International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

IJISAE

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

Energy-Efficient and Intruder Detection Method Using IDTSML Technique

Kiruthika B.^{1,*}, Shyamalabharathi P.^{2}

Submitted: 23/05/2023 **Revised:** 16/07/2023 **Accepted:** 27/07/2023

Abstract: **Aim**:Wireless sensor networks are a rapidly developing technology. It has a wide range of applications. Because of its haphazard placement in the battlefield, it is vulnerable to a variety of attacks.

Objective: The dependability, privacy, and security of WSNs are the primary areas of study in our lab. To implement the encryption technique in SDN, we suggested a cryptography-based security mechanism.

Methods: We propose an IDTSML (Intelligent Dynamic Trust Secure Machine Learning) method for delivering security services to WSN mobos, and we analyze the associated energy and space costs. Secure Attacker Detection with Intelligent Dynamic Trust Routing is a revolutionary energy-aware routing strategy for Adhoc networks that will be proposed. IDTSML is an energy-efficient routing technique that determines the most energy-efficient end-to-end packet traversal paths while also increasing malicious node detection.

Conclusion: Improving the encryption and decryption parts of an existing technique, which paves the path for superior security.

Keywords*: Intruder detection, IDTSML, SDN.*

1 Introduction

In wireless sensor networks, small, low-cost, low-energy sensor nodes are dispersed in a field in a planned or random way to measure and react to events or phenomena there. Monitoring metrics such as free, pressure, and temperature in this area could be done in a physical location, or in a biological place for healthcare applications, such as remote blood pressure and heart rate monitoring. Depending on the application, the number of sensors placed might range from a few hundred up to several thousand. Sensing, processing, and communication are the three primary roles of sensor nodes in WSNs. Because communication uses more energy than other functions, developing an energy-efficient data transmission protocol is critical for balancing energy and extending network life [1] [2].

The wireless sensor network (WSN) has been extensively employed in a variety of sectors owing to its cheap cost, compactness, and multi-function qualities with the progress of efficient wireless communication & electronic information technology. However, most WSN nodes rely on battery power, and they are often deployed in unsupervised outdoor or more hazardous environments, where recharging the batteries might be difficult. The cost of deploying redundancy and replacing nodes is usually quite high as well. As a result, to reduce network energy consumption and extend network lifetime, an effective routing mechanism is necessary [4].

Security-related solutions for WSNs, such as authentication, key exchange, and safe routing, have been developed in order to prevent certain attacks. This is not enough, however, to protect WSNs from a wide range of assaults and threats [5]. Because of its widespread use in a wide range of applications, security has emerged as the most pressing concern in WSNIt is more difficult to secure sensor networks than MANETs due to the limited resources of individual sensor nodes. There are some resource limits, such as restricted memory, compute, and communication capabilities, as well as limited energy and power supply. This is why typical cryptographic algorithms cannot be

1 Research scholar, Department of ECE, Saveetha school of engineering, Saveetha institute of medical and technical sciences,Chennai,India
2 Assistant professor, Department of ECE, Saveetha school of engineering, Saveetha institute of medical and technical sciences, Chennai, India.
Corresponding Author: B. Kiruthika. Email: kiruthika.bk@gmail.com

used on sensor networks, resulting in a necessity for increased security in WSNs [6].

For the most part, prior research has relied on tried-and-true encryption and authentication procedures to provide a safe environment for cooperating sensors. Nonetheless, sensors are easily captured or compromised due to the unreliable wireless networks and unattended operation. The sensors must be inexpensive and resistant to manipulation. It would be simple for an insider attacker to fabricate a false event report in order to fool decision-makers, or to keep introducing false data in order to cause network disruptions, etc. [7]. As a result, we improve security in WSN by implementing our proposed IDTSML.

2 Literature Survey

By Edith C.H. Ngai and colleagues [8] Using a network of wireless sensors, they found a way to monitor for sinkhole assaults. There are two sections to the algorithm. Data consistency is used to establish a list of suspect nodes, and then traffic data is used to identify the intruder in the list. For those malicious nodes that try to mask the real intruder by interfering with detection, we also advised a series of upgrades. The performance of the proposed approach was evaluated using simulations. The outcomes proved the algorithm's efficacy and precision. They also claimed that the communication and processing overheads for wireless sensor networks are relatively low.

Khalid M. Abdullah et al. [9] As a result, they came up with an algorithm (HCA) that combines both public and symmetric cryptography's advantages. Using this method of data transmission security is both secure and efficient. As a whole, HCA offers a number of advantages, such as a simple design and good security. Reduces the number of packets that are dropped as wel. When the proposed hybrid algorithm was compared to a number of other algorithms, the HCA was found to offer the best overall results.

Choi, Kyung Jun, et al. [10] Several methods of molecular encryption are studied for use in wireless sensor networks using MICAz-type motes. Memory, CPU time, and power consumption of cryptographic algorithms have all been analyzed. For MICAz-type motes-based wireless sensor networks, the RC4 & MD5 cryptographic algorithms provided the best performance in terms of processing time. When it came to low-power wireless sensor network systems like MICAz-type motes, however, their cryptographic processing time was still too long. The usage of assembly-based code in the development of cryptographic algorithms is necessary to further minimise processing time.

Muhammad Hammad Ahmed et al. [11] A 160-bit ECC processor was proposed by them. In order to address the ever-increasing security requirements of wireless sensor networks, this processor was created. In the end, a space- and time-saving ECC processor was constructed. Small key sizes make Elliptic Curve Cryptography (ECC) an excellent choice. Because of their high level of security, crypto systems are both space and power efficient, despite their lower key size. Wireless sensor networks using Elliptic Curve-based asymmetric cryptosystem are described here in hardware terms. The elliptic curve field is defined over prime numbers.

RawyaRizk et al. [12] For WSNs, a robust hybrid security technique is presented. It is intended to address a number of issues, including practical implementation, quick reaction time, efficient calculation, and cryptosystem strength.The proposed THCA divides the plain text and then employs two separate ways to trap the invader. First, it employs both AES and ECC algorithms to take use of the benefits of mixing symmetric and asymmetric cryptography methodologies. Second, because XOR-DUAL RSA is more resilient and difficult to crack, it is used. The performance of THCA is compared to various well-known security methods. In return for a faster encrypt and decrypt time and a lower cypher text size, it gives higher security. As a result, processing overhead is reduced, and energy consumption is reduced. It has been proven to be resistant to several types of attacks.

Summary:

- More study is needed to identify better node features that address specific vulnerabilities, as well as to develop superior detection algorithms that take into account sensor node capabilities.
- To further minimise some of the existing computing time, optimization of the source code for cryptographic methods, including the usage of assembly-based code, is required.

- Our proposed solution will considerably increase the network's lifetime and security level.
- Our system's overall energy consumption is lowered, which improves network performance and extends network life.

3 Proposed System

Attacker Detection using Intelligent Dynamic Trust in a Secure Environment We propose a game-changing energy-aware routing technique for Ad hoc networks. IDTSML satisfies essential IoT needs such energy efficiency, dependability, data aggregation, and threat detection. We developed a unique energy-aware routing (IDTSADR) strategy for WSN-IoT networks [1] called IntelligentDynamic Trust Secure Attacker Detection Routing. IDTSADR Enhancing the existing encryption and decryption capabilities of the method is a step toward achieving maximum security. In this research, we introduce IDTSML, a routing strategy that minimizes energy consumption while improving detection of rogue nodes and allowing packets to go from end to end. We proposed a cryptography-based security methodology for implementing the Advanced encryption method in IoT. Raising the bar on a technology's encryption and decryption capabilities to make it more secure.

a. The proposed IDTSML includes algorithms that analyse the reliability of links in order to develop more reliable pathways.
b. Algorithms that look for the greatest energy-saving options
c. Algorithms that try to improve network lifetime by locating routes made up of nodes with higher battery energy.

3.1 IDTSML Energy-efficiency

Because packets are transported across an unreliable network, energy efficiency is a tough subject to research. A variety of energy-saving techniques have been presented. On the other hand, clustering routing methods are one of the most reliable protocols for energy efficiency, load balancing, communication cost, and transferring packets from the sink node to the base station (BS) [3].

Transmission energy efficiency ratio, node I index weight wb P(a), the degree of idleness G, the triangle membership function model Cidle(a), and the energy density factor J(a). Output: The following hop j

Algorithm1. IDTSML Energy-efficiency Algorithm

```
In the case of a = 1: The number of node's forward neighbour nodes is m /m. I
CNnext, j = 1 (i) ← Φ.
Take G's instruction and travel through m:
g(a) ← P(a), g(a) ← Cidle(a), g(a) ← J(a),
Find gmax← max, the highest g(a), and gmin, the lowest g(a).
Make a membership function that is triangular. Gt(g(a))
Create the BPA function by combining Gt(g(a)) with the associated weight.
mb (Aat ) ← G(g(a)), wb
For (j=1 to j≤m)
Imax= argmax (i=j, …m, abs(A[I,j])
If(A[i_max,j]=0
Compute x[n]=a[n][n+1]/a[n][n],
End
Display the result x[k]
Stop
```

The proposed method's energy efficiency improves when the volume of data transferred is lowered. According to the previous paragraph, data transmission is responsible for the majority of the energy use.

In order to convey data, a sensor must know the numerical ranges within which the system's condition is stable. To achieve this, the following steps must be taken on previously known data in order to build a model. On selecting a specific set of predicates from a larger set of predicates;sorting predicates in ascending order (the predicates in the tree have been placed randomly) and on communicating the predicate list derived from this to the sensor.

3.2 IDTSML Intruder detection

Detecting a sinkhole assault and tracking down the intruder are the next steps on our checklist, so stay tuned! As a starting point, we'll look at the example of an invader, a single malicious node (SH). In this simple scenario, we assume that the SH will drop or change control signals, but not the detection process, to halt sensor data collection. When dealing with a large number of malicious nodes, we'll discuss how to deal with them in the next section.

Algorithm2. IDTSML Intruder detection Algorithm

```
Input : Observe user behaviour over time ut, tf, ttf.
Output :Prediction result
ProcedureGET_LSTM(cot, Bi)
GET(tlt)
If ut>T
CALCULATE tf
If tf> G
Result= 1
Else if tf<G
cot->LSTM.predict(t)
if cot=0
gotobrnode:
if cot>0
Result=-1
end if
end if
R = R
for each v, 2S
if v not intrusion
R = R get (v)
end for
subroutine get (node u)
R’ = ϕ
if u didn’t get
say u is found
else
return ϕ
return Result
end Procedure
```

If the expected result of the compromised node detection algorithm is 1, it means the node is normal and has no odd patterns; The network may be vulnerable to an intruder or have a faulty node if the value is less than 1. When the result is 0, the node is considered to be damaged. When a node returns -1, it means it has been hacked and is sending data to a remote server. Simply sounding an alert if an unexpected value is found for the trust parameter is not sufficient for the proposed system. Cloud users' tf or ttf are determined at this point in the anomaly detection process by sending the data there. New users' trust levels are assessed, but those of long-term users are calculated based on the amount of data they've provided. When an insider attacker is found, the alarm is only triggered. The number of false warnings caused by misbehaving nodes is reduced to the absolute minimum.

3.3 Proposed Cryptography

Being based on both modular and elliptic curve arithmetic makes the Elliptic Curve Cryptosystem one-of-a-kind. Point multiplication, addition, and doubling are all part of elliptic curve arithmetic. This section will go through both of their backgrounds. The ECC equation defined over prime field is,

$$b^2 modp = a^3 + xa + y \quad (1)$$

Where,

$$4x^3 + 27x^3 modp \neq 0 \qquad (2)$$

All of the elements in the finite field fall inside the range [0, p-1]. Both a and b are fixed values, whereas x and y represent the axes.This implementation requires a prime number of length p, hence p should be 160 bits in length if the key size is to be a prime integer. Curves are employed in Certicom in SEC 2 for testing purposes.

The steps for ECC cryptography are as follows [6]:

1. To begin, any message M must be encoded as a point on the elliptic curve Pm.
2. 2As in Diffie-Hellman, choose a suitable curve and point G.
3. PA=nAG is generated by each user selecting a private key PA=nAnAG.
4. Take a random integer k and encrypt the values Pm, Cm=kG, and Pm+kPb.
5. Calculate the following to decipher Cm: Hence, Pm+kPb-nB(kG) = Pm+k(nBG)-nB(kG) = Pm+k(nBG)-nB(kG) = Pm

Algorithm 3. Cryptography Algorithm

```
Divide C into (C1 , C2);
t =k=128n(nk)ECC
Encryption Odd_Msg by ACC-128 using t
Return Encryption 1
create key (public and private)
Encryption Ev_Msg by ECC using (public)
Return Encryption 2
Let (f, y) public key.
do{
Oi = i=m i=m/2(Bi) sec ond part of plain text;
Vi =(xi) f mod y;
Si =ECC (Bi);
Pi =(Ri) XOR (si);
Ei = VD5 (Ci);
i++;
}
while(I <n);
Add Encryption3 to cipher
Add Encryption4 to cipher
Return cipher and s
```

The stages below are utilised for authentication and discuss the proposed technique for WSNs in detail.

- Both nodes send an encrypted message to each other.
- The feeble one requests a public key from the robust one.
- The feeble one then delivers its public key to that one.
- The robust one then sends an encrypted message to the frail one; and
- Authentication between nodes is successful.

Table I. No of Nodes versus End to Control Overhead.

No. of nodes	AoDV	Exist	IDTSADR	IDTSML
		Control Overhead (pkt)		
10	15	5	5	5
20	42	23	18	16
30	40	34	28	22
40	35	30	25	22
50	34	29	25	20

4 Graph & Result

The experimental hardware 377 consists of a 2.60GHz Intel Core i7-10750H processor, 8GB of RAM, the Windows 10 operating system, and a network simulator2.

4.1 No of Nodes Vs Control Overhead

Routing overhead is defined as the percentage of packets sent that include routing information to a total number of packets successfully sent. The results show that IDTSML is superior to other techniques in terms of No of Nodes versus End to Control Overhead.

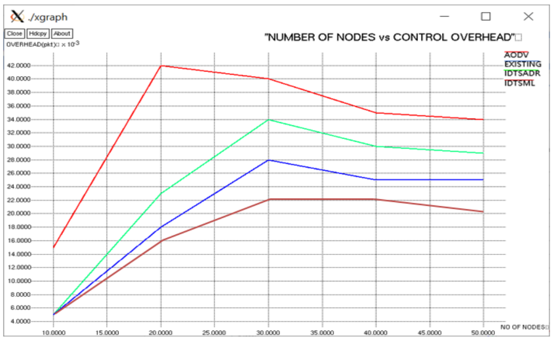

Fig 1. No of Nodes Vs Control Overhead

4.2 Energy Efficiency Vs Speed

Energy efficiency for various mobility situations, as shown in Figure 2. IDTSADR and AODV. This demonstrates that, at any given speed, both procedures exhibit a dramatic improvement in their energy efficiency. IDTSML is better than IDTSADR when compared with Energy Efficiency Vs Speed.

Table II. Energy Efficiency Vs Speed

Speed	AoDV	Exist	IDTSADR	IDTSML
	Energy efficiency			
0	20	10	0	0
10	60	40	24	10
20	64	68	61	55
30	65	68	62	55
40	70	71	62	55
50	70	72	64	60

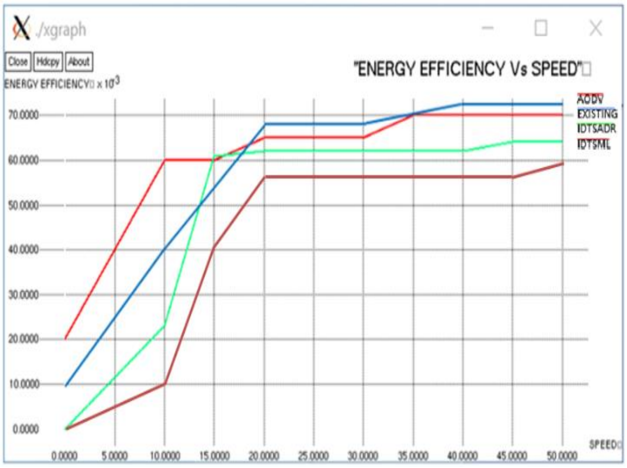

Fig 2. Energy Efficiency Vs Speed

4.3 No.of Nodes Vs Network LifeTime

Table 3 & Figure 3 below show the relationship between the number of nodes in the network and the current, AoDV, IDTSADR, and IDTSML values throughout the lifetime of the network, respectively. If we look at the IDTSML number in No of Nodes versus Network Lifetime, we can see that it is more than that of the other techniques, hence it is the superior choice. Then IDTSML have a higher Network Lifetime than other methods, so the WSN networks will have more Network Lifetime than other methods.

Table III. Network Lifespan vs. Number of Nodes

No. of nodes	AoDV	Exist	IDTSADR	IDTSML
	Network Lifetime			
10	5	10	15	20
20	22	50	65	65
30	34	35	40	45
40	30	30	35	45
50	29	30	34	42

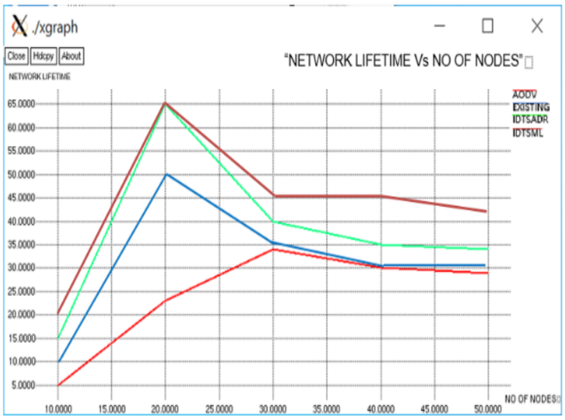

Fig 3. Network Lifespan vs. Number of Nodes

4.4 Throughput vs Speed

Figure 4 shows IDTSADR and AODV throughput (Kbits/sec) for various mobility types. Table 4 and figure 4 IDTSML is better than IDTSADR, existing and Advoc when compared with Throughput Vs Speed. From the value result IDTSML value inThroughput Vs Speed is low than other method, so it is better than other methods.

Table IV. Throughput Vs Speed,

Speed(ms)	AoDV	Exist	IDTSADR	IDTSML
	Throughput (x10^{-3})			
2	5	5	3	1
4	7	6	5	4
6	19	18	16	16
8	7	7	5	4
10	6	4	4	2

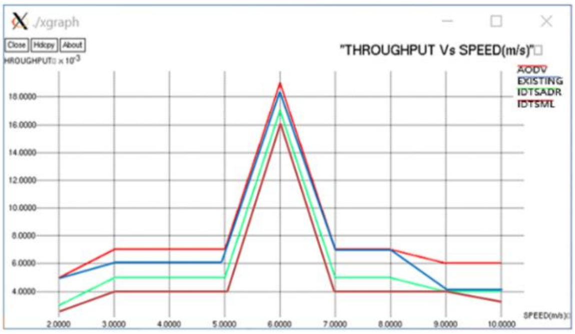

Fig 4. Throughput Vs Speed

4.5 No of nodes vs Throughput

From the table 5 and figure 5 result IDTSADR is better than AoDV and existing methods. From the value result IDTSML value inNo of nodes Vs throughput is low than other method, so it is better than other methods. And IDTSML is better than IDTSADR when compared with Number of nodes vs data transfer rate.

Table V. Number of nodes vs data transfer rate.

No. of nodes	AoDV	Exist	IDTSADR	IDTSML
	Network Lifetime			
10	5	5	5	5
20	28	26	24	22
30	20	24	16	14
40	24	22	18	16
50	24	22	18	16

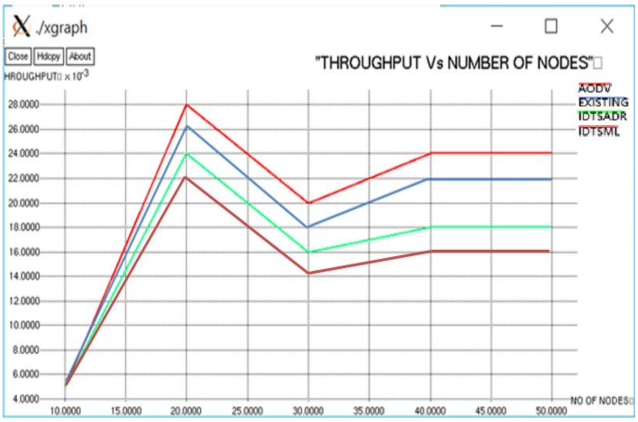

Fig 5. Number of nodes vs data transfer rate.

4.6 Delay Vs Data rate(kbps)

Average delays (m/sec) for several mobility models such as IDTSADR and AODV are shown in Figure 6. As the amount of data being sent grows, the average delay experienced by both protocols is expected to rise sharply. AODV has better latency performance than IDTSADR at both low as well as high data rates. From the table 6 and figure 6 result IDTSADR is better than AoDV and existing methods. From the value result IDTSML value inDelay Vs Data rate is high than other method, so it is better than other methods. And IDTSML is better than IDTSADR when compared with Delay Vs Data rate.

Table VI. Delay Vs Data rate

Data rate	AoDV	Existing	IDTSADR	IDTSML
	Delay (m/sec)			
25	73	72	78	79
35	68	70	60	62
45	68	65	60	62
55	60	52	50	45
65	60	54	50	45
75	55	48	43	42

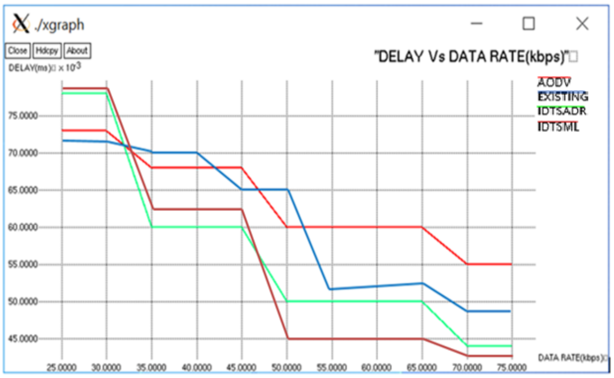

Fig 6. Delay Vs Data rate

4.7 No of Nodes Vs Packet Delivery Ratio

The packet delivery ratio is calculated by dividing the total number of packets transmitted by the transmitter by the total number of packets successfully received by the client. Table 4 & Figure 4 below show the relationship between the number of nodes and the existing, AoDV, IDTSADR, and IDTSML values for packet delivery ratio. Results show that IDTSML has a superior No. of Nodes to Packet Delivery Ratio than competing techniques.

Table VII. No of Nodes Vs Packet Delivery Ratio

Number of nodes	AoDV	ExisT	IDTSADR	IDTSML
	Packet Delivery Ratio (%)			
10	77	65	75	68
20	79	68	78	70
30	80	78	88	78
40	82	85	95	85
50	82	90	96	92

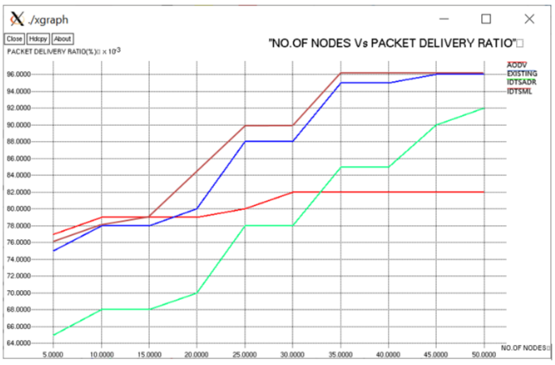

Fig 7. No of Nodes Vs Packet Delivery Ratio

4.8 Number of Nodes Vs End to End Delay

Mean time for a packet of data to travel from its origin to its destination. The queue for sending data packets and the time it takes to choose the best route are also taken into account. There was no consideration for data packets that failed to arrive at their destinations. The following table and graph show the relationship between the number of nodes and the existing, AoDV, IDTSADR, and IDTSML values for end-to-end delays. Compared to other approaches, IDTSML yields a lower number in No of Nodes versus End-to-End Delay, suggesting that it is superior.

Table VIII. No of Nodes versus End-to-End Delay

Number of nodes	AoDV	Existing	IDTSADR	IDTSML
	End to EndDelay (ms)			
10	15	15	8	8
20	45	23	13	12
30	40	24	15	13
40	35	29	20	16
50	35	26	20	16

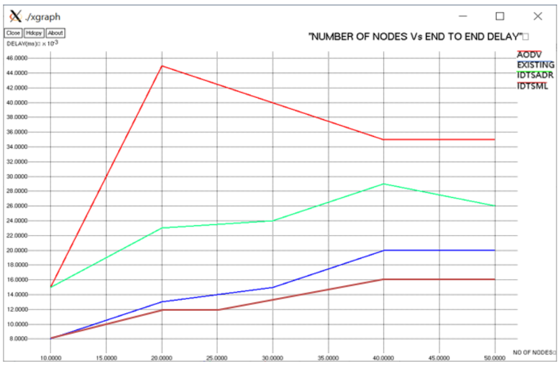

Fig 8. No of Nodes versus End-to-End Delay

4.9 No of Nodes Vs Energy Consumption

It represents a mean value for the total network energy spent by communication during a certain time frame and data rate. If we have a total communication expenditure of E and a total number of nodes of N, then the average communication expenditure is E/N (energy per node). One should use a protocol that requires less average communication energy on the whole. The following table and picture show the relationship between the number of nodes and the current AoDV, IDTSADR, and IDTSML values for energy consumption. The results show that IDTSML is superior to competing approaches by providing a lower No of Nodes vs. Energy Consumption value.

Table VIII. No of Nodes Vs Energy Consumption of existing, proposed and Adhoc on Demand Vector Protocol

Number of nodes	AoDV	Existing	IDTSADR	IDTSML
	Energy Consumption (J x 10^{-3})			
0	30	28.5	25	24
10	28	23.6	20	18
20	24	14	13	13
30	15	14	13	13
40	15	5.6	5	4
50	6.5	5.1	4.7	4

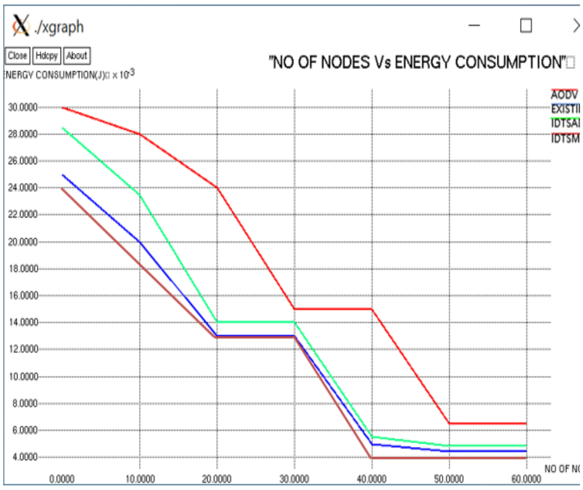

Fig 8. No of Nodes Vs Energy Consumption

The data above compares our suggested method to current approaches in terms of the number of nodes required to complete a task, the amount of energy required to do so, the amount of control overhead, the packet delivery ratio, and the end-to-end delay. Based on these findings, it's safe to say that the suggested approach is an improvement above the state of the art.

5 Conclusion

The technology behind wireless sensor networks is progressing quickly. It has a wide range of applications. Because of its haphazard placement in the battlefield, it is vulnerable to a variety of attacks. Energy consumption is regarded as the most significant difficulty in wireless sensor networks. In this research, we examine the space and power requirements for delivering security services to WSN nodes using our proposed IDTSML architecture. Our primary research goals center on making WSNs more trustworthy, secure, and private for their users. Intelligent Dynamic Belief Secure Detection of Attackers Routing is a revolutionary energy-aware routing strategy for Adhoc networks that will be proposed. IDTSML is an energy-efficient routing method that optimizes packet transmission costs and improves the ability to identify malicious nodes.

It was the major goal of this research to create a safe sensor protocol that would only allow authenticated nodes to communicate with each other, reducing network risk and expense. We proposed a cryptography-based security mechanism as a means of enforcing confidentiality in software-defined networks. Enhancing the security of a method by enhancing its encryption and decryption components. Our proposed solution will considerably increase the network's lifetime and security level. In our approach, overall energy consumption is lowered, which improves network performance and extends network life.

Future Scope:

There could be numerous potential paths for improving this work; As an example, we are improving our system's ability to identify suspect nodes in sinkhole attacks by creating more efficient statistical methods for identifying data discrepancy.

References

[1] Kiruthika, B. (2023). Intelligent dynamic trust secure attacker detection routing for WSN-IoT networks. *Mathematical Biosciences and Engineering*, *20*(2), 4243-4257.

[2] N. A. Morsy, E. H.AbdelHay and S. S. Kishk,"Proposed energy efficient algorithm for clustering and routing in WSN," *Wireless Personal Communications* 103, no. 3: 2575-2598, 2018.

[3] M. Shafiq,H. Ashraf, A. Ullah and S. Tahira, "Systematic literature review on energy efficient routing schemes in WSN–A survey," *Mobile Networks and Applications* 25, no. 3: 882-895, 2020.

[4] L. Tang, Z. Lu, and B. Fan. "Energy efficient and reliable routing algorithm for wireless sensors networks," *Applied Sciences* 10, no. 5: 1885, 2020.

[5] N. A. Alrajeh, and J. Lloret, "Intrusion detection systems based on artificial intelligence techniques in wireless sensor

networks," *International Journal of Distributed Sensor Networks* 9, no. 10: 351047, 2013.

[6] P. Singh and R. K. Chauhan, "A Survey on Comparisons of Cryptographic Algorithms Using Certain Parameters in WSN," *International Journal of Electrical & Computer Engineering (2088-8708)* 7, no. 4, 2017.

[7] F. Liu, X. Cheng and D. Chen, "Insider attacker detection in wireless sensor networks," In *IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications*, pp. 1937-1945, 2007.

[8] E. C. Ngai, J. Liu, and M. R. Lyu, "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks," *Computer Communications* 30, no. 11-12: 2353-2364, 2007.

[9] K. M. Abdullah, E. H. Houssein, and H. H. Zayed, "New security protocol using hybrid cryptography algorithm for WSN," In *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, pp. 1-6, 2018.

[10] K. J. Choi and J. I. Song, "Investigation of feasible cryptographic algorithms for wireless sensor network," In *2006 8th International Conference Advanced Communication Technology*, vol. 2, pp. 3-pp, 2006.

[11] M. H. Ahmed, S. W. Alam, N. Qureshi, and I. Baig, "Security for WSN based on elliptic curve cryptography," In *International Conference on Computer Networks and Information Technology*, pp. 75-79, 2011.

[12] R. Rizk, and Y. Alkady, "Two-phase hybrid cryptography algorithm for wireless sensor networks," *Journal of Electrical Systems and Information Technology* 2, no. 3: 296-313, 2015.

[13] Dinakar, J. R. ., & S., V. . (2023). Real-Time Streaming Analytics using Big Data Paradigm and Predictive Modelling based on Deep Learning . International Journal on Recent and Innovation Trends in Computing and Communication, 11(4s), 161–165. https://doi.org/10.17762/ijritcc.v11i4s.6323

[14] Christopher Davies, Matthew Martinez, Catalina Fernández, Ana Flores, Anders Pedersen. Predicting Dropout Risk in Higher Education Using Machine Learning. Kuwait Journal of Machine Learning, 2(1). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/170