computing comprehensive trust value adapting direct, indirect and energy trust values. Fast identification of malicious nodes is achieved by using adaptive penalty mechanism and volatilization factors. Nodes evaluate direct trust value using adaptive penalty and volatilization factor considering time and space for evaluating trustworthy nodes accurately. Comprehensive trust value is calculated at sink based on the trust values forwarded by nodes to avoid any information congestion. Misbehaving nodes are monitored by inspector nodes, which updates about secure multiple routes towards sink through CH's. The results found after simulation shows best performance with respect to communication overhead, and packet deliver. However, no optimal CH selection and complex trust calculation. Summary of the above related works focus on establishing secure routes through trust model However, the above schemes have higher computational functions to compute trust values which require more resources. In [26], author proposed multidimensional secure cluster-based routing integrating binomial distribution to defend against internal attack. This trust-based model computes both direct as well as trust value to choose CH & rotation of CH takes place based on the trust values. However, this scheme does not consider network resources and does not prolong network lifetime. In [27], author proposed multi-attribute secure trust model for mobile-IoT to extend network lifetime. To ensure secure and energy efficient routing this scheme computes multiple attributes of nodes such as trustworthiness, energy and distance to achieve robust security. During trust assessment, the nodes energy value is made aware to the next forwarder node to reduce retransmission and balance network energy. This scheme employs hybrid k-model clustering for cluster construction and CH are chosen using spider monkey optimization. In [28], author presented enhance multi attribute-based trust attack resistance (EMBTR) model for secure routing for WSN. EMBTR algorithm is designed to isolate misbehaving node based on their trust metrics and attributes like stability rate (SR), reliability rate (RR) and elapsed time (ET) to establish secure as well as reliable routes to destination. This scheme offers robust solution in identifying malicious nodes and resist attacks in resource constrain environments. In [29], author proposed energy optimization along with secure communication for resource constrained WSN named Trust aware neuro-fuzzy based cluster with sparrow search Optimization in wireless sensor network (NFSSOA). Neuro fuzzy algorithm is employed for efficient cluster formation and energy efficient routes are discovered using sparrow search optimization algorithm. ECC-based cryptographic scheme has been employed for lightweighted key generation, authentication and verification. Hop-to-hop authentication is computed to verify authenticity of nodes through encryption and decryption ensuring secure multihop transmissions. Pseudo-random identity generation is integrated to perform anonymous authentication. In [30], author proposed attribute trust-based routing (ABETBSRA) integrating bilinear paring and Diffie-Hellman combining with RSA algorithm for encryption as well as decryption. Proposed method also integrates trust management scheme for secure communication between nodes and base station (BS). To improve routing reliability, nodes trust scores are computed depending upon encryption and decryption attempts by the nodes enhancing better security. RSA algorithm and Diffie-Hellman scheme are utilized to generate keys, authentication and verification. Communication between nodes and BS is established through computing nodes direct and indirect trust values which offers better security and functionality. Summary of the above related works focus on establishing secure routes through trust model However, the above schemes have higher computational functions to compute trust values which require more resources.

Table 1 Summary of Literature Review

Reference	Acronym	Advantages	Disadvantages
[19]	Trust based adaptive genetic algorithm (TAGA)	Security and energy savings	Higher computation cost
[20]	Dynamic secure trust-based routing (DSTR)	Dynamic and reliable	Lack of feedback control
[21]	Energy-aware trust and	Optimal routes for effective	Cannot reflect accurate node

RESEARCH ARTICLE

	opportunity-based routing (ETOR)	transmission	behaviour
[22]	Energy temperature degree-low energy-adaptive clustering hierarchy (ETD-LEACH)	Improved network lifetime	Higher overhead computation due to complex functionalities
[23]	Fuzzy Based Hierarchical Trust Management Scheme in WSN (HTMS)	Constructive utilization of memory and communication overhead through trust evaluation	Lack of dynamic adaptability
[24]	Trust Index Optimized Cluster Head Routing (TIOCHR)	Optimized CH selection and energy load balance	Reduced convergence rate
[25]	Trust Based Secure and Energy Efficient Routing Protocol (TBSEER).	Fast identification of malicious nodes through adaptive penalty function	Limited attributes and restricted to types of attacks.
[26]	Multi-dimensional Secure Clustered routing scheme in hierarchical wireless sensor Networks (MSCR)	Improves availability of network and enhances network security based on environmental parameters	Applicable to centralized network.
[27]	Energy-aware Multi-Attribute Trust (EMAT)	Multi objectives function enhances reliable energy efficient routing and secure communication	Higher delay due to dynamic changes in network topology
[28]	An Enhanced Multi Attribute Based Trusted Attack Resistance (EMBTR)	Influences Quality of Service (QoS) attributes like stability rate (SR), reliability rate (RR), and elapsed time (ET) for betterment of working of networks	Higher energy consumption due to computation of multi criteria functions
[29]	Trust-aware neuro-fuzzy-based clustering along with sparrow search optimization algorithm (NF-SSOA)	Resistance to various security and improves network parameters	Complex function due to cryptographic operations
[30]	Attribute-Based Encryption and Trust Based Secure Routing Algorithm (ABE-TBSRA)	Scheme combines bilinear pairing and Diffie Hellman encryption scheme with RSA algorithm to encrypt and secure the data.	Higher computation overhead due to complex cryptographic evaluations.

3. PROPOSED LRTARS

3.1. Network Model

The Architecture diagram is as shown in Figure 2. Network in LRTARS comprises of numerous sensor nodes n randomly deployed in a sensing area that are interconnected via wireless radio links. The sensor network has been segmented into different cluster groups. Base Station has been placed away from nodes; CH aggregates the gathered data from nodes and forwards aggregated data to BS. Euclidean distance $D = \sqrt{(y_i - y_j)^2 + (x_i - x_j)^2}$ is used to calculate distance between nodes and following are the network assumptions after node deployment.

- Nodes in the network area are static including BS
- Same amount of initial energy, transmission range, storage are assigned to all nodes.
- Trust value of nodes and trustworthy nodes are selected based on direct, indirect and comprehensive trust value evaluation.

3.2. Energy Consumption Model

The energy model uses the multipath channel model d^4 and the free space channel model d^2 to determine the energy

RESEARCH ARTICLE

consumption of nodes. The computation will be done considering distance between sender and recipient nodes. Amount of energy needed for transmitting data packet of γ bits all over the distance D is computed as shown in equation (1):

$$E\mu_{TX} = \begin{cases} \gamma * E_{elec} + \gamma * \varphi_{fs} * d^2 & d \leq d_0, \\ \gamma * E_{elec} + \gamma * \varphi_{mp} * d^4 & d > d_0, \end{cases} \quad (1)$$

d_0 will be computed as $d_0 = \sqrt{\varphi_{fs}/\varphi_{mp}}$, where φ_{fs} and φ_{mp} are the amplification factor and d_0 is the threshold when $d \leq d_0$and $d > d_0$, E_{elec} circuit energy consumed for digital coding and modulation.

Reception node energy to receive γ bits is expressed as shown in equation (2):

$$E\mu_{RX} = \gamma * E_{elec} \quad (2)$$

Energy consumed during aggregation of m bits of data is expressed as shown in equation (3):

$$E_{AG} = m * E_{RD} \quad (3)$$

where $E_{RD}$is radio energy per packet

The remaining energy of node is calculated as shown in equation (4):

$$RE = e_{init} - E\mu_{TX} - E\mu_{RX} - E_{AG} \quad (4)$$

where e_{init} is initial energy and energy trust is denoted as shown in equation (5):

$$E_T = \frac{RE}{e_{init}} \quad (5)$$

3.3. Channel Busy Ratio

When node has some data to be sent it tries to access channel, the packet gets queued in nodes temporary cache. In large scale network, multiple nodes try to access channel simultaneously which may lead to collision and packet drop. If the drop ratio is more than the specified limit, then the network is said to be congested therefore it is necessary to detect and alleviate congestion to improve overall network Quality of Services, (QoS) parameters).

It is required to know the status of the channel to avoid data collision. The channel busy ratio parameter can be integrated for capturing the channel status until the node finds channel busy with a certain interval of time

In proposed LRTARS, we include the parameter channel busy ratio ψ to know the status of the channel to avoid data collision. The channel busy ratio ψ for recording the channel situation until the node finds the channel is busy for a definite time interval.

Assume t_i be the slot length which has t_n time slots and ratio ψ is expressed as shown in equation (6):

$$\psi = \frac{\sum_{i=1}^{t_n} \varepsilon_i t_i}{\sum_{i=1}^{t_n} t_i} \quad (6)$$

where ε_i is channel status indicator function given as shown in equation (7):

$$\varepsilon_i = \begin{cases} 1, if\ t_i\ slot\ is\ busy \\ 0, if\ t_i\ slot\ is\ idle \end{cases} \quad (7)$$

Accurate channel estimation of ε_i can be obtained by considering the external interference and transmission collisions. Let T_n be the number of transmissions of a node in a given time interval and T_s are successfully transmitted. The channel collision probability ε_c and channel error probability ε_e can be estimated if the node does not transmit in T_r slot and T_s be the successful transmission and I be the channel idle. The channel collision probability is given as shown in equation (8):

$$\varepsilon_c = \frac{T_r - I}{T_r} \quad (8)$$

Channel error probability is given as shown in equation (9):

$$\varepsilon_e = 1 - \frac{1-(T_n - T_s)/T_n}{1-\varepsilon_c} \quad (9)$$

The updated channel busyness ratio with the collision and error probability is expressed as shown in equation (10):

$$\psi' = \frac{\varepsilon_c}{\varepsilon_c + \varepsilon_e} \frac{\sum_{i=1}^{t_n} \varepsilon_i t_i}{\sum_{i=1}^{t_n} t_i} \quad (10)$$

3.4. Light Weighted Trust Model

Direct Trust Value:

Direct trust value of node will be calculated through monitoring the behaviour of adjacent or neighbour node through the status update of received and sent packets of neighbour nodes.

The direct trust value of node x_i estimating its adjacent neighbour node x_j is calculates as shown in equation (11):

$$DT_{i,j} = \omega * PT_{i,j} + (1 - \omega) * NT_{i,j} \quad (11)$$

Where, $PT_{i,j}$ was the past trust value of node x_i has calculated node x_j in the previous history. $NT_{i,j}$ denotes trust value of node x_j calculated by node x_i in the current round and convinces $NT_{i,j} = r_j + s_j$. ω and $1 - \omega$ are weight of the trust value measurement of past and present trust values, $0 < \omega < 1$ and the measuring factors of ω are set to 0.5.

The penalty mechanism ratio of total number of data sent as well as received by node x_j is denoted as r_j and s_j which are expressed as shown in equation (12) and (13):

$$r_j = \frac{\varphi * R_j - RJ_j}{M_j} \quad (12)$$

RESEARCH ARTICLE

$$s_j = \frac{\varphi * S_j - NJ_j}{M_j} \quad (13)$$

Where, R_j and S_j are the packet accepted and forwarded by node x_j , RJ_j and NJ_j represents the data packet that node x_j denies to receive and sent. M_j is the sum of message packets accepted and forwarded by node x_j . For enhancing the decline of trust value of misbehaving nodes, the adaptive penalty factor φ is used and it is expressed as shown in equation (14):

$$\varphi = \frac{-z}{1+e^{-f*(AN_j+k)}} + 1 \quad (14)$$

$$AN_j = \frac{MB_j}{NB_j} \quad (15)$$

Where AN_j is the ratio of malicious behaviour MB_j to the normal behaviour NB_j during previous 5 trust evaluation cycles of trust, which is calculated shown in equation (15). The changeable parameters of φ are given as z, f and k respectively. Whenever, malicious activity of node x_j is detected, MB_j increases sharply resulting decrease of AN_j ratio. Malicious nodes trust value begins to fall, whenever there is an action of AN_j and φ starts decreasing.

3.5. Cluster Member to Cluster Member Trust Evaluation

The neighbours of CM use direct trust evaluation by observing total of successful communication as well as unsuccessful communications which is given as shown in equation (16):

$$DT_{i,j}(\Delta t) = \left(\frac{x_{i,j}(\Delta t)}{x_{i,j}(\Delta t)+v_{i,j}(\Delta t)}\right)\left(\frac{1}{\sqrt{v_{i,j}(\Delta t)}}\right) \quad (16)$$

Where $DT_{i,j}(\Delta t)$ is the direct trust between node x_i and x_j in CM with time window Δt which is varied according to network scenarios. $x_{i,j}(\Delta t)$ and $v_{i,j}(\Delta t)$ are the total number of successful and unsuccessful interactions between two nodes in CM x_i and x_j at time Δt.

If there exists $k-1$ CM's in cluster, whenever there is a request from the CH to CM, the CH accepts the trust value from a particular CM and stores the CM trust value in a data matrix U which is represented as shown in equation (17):

$$U = \begin{pmatrix} DT_{1,1} & DT_{1,2} \cdots & DT_{1,k-1} \\ DT_{2,1} & DT_{2,2} \ldots & DT_{2,k-1} \\ DT_{k-1,1} & DT_{k-1,2} & DT_{k-1,k-1} \end{pmatrix} \quad (17)$$

In the above matrix U, if $i = j$ the actual indirect trust from CH to CM is calculated making use of beta probability density function which is computed as shown in equation (18):

$$IDT_{CH,j}(\Delta t) = Q(\varepsilon(b|c,g)) \quad (18)$$

Where $IDT_{CH,j}$ is the indirect trust between the CH and CM j. For the events of (c,g) in which c is positive feedback $DT_{i,j} \geq 0.5$ and g denotes negative feedback$DT_{i,j} \leq 0.5$, b is the probability of these events. Statistical expectation of $Q(\varepsilon(b|c,g))$ is computed as shown in equation (19):

$$Q\big(\varepsilon(b|c,g)\big) = \frac{c+1}{c+g+2} \quad (19)$$

3.6. Evaluation of Inter Cluster Trust CH to CH

During inter-cluster routing, the CH plays an vital role in transmitting aggegated data towards BS using multiple CH's through single or multihop transmissions. Likewise the trust calculation among CM, CH also evaluates direct trust value to observe trustworthiness of its neighbouring CH using successful and unsuccessful interactions. The CH-to-CH trust value is calculated as shown in equation (20):

$$DT(CH)_{i,j}(\Delta t) = \left(\frac{x(CH)_{i,j}(\Delta t)}{x(CH)_{i,j}(\Delta t)+v(CH)_{i,j}(\Delta t)}\right)\left(\frac{1}{\sqrt{v(CH)_{i,j}(\Delta t)}}\right) \quad (20)$$

Where $DT(CH)_{i,j}(\Delta t)$ is the direct trust between $x(CH)_i$ and $x(CH)_j$ in with time window Δt . $x(CH)_{i,j}(\Delta t)$ and $v(CH)_{i,j}(\Delta t)$ which represents the overall total number of successful as well as unsuccessful interactions in between two CH's.

3.7. BS to CH Trust Evaluation

At regular time interval, the Base station communicates the request packet across the network. CH's upon receiving BS request packet will reply trust value update with other CH to BS. The trust values of the requested CH's are stored in the matrix U_{CH} maintained by BS which is represented as shown in equation (21):

$$U_{CH} = \begin{pmatrix} CHT_{1,1} & CHT_{1,2} \cdots & CHT_{1,n} \\ CHT_{2,1} & CHT_{2,2} \ldots & CHT_{2,n} \\ CHT_{n,1} & CHT_{n,2} & CHT_{n,n} \end{pmatrix} \quad (21)$$

Indirect trust between BS- CH is computed as shown in equation (22):

$$IDT_{BS,j}(\Delta t) = \left(\frac{Q\big(\varepsilon(b|t,u)\big)CT_{k,j}(\Delta t)'}{2}\right) \quad (22)$$

where, $IDT_{BS,j}(\Delta t)$ is the indirect trust feedback between BS and CH at time Δt. t and u are the positive and negative response and $CT_{k,j}(\Delta t)'$ is the mean feedback from $t+u$ CH's which is expressed as shown in equation (23):

$$CT_{k,j}(\Delta t)' = \frac{\sum_{k=1}^{t+u} CT_{k,j}(\Delta t)'}{t+u} \quad (23)$$

3.8. Optimal CH Selection and Cluster Formation

The threshold value $T_v(n_i)$ and random function is evaluated to determine CH in LEACH. Initially nodes generate random

RESEARCH ARTICLE

number$R$ $(0 \leq R < 1)$. If $R \leq T_v(n_i)$ then node is chosen as CH for current round, where $T_v(n_i)$ is calculated as shown in equation (24):

$$T_v(n_i) = \begin{cases} \frac{CH_{total}}{1-CH_{total}*(r_{curr}*mod(1/CH_{total}))} * ((1-\beta)*DT(CH)_{i,j}(\Delta t), \\ \beta * E_T \quad n \in w \\ 0, \qquad\qquad n \notin w \end{cases} \quad (24)$$

Where CH_{total} is the total number of CHs from nodes n_i being elected as CH in 0^{th} round. The current round is represented as r_{curr}, w denotes group of sensor nodes which were not selected as Cluster Head recently. $1/CH_{total}$ round and modulus operator. To adapt dynamic network conditions, the weighting factor β is integrated to minimize network resource and expressed as shown in equation (25):

$$\beta = \begin{cases} G & if\ r \leq r_1 \\ \frac{1-\sqrt{1+0.75*(\partial(ER)-2)^2}}{\partial(ER)-2} & else\ r > r_1 \end{cases} \quad (25)$$

Following Cluster Head selection, Cluster Head communicates via broadcasting cluster head advertisement message CH-ADV including Cluster Head ID, location using carrier sense multiple access (CSMA). The CM within the transmission range of CH, receives the CH-ADV message and determines its CH and replies with join request message (JOIN-REQ) and forms cluster. During data transmission, the trusted CH's are chosen and information will be transferred to BS making use of multihop Cluster Head's transmissions.

However, conventional trust aware model schemes suffer some drawbacks such as trust value calculation whenever node is revoked, not being fast enough to compute trust value to identify malicious node due to complex operations, more information resulting congestion and not being to defend against multiple attacks and not considering multi attributes such as energy balance, optimal CH selection and channel condition to avoid data collision. The procedure for CH selection, procedure for cluster formation, procedure for trust value computation, secure data transmission is depicted in algorithm 1.

Data transmission occurs between the cluster head (CH) and base station (BS) following cluster formation. Communication takes place between inter-cluster and intra-cluster communication. While CM transmits gathered data to its cluster head (CH) in intra-cluster communication, CH transmits data to the subsequent CH in inter-cluster communication. To prevent sending redundant data to BS, CH uses a data aggregation approach to combine data and then uses single hop or multihop routing to transfer the aggregated data to BS. During transmission, the CH senses the channel busyness ratio parameter channel busy ratio ψ to know the status of the channel to avoid data collision. The channel busy ratio ψ for recording the channel situation until the node finds the channel is busy for a definite time interval from equation (6) and channel status indicator from equation (7). LRTARS updates the ratio of malicious behaviour MB_j to the normal behaviour NB_j from equation (15). During intra communication the neighbours of CM uses direct trust evaluation by observing total of successful communication as well as unsuccessful communications by computing equation (16) and cluster member to cluster head trust is calculated making use of beta probability density function from equation (18). Likewise the trust calculation among CM, CH also evaluates direct trust value to observe trustworthiness of its neighbouring CH using successful and unsuccessful interactions. The CH-to-CH trust value is calculated as shown in equation (20). During inter cluster communication the CH to CH, LRTARS selected trusted CH such that the data is reliably transferred between CH's. Finally, during CH to BS communication, CH's upon receiving BS request packet will reply trust value update with other CH to BS and Indirect trust between BS- CH is computed from equation (22), the positive and negative response and mean feedback is computed from equation (23) and the data is transmitted to BS.

Step 1: Network initialisation

Deploy n_i nodes in network area of (X, Y)

Step 2: Procedure CH selection,

Generate random number

for R $(0 \leq R < 1)$

Compute $T_v(n_i)$ from equation (24)

if $R \leq T_v(n_i)$

Step 3: Select node as CH

end if

Step 4: Compute $DT_{i,j}$ from equation (11)

Set ω to 0.5. then

Declare node as trusted CH

end procedure

end

Step 5: Procedure cluster formation

Broadcast CH-ADV

CM determines its CH

Replies JOIN-REQ

Forms cluster

end procedure

end

RESEARCH ARTICLE

Step 6: procedure trust value computation

CM to CM trust

Compute $DT_{i,j}(\Delta t)$ direct trust from equation (16)

Compute $IDT_{CH,j}(\Delta t)$ from equation (18)

for events of (c, g)

if positive feedback for c= $DT_{i,j} \geq 0.5$

Normal behaviour

if negative feedback g= $DT_{i,j} \leq 0.5$

Malicious behaviour detected

Compute $Q\big(\varepsilon(b|c,g)\big)$ from equation (19)

end if

end procedure

end

Step 6: while data transmission

Compute CH to CH trust value

Evaluate $DT(CH)_{i,j}(\Delta t)$ from equation (20)

Compute $IDT_{BS,j}(\Delta t)$ from equation (22)

Compute $CT_{k,j}(\Delta t)'$ feedback from equation (23)

Compute AN_j to speed up malicious detection from equation (15)

Step 7: Check for channel status ψ from equation (6)

Step 8: Check for channel busy ratio ψ' to avoid collision from equation (10)

Step 9: Select free and secure channel for data transmission

end while

end procedure

end

Algorithm 1 Secure Trust Based Routing

4. SIMULATION RESULTS AND PERFORMANCE

4.1. Simulation Environment

Simulation experiments of proposed LRTARS are conducted on discrete network simulation tool (NS2). A network made of 100 nodes placed randomly in a sensing area of 200 X 200 mts. BS is placed top and far from the network area.

Attack such as blackhole, on-and-off attack and selective forwarding attacks are induced into the network and nodes behaviour is analysed. Experimental results of LRTARS are compared with TAGA [19] and TIOCHR [24]. The complete experimental specifications are as mentioned in Table 2.

Table 2 Specifications of Simulation

Specifications	Value
Node Size	100
MAC	802.11
Run time of Simulation	100 sec
Area of Deployment	600 X 600 mts
Packet size	512 bytes
Comparing scheme	TAGA and TIOCHR
Traffic	CBR
Base Station	1
No of Malicious nodes	25
Initial trust value	0.5

4.2. Packet Loss

Packet loss is the loss of data packets travelling across the network from source but fails to arrive at destination, packet loss is the difference of sent packet minus received packets. Packet loss is calculated as shown in equation (26):

$$Packet\ loss = Sent\ packet - Received\ Packets \quad (26)$$

4.2.1. Packet Loss Under Black Hole Attacks

The Figure 3 illustrates the percentage of packets rejected by the mischievous nodes. As shown in the graph, when the number of mischievous nodes increases across the network, the packet drop in the network gradually increases. The misbehaving node tries to mimic as authentic node and tricks the normal nodes to establish connection with it during route establishment.

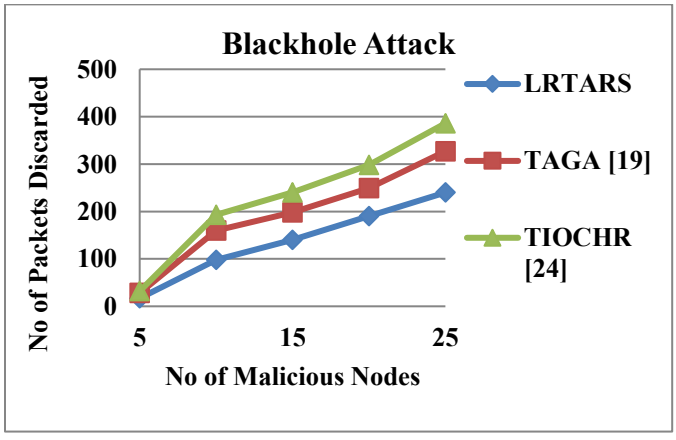

Figure 3 Packet Loss Under Black Hole Attacks

RESEARCH ARTICLE

When normal node makes a contact with misbehaving node, the normal node gets compromised to attacker node resulting in packets to be forwarded being intentionally dropped. Therefore, according to equation 11 computes the trust value based on the packet sent and received. Penalty Mechanism Ratio of total number of packets sent & received is also been evaluated. Whenever there is a packet drop in the network, the trust value will decrease rapidly. Whenever, malicious activity is detected in LRTARS, MB_j increases sharply resulting decrease of AN_j ratio. Trust Value of mischievous sensor nodes begins to fall, whenever there is an action of AN_j and φ starts decreasing when trust value of the misbehaving sensor nodes drop under the inception trust value and speeds up the identification of malicious nodes compared to TAGA and TIOCHR. Blackhole nodes in TAGA are identified by constructing the comprehensive trust value through adaptive penalty and volatilization factors which needs to be computed. Whenever the malicious node is detected during the route discovery, TAGA restarts its adaptive penalty factors again from the first node making it difficult to speed up detection which may result in more packet drops. The trust index values in TIOCHR assess the node behaviour due to inconsistency in packet forwarding probability rate by the misbehaving node affecting the network performance. LRTARS reduces packet loss of 26% and 37% compared to TAGA and TIOCHR respectively. The channel busy ratio ψ for capturing the channel status until the node finds channel busy with a certain interval of time helps LRTARS to transmit data through secure channel without any collision or congestion in the network compared to TAGA and TIOCHR

4.2.2. Packet Loss Under On-Off Attacks

The Figure 4 illustrates the number of data packets discarded by malicious sensor node during the launch of on-off attack. It can be seen from the graph; the packet drop increases gradually across the network as number of misbehaving sensor nodes are increased. In case of on-off attack the malicious node performs both good and misbehaving activities, which is a challenging task to evaluate node trustworthiness. In LRTARS, direct trust value decreases rapidly whenever the network experiences packet drops this is due to unsuccessful interactions between two nodes and the use adaptive penalty factor φ speeds up the identification rate and strictly punishes malicious behaviour.

The indirect trust in LRTARS is computed using beta probability density function using equation (18) for different events and the statistical is represented through positive and negative feedback. However, TAGA uses the historical values to represent feedback, direct trust is computed based on the factors of historical and the measuring trust values under specific conditions making trust evaluation cycle long making it a disadvantage of fast detection rate and TIOCHR employs packet consistency metric to determine malicious behaviour under on-off attack. The retransmission is affected due to packet inconsistency occurred due to packet loss. The threshold value in TIOCH is set for CH to find the trustworthy path and does not help in fast detection of malicious node in the discovered path. LRTARS reduces packet loss of 21% and 35% compared to TAGA and TIOCHR respectively.

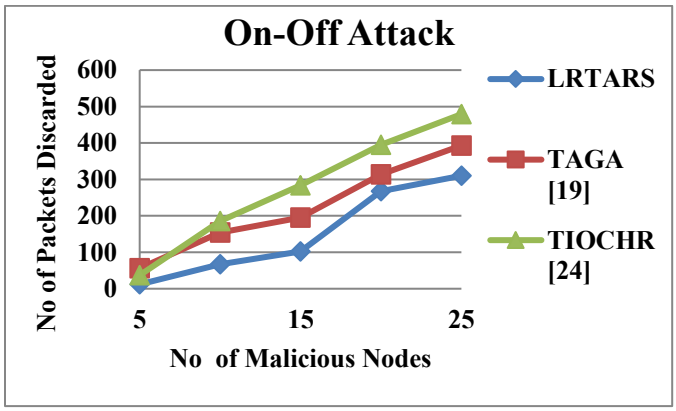

Figure 4 Packet Loss Under On-Off Attacks

4.2.3. Packet Loss Under Selective Forward Attack

Figure 5 illustrates the total number of packets discarded by malicious sensor node during the launch of selective forward attack. Misbehaviour nodes in selective forward attack have the ability to selectively drop sensitive packets instead of forwarding with certain probability. This may be aimed at certain nodes or clusters of nodes. If the misbehaviour nodes discard packet with 100% probability this results in blackhole attack. It is observed from the graph; the packet drop ratio is less in proposed LRTARS compared to TAGA and TIOCHR.

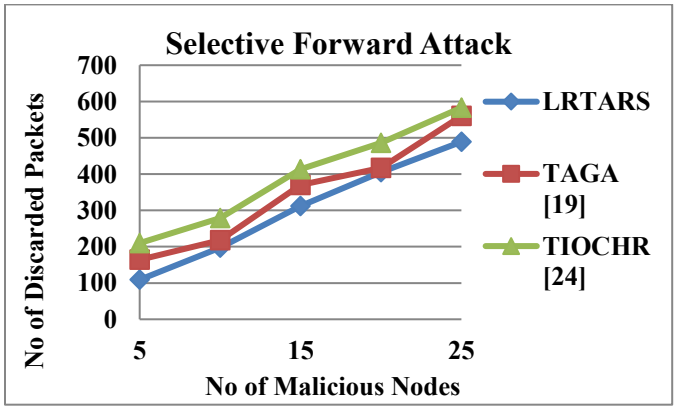

Figure 5 Packet Loss Under Selective Forward Attacks

Trust value of nodes in LARTS are monitored by the behaviour of adjacent or neighbour node through the status update of received and sent packets of neighbour nodes. To speed up decline of trust value of misbehaving nodes, the adaptive penalty factor φ and the AN_j the ratio of malicious

RESEARCH ARTICLE

behaviour MB_j to the normal behaviour NB_j in the previous five trust evaluation cycles is computed to know the drop ratio in LRTARS and trust feedback between BS and CH for the successful and unsuccessful transmission along with the positive and negative response is obtained by computing the mean feedback from $t + u$ CH's from equation 25.

However, the TAGA uses only adaptive factor and comprehensive trust value to obtain drop probability. The genetic algorithm in TAGA aids to find the secure route using adaptive crossover and mutation probability evaluated using penalty and volatilization factors as compared to LARTS that monitors the behaviour of adjacent or neighbour node through the status update of received and sent packets of neighbour nodes and speed up the detection from equ (15).

The packet consistency rate and packet forwarding rate metrics are determined to estimate the drop ratio in TIOCHR ignoring the feedback required for trust value update. LRTARS reduces packet loss of 12% and 16% compared to TAGA and TIOCHR respectively.

4.3. Average End-to End Delay

It is the average time a data packet needs to get across a network from its source to its destination, taking into account various types of delays such buffering, MAC, interface queue, and propagation delays. It is expressed as shown in equation (27):

$$E2Edelay = \sum \frac{Packet\ arrival\ time - packet\ sent\ time}{Total\ no\ of\ packets} \quad (27)$$

Figure 6 illustrates the mean end-to-end delay of the proposed LRTARS equated alongside TAGA as well as TIOCHR through varying number of malicious nodes. From the graph, it is observed, the delay of all the three schemes increases as the number of malicious nodes in the network is increased. Due to malicious activities network experience frequent packet loss resulting in re-transmission of lost packets increasing network delay.

When maximum number of malicious node present in network LRTARS maintains route stability during retransmission of packet through estimating channel conditions to avoid congestion in the network caused by the malicious nodes and other retransmission of packets and also LRTARS considers previous five trust evaluation cycles computation to know the drop ratio and trust feedback between nodes and tries to avoid communication with malicious nodes.

TAGA considers volatilization factor to determine routes, during retransmission TAGA evaporates the historical values leading to high delay. Integration of channel busyness ratio helps to find congestion free channel such that the data is retransmitted with minimum delay in LRTARS. However, the TAGA restarts its retransmission from the beginning through computing crossover and mutation process to find next alternate secure route consuming more delay.

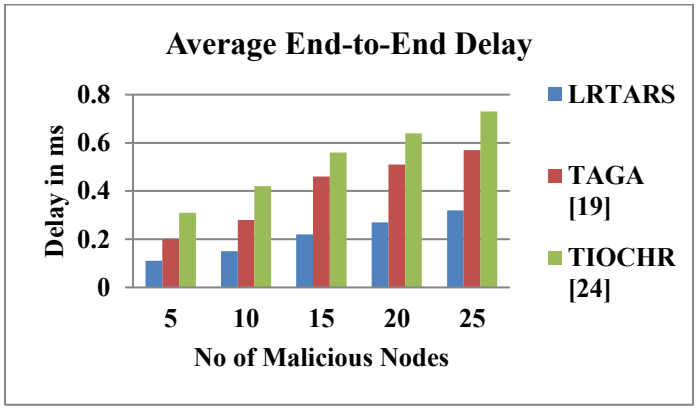

Figure 6 End-to-End Delay vs No of Malicious Nodes

However, TIOCHR considers timestamp during trust evaluation and the table is updated at regular interval. During retransmission the new routes are chosen based on the packet flow rate and packet consistency resulting higher delay. LRTARS reduces delay of 24% and 32% compared to TAGA and TIOCHR respectively.

4.4. Routing Overhead

Routing Overhead is the ratio of total number of routing control packets sent divided by overall number of successful data packets delivered. It is expressed as shown in equation (28):

$$Routing\ Overhead = \frac{Total\ number\ of\ control\ packets\ generated}{Total\ number\ of\ data\ packet\ deliverd} \times 100 \quad (28)$$

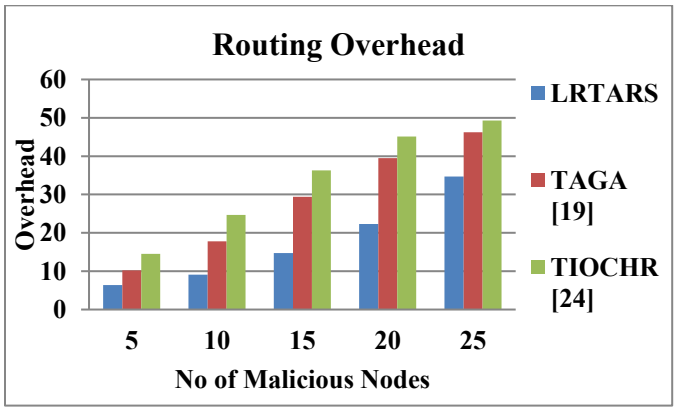

Figure 7 Overhead vs No of Malicious Nodes

Figure 7 illustrates the routing overhead of proposed LRTARS compared with TAGA and TIOCHR through varying number of malicious nodes. Routes towards BS in LRTARS are determined through inter cluster transmissions. The changeable parameters of φ in LRTARS monitors the

RESEARCH ARTICLE

behaviour of malicious and if any malicious activity is detected, MB_j increases sharply resulting decrease of AN_j ratio. The malicious nodes trust value begins decreasing, whenever there is an action of AN_j and φ starts decreasing and accurate channel estimation of ε_i from equation (7) can be obtained by considering the external interference and transmission collisions such that the routing overhead is minimised.

The optimal cluster head selection through improved LEACH chooses secure and efficient CH's during multihop transmissions. However, TAGA the routes are determined using fitness function and after completion of each round the re-clustering is done to determine CH and fitness function is computed through crossover and mutation to discover new secure routes which results in higher routing overhead. During inter cluster communication the CH are chosen based on the trust index value with different time stamp at regular intervals and each time the CH is rotated based on the best trust index in TIOCHR. Therefore, while routing and re-routing TIOCHR experiences higher computation overhead. Whereas, LRTARS updates routes based on successful transmission with lower transmission collisions resulting reduced routing overhead of 24% and 29% compared to TAGA and TIOCHR respectively

4.5. Energy Consumption

Energy Consumption is the quantity of energy absorbed during experiment for the transmission and receiving of packets. The residual energy of node is computed as shown in equation (29):

$$Residual\ Energy = \sum initial\ energy - consumed\ energy \quad (29)$$

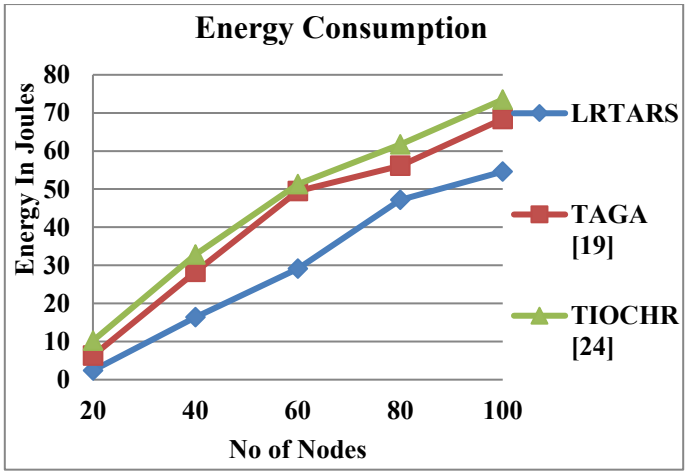

Figure 8 Energy vs No. of Malicious Nodes

The energy consumption of LRTARS, TAGA and TIOCHR under the same simulation settings is plotted against the number of nodes in Figure 8. It is believed that nodes are randomly placed and that each sensor node regularly broadcasts a HELLO message to obtain information about its neighbors, which results in energy dissipation. The improved threshold value $T_v(n_i)$ helps to select energy efficient CH and also the best path to BS via single or multihop communication for message transfer. To adapt dynamic network conditions, the weighting factor β is integrated to minimize network resource in LRTARS.TAGA adopts basic LEACH framework during CH selection based on residual threshold energy value, during inter cluster communication TAGA consumes more energy and does not balance energy among nodes and also energy is consumed more during retransmission and also during route discovery process using comprehensive trust value for each hop. While in TIOCHR the CH selection and routes are estimated through training session among CH and cluster members. The energy efficiency gain depends of cluster member competency. TIOCHR does not employ any LEACH and CH is chosen based on trust value and minimum hops. However, LRTARS adopts improved LEACH to balance nodes energy and gives the chance to every node become CH in different rounds thus extending network lifetime compared to TAGA and TIOCHR.

5. CONCLUSION AND FUTURE ENHANCEMENT

Ensuring secure routing for WSNs with limited resources is crucial. WSNs are susceptible to different kinds of threats due to their deployment in hostile environments. For large-scale WSN applications, hierarchical routing schemes simplify the network topology and improve transmission efficiency. As a part of this paper, we put forward light weighted reputation-based trust aware routing scheme (LRTARS) to defend against malicious activities during routing, especially internal attacks. LRTARS is designed through trust model evaluating direct and indirect trust values. Channel busy ratio is estimated at MAC for congestion free and secure data transmission through channel during retransmissions to avoid communication congestion. Optimal cluster head (CH) are chosen through modifying LEACH considering energy and trust parameters to improve network lifetime. Various attacks like blackhole, on-and-off attack and selective forwarding attacks are analysed and experimental results of LRTARS are compared with TAGA and TIOCHR. Simulation results show that proposed LRTARS has reduced packet drop compared to other two schemes and performs better to defend against malicious nodes. In future, energy and trust aware routing scheme can be modelled considering energy parameters to extend network lifetime since nodes suffer from energy usage restrictions.

REFERENCES

[1] I.F. Akyildiz, Su WY, Sankarasubramaniam, E.Cayirci, "Wireless sensor networks: a survey", Computer Network. J. Volume 38, Issue 4, 15 March 2002, Pages 393–422.

RESEARCH ARTICLE

[2] Zhu Yong, Qing Pei, A energy efficient clustering routing Algorithm Based on Distance and Residual Energy for Wireless Sensor Networks", Procedia Engineering Volume 29,2012, Pages 1882-1888.
[3] Amit Sarkar, T.Senthil Murugan,:"Routing Protocols for wireless sensor networks: What the literature survey says?",Alexandria Engineering Journal, Volume 55, Issue 4, December 2016, Pages 3173-3183.
[4] Asif Ali Laghari, Kaishan Wu,Rashid Ali Laghari,Mureed Ali,Dr.Abdullah Ali Khan, "A review and state of art of Internet of Things (IoT).", Archives of Computational Methods in Engineering, Volume 29,14 July 2021, Pages 1395–1413.
[5] Shayma Wail Nourildean, Mustafa Dh. Hassib, Yousra Abd Mohammed, "Internet of things based wireless sensor network: A review". Indonesian journal of Electrical Engineering and Computer Science, Volume 27, July 2022, Pages 246–261.
[6] Kamal Gulati: Boddu, Raja Sarath Kumar; Dhiraj Kapila.;Sunil L Bangare,;Neeraj Chandnani, Saravanan, G. "A review paper on wireless sensor network techniques in Internet of Things (IoT)". Materials Today Proceedings. Volume 51, Part 1, 2022, Pages 161–165.
[7] M. Almazaideh and J. Levendovszky, "Novel reliable and energy-efficient routing protocols for wireless sensor networks," Journal of Sensor and Actuator Networks, Volume 9, Issue 1, 2020, Pages 1-13.
[8] Osmah Ibrahim Khalaf and Ghaida Muttashar Abdulsahib, "Energy efficient routing and reliable data transmission protocol in WSN," International Journal of Advance Soft Computing and Its Applications, Volume 12, No. 3, November 2020, Pages 45–53.
[9] L. Chan, K. Gomez Chavez, H. Rudolph, and A. Hourani, "Hierarchical routing protocols for wireless sensor network: a compressive survey," Wireless Networks, Volume 26, No.5, Pages 3291–3314, 2020.
[10] Ikram Daanoune, Boghdad Abdennaceur, and Abdelhakim. Ballouk, "A comprehensive survey on LEACH-based clustering routing protocols in wireless sensor networks," Ad Hoc Networks, Volume 114, Article 102409, 2021.
[11] Shio Kumar Singh, M P Singh and D K Singh "Routing Protocols in Wireless Sensor Networks-A Survey", International Journal of Computer Science and Engineering Survey (IJCSES), Volume 1, No.2, November 2010, Pages 63-83.
[12] Aliyu Musa Bade, Adamu abdullahi Garba "A Review on Security Issues in Wireless Sensor Networks". International Journal of Recent Academic Research, August 2019, Volume 1, Issue 5, Pages 159-164.
[13] Kahina Chelli, (2015). "Security issues in wireless sensor networks: Attacks and countermeasures." in Proceedings of the World Congress on Engineering, 2015, Volume 1(20), 876-3423.
[14] Thangaramya Kalidoss, Logambigai Rajasekaran, Kulothugan Kanagasabai, Ganapathy Sannasi, and Arputharaj Kannan, "QoS aware trust based routing algorithm for wireless sensor networks". Wireless Personal Communications, 2020, Volume 110(3), Pages 1637-1658.
[15] Nor Azimah Khalid, Quan Bai,and Al-Anbuky,(2019)," Adaptive trust-based routing protocol for large scale WSNs." IEEE Access, Volume 7, Pages 143539-143549.
[16] Venkatesh Prasad B.S, H.R. Roopashree, "Energy aware and secure routing for hierarchical cluster through trust evaluation" Measurement: Sensors, June 2024, Volume 33, 101132, Pages 1-8, https://doi.org/10.1016/j.measen.2024.101132.
[17] M. Selvi, K. Thangaramya, S. Ganapathy, K. Kulothungan, H. K. Nehemiah, and A. Kannan, "An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks," Wireless Personal. Communications. Volume 105, Pages 1475_1490, February 2019.
[18] M. Mathapati, T. S. Kumaran, A. Muruganandham, and M. Mathivanan,"Secure routing scheme with multi-dimensional trust evaluation for wireless sensor network," Journal of. Ambient Intelligence Humanized Computing., June 2020, Volume 12, Pages 6047-6055, doi: 10.1007/s12652-020-02169-7.
[19] Yougia Han, Huangshui Hu and Yuxin Guo, "Energy-Aware and Trust-Based Secure Routing Protocol for Wireless Sensor Networks Using Adaptive Genetic Algorithm," in IEEE Access, 2022, Volume10, Pages11538-11550, doi: 10.1109/ACCESS.2022.3144015.
[20] Guiping Zheng; Bei Gong; Yu Zhang, "Dynamic Network Security Mechanism Based on Trust Management in Wireless Sensor Networks". Wireless Communications and Mobile Computing. 2021, Volume 2021, Issue 1, Pages 1-10.
[21] Maryam Hajiee, Mehdi Fartash, and Naiseh Osati Eraghi, ``An energy-aware trust and opportunity based routing algorithm in wireless sensor networks using multipath routes technique," Neural Processing Letters., Volume. 53, Issue No. 4, Pages 2829-2852, August. 2021. https://doi.org/10.1007/s11063-021-10525-7.
[22] Asad Ullah Khan, Maimoona Bint E. Sajid, Abdul Rauf, Malik Najmus Saqib, Fawad Zaman, Nadeem Javaid, "Exploiting Block chain and RMCV-Based Malicious Node Detection in ETD-LEACH for Wireless Sensor Networks", Wireless Communications and Mobile Computing, Volume 2022, Issue 1, 15 pages, 2022.
[23] Das, R.; Dash, D.; Sarkar, M.K. "HTMS: Fuzzy Based Hierarchical Trust Management Scheme in WSN"; Wireless Personal Communications, Springer: New York, NY, USA, January 2020; Volume 112, Pages 1079-1112.
[24] S. Suresh Babu, N. Geethanjali, "Lifetime improvement of wireless sensor networks by employing Trust Index Optimized Cluster Head Routing (TIOCHR), Measurement: Sensors, Volume 32, 2024, 101068.
[25] H. Hu, Y. Han, M. Yao and X. Song, "Trust Based Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks," in IEEE Access, Volume 10, Pages 10585-10596, 2022, doi: 10.1109/ACCESS.2021.3075959.
[26] W. Fang, W. Zhang, W. Chen, J. Liu, Y. Ni, and Y. Yang, "MSCR: Multidimensional secure clustered routing scheme in hierarchical wireless sensor networks," EURASIP Journal on Wireless Communications and Networking, Volume. 2021, Article number 14, Pages 1-20, January 2021.
[27] Aravindan, S. & Rajaram, A. "Energy-aware multi-attribute trust model for secure MANET-IoT environment." Multimedia Tools and Applications". Volume 83, Pages 85637-85662, August 2024, https://doi.org/10.1007/s11042-024-20075-4.
[28] A. B. Feroz Khan "An Enhanced Multi Attribute Based Trusted Attack Resistance (EMBTR) for the Secure Routing of Sensor Nodes in Wireless Sensor Network". Wireless. Personal Communications, Volume 137, Issue 4, Pages 2397-2407, August 2024.
[29] Dinesh, K. & Kumar Svn, Santhosh "Energy-efficient trust-aware secured neuro-fuzzy clustering with sparrow search optimization in wireless sensor network". International Journal of Information Security. Volume 23, Pages 199-223, 2023.
[30] Selvi, M., Santhosh Kumar, S.V.N., Thangaramya, K. et al. "Energy efficient trust aware secure routing algorithm with attribute based encryption for wireless sensor networks." Scientific reports 15, Article number 19724 (2025). June 2025, https://doi.org/10.1038/s41598-025-03558-8.

Authors

N. Shantha Kumar is a Research Scholar in Department of Computer Science and Engineering, K R Pet Krishna Government Engineering College, K.R.Pet, Mandya - 571401, Karnataka, India. N.Shantha kumar obtained his Bachelor of Engineering in Computer Science and engineering from PESIT, Bangalore, Karnataka, India and Master of Technology in Computer Science and Engineering from SJBIT, Bangalore, Karnataka, India. N.Shantha kumar have nearly 16 years teaching experience across various Engineering Colleges and Universities. His region of intrigue incorporates Computer systems, Sensor Networks Data Communications, Web Technologies, Research techniques, Data science;

RESEARCH ARTICLE

Database the board frameworks, Software Engineering, Information Security, Entrepreneurship and the board. His flow research work remembers Security for Wireless Sensor Networks. He has published numerous papers in various journals.

Dr. Hareesh. K is Professor in the Department of Computer Science and Engineering, K R Pet Krishna Government Engineering College, K.R.Pet, Mandya - 571401, Karnataka, India. Dr. Hareesh. K got his PhD degree from Jawaharlal Nehru Technological University, Anantapur, Andhra Pradesh, India. Master of Technology in Computer Science and Engineering from Visvesvaraya Technological University, Belgaum, Karnataka, India and Bachelor of Engineering in Computer Science and Engineering from Bangalore University, Bangalore, Karnataka, India. He has more than 20 years wide scholarly, Industrial as well as Research Experience. He has published more than 20 papers in various national and international journals. His area of research is centered around Network execution and examination, Advanced Computer Networking, Mobile / Wireless Communication, Wireless Sensor Networks, Network Security, Interactive media applications, P2P Networks and Web Technologies.

How to cite this article:

N. Shantha Kumar, Hareesh. K, "Secure Routing Through Trust Evaluation for Aggregator Node in Hierarchical Wireless Sensor Networks (WSN)", International Journal of Computer Networks and Applications (IJCNA), 12(6), PP: 1005-1018, 2025, DOI: 10.22247/ijcna/2025/59.