Mathematical Biosciences and Engineering

MBE, 20(2): 4243–4257.
DOI: 10.3934/mbe.2023198
Received: 11 October 2022
Revised: 18 November 2022
Accepted: 25 November 2022
Published: 21 December 2022

http://www.aimspress.com/journal/MBE

Research article

Intelligent dynamic trust secure attacker detection routing for WSN-IoT networks

B. Kiruthika* **and Shyamala Bharathi P**

Department of ECE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India

* **Correspondence:** Email: kiruthika.bk@gmail.com.

Abstract: Introduction: IoT networks require a variety of safety systems, because of evolving new technologies. They are subject to assaults and require a variety of security solutions. Because of the sensor nodes' limited energy, compute capabilities and storage resources, identifying appropriate cryptography is critical in wireless sensor networks (WSN). Objective: So, we need a new energy-aware routing method with an excellent cryptography-based security framework that fulfills critical IoT needs such as dependability, energy efficiency, attacker detection and data aggregation. Methods: Intelligent dynamic trust secure attacker detection routing (IDTSADR) is a novel energy-aware routing method suggested for WSN-IoT networks. IDTSADR fulfills critical IoT needs such as dependability, energy efficiency, attacker detection and data aggregation. IDTSADR is an energy-efficient routing technique that discovers routes that use the least amount of energy for end-to-end packet traversal and improves malicious node detection. Our suggested algorithms take connection dependability into account to discover more reliable routes, as well as a goal of finding more energy-efficient routes and extending network lifespan by finding routes with nodes with greater battery charge levels. We presented a cryptography-based security framework for implementing the advanced encryption approach in IoT. Conclusion: Improving the algorithm's encryption and decryption elements, which currently exist and provide outstanding security. From the below results, we can conclude that the proposed method surpasses the existing methods, this difference obviously prolonged the lifetime of the network.

Keywords: WSN; IDTSADR; IoT networks; security; attacker detection; data aggregation; cryptography

1. Introduction

WSNs are an important component of the IoT. Sensors in IoT-based WSNs continuously monitor the surroundings and alert the BS to any events. This behavior causes a number of critical problems in the network, including long communication delays and a significant energy imbalance between distributed sensor nodes. For energy-efficient data transmission, the whole network is separated into multiple clusters in this application. Existing clustering-based data routing techniques, on the other hand, have a number of major flaws, including long communication delays, limited throughput and energy-hole difficulties. Furthermore, the conventional clustering strategy necessitates a significant amount of message overhead in order to partition the whole network into various clusters [1].

WSNs have accomplished remarkable things in both academics and the field of information technology. In a WSN context, remote access of clients to approved sensor nodes and information transmission between the nodes and the server are required with the advent of IoT technology. Sensors and processing nodes make up a WSN. Sensor nodes are often placed at random in a target region to detect important data from integrated fields and then transfer that data to a nearby base station. Deciphering cryptographic methods in WSNs and designing energy-efficient ciphers to meet security needs have been the attention of several researchers. Although data transmission consumes the most energy in a WSN [1,2]. Information security is essential due to the vital nature of services, as information interception or change can result in considerable loss of life and money. As a result, the goal of this work is to build an energy-efficient and cryptography-based method for finding routes with nodes and security, extending network lifespan, and obtaining more energy-efficient routes.

A base station (sink) that connects wirelessly with additional sensors is characteristic of WSN. Each sensor sends information to the BS nodes. The obtained data for the relevant parameter is analyzed in the basic station, and its precise value is estimated with relative precision [3]. Node and network-level demands were included as fundamental design objectives as WSNs and communications networks combined to become information networks [4]. For sensor nodes in a WSN, the lightweight block cipher, known as: Byte-oriented Substitution-Permutation Network (BSPN) [2] achieves great performance while offering adequate security. With our approach, we created a novel energy-aware routing strategy and a top-notch cryptography-based security framework that satisfies key IoT requirements like dependability, energy efficiency, attacker detection, and data aggregation, outperforming lightweight block ciphers [2].

Energy efficiency and cryptography, which are considered particularly difficult and energy-intensive in the context of node resource availability, are among the security-related methods to avoid harmful activities. As a result, in order to increase network throughput, a lightweight solution to the problem is required. We describe IDTSADR, a novel energy-aware routing method that will be suggested for WSN-IoT networks (IDTSADR). Improving the algorithm's encryption and decryption features, which currently exist and pave the path for exceptional security and we created a better method when comparing with existing works.

2. Literature survey

Shrestha et al. [5] included a WSN dependability model generated automatically from the WSN architecture, as well as data on the routing algorithms employed and the battery state of the mote in their study. In their paradigm, WSN failure is believed to occur at two points: connections and sensor nodes. Three scenarios were used to assess the proposed models. It was easy to see how the routing protocol used.

Duan et al. [6] provided an overview of WSN dependability strategies. In order to recover lost data utilizing hop-by-hop or end-to-end processes, we investigate a variety of reliability systems based on redundancy and retransmission techniques that use different combinations of reliability of packets or events.

The research of Hemanth and Ramesh [7] addresses the issue of cluster heads broadcasting data to base stations through one-hop communication in cluster-based and homogeneous WSNs, and provides an EEBCDA. The more sensor nodes participating in the rotation of the cluster head and sharing power load in the grid with the most energy-consuming cluster head, allowing it to balance energy dissipation. It also employs a number of energy-saving techniques.

Zhou et al. [8] implemented and examined the Optimal Aggregation Problem using an ant-based method. Extensive simulation is used to ensure that the algorithm is valid. It has been discovered that the energy efficiency of aggregation is affected by the number of sources. The simulation findings show that optimal aggregation saves up to 45 percent of energy for a moderate number of source nodes.

Misra and Mandal [9] presented several encryption approaches for MICA z-type motes-based wireless sensor network systems are investigated. The utilization of memory, computing power, and time by crypto-graphic algorithms was investigated. The RC4 and MD5 cryptographic algorithms performed the best in terms of crypto-graphic processing time for WSN based on MICA z-type method.

Ebrahim and Chong [10] have presented a unique anomaly detection algorithm-based security strategy based on the property that surrounding nodes in networks can give stable information. They showed that by evaluating a modest number of incoming packet properties, a node may quickly detect an attacker. They handled the anomaly detection algorithm as though it ran at each node separately in their implementation. A low-complexity cooperation method could help in detection and containment. When intruders are spotted, nearby nodes will take coordinated action against them.

Rostami et al. [11] presented one strategy for reducing dimensionality that can increase job accuracy while lowering computational cost is feature selection. The goal of the feature selection strategy is to choose a subset of features that are most relevant to the target class and have the least inner similarity. Deleting unneeded, redundant, or noisy data, reduces the dimensionality of the data. In this study, various feature selection procedures are compared, analyzed, and categorized. This study also examines the use of wrapper and filter SI-based techniques (such as PSO, ACO, ABC, DE, GSA, FA, BA, COA, GWO, WOA, and SSA) in feature selection. The advantages and disadvantages of the various SI-based feature selection approaches that have been investigated are also discussed, along with the potential drivers of their supremacy.

Nasiri et al. [12] introduced a new robust graph regularization nonnegative matrix factorization for attributed networks (RGNMF-AN), in order to capture both the topology structure of networks and their node properties for direct link prediction. This particular model uses the structure-attribute random walk similarity (SARWS) approach to compute high-order proximities between nodes while incorporating two forms of information, namely network topology and nodal attribute information. In contrast to graph regularization technology, which combines the SARWS score matrix with topological and attribute information to collect more valuable attributed information in high-order proximities, the SARWS score matrix is an indicator structural and attributed matrix that collects more valuable attributed information in high-order proximities. Additionally, the RGNMF-AN uses the l2,1-norm to constrain the regularization and loss function parameters, significantly lowering spurious links and random noise. Using attributed and topological information together enhances prediction accuracy greatly when compared to the baseline and other NMF-based approaches, according to empirical results on nine real-world complex network datasets.

The main problems identified from above survey as follows:

- Using existing protocols for route discovery may result in network-wide flooding of routing requests, which can consume a significant amount of network resources such as energy. Harmful nodes engage in malicious actions like as packet dropping, flooding and packet delaying, among others, in order to take advantage of a node's limited resources. Breaking the routes increases packet delivery time and may result in network segmentation, resulting in multi-hop communications failure.
- Cryptography and authentication operations, which are considered particularly difficult and energy-hungry in the context of the availability of resources in the node, are among the security-related methods to avoid harmful activities. As a result, a lightweight solution to the problem is necessary in order to boost network throughput.
- The lack of fixed infrastructures and monitoring sites makes collecting audit data for the entire network problematic.
- WSN's frightened resources should be taken into account when creating the IDS framework. It is more difficult to distinguish between false alarms and real positives in WSN. When an intrusion is detected but the malicious host is not removed, the protection becomes passive.

3. Proposed system

We present an updated energy-aware routing algorithm called IDTSADR in WSN-IoT. The fundamental WSN-IoT model and its aspects are discussed.

In the proposed authentication strategy's predicted network architecture, in which end-users interact with multiple edge devices to obtain specific information or services. End users might be human or virtual entities, and edge networks can include a range of devices.

According to the proposed authentication strategy, authentication is taken into account for three communication contexts in particular:

1). Two sensor nodes in the same WSN (Link A).
2). Two sensor nodes in two separate WSNs (Link B).
3). A sensor node and an end-user (Link C).

The two entities can mutually authenticate using a valid certificate independent of their local network. Adding extra nodes may readily extend data acquisition and service provision networks, regardless of network size. The CA should be able to recognize genuine identities and connect with network entities that require security credentials. The system depicts how network entities communicate with CA using pre-existing communication channels that travel through an IoT cloud.

The WSN-IoT is largely used in this strategy to achieve network virtualization in a sensor network. The enhanced WSN-IoT is built on a four-layer framework from bottom to top.

In this section, we use IDTSADR a novel energy-aware routing method and it provides a cryptography technique. In our method we use advanced encryption and decryption for the cryptography technique. The following sections describe our energy efficiency, data aggregation, and cryptography in our IDTSADR method for better security.

3.1. IDTSADR

IDTSADR is a novel energy-aware routing method for WSN-IoT networks. IDTSADR covers key IoT requirements such as energy efficiency, dependability, data aggregation and the identification of attackers. Some attacks may sometimes create a serious issue in the wireless sensor network and hence a new attack detection mechanism has been proposed that detects the severe attacks and thus defends against those attacks and implements the attack detection system with an increased detection rate in WSN during the process of data aggregation. IDTSADR also concentrates on other important requirements of WSN like energy efficiency and enhanced network lifetime. Routing algorithm that is used in IDTSADR finds the routes by minimizing the total energy required for end-to-end packet traversal and thus making the network more energy efficient. To deploy an advanced encryption approach in IoT, we suggested a cryptography-based security mechanism. Improving the algorithm's encryption and decryption features, which currently exist and pave the path for exceptional security.

3.1.1. Attack detection model trust computation

To make a security choice based on the computed trust value, we must first determine how much risk is acceptable for each ongoing job. In other words, a trust value threshold (Threshold) must be specified for each activity. This trust value can be adjusted based on the security requirements of each ongoing task. The number of successes is α, the number of failures is β.

Trust computation-based attacker detection T_{ij}^{d} -Trust value, I and j nodes, $T_{ij}^{d} = \frac{\alpha_{ij}}{\alpha_{ij} + \beta_{ij}}$.

Energy Efficiency: This section explains the proposed strategy for reducing energy usage in WSN, which includes game theory (WSNs). Every node in the network has two options. That is, it has the ability to function as the cluster head or not. Because nodes are selfish, they seldom act as cluster leaders and instead outsource head clustering to other nodes. If none of the nodes act as cluster heads, they will be unable to transmit data to the main station and will thus be of no use. When a node isn't picked for cluster leadership, but at least one of the other residual nodes is, the optimum approach for each node is determined. V and C represent the utility gained by each node from data transmission and the cluster heading cost [3].

$$u_i(s) = \begin{cases} 0 & if\ si = ND \\ v - c & if\ si = D \\ v & if\, si = ND\ and\ sj = D \end{cases} \tag{1}$$

As a result, if $S = D, ND$, Eq (1) determines the utility function of each node:

As a consequence, when one node is the cluster head and the other nodes are not, the ideal manner happens. The node is defined based on the interaction between the two nodes, and D and ND stand for the node that chooses itself for cluster heading and the node that is not considered the cluster head, respectively. Each node in this technique makes a random choice based on a probability distribution. Cluster (P) and one chance of heading in a noncluster $(q = 1 - p)$. Equation is used to calculate the value of the utility function for the latter Eq (2):

$$u_{nd} = v.\left(1-(1-p)\right)^{n-1} \tag{2}$$

The projected utility of non-cluster heading $(v-c)$ is assumed to be equal as seen in Eq (3), and the P value is determined using Eq (4):

$$v-c = v.(1-(1-p))^{n-1} \tag{3}$$

$$P = 1 - w^{1/(N-1)} \tag{4}$$

W is a positive number that is less than one. As a result, the probability of P is always between 0 and 1. As the number of nodes grows, the P value drops. Reducing the number of nodes, on the other hand, raises the P value. Because of their selfish behavior, nodes are less likely to join the network as the number of nodes grows. Consequently, calculating C and V and determining the energy model in ordinary and cluster head nodes yields the P probability of each node [3]. Equation (5) calculates how much energy each node uses during data transmission. The amount of bits sent and the distance between node I and the cluster head are represented by K and d, respectively. As a consequence, each node sends data bits to the cluster head using $Etx(k,d)$ at a distance from d. Equation (6) also calculates how much energy each node uses to receive data. (To receive the data bit K, each node requires $Erx(k)$):

$$Etx(i,CHi) = k \times (Elec + \varepsilon amp \times di^2) \tag{5}$$

$$Erx(k) = Eelec \times k \tag{6}$$

Eelec and eamp are well-known constants for deciphering internal circuits of sensors for data transmission and reception, as well as other energy-intensive operations. When data from regular nodes is sent to cluster heads, they combine it and send it to the main station [3].

Equation (7) measures the energy needed for package aggregation if Nu is the number of packages with the same height (k) received by the cluster leader.

$$Eaggr = Nu \times k \times effuse \tag{7}$$

$effuse$ is a data aggregation constant. Equation (8) also calculates the amount of energy used to send data from cluster heads to the main station and di is distance:

$$Etx(CHi, \operatorname{Sin} k) = k \times (Elec + eamp \times di^4) \tag{8}$$

When a node provides data to the cluster head, it utilizes $Etx\ (i,CHi)$, according to the equations above [4]. The cluster head receives the data supplied by the member nodes after aggregation and sends it to the main station. Equation (9) calculates the cluster head node cost c as a result:

$$Etx(CHi, Sink) \times c = Nu \times Erx \times Eaggr \tag{9}$$

Equation (10) calculates the exchanged energy for each node (ED) if α and β are the data transmission rate and data receipt rate, respectively [4]. Equation (11) is used to calculate the resulting utility v.

$$ED = \alpha.Etx\left(i, CHi\right) + \beta.Erx \tag{10}$$

$$v = \left(\alpha + \beta\right) \times Etx - ED \tag{11}$$

As a result, the probability of node cluster heading p is calculated in Eq (12):

$$p = 1 - \left(\left(c - t\right) / \left(v - t\right)\right)^{1/(1-N)} \tag{12}$$

Each cluster's members (cluster heads) are chosen depending on their proximity to the next cluster or cluster head [4].

Reliability: Components and procedures fall into two groups when it comes to WSN dependability. The dependability of the nodes that make up dispersed networks is addressed at the component level. All of the WSN's processes, hardware components, and communication paths are covered by process-level dependability [4]. It is given by Eq (13):

$$R\left(t\right) = \exp\left(-\lambda t\right) \cong 1 - \lambda t, (when\ \lambda t\ is\ small) \tag{13}$$

where λ is the mean component failure, R(t) is the component reliability with respect to time.

Data aggregation: Data aggregation, or the process of combining data from several nodes to reduce duplicate transmission and provide fused data to BS, is viewed as a useful way for WSNs to save energy.

Intrusion detection algorithm: If an attacker takes a node and uses it for his own purposes, there's a chance that the node's abnormal behavior will be noticed and the node will be reclaimed, ultimately terminating the attack. We will create a detection mechanism to identify this intrusion in this part. Packet delivery is hampered by the Blackhole assault, which also results in packet loss.

A detection algorithm detects infiltration patterns based on a set of rules. In this case, we choose average receive power to describe the behavior of an adjacent node. A sliding window strategy based on packet count is used in this technique. If the statistics of a neighbor match, the packet is considered original.

Anomaly packets must be kept apart from ordinary arrivals and retained in a buffer until a judgement is reached in the latter scenario.

The buffer utilized for this intrusion is referred to as a buffer, and its length is defined as N1.

The following is the detection flow based on the aforesaid algorithm:

- Packets are being received.
- Using the IDS rule to determine if the packet is an unusual packet. It will be sent to the intrusion buffer.
- Setting off the alarm.
- Changing the rule (specifically, changing the model's statistics value). The rule may be

modified with each packet insertion.

If there are N anomalous packets that can't be efficiently detected, they'll alter the main packet buffer's behavior and go unnoticed. As a result, N2 must be less than N. The selection of appropriate N1 and N2 numbers (depending on security vulnerabilities) has a significant impact.

For a major attack in this received power anomalous detection technique, the intruder must maintain its distance measure for every node already. If the attacker's position is significantly different, the likelihood of identification due to received power anomalies increases. To get access to the network, the intruder must have the same transmitter circuits or voltage regulation capabilities as the unmasked node's transceiver (s). Our intrusion detection system forces the intrusion to comprehend the typical packet-forwarding behaviors of the impersonated node (s).

AODV: Being a reactive or on-demand routing system, AODV (Ad-hoc On-demand Distance Vector) only determines a route between two nodes when data needs to be transmitted. The next hop to a particular destination is all that is stored in each node's routing table, so information on the path a packet will follow is spread out among all nodes along the network. Reactive packet routing protocols include AODV. Only when necessary does it create a path from source to destination. Route discovery is done reactively using the AODV routing protocol [13].

Cryptography: Because the information broadcast by a sensor node may contain sensitive information, such as a patient's health status, data confidentiality is occasionally critical in many WSNs. For this, we'll look into symmetric key cryptography approaches and tactics for a sensor node's fundamental communication behavior. The communication is decrypted by the recipient, which might be a cluster head, an aggregator, or the base station.

Two forms of ciphers, symmetric key ciphers and asymmetric (or public) key ciphers, use different strategies to ensure security. We show the two types of ciphers used in symmetric key cryptography methods: stream ciphers and block ciphers. The method of operation of a block cipher is frequently changed to fit a specific purpose.

The same cipher key is used for encryption and decryption in a symmetric key block cipher, and both parties are expected to know it. As a result, we assume that the encryption key is established prior to our research in a sensor node, and we do not evaluate the consequences of key establishment in our research. By preventing potentially sensitive information from falling into the wrong hands, encryption preserves the privacy of two communicating parties.

3.1.2. IDTSADR algorithm steps

The source node ignores any more RREPs from black holes or grayholes and broadcasts a list of cooperating black holes instead. The method loops from step 7 to step 24 if NHN is an unreliable node; in this case, the source node interprets the current NHN as an updated IN and transmits FRq to the updated IN's next hop node.

```
IF (RREP is from DN)
{
Route data packets (Secure Route)
  }
ELSE
{
Do
```

```
    {
      For i=1 to Np do
    Pv ← Rv()
    Pp← Random Position (Np)
    Lbp←Pp
    For each particle calculate the value of fitness function
    If fitness (Lbp) ⩽ fitness (Gbp) then
    Gbp ←Lbp
    ELSE
    {
    Insecure Route
    IN is a Grayhole & black hole
    All of the nodes between IN and the node that created RREP are grey and black holes.
    }
    }
    ELSE
    Current IN = NHN
    }
While (IN is NOT a reliable node)
```

4. Graph and result

An Intel Core i7-10750H CPU running at 2.60 GHz, 8 GB of RAM, Windows 10 OS, and a network simulator2 make up the hardware experimental environment 377.

4.1. No of nodes vs packet delivery ratio

The packet delivery ratio is the number of received packets successfully to a client divided by the number of packets sent by the transmitter. Table 1 and Figure 1 show the No of nodes vs packet delivery ratio in existing and IDTSADR method. And IDTSADR is better than existing methods in No of Nodes Vs Packet Delivery Ratio.

Table 1. No of nodes vs packet delivery ratio.

Number of nodes	AODV	Existing	IDTSADR
	Packet delivery ratio (%)		
10	77	65	75
20	79	68	78
30	80	78	88
40	82	85	95
50	82	90	96

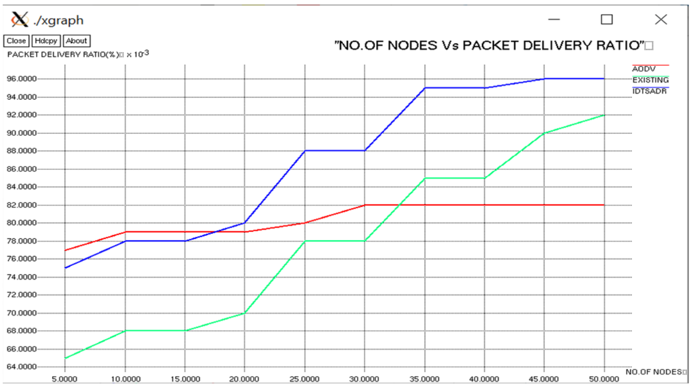

Figure 1. No of nodes vs packet delivery rati.

4.2. Number of nodes vs end to end delay

The time it takes for a data packet to reach at its destination on average. It also considers the delay introduced by the route discovery process and the data packet transmission queue. Only data packets that made it to their intended destinations were counted. Table 2 and Figure 2 show the no of nodes vs end to end delay in existing and IDTSADR method. And IDTSADR is better than existing methods in no of nodes vs end to end delay.

Table 2. No of nodes vs end to end delay (ms).

Number of nodes	AODV	Existing	IDTSADR
	End to end delay (ms)		
10	15	15	8
20	45	23	13
30	40	24	15
40	35	29	20
50	35	26	20

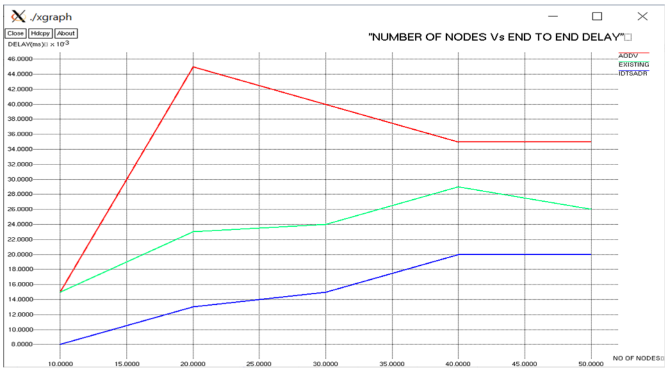

Figure 2. Number of nodes vs end to end delay.

4.3. No of nodes vs control overhead

The ratio of the total number of routing packets to the total number of properly transmitted packets is known as routing overhead. The routing layer's overhead packets contain packets for both destination node and route maintenance. Table 3 and Figure 3 show the no of nodes vs end to control overhead in existing and IDTSADR method. And IDTSADR is better than existing methods in no of nodes vs end to control overhead.

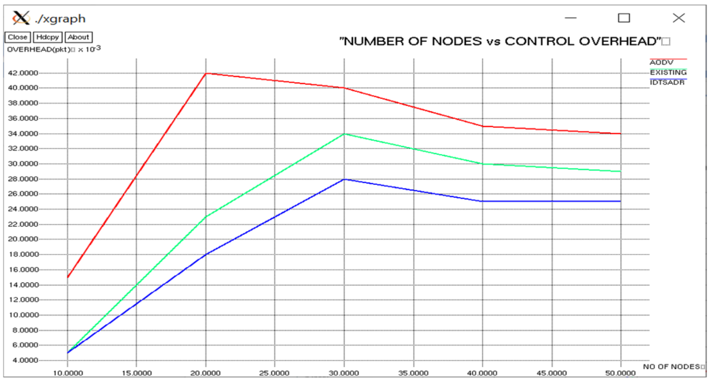

Figure 3. No of nodes vs control overhead.

Table 3. No of nodes vs end to control overhead.

Number of nodes	AODV	Existing	IDTSADR
	Control overhead (pkt)		
10	15	5	5
20	42	23	18
30	40	34	28
40	35	30	25
50	34	29	25

4.4. No of nodes vs energy consumption

It is the average of the total energy consumed in the network as a result of communication during a given time period and at a given data rate. If E is the total amount of energy spent on communication and N is the total number of nodes in the system, E/N (energy per node) is the average communication energy. It's best to use a protocol with a lower average communication energy. Table 4 and Figure 4 show the no of nodes vs energy consumption in the existing IDTSADR method. And IDTSADR is better than existing methods in no of nodes vs energy consumption.

Table 4. No of nodes vs energy consumption.

Number of nodes	AODV	Existing	IDTSADR
	Energy consumption (J x 10-3)		
0	30	28.5	25
10	28	23.6	20
20	24	14	13
30	15	14	13
40	15	5.6	5
50	6.5	5.1	4.7

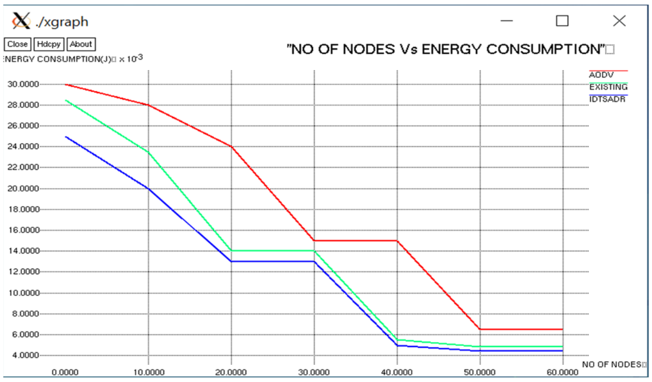

Figure 4. No of nodes vs energy consumption.

4.5. No of nodes vs network lifetime

In terms of network longevity, the proposed protocol outperforms the present standard as seen in Table 5. As the number of nodes in the network grows, more sensor nodes begin providing data at random as seen in Figure 5, and in the suggested protocol, such as existing and AODV, there is a considerable danger that a sensor node will die at any time. Only the best node is chosen to deliver data in the proposed protocol, resulting in a gain in network lifetime and battery life.

Table 5. No of nodes vs network lifetime.

Number of nodes	AODV	Existing	IDTSADR
	Network lifetime		
10	5	10	15
20	22	50	65
30	34	35	40
40	30	30	35
50	29	30	34

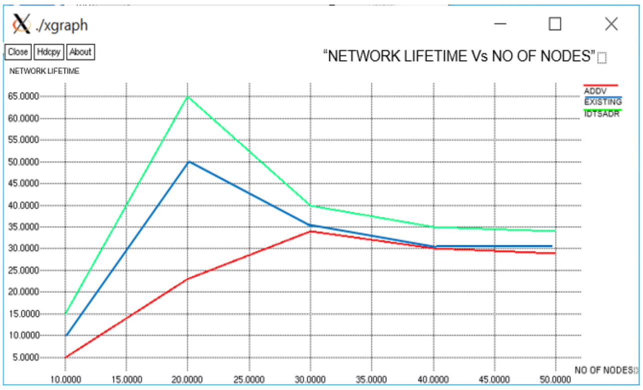

Figure 5. No. of nodes vs network lifetime.

4.6. Control overhead vs data rate

The network control overhead is increased as the data rate is increased, as seen in Figure 6. The control overhead of AODV is higher than that of IDTSADR as seen in Table 6. This results in lower control overhead traffic. The reductions of network control overhead at higher data rate are very significant.

Table 6. Control overhead vs data rate.

Number of nodes	AODV Control overhead	Existing	IDTSADR
25	92	94	95
35	68	60	55
45	64	60	55
55	60	50	42
65	60	50	40
75	50	38	30

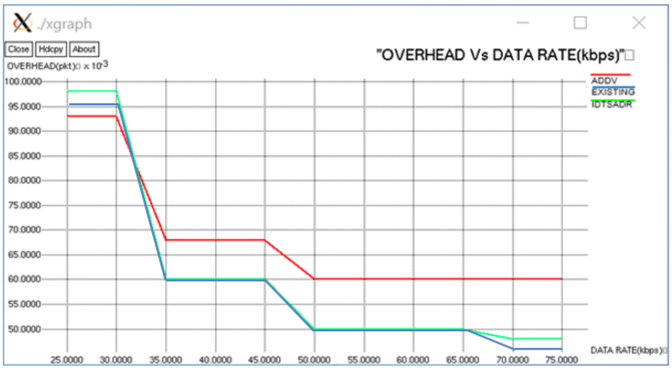

Figure 6. Control overhead vs data rate.

4.7. Energy efficiency vs speed

Figure 7 depicts the energy Efficiency of IDTSADR and AODV across mobility scenarios. It can be shown here that, regardless of the environment, the energy efficiency of both protocols increases fast as the speed is increased. In terms of energy efficiency, AODV outperforms IDTSADR at both low and high data rates as seen in Table 7.

Table 7. Energy efficiency vs speed.

Speed	AODV Energy efficiency	Existing	IDTSADR
0	20	10	0
10	60	40	24
20	64	68	61
30	65	68	62
40	70	71	62
50	70	72	64

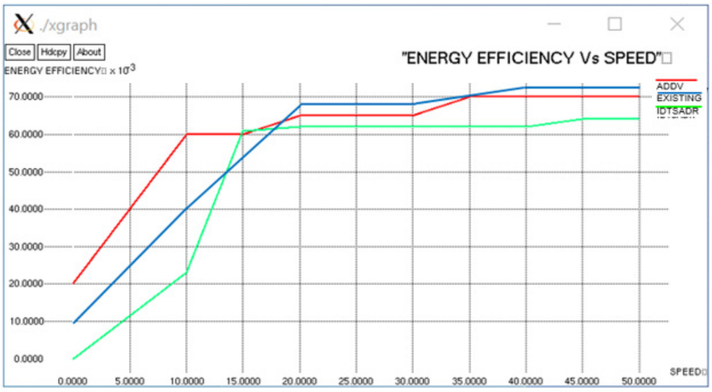

Figure 7. Energy efficiency vs speed.

Above Figures 1–7 shows the difference between our proposed approach and other existing technique and adhoc on demand vector protocol in No of nodes vs energy consumption, control overhead, packet delivery ratio and end to end delay, efficiency vs speed, and control overhead vs data rate. From the above results of Tables 1–7, we can conclude that the proposed method surpasses the existing methods, this difference obviously prolonged the lifetime of the network.

5. Conclusions

Because of evolving new technologies, IoT networks require a variety of safety systems. They are subject to assaults and require a variety of security solutions. Because of the sensor nodes' limited energy, compute capabilities, and storage resources, identifying appropriate cryptography is critical in WSN. IDTSADR is a novel energy-aware routing method suggested for WSN-IoT networks. IDTSADR fulfills critical IoT needs such as dependability, energy efficiency, attacker detection, and data aggregation. IDTSADR is an energy-efficient routing technique that discovers routes that use the least amount of energy for end-to-end packet traversal and improves malicious node detection. We presented a cryptography-based security framework for implementing the advanced encryption approach in IoT. Improving the algorithm's encryption and decryption elements, which currently exist and provide outstanding security. Our suggested algorithms took connection dependability into account and discovered more reliable routes, as well as more energy-efficient routes and extending network lifespan by finding routes with nodes with greater battery charge levels. From the above results, we can conclude that the proposed method surpasses the existing methods, this difference obviously prolonged the lifetime of the network.

For future research, to prolong the lifetime of the network, we are going to research by assessing the better energy-efficient routes and advanced cryptography for security in the WSN-IoT networks.

Conflict of interest

The authors declare that there is no conflict of interest.

References

1. G. Kaur, P. Chanak, M. Bhattacharya, Energy-efficient intelligent routing scheme for IoT-enabled WSNs, *IEEE Internet Things J.*, **8** (2021), 11440–11449. https://doi.org/10.1109/JIOT.2021.3051768
2. X. Zhang, H. M. Heys, C. Li, Energy efficiency of symmetric key cryptographic algorithms in wireless sensor networks, in *2010 25th Biennial Symposium on Communications*, (2010), 168–172. https://doi.org/10.1109/BSC.2010.5472979
3. G. H. Kumar, G. P. Ramesh, C. R. Murthy, Energy efficient multi-hop routing techniques for cluster head selection in wireless sensor networks, in *Further Advances in Internet of Things in Biomedical and Cyber Physical Systems*, **193** (2021), 3–9. https://doi.org/10.1007/978-3-030-57835-0_1
4. M. Esmaeeli, S. A. H. Ghahroudi, Improving energy efficiency using a new game theory algorithm for wireless sensor networks, *Int. J. Comput. Appl. Technol.*, **136** (2016), 1–4.
5. A. Shrestha, L. Xing, H. Liu, Modeling and evaluating the reliability of wireless sensor networks, in *2007 Annual Reliability and Maintainability Symposium*, (2007) 186–191. https://doi.org/10.1109/RAMS.2007.328105
6. Y. Duan, W. Li, X. Fu, Y. Luo, L. Yang, A methodology for reliability of WSN based on software defined network in adaptive industrial environment, *IEEE/CAA J. Autom. Sin.,* **5** (2018), 74–82. https://doi.org/10.1109/JAS.2017.7510751
7. K. Hemanth, G. P. Ramesh, Energy efficiency and Data packet security for wireless sensor networks using African Buffalo Optimization, *Int. J. Control Automation*, **13** (2020), 944–954.
8. L. Zhou, C. Ge, S. Hu, C. Su, Energy-efficient and privacy-preserving data aggregation algorithm for wireless sensor networks, *IEEE Internet Things J.*, **7** (2020) 3948–3957. https://doi.org/10.1109/JIOT.2019.2959094
9. R. Misra, C. Mandal, Ant-aggregation: ant colony algorithm for optimal data aggregation in wireless sensor networks, in *2006 IFIP International Conference on Wireless and Optical Communications Networks*, (2006), 1–5. https://doi.org/10.1109/WOCN.2006.1666600
10. M. Ebrahim, C. W. Chong, Secure force: a low-complexity cryptographic algorithm for wireless sensor network (WSN), in *2013 IEEE International Conference on Control System, Computing and Engineering*, (2013), 557–562. https://doi.org/10.1109/ICCSCE.2013.6720027
11. M. Rostami, K. Berahmand, E. Nasiri, S. Forouzandeh, Review of swarm intelligence-based feature selection methods, *Eng. Appl. Artif. Intell.*, **100** (2021), 104210. https://doi.org/10.1016/j.engappai.2021.104210
12. E. Nasiri, K. Berahmand, Y. Li, Robust graph regularization nonnegative matrix factorization for link prediction in attributed networks, *Multimedia Tools Appl.*, (2022), 1–24. https://doi.org/10.1007/s11042-022-12943-8
13. J. von Mulert, I. Welch, W. K. G. Seah, Security threats and solutions in MANETs: A case study using AODV and SAODV, *J. network comput. Appl.*, **35** (2012), 1249-1259. https://doi.org/10.1016/j.jnca.2012.01.019

AIMS Press

©2023 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0)