International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Intelligent Secure and Malicious-Free Route Management Strategy for IoT-based Wireless Sensor Networks

[1]Mohammad Sirajuddin, [2]Dr. B. Sateesh Kumar

Submitted:23/03/2023 **Revised:**26/05/2023 **Accepted:**10/06/2023

Abstract: Advancements in smart-network technologies enabled the Internet of Things to expand globally. IoT-based Wireless sensor networks play an essential role in collecting and aggregating data in applications like military and health care, where security and power efficiency are significant challenges. Due to vulnerable attacks on several nodes or devices, IoT-based WSN becomes an uncertain environment. This paper aims to offer a fault tolerant, robust, and secure packet forwarding scheme that incorporates more intelligent features and powerful algorithms to eliminate DoS attacks. Initially, routing is performed, with the optimal path determined by recovering malicious nodes detected in an IOT-based WSN environment using the proposed algorithm ICARS- Intelligent Channel aware Reputation scheme based on generation of Resolver Node and Intelligent Route Request and Route Response methods. Next to that, encryption is used to ensure safe transmission. This paper proposes a Modified Rijndael Algorithm (MRA) for secured authentication. By integrating ICARS with MRA, this proposed strategy removes the attacking situation and makes the system more resistant to DoS attacks. The result section proved that the proposed approach increases the throughput, decreases the retransmission ratio, increases energy efficiency, decreases end-to-end delay, and increases Packet Delivery Ratio.

Keywords: *ICARS; IoT Security; Secure routing; MRA; Wireless sensor networks*

1. Introduction

IoT is a technique that enables connectivity between devices through the Internet. As information and communication technology has progressed, the usage of IoT equipment has increased enormously. Using sensors, environmental information in which they are deployed can be collected. WSNs are built up with cheap, small equipment that gathers data and has the limitation of computational, processing, memory, and energy resources, and they play a vital function in developing IoT [1]. However, WSN's significant problems are reliability and data security in an environment prone to malicious attacks with these restrictions [2].

The primary source of information security issues in IoT-based WSNs is security attacks. Generally, these security threats on WSNs are classified as internal and external attacks. The compromised node initiates the internal attacks and performs forging, discarding, replaying, and tampering. The latter include eavesdropping, jamming, and decoding attacks. External attacks may be prevented by using encryption, authentication, and other established security precautions, but these security mechanisms can't protect from internal attacks.

Data transmission has been protected using secure routing protocols and encryption schemes. In the case of a malicious node in the network, routing protocols create delays, increase the number of retransmissions, and require the reconstruction of the same routing mechanism repeatedly. These malicious nodes may impact the system's general functionality and purpose. By using trust-score-dependent protocols, the problem of malicious nodes obtaining data and compromising the entire WSN can be addressed more effectively. These approaches only include reliable and trusted nodes in the routing process. [2]. High-complexity security approaches are challenging to implement on resource-constrained sensor nodes. So in WSNs, the primary focus is on ensuring the safe transfer of sensed data using lightweight encryption or authentication mechanisms [1]. However, since sensor nodes are deployed unsupervised, there are no effective strategies to protect nodes from being captured and compromised. As a result, internal attacks initiated by compromised nodes are unavoidable. So there is a need for an efficient, secure routing scheme that offers node-level security to deal with compromised nodes and a cryptographic scheme.

The following Figure 1 depicts how IoT-based WSNs are organized in open areas and are highly vulnerable to security threats due to their lack of infrastructure and

[1]*Research Scholar, Department of Computer Science & Engineering JNTU, Hyderabad, Telangana, India*
mohdsiraj569@gmail.com.
ORCID ID: 0000-0003-1180-3813
[2]*Professor, Department of Computer Science & Engineering JNTUH-College of Engineering, Jagitial, Telangana, India.*
sateeshbkumar@jntuh.ac.in

limited resources. As resources become scarce, the risk of devastating security attacks has increased. WSNs have become insecure environments due to attacks on several nodes. Denial-of-Service attacks like Worm-hole, Black-hole, and Sybil attacks cause network traffic to be disrupted, resulting in packet modification and Routing disruption. Data packet duplication and bandwidth reduction, Nodes deteriorate, making it easier to obtain data from them. Removing these black hole nodes from the network increases Packet Delivery Ratio (PDR), improves energy efficiency, decreases retransmission ratio, increases throughput, and decreases delay. Secure routing is a term that relates to routing that resists unintended packet drops, alterations, and path disruptions [3]. The utilization of a proposed method for identifying and recovering malicious nodes, along with the integration of cryptographic techniques into routing algorithms, can greatly enhance the routing methodology's capabilities and provide protection against various types of attacks, such as black hole attacks, DoS attacks like jamming, sinkhole, wormhole, selective forwarding attacks, floods, and more. This secure routing methodology can ensure the network's reliability and safeguard against potential disruptions caused by malicious nodes. So there is a need for new secure and efficient networking and route management solutions to eliminate black hole attacks.

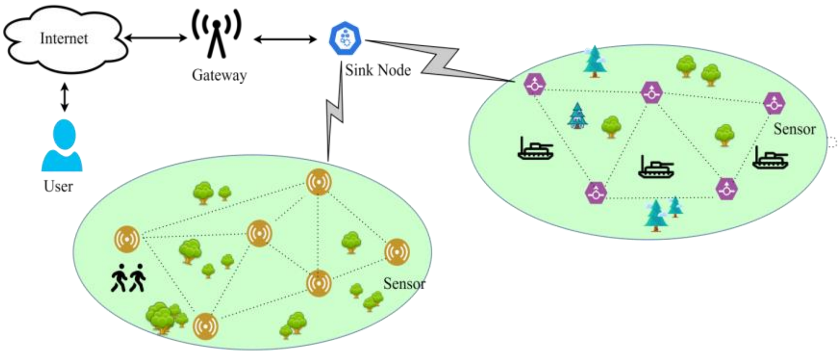

Fig 1. IoT based Wireless Sensor Networking Architecture.

The following are the primary objectives of this work.

- The main objective of this system is to provide a reliable, secure, and failure-free wireless communication method over a WSN with a large number of nodes.
- To identify and recover the malicious nodes from network scenarios by using the trust metrics of the node.
- To provide enhanced security while data is being transmitted from sender to receiver, using a lightweight cryptographic procedure known as the Modified Rijndael Algorithm (MRA).
- To compute a secure wireless communication [2] route using intelligent data forwarding approaches such as RREQ and RREP.

The article is organized as follows: Section II gives the literature review. Section III illustrates the methodology used to develop the Secure Routing framework in WSN. Section IV depicts an intelligent channel-aware reputation scheme for optimal path selection. Section V depicts secure transmission using a cryptographic scheme called Modified Rijndael Algorithm. Finally, sections VI and VII describe the results and conclusions.

2. Literature Review

Numerous studies have addressed the many types of security attacks in IoT-based WSN. A multi-hop-based Uniform Routing Mechanism using Fuzzy Logic on WSNs proposed in [4] uses an evaluation technique with more than one hop transmission to balance loads, reduce the energy required, and extend the network's life. The protocol selects the cluster leader using fuzzy logic and a competition radius to form uneven clusters (CH). All input variables are the distance between the nodes, base station, and remaining power. The simulation and results section indicates the higher performance of the suggested protocol.

Blackhole attacks were implemented on the AODV protocol in [5]. This paper uses three approaches: normal AODV, AODV with the black holes, and AODV with the detected black holes. Blackhole attacks are prevented by using IDS and digital signatures. In comparison to the standard AODV protocol, simulation findings reveal that the BH AODV and BH-AODV protocols give improved QoS characteristics.

A Wireless network routing scheme that is reliable, secure, and efficient has been suggested in the paper [6]. This technique employs mesh topology and selects the safe path for transferring packets. In this article, connections between nodes are established depending on the data distribution efficiency of the connections.

A load-balanced and secure path forwarding scheme for clustered-based heterogeneous WSN is discussed in [7]. The proposed strategy is a security measure based on trust that addresses the issue of sensors swinging between good and bad states and vice versa. Additionally, this method balances cluster head loads. As a result, it assists in obtaining higher levels of security and packet transport. Results assess the proposed SLBR model's performance compared to the conventional model. The outcome demonstrates that the SLBR model outperforms the ECSO model regarding energy efficiency.

An ant colony optimization-based secure routing strategy for WSNs that is QoS aware and energy balancing is presented in [8]. The suggested QEBSR approach takes QoS, security, and energy balance into account and determines the network's routing plan using an updated ACO. The simulation results indicate that the suggested QEBSR process is better than the conventional techniques.

A new secure routing [9], which is power-conscious, secure data forwarding technique based on trust for Effective Communication in WSNs, is introduced in to provide WSN with optimum and secure routing Trust scores are utilized in this technique to identify attackers in WSNs better, and routing strategy depends on decision tree is used to pick the best secure path. Additionally, spatial constraints have been applied to improve the effectiveness of routing decisions. Finally, based on simulations, The suggested EATSRA increases performance by decreasing energy usage and boosting PDR and security.

A systematic strategy to avoid intrusions is proposed in [10], utilizing machine learning on structured data. This method includes the following steps: Input, selection of data sets, application of the algorithm to the acquired data, processing of the received data, and finally, a final choice based on the output. The paper [11] proposed an extremely secure and robust WSN packet forwarding method to improve QoS and energy efficiency. It is also used to identify malicious nodes by exploiting dynamic node network properties.

A novel Trust-Distrust Protocol proposed in [12], the first stage of the protocol, employs an improved k-means algorithm for topology management. Then there's the Link Quality Assessment (fitness evaluation). Finally, there is grading. The final stage establishes a safe route.

A technique for identifying intrusions based on energy trust is proposed in [13]. It depends on forecasting and analyzing power usage to determine the nodes' security levels. It makes use of a forecasting algorithm for energy usage.

The MOLSR and AOMDV protocols' features are merged to build a safe hybrid routing protocol based on encryption and authentication in paper [14]. Using the Eligibility Weight Function (EWF), it is demonstrated that the suggested strategy has a higher percentage of monitoring nodes than existing routing systems. Additionally, the suggested routing technique is robust against several mobile adversaries, ensuring multipath delivery.

The article [15] describes a unique routing protocol for multi-agent systems that optimize an ant colony that efficiently controls the network. The pheromones released by each ant along the route may be used to discover an ideal path after some low-cost iteration. The simulation results demonstrate that this protocol significantly improves network performance.

The paper [16] discusses the ideas of energy-efficient charging of sensor nodes of wireless networks. This paper investigated the principles of wireless charging nodes in WSNs by examining the literature and comparing well-known works. [17] presented Offloading recharging work to neighbourhood chargers via a collaborative recharging approach. Compared to global charger-based recharging, it extends the average network lifetime and boosts average charging throughput and latency.

A secure routing protocol controlled by the base station was introduced in [18], and it intends to distinguish malfunctioned nodes from proper nodes, an approach based on trust that protects the network against fraudulent data insertion while also providing an efficient path free of attacks. The efficiency of BSCSRP is determined by comparing it to conventional approaches and determining which ways perform better.

The paper [19] offers a theory-based correlation method for spotting hostile nodes that prevents fault data injection attacks. The first step is to utilize temporal correlation to find anomalies in similar kinds of sensor data. Second, by exploiting geographical correlation, malicious nodes are found. Third, utilizing event correlation, the malicious identified nodes are validated. In terms of recall and false-positive and false-negative rates, the experimental findings and comparisons with current approaches reveal that the proposed method surpasses the standard fuzzy reputation system and normalized strategies.

3. Proposed Work

This section presents a route management scheme for Wireless Sensors Networks that is efficient and secure against security attacks. Conventional route management methods use classical routing protocols such as DSR, AODV, LEACH, and many others; however, most protocols do not prioritize security in routing. Therefore, new secure and efficient networking and route management solutions are necessary to prevent black hole attacks. A robust, secure, and fault-free routing strategy is provided in the proposed system, together with more intelligent factors and powerful algorithms, which successfully avoid black hole attacks and ensures data reach its destination securely by recovering malicious nodes identified by node trust parameters.

Intelligent data forwarding methods like RREQ and RREP are used to create a wireless communication route free of attacks. The primary goal of this system is to offer a reliable, secure, and fault-tolerant wireless communication link over a WSN with many nodes by recovering malicious nodes of the network by using a resolver node. A novel wireless communication technique, Intelligent Channel-aware Reputation Scheme, is provided here. This methodology enables sensor nodes to interact with sequentially neighbouring nodes with increasing security; for additional security, a powerful cryptographic technique known as the Modified Rijndael Algorithm provides heightened security when packets are being sent from sender to receiver.

Trust Value Evaluation

Trust value in Wireless sensor node is calculated in two different first calculated by acknowledgments, temporal and special scores, second is calculated by packet drop ration [9].

$$\mathrm{T1} = \frac{\left[w1*\left(\frac{NA}{RC}*100\right)+ w_2*TS+w_3*SS\right]}{w_1+w_2+w_3}$$

Here T1 is the first trust value, NA is the number of acknowledgements sent to neigbours, RC is the packets received from the neigbours, TS and SS are the temporal and spatial scores, respectively w1 w2, w3 are the weights given for various trust values.

$$\mathrm{T2} = 100 - \left[\left(\frac{PD}{TPD}\right)*100\right]$$

Here T2 is the second trust value, DP is the number of dropped packets, and TPD is the total number of packets dropped in the network. The following equation calculates the final trust.

$$\mathrm{T}=\frac{(T_1+T_2)}{2}+K$$

Threshold

The mean of the trust values is considered the network threshold, is used to find suspicious nodes from the WSNs, and is calculated by the following equation.

$$T_c = \sum_{i=1}^{\mathrm{n}} \frac{\mathrm{Ti}}{\mathrm{n}}$$

Trust Metrics

Dos attacks are identified and detected by node behavior, packet delivery ratio, residual energy.

Packet Delivery Ratio: Monitoring node packet delivery ratios can detect a DoS attack immediately. The PDR is 1 if all packets are successfully delivered. The PDR is 0 if no packets are transferred successfully. The following equation calculates the packet delivery ratio x.

$$x = \frac{\text{Number of successfully delivered packets}}{\text{The total number of packets sent}}$$

Node Behaviour: The node behaviour is calculated using the trust value T, node mobility M, and w1 w2 are the weights of trust value and mobility, respectively.

$$Y = w_1 * T + w_2 * M$$

Residual Energy: The residual energy is the energy that remains after a series of communication acts have been completed is considered as residual energy. The residual energy is calculated using the equation below adopted from [9, 20]. Here R is the transmission range, T is the trust value.

$$\mathrm{Z} = E_0 - [T * E_t + R * E_r]$$

Trust Metrics Normalization: Normalization of trust values is performed by the following equation.

$$\mathrm{N}=\frac{(X+Y+Z)}{3}$$

Intelligent Channel aware Reputation Scheme (ICARS)

The source node communicates with the adjacent node using Route Request in WSNs. The neighbouring node validates the request and replies to the sender on time. The neighbour node's correct and relevant answer identifies it as a valid node, and the neighbour counter is incremented by one. Count incremented if the node is valid; otherwise, the node includes attack information. This type of node is correctly excluded from the current routing path, and the sender looks for another neighbour node to communicate with. As is the case with conventional network techniques, the selection of nodes is solely based on the Shortest Path Routing approach. This mechanism, in which an alternate path is chosen for route establishment, is not well suited for wireless sensor networks due to varying limited transmission ranges, resource scarcity, dynamic topologies, and high time requirements for routing table updates. It also results in packet overhead and, more importantly, security issues. This strategy increases the vulnerability of WSNs to a variety of security risks.

Routing is performed first, with the best path identified by recovering malicious nodes found in an IOT-based WSN environment. Residual energy, node behaviour, and trust score are used to identify malicious nodes. Once a malicious node has been identified, an idle node near the malicious node is elevated to monitor the impacted node's efficiency level. The malicious node is recovered with the help of the resolver node by giving the needed parameters; once the malicious node has been recovered, the sender and receiver create a secure path. After establishing the connection to ensure safe communication, route encryption is implemented. The cryptography system proposed for secure authentication is provided using the Modified Rijndael Algorithm (MRA), which is light, requires less computing time, and is suitable for IoT-based WSN environments. This proposed technique eliminates the attacking circumstance and makes the system more resistant to DoS attacks by combining ICARS with MRA. The following tasks are listed as part of constructing a safe path from the sender to the receiver that successfully eliminates malicious nodes from the routing path. Figure 2 shows the intelligent channel aware reputation scheme.

- Malicious Node Identification
- Resolver Node generation and Node recovery process
- Route Discovery and Route Maintenance

Algorithm 1: ICARS

```
    1. Source Node SN, Resolver Node RN
    Destination Node DN, Nearest Neighbor NN
2. Set the SN and DN to default values
3. All the nodes are bonded with Random Energy levels of the defined    threshold
4. Use distance between nodes to identify the closest neighbour
5. The 'RREQ' message transmits to its neighbour node.
6. Verify RREP from neighbour to know its validity
7. If (forwarding node is appropriate) then
        Continue further communication.
    Else Raise the Resolver node
8. The evaluator node examines the eligibility of the damaged neighbour and
supplies enough energy    to restore it to regular status and allow it for re-
communication.
9.  The Routing Table is Updated
10. The secure path is created between the sender and receiver.
```

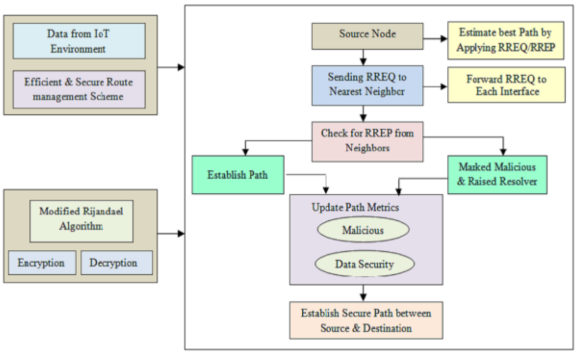
Data from IoT Environment
Efficient & Secure Route management Scheme
Modified Rijandael Algorithm
Encryption
Decryption
Source Node
Estimate best Path by Applying RREQ/RREP
Sending RREQ to Nearest Neighbcr
Forward RREQ to Each Interface
Check for RREP from Neighbors
Establish Path
Maked Malicious & Raised Resolver
Update Path Metrics
Malicious
Data Security
Establish Secure Path between Source & Destination

Fig 2. Intelligent Channel Aware Reputation Scheme.

Malicious node identification: Malicious nodes are identified using trust metrics such as PDR, Node Behavior and Residual Energy. The proposed method also considers the network's Trust Value and Threshold when identifying malicious nodes.

Algorithm 2: Malicious Node Identification

```
1. First Trust Value T1, Second Trust Value T2
   Final Trust Value T, Threshold Value TC
2.   Number of Acknowledgements NA
     Number of Packets Received RC
3. Temporal Score TS, Special Score SS
4. weights w1, w2, w3
5. Number of Packets Dropped PD, Total
```

```
    packets dropped in network TPD
6. Packet Delivery Ratio X, Node Behavior Y
    Residual Energy Z,  Normalized Value N
7.  T1 = $\frac{\left[w1*\left(\frac{NA}{RC}*100\right)+ w_2*TS+w_3*SS\right]}{w_1+w_2+w_3}$
8.  T2 = $100 - \left[\left(\frac{PD}{TPD}\right) * 100\right]$
9. T=$\frac{(T_1+T_2)}{2} + K$
10.  $T_c = \sum_{i=1}^{n} \frac{\mathrm{Ti}}{\mathrm{n}}$
11. N=$\frac{( X+Y+Z)}{3}$
12.  if ( (T> TC)&&(N>0.75)) then  return Node is Normal
     Else  return node is Malicious
```

Affected Node Recovery Process: The idle node close to the malfunctioned node operates as a Resolver node. Dynamic routing scenario generates Resolver Node. The Resolver Node checks the affected node instantly. The issue is resolved by the resolver node transferring required touting information to the impacted node, allowing it to continue.

Route Discovery and Route Maintenance: The sender sends RREQ to its neighbours; in turn, they forward it to their neighbours, and so on. This method is repeated until the destination or an intermediary node (which understands the way to the destination) is discovered. The source node regularly transmits RREQ to determine its nearest neighbour's state in Route Maintenance. When a node along the path moves, the upstream node detects and sends out a link failure notification. Re-initiate route discovery after getting a Link-failure message.

Modified Rijndael Algorithm: Lightweight cryptography has become popular due to its ability to deal with devices with limited battery life, compact areas, and small memory sizes. Modifying current algorithms, enhancing existing ones, or designing new ones with lightweight concerns are all options for building lightweight cryptography.

Rijndael is a block encryption algorithm, NIST has chosen Rijndael as the standard symmetric key encryption technique for encrypting sensitive (unclassified) American federal data. The decision was made after a thorough examination of Rijndael's algorithm's security and efficiency properties. The Rijndael algorithm operates on blocks of data of fixed size, typically 128 bits. It uses a key, also of fixed size, to transform the data in the block using a series of mathematical operations. The key can be of any length, but 128, 192, and 256-bit keys are most commonly used. One of the strengths of the Rijndael algorithm is its versatility. It can be implemented in a variety of block sizes and key lengths, and it is resistant to various attacks, including differential and linear cryptanalysis. It is also relatively fast and efficient, making it suitable for use in a wide range of applications [21].

The Rijndael algorithm is widely used in a variety of applications, including internet security, file encryption, and authentication protocols. It is often used as a replacement for the Data Encryption Standard (DES), which is considered to be less secure. Rijndael is a block cypher that is iterated. As a result, each iteration (round) of a given transformation is used to encrypt or decode a data block. In addition, Rijndael proposes a mechanism for generating a succession of subkeys from the original key. The round function takes the generated subkeys as input. Belgian cryptographers Joan Daemen and Vincent Rijmen Rijndael algorithm. The algorithm developed as a simple mathematical structure that can be broken down into simple components and provides the following benefits

- Resistant to all known attacks
- Speed and code compactness;
- Simplicity in design

Wireless sensor nodes do not tolerate complicated cryptography in routing due to their limited resources. Existing data encryption algorithms in WSNs have either a very long response time or a very long computing time [21]. As a result, there is a high demand for lightweight encryption techniques. The Modified Rijndael Algorithm is a light-weight encryption mechanism designed for resource-constrained wireless sensor devices. It aims to balance complexity and speed, and several changes have been made to the conventional Rijndael Algorithm to reduce execution and computation time. The modified algorithm applies a mapping and crossover procedure to the plain text and reduces the number of rounds to six, with each round containing three steps: Shift Columns, MixColumn, and AddRoundKey (excluding the last round which only has two steps). The MixColumn function is the most critical operation in terms of complexity and security, but it also requires a significant amount of time for calculations. The algorithm also includes a crossover phase, which rearranges the characters of the plain text to disrupt the analytical relationships between them. This phase is only applied once before encryption to replace the S-box round of the conventional Rijndael algorithm. The Modified Rijndael Algorithm uses a crossover phase to increase the complexity of the encryption process and compensate for the absence of the Sub Bytes step. The crossover phase reorganizes the characters in the plain text and applies a mapping and two-point crossover operation from a genetic algorithm to create a 4*4 state matrix. The mapping step maps the input bits based on a specific pattern to create a zigzag effect and increase the difficulty of prediction. The two-point crossover operation combines two 8-bit parent chromosomes to create new child chromosomes, which are then used to create the final 44 state matrix. This matrix is then passed on to the next step in the encryption process.

Pseudo code for Modified Rijndael Algorithm

```
Modified Rijndael Algorithm_Encryption( plaintext, key)
{
    blocks= divideIntoBlocks(plaintext);
    For Each block of size 4*4 in plaintext do     {
         Crossover(block);
         AddRoundKey(RounKey[0], block);
         For i=1 to 6 do           {
               ShiftColumn(block);
               MixColumn(block)
               AddRoundKey(RounKey[..], block);
            }
        ShiftColoum(block)
       AddRoundKey(RounKey[5], block);
    }
   ciphertext=reassemble(block);
   return ciphertext;
}
```

Table 1. Avalanche effect

Plain Text	Ciphertext (Rijndael)	Avalanche	Cyphertext (MRA)	Avalanche
0000111123456789	sa89dgew6tfrejhddfgg093jfur yewid	57%	K6f37dc2y2b9d7cbf4 880c90b20b4e70	69.4%
A1B2DDE3245BC6F8	ikv48etyos9234mncc4dclffgn bbgtr4	55%	7997144b4a6e06e75d 0f251fb253e980	66.9%
amjvtrhcqsjhgawl	gh34lk8cmn94ls39gasjh2dkv 45uv709	56%	ty1b64574db79ebb83b da57976854f	71.8%
5876661234567891	kg93i6vhas2qr492kdjfyur8ek fnehdu	59%	98bcce4489a6e06e75d 0f25828swf496	70.9%

4. Results and Discussion

This section proves with experimental results that the proposed policy of integrating ICARS with MRA removes the attack situation to make the system more resistant to DoS attacks. The proposed technique uses NS2, a powerful network simulation application that produces reliable results. The table below lists the parameters necessary for the simulation.

Table 2: Simulation Parameters

Parameters for simulation	Values
Simulation Area	1000X1000m
Number of Nodes	20 to 100
Length of the Queue	1000
Transmission Range	3200 m
Presence of Sink Node	YES
Type of Antenna	Omni Antenna
Transmission Rate of Packets	8 to 320 kbps
Transmission Frequency	2.5 to 5 GHz
Size of the packet	1000 to 1200 kb
Transmission Speed	30-70 bps
Type of Channel	Wireless Communication Channel

The table 1 illustrates the whole network construction in the communication scenario. In this figure, the number of initialized nodes is 20, 200m is the transmission range, the packet transmission speed is 30bps, the average delay is 2ms, 2.5 GHz is packet transmission frequency, the packet rate is 8kbps, the packet size is 1000kb, multiple nodes are present between two nodes, and there may be malicious nodes. The optimum path between sender and recipient is determined using the neighbour node selection process sequentially. The proposed technique, ICARS, is used for failure node recovery. The resolver nodes are selected from the communication environment, offering adequate parameters or bandwidth to the damaged node and restoring the node to its original position. So that channel loss does not occur when the proposed routing mechanism is used.

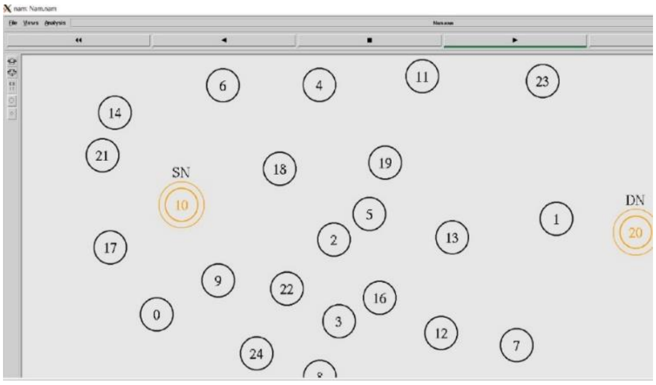

Fig 3(a). Node Scenario.

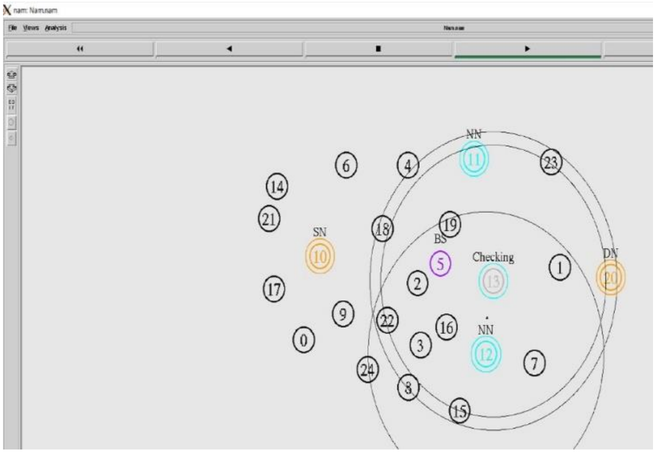

Fig 3(b). Checking the ability of the neighbor.

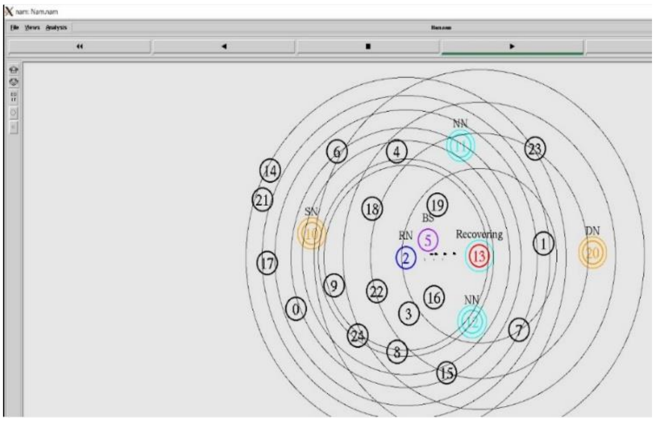

Fig 3(c). Node 13 identified as affected by neighboring node 12.

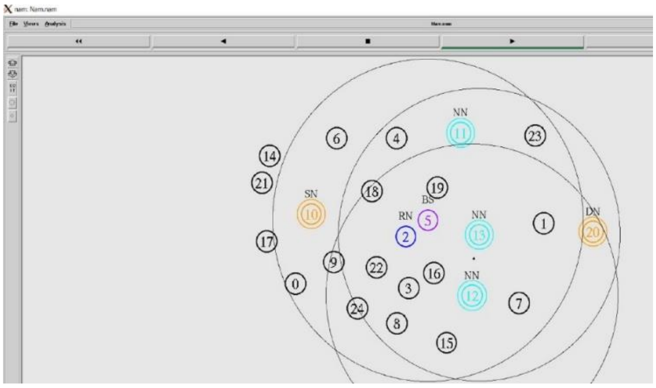

Fig 3(d). Resolver Node recovered the affected node 13.

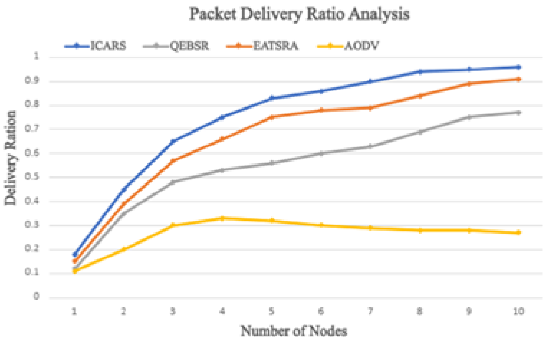

Fig 4. PDR Analysis

The packet delivery ratio of a network is the ratio between number of packets that arrive at their destination successfully to packets transmitted. Figure 4 describes the proposed strategy ICARS has improved packet delivery ration than existing strategies like QEBSR, EATSRA and conventional packet forwarding scheme AODV and shows that the presented strategy is superior to the traditional methods.

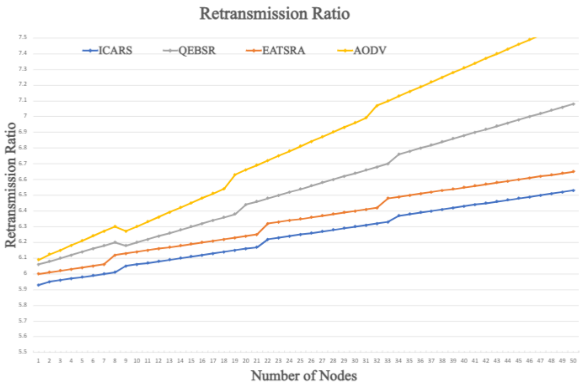

Fig 5. Retransmission Ration Analysis.

Figure 4 shows how the proposed scheme's retransmission ratio is better to the traditional packet forwarding technique like QEBSR, EATSRA, the present strategy ICARS is also compared with the classic routing mechanism AODV and figure demonstrates that the presented strategy is superior to the classical method.

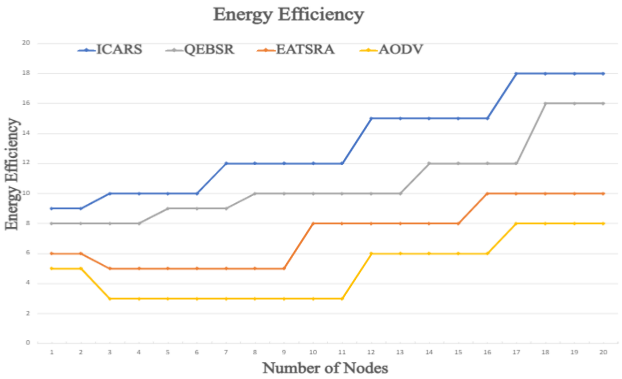

Fig 5. Energy Efficiency Analysis.

The energy consumption of the whole network was measured while packets were being sent and are displayed in Figure 5. Consumption of energy depends on connection efficiency and distance; the proposed mechanism consumes less minimal energy than compare the techniques QEBSR, EATSRA and AODV. The Figure 5 is demonstrating that the presented method is superior to the traditional method.

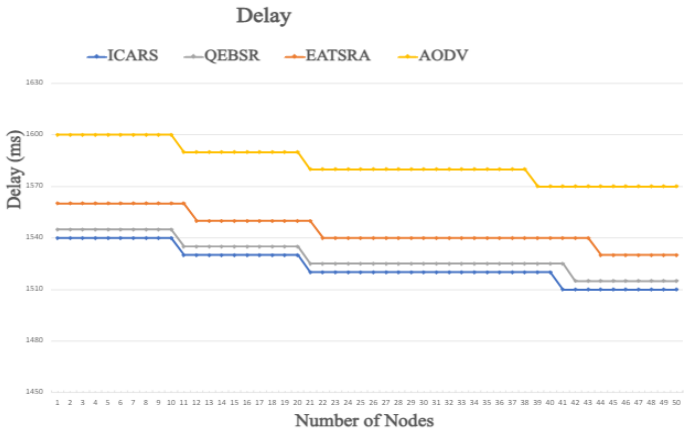

Fig 6. Delay Analysis.

The delay is the variation between the transmission time and received time. Milliseconds are the units for the delay. Data transmission time is decreased to a specific degree in the proposed ICARS approach compare to QEBSR, EATSRA, as seen in Fig.6, ICARS is also superior to the existing AODV protocol.

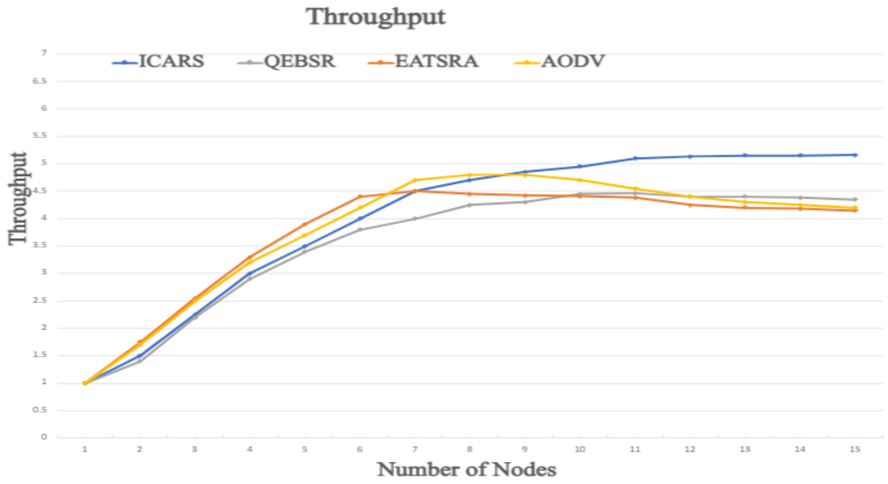

Fig 7. Throughput Analysis.

Throughput is defined as the number of packets received divided by the number of packets sent without a service interruption. The results demonstrate that the proposed methodology has a slightly higher throughput value than the QESBR, EATSRA and traditional Routing protocol AODV, Figure 7 shows the throughput analysis.

5. Conclusion

This article presented a robust, secure, and failure-free routing system, which includes more intelligence features and robust algorithms and successfully eliminates the black hole attacks. By proposed methods, ICARS and the MRA ensure that the data is delivered to its intended location without any errors or attacks. The approaches such as RREQ and RREP procedures and Resolver Node generation are an added advantage. In this security framework, malicious nodes are identified using trust scores and node behavior efficiently. Malicious nodes are effectively recovered to avoid packet overhead and unnecessary routing table updating. Cryptographic scheme MRA is light and requires less computation time. With the suggested system, the WSNs maximize techniques such as Lifetime. Throughput and PDR are improved compared to traditional AODV protocol. In the future, the suggested work might be enhanced even further by using genetic algorithms for replacing failure nodes.

References

[1] Fang W., Zhang W., Chen W., Liu J., Ni Y., Yang Y. MSCR: Multidimensional secure clustered routing scheme in hierarchical wireless sensor networks. EURASIP Journal on Wireless Communications and Networking. 2021. 2021:1-20.

[2] Sirajuddin M., Kumar B.S. Efficient and Secured Route Management Scheme Against Security Attacks in Wireless Sensor Networks. In2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC). 2021. 1045-1051. IEEE.

[3] Alotaibi M., Improved blowfish algorithm-based secure routing technique in IoT-based WSN. IEEE Access. 2021. 9:159187-97.

[4] Adnan M., Yang L., Ahmad T., Tao Y. An unequally clustered multi-hop routing protocol based on fuzzy logic for wireless sensor networks. IEEE Access. 2021. 9:38531-45.

[5] Talukdar M.I., Hassan R., Hossen M.S., Ahmad K., Qamar F., Ahmed A.S. Performance improvements of AODV by black hole attack detection using IDS and digital signature. Wireless Communications and Mobile Computing. 2021. 2021:1-3.

[6] Payton E., Khubchandani J., Thompson A., Price J.H. Parents' expectations of high schools in firearm violence prevention. Journal of community health. 2017. 42:1118-26.

[7] Gousia Thahniyath., Jayaprasad M. Secure and load balanced routing model for wireless sensor networks. Journal of King Saud University-Computer and information sciences. 2023. 35(7); DOI:https://doi.org/10.1016/j.jksuci.2020.10.012.

[8] Rathee M., Kumar S., Gandomi A.H., Dilip K., Balusamy B., Patan R. Ant colony optimization based quality of service aware energy balancing secure routing algorithm for wireless sensor networks. IEEE Transactions on Engineering Management. 2019. 68(1):170-82.

[9] Selvi M., Thangaramya K., Ganapathy S., Kulothungan K., Khannah Nehemiah H., Kannan A. An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. Wireless Personal Communications. 2019. 105:1475-90.

[10] Chandre P.R., Mahalle P.N., Shinde G.R. Machine learning based novel approach for intrusion detection and prevention system: A tool based verification. In2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN). 2018. 135-140. IEEE.

[11] Sunitha R., Chandrikab J., Evolutionary computing assisted wireless sensor network mining for qos-centric and energy-efficient routing protocol. International Journal of Engineering. 2020. 33(5):791-7.

[12] Rana, P. ., Sharma, V. ., & Kumar Gupta, P. . (2023). Lung Disease Classification using Dense Alex Net Framework with Contrast Normalisation and Five-Fold Geometric Transformation. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2), 94–105. https://doi.org/10.17762/ijritcc.v11i2.6133

[13] Karthick S., Devi E.S., Nagarajan R.V. Trust-distrust protocol for the secure routing in wireless sensor networks. In2017 International conference on algorithms, methodology, models and applications in emerging technologies (ICAMMAET). 2017. 1-5. IEEE.

[14] Jinhui X., Yang T., Feiyue Y., Leina P., Juan X., Yao H. Intrusion detection system for hybrid DoS attacks using energy trust in wireless sensor networks. Procedia computer science. 2018. 131:1188-95.

[15] Deebak B.D., Al-Turjman F. A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks. Ad Hoc Networks. 2020. 97:102022.

[16] Seyyedabbasi A., Kiani F. MAP-ACO: An efficient protocol for multi-agent pathfinding in real-time WSN and decentralized IoT systems. Microprocessors and Microsystems. 2020. 79:103325.

[17] Prakash S., Saroj V. A review of wireless charging nodes in wireless sensor networks. Data Science and Big Data Analytics: ACM-WIR 2018. 2018. 177-88.

[18] Amin A., Liu X.H., Saleem M.A., Henna S., Islam T.U., Khan I., Uthansakul P., Qurashi M.Z., Mirjavadi S.S., Forsat M. Collaborative wireless power transfer in wireless rechargeable sensor networks. Wireless Communications and Mobile Computing. 2020. 2020.

[19] Jasper J. A secure routing scheme to mitigate attack in wireless adhoc sensor network. Computers & Security. 2021 Apr 1;103:102197.

[20] Faris, W. F. . (2020). Cataract Eye Detection Using Deep Learning Based Feature Extraction with Classification. Research Journal of Computer Systems and Engineering, 1(2), 20:25. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/7

[21] Lai Y., Tong L., Liu J., Wang Y., Tang T., Zhao Z., Qin H. Identifying malicious nodes in wireless sensor networks based on correlation detection. Computers & Security. 2022. 113:102540.

[22] Heinzelman W.B., Chandrakasan A.P., Balakrishnan H. An application-specific protocol architecture for wireless microsensor networks. IEEE Transactions on wireless communications. 2002. 1(4):660-70.

[23] Raju B.B., Krishna A., Mishra G. Implementation of an efficient dynamic AES algorithm using ARM based SoC. In2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON) 2017 Oct 26 (pp. 39-43). IEEE