Trust Based Cooperative Secure Routing Protocols for IOT

Abstract: **The Internet of Things has rapidly emerged and continues to create services, software, sensors-embedded devices, and protocols. IoT allows physical objects to communicate, exchange information, and make decisions while performing critical jobs. The Internet of Things is enhanced by wireless sensor networks, which serve as a continuous layer. To gain adoption and spread, Internet of things–based sensor networks must overcome serious general and specialized risks and technological hurdles. The main drawbacks of wireless sensor networks are insufficient resources. Internet of Things (IOT)-based Wireless Sensor Networks have issues in energy consumption, longevity, throughput, routing, and security. The goal of this effort was to enhance network longevity, throughput, packet latency/loss, and better encounters with hostile nodes. Consider wireless energy harvesting in the proposed three-layer cluster-based wireless sensor network routing protocol to enhance network lifespan. The proposed approach is a Trust based Cooperative Secure Routing Protocol (TCSRP) technique with security system to obtain malicious activities of objects and to slant them into blacklist. Finally, experiments were done to test the methodology. It outperforms most traditional routing protocols like AODV, DSR, and DSDV.**

Index Terms: **Internet of Things, Wireless Sensor Networks, Energy Consumption, Delay, Trust, Routing.**

I. Introduction

Internet of Things (IoT) has become a hot topic in academia and the data development industry. While becoming more universal, IoT supports a far-reaching portrayal of the shape with good physical world collaboration. Smart homes, wearable's, human services, automotive enterprises, business, and many more and Power Matrixes are among the prospective uses of IoT devices [1][2][3]. System security is crucial in the Internet of Things when you unite the target area unit via smart hubs and an online server. Dynamic and weak topologies on hidden systems raise unit area and two essential Internet system issues that demand thought. Keeping consistency across systems for the simplest end-to-end packet connection between Internet devices relies on issue direction and attention. To operate millions or billions of Internet devices worldwide, several problems from homogeneity, heterogeneity, capacity, mobility, guidance, and safety must be addressed [1]. In a certain setting, a person's or object's dependency on an object's behavior is fundamentally different from trust. Trust in internet stuff means a factor can perform what you claim without causing purchasers property harm. If someone is dependable, it's likely that their tasks will be accomplished safely and positively. The centers' conduct suggested assessing Internet confidence from 0 to 1 as a degree of debt. The trust and zero-confidence variables represent trust and distrust, respectively [1][4]. Making a secure offer on specifically developed systems increases protection and system competitiveness. For particularly designated distributed systems, trust management has three initial examination regions. This involves specific confidence-building and trust-building activities[5]. Creating IOT trust management requires precise calculations of the following:
Accuracy of Trust: Trust accounts must be successful with a trust figure even with the display of malicious positions. Malicious nodes Detection: The total area of the operations unit used to identify the harmful node must be forced to multiply in the neighboring centers in relation to its suspicious movement[1][6][7][8]. For example, the way you trust node X in node Y in some sense, by chance, means that the node X trusts that the node Y can work fully and can develop some activity under specific associated conditions.

II. Trust Protocol Description

There are many console protocols that can be used in IOT as shown in figure 1. In Trusted aware routing protocols [1][4], reliable test protocols employ an upgraded link state routing protocol that leverages trust tone information to adjust each node to assess the alternative axis's trust behavior. Provide a three-stage confidence-based response to preserve the OLSR routing protocol [8][10]. An examination of the notion shows linkages. This study proposes process abuse to increase solid OLSR; hence, data was included in the procedure. In the second phase, they must establish damage centers. The dependable OLSR enables you to think about each center, examine the consistency of many centers, and approve trust connections. The third stage replaces the second by identifying safe OLSR protocol weaknesses and solutions to prevent and isolate hazardous centers. This advice concerns faith that each alternate center is over. Prevention and separation of poorly performing centers are the main goals of advanced stock and countermeasure recreation. Prank centers use aversion structures and defenses to detect irregularities and hazardous centers. Based on system data, the center will recognize bad centers. OLSR signals like TC, greetings, and trusted thinking may be consistent with each focal center's system capabilities in anomaly detection. Clearly, this may be a "qtiperar" title = "to detect the detection of" id = "tip_1"> to detect center trust in advance, i.e., event detection messages for the board of directors: Trusted Protocols OLSR (Critical Biology and MPR) warns of alternative centers and trust connections by transmitting the assault site [10]. The character system is designed individually to verify message validity.

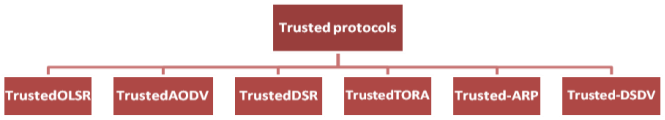

Figure 1. Trust based Protocols

Trusted AODV (TAODV) [9], a Safe Routing Protocol detects Internet attacks. Spread the heart to mix accounts

Received on 30.03.2023, Revised on 18.05.2023, Accepted on 26.05.2023.

and ensure mapping in this approach. The AODV proposes a secure TAODV Internet routing protocol. Message routing and an ADOV routing table use secure information that space observers may find. The creators have a portion of the directed conclusions and construct a low-weight contact routing each part of the new evaluation once the activity sets the stock in path detection, unlike the logical encryption procedures that execute the signature or confirmation era in each package of directives. Lines reduce overcrowding and ensure routing plan accountability. To match the safe model of the AODV (TAODV) system, developers protect remote systems in a bad or good way and introduce many uncertainties [11][12]. Instead of link layer routing protocol security, the originator refers to network layer security. Slash errors, a remote, unstable channel, and the ability to transfer affected data are exploited by internet-focused gadgets to communicate detachable components. Trusted AODV detects bypass neighbors' activities using two verification devices or interrupt recognition sections in the application or system layers. Since cardiac contents may reach the display, a system-layer demonstration center is planned. Alternative: After routing routes with other nodes, new columns in the node routing database record reliability assessments as negative or positive [9][11][14]. The Trusted DSR (TDSR) [16], reduces node packet degradation and manages positive/negative send confirmation. Contract trust is determined by information transfer or node receipt. Node ack (+ve ack) and nack (-ve ack) determine trust. The Trusted DSR network trust may be updated, written, and maintained securely from the display to the tank. Our network employs the simplest and most reliable secure node technologies to establish new routes from yours. This network's nodes sometimes update their record tables with adjacent node information and trust levels. Nodes feel satisfied and confident after receiving packets. When created from the node, trust drops. Every node may update its security values occasionally and maintain the trust value for surrounding nodes, helping find the most trustworthy way in the table [16].

The Trusted TORA (TTORA) [14], uses a special model for the IoT systems to be created, while it is not a true confidence framework with the major distribution systems associated with the certification authorities, along with an exceptional planned approach to control the disclosure of content and adapt it to the heart of unregulated systems deprived of foreign insurance. In support of this, the associated effort depends primarily on showing confidence in a highly redistributed way of creating a robust stand-alone system [17]18]. In terms of the light utility, the confidence model can be isolated in the three relevant parts: a) The confidence factor separates the confidence information from the events performed by the axis exactly. b) The name operator shares location inventory information with completely different centers within the system. c) The consolidated computation of the mix of confidence in the same center based on the information of trust and name operators. TORA is a schematic of many events that support the pass rate. Thus, the unsuccessful rate of these events is recorded in the tables, and the trusted factor uses the information generated when events normalize the method. Most events make a relationship of trust with all neighbors. Otherwise, the trust of the node disposing of the trust node is calculated to hurt, therefore, the name of the node. The top of the same three sectors maintains and updates the trust values that match the number of events. These values are applied in completely different positions to QoS, track maintenance and path discovery.

Trust Aware Routing Protocol (Trusted-ARP) [18], used to protect a safe way in Internet system things. This protocol is integrated inseparably with the guidance protocol each time each center assesses the level of confidence of its neighbors in the light of the meeting of characteristics and determining the visual path of those attributes. The measured security features show that the hub trust level on a very specific path includes: a) the computer code pattern, tool layout, main battery, customer registration, and separation order. Each center evaluates the purpose of its neighbors' trust, which can be seen above the characteristics and integrated by recording the subsequent jump center into the general accounts of the most restrictive cycle. This protocol uses two basic features, such as battery power and programming settings. In the Internet things, the battery management can be operated by capacitors of limited quality. Each center uses its energy to send and receive it, as well as to maintain it as a transformer by updating the causation and message directives. Thus, logical methods of encryption encrypt and increase security, and increase the energy usage of the tool. Energy can be an important feature designed to assess the level of confidence of a tool, so the design of the computer code includes the coding capability of a tool [18][19]. To maintain confidentiality, convenience and integrity, distinct encryption systems are expected. Some rely on symmetric encryption and remain in non-symmetric encryption. Each hub receives a reciprocal ambiguous key or an open key set that depends on the type of logical cryptosystems. The safe path between the supply and the sink is visible to the level of certainty adopted by the consumer or an application associated with these characteristics.

The Trusted Destination Sequenced Distance Vector (T-DSDV) [15], the routing protocol for internet objects can be a proactive protection protocol. In the proactive routing protocol, each axis maintains the path of the front edge of each different axis within the system, and routing information is sent at fixed time intervals throughout the system. Keeping in mind that the main goal is to protect the network routing table, once the path detection process has been initiated, the avant-garde estimates, for example, the transport capacity and the change in the vitality of the residue will be observed. The routing table is updated in each center by finding the variation in routing information on all current targets with the number of centers for the goal [20].

III. TRUST BASED COOPERATIVE SECURE ROUTING PROTOCOL

Our enthusiasm for this work is the guidance in Internet of Things. The directive includes the activity method. Fake packets are sent and controlled within the system, allowing a similar adjustment of the packages from the display to the ultimate goal. In addition, with the interconnection of

Received on 30.03.2023, Revised on 18.05.2023, Accepted on 26.05.2023.

billions of devices within the system, the big problem is that by making sure the Internet setup objects from completely different attacks, for example, Range, Selective Redirection, Sink, Flood-flow, Wormhole, Denial of Service, Black-hole, A variety of versions, Sybil and identity attacks. These attacks have a tendency to destabilize the topology and guidance forms that are in Internet objects systems. The agreement seeks to deal with related aggressions along with grade attacks, Black-hole attacks, Sybil attacks and selective reorientation, as they prove to pose a significant risk to the stability of Internet systems [3]. We tend to present here the preparatory setup for Secure Trust, a secure Trust-based Cooperative Secure Routing Protocol (TCSRP) for internet objects. This provision combines the thinking of trust between the various centers of Internet devices things and quality limits have an impact on the centers within the system. Trust can be one of the characteristics that shows the degree of conviction one center has for another, and therefore the need to implement it as desired. Secure Trust organizes and makes efforts to identify and limit the four routing attacks recorded at the top of Internet systems. Trust in Internet of things becomes a real tool for safe policies, keeping in mind that these centers are not connected they do not have a previous connection and need to align an appropriate level of trusted connections to convince the router between them (Internet of Things). These centers are heterogeneous by nature and may be necessary for mobility in heterogeneous systems.

Performance of the Trust-Based Cooperative Secure Routing Protocol (TCSRP) is compared with different algorithms such as AODV, DSDV, and DSR. We evaluate performance according to the following criteria:

Average Energy Consumption: The average energy consumed by the nodes in receiving and sending the packets. Packet Delivery Ratio: It is defined as the number of data packets received successfully with the total number of packets sent. Average end-to-end delay: It includes the localization delay, tracking delay and transmission delay. Estimation Error: It is the estimation error, which indicates how close the estimated location is to the actual location.

IV. RESULTS ANALYSIS

This simulation is obtained by taking 50 to 100 nodes and a sink node that is used to send the information. Here we have a tendency to use three protocols known as AODV, DSR, and DSDV to connect the network. These are used to send the type of information to the destination and verify the performance of the contract. The proposed work was simulated in NS2. The proposed simulation parameters for work are shown in the following table. The proposed work is compared with current AODV, DSDV, and DSR routing algorithms. The end-to-end delay parameters, packet delivery ratio, power consumption and rated error are evaluated for the proposed Trust-Based Cooperative Secure Routing Protocol (TCSRP) technology and compared with the previous routing algorithms.

A. Based on Transmission Range:

The range of transport ranges from 150 meters to 600 meters and performance is assessed for all techniques. Tables show the results obtained for TCSRP and all current techniques for changing the range.

TABLE I.
Transmission Range Vs Discovery Delay

Range	Discovery Delay			
	TCSRP	AODV	DSDV	DSR
150	2.862352	3.128652	3.658621	3.856472
250	3.254861	3.401565	3.726587	3.923451
350	3.399581	3.644742	3.835456	4.015245
450	3.502457	3.914565	4.125876	4.315487
600	4.012548	4.212586	4.425684	4.623457

Based on the transmission range, the transmission range ranges from 150 meters to 600 meters and performance is evaluated among several techniques.

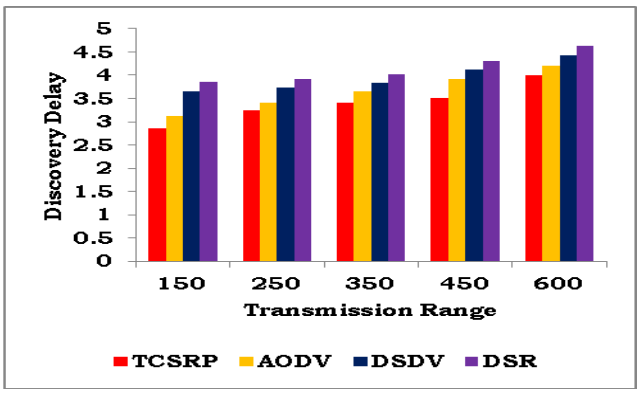

Figure 2. Discovery Delay Vs Transmission Range

The previous figure shows the delay for all TCSRP, AODV, DSDV, and DSR techniques when increasing the range. Because TCSRP uses node factors for the site, the delay is reduced by 8.75% compared to other routing algorithms.

TABLE II.
Transmission Range Vs Delivery ratio

Range	Delivery Ratio			
	TCSRP	AODV	DSDV	DSR
150	0.97254	0.929097	0.949697	0.969291
250	0.96544	0.843206	0.733156	0.638156
350	0.90258	0.811294	0.731384	0.605284
450	0.93534	0.828042	0.798042	0.768042
600	0.86237	0.755661	0.725868	0.695863

Received on 30.03.2023, Revised on 18.05.2023, Accepted on 26.05.2023.

Range	Estimation Error			
	TCSRP	AODV	DSDV	DSR
150	0.08	0.12	0.14	0.17
250	0.11	0.14	0.16	0.19
350	0.15	0.19	0.23	0.28
450	0.16	0.23	0.28	0.32
600	0.21	0.25	0.29	0.34

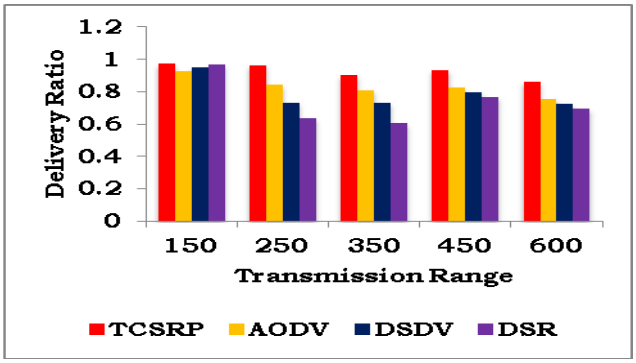

Figure 3. Transmission Range Vs Delivery ratio

The figure 3, illustrates the packet delivery relationship between TCSRP, AODV, DSDV, and DSR. As shown in Figure, the TCSRP delivery rate is 10% higher than other techniques. The table shows the percentage of TCSRP improvement compared to other technologies to change the transmission range.

TABLE III.
TRANSMISSION RANGE VS ENERGY CONSUMPTION

Range	Energy Consumption			
	TCSRP	AODV	DSDV	DSR
150	6.15185	6.77162	7.17182	7.57166
250	6.23253	6.78122	7.28128	7.68152
350	6.26334	7.35327	7.85382	8.25387
450	6.26572	7.24892	7.74297	8.74286
600	6.25731	7.44831	7.94839	8.34733

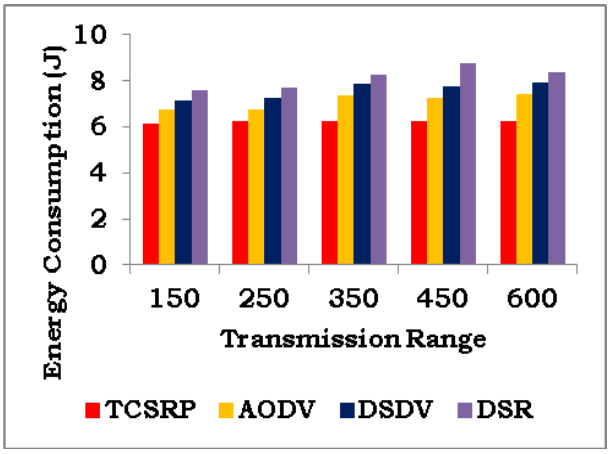

Figure 4. Transmission Range Vs Energy Consumption

From the previous figure, it was observed that when the transport range increases, the energy consumption increases slightly. But the energy consumption of TCSRP is 10% lower, compared to current techniques, where pheromone is created per intermediate node according to the remaining energy.

TABLE IV.
TRANSMISSION RANGE VS ESTIMATION ERROR

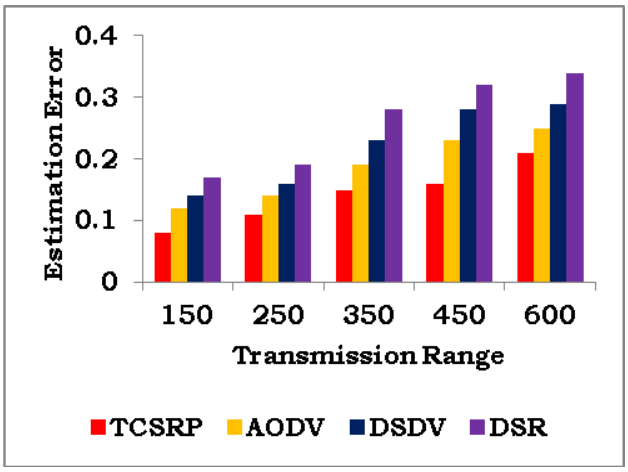

Figure 5. Estimation Error Vs Transmission Range

The graph above illustrates the estimation error that occurred during the TCSRP, DSDV, AODV, and DSR technologies. The figure shows that the grading error is 22% lower in TCSRP compared to the current techniques, since the fixed nodes are accurately installed using MDS.

TABLE V.
PERCENTAGE WISE IMPROVEMENT OF TCSRP FOR VARYING TRANSMISSION RANGE

Range	Delay (%)	Delivery ratio (%)	Energy (%)	Error Rate
150	6	5.6	10	31
250	8.1	14	8	26
350	8.4	12	12.3	23
450	13.7	10.1	14.6	20
600	12.5	8.9	15.8	14

Received on 30.03.2023, Revised on 18.05.2023, Accepted on 26.05.2023.

B. *Based on Object Speed*

To analyze the performance of tracking the objectives of both technologies in terms of moving targets, the moving target speed varies from 5 m / s to 25 m / s.

TABLE VI.
RESULTS FOR VARYING TARGET SPEED

Speed (m/s)	Delay			
	TCSRP	AODV	DSDV	DSR
5	0.810509	1.215127	2.318123	3.918182
10	3.628091	5.756392	7.556991	8.956328
15	6.205768	8.799213	9.989314	11.18032
20	8.887619	10.36113	11.96123	12.95173
25	9.886632	11.19862	12.98872	13.98152

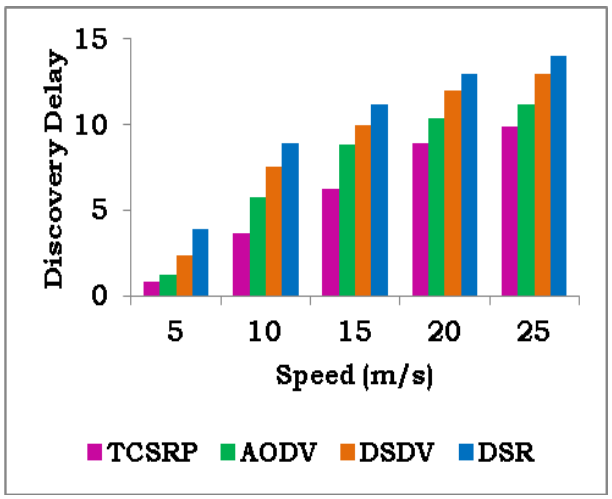

Figure 6. Discovery Delay Vs Speed

The figure shows the delay for all TCSRP, AODV, DSDV, and DSR technologies. When the target speed increases, the site delay becomes linear. However, the delay is 28% lower for TCSRP, compared to other techniques, as shown in Fig. This is due to the fact that TCSRP technology is used in the process of goal setting and tracking.

TABLE VII
SPEED VS DELIVERY RATIO

Speed (m/s)	Delivery Ratio			
	TCSRP	AODV	DSDV	DSR
5	0.970603	0.760201	0.590285	0.370219
10	0.886556	0.594551	0.304321	0.298953
15	0.685872	0.475932	0.386271	0.295581
20	0.490817	0.380618	0.220714	0.191589
25	0.389142	0.279172	0.198242	0.099152

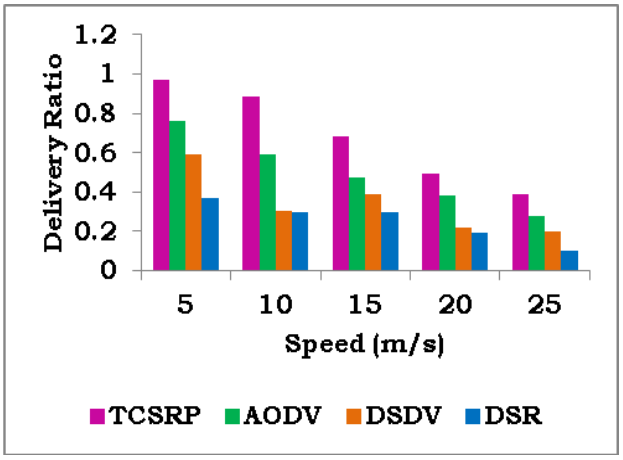

Figure 7. Delivery Ratio Vs Speed (m/s)

The figure shows the delivery relationship for all TCSRP, DSDV, DSR and AODV. Delivery rate decreases with increasing speed. The figure shows that the delivery rate for TCSRP is 38% higher than other existing technologies.

TABLE VIII.
SPEED VS ENERGY CONSUMPTION

Speed (m/s)	Energy Consumption			
	TCSRP	AODV	DSDV	DSR
5	5.46117	6.598571	7.590215	8.470211
10	5.54286	6.832073	7.304521	8.698955
15	5.68487	6.864781	7.388241	8.595588
20	5.79875	6.872556	7.290624	8.691587
25	5.87272	6.894585	7.197243	8.899155

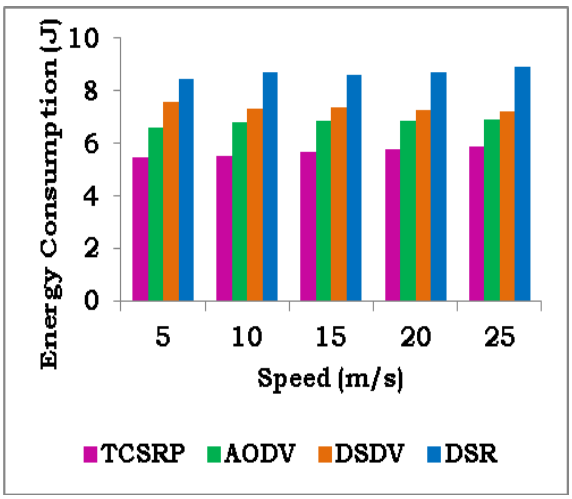

Figure 8. Energy Consumption Vs Speed

Figure shows energy consumption for all techniques presented in the graph. From the chart, it was observed that when the speed increases, the energy consumption increases slightly. It shows that energy consumption is 15% less for TCSRP, compared to other techniques, where the pheromone of each intermediate node is created based on the remaining energy.

Received on 30.03.2023, Revised on 18.05.2023, Accepted on 26.05.2023.

TABLE IX.
SPEED VS ESTIMATION ERROR

Speed (m/s)	Estimation Error			
	TCSRP	AODV	DSDV	DSR
5	0.04	0.07	0.10	0.17
10	0.05	0.09	0.15	0.19
15	0.07	0.1	0.20	0.28
20	0.09	0.14	0.25	0.33
25	0.11	0.18	0.33	0.35

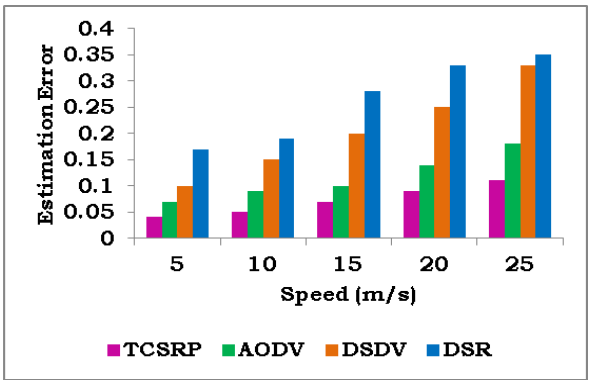

Figure 9. Speed Vs Estimation Error

The figure shows that the estimation error occurred during the localization of all TCSRP, DSDV, DSR and AODV techniques, when the speed increased. The figure shows that the Estimation error is 41% lower in TCSRP than in the DSR, since the fixed nodes are accurately installed using MDS.

TABLE X.
THE PERCENTAGE WISE IMPROVEMENT OF TCSRP OVER DSR FOR VARYING THE TRANSMISSION RANGE

Range	Delay (%)	Delivery ratio (%)	Energy (%)	Error Rate
5	35	24	16	51
10	38	36	18	52
15	32	54	16.3	40
20	15	39	14.6	30.91
25	18	44	13.8	36.3

III. CONCLUSIONS

This paper proposes the trust-based cooperative secure routing protocol (TCSRP) using connection points. Synthetic trust packets in Internet objects are used to sample possible pathways between sources and recipient nodes to acquire routing information. When doing the Bernoulli test, we selected anchor points and continue until the minimum anchor points are reached. Using route detection, our TCSRP finds the optimum path. After this route discovery technique, each node's routing database has the ideal path between binding nodes. Using binding node proximity information, the shortest jump distance is estimated to expand network coverage. Multi-Dimensional Scaling estimates anchor point locations after shortest route distance. Anchor points operate the site when the target sensor node is detected. Tracking the target site using trust node proxies sends data to the sink. Anchor point detection and deployment density decrease with on-demand localization. The suggested technique offers a lower delay and greater energy usage against package delivery, according to simulations.

REFERENCES

[1] Ammar M, Russello G, Crispo B. Internet of things: a survey on the security of IOT frameworks. *Journal Information Security Appl*. 2018;38: 8–27.

[2] S Mekala, KS Chatrapati "Present State-of-the-Art of Continuous Neighbor Discovery in Asynchronous Wireless Sensor Networks", *EAI Endorsed Transactions on Energy Web* 8 (33), 2021.

[3] S Mekala, KS Chatrapati "Continuous Neighbour Discovery with Efficient Asynchronous Wake-up Schedules in Wireless Sensor Networks" *Journal of Theoretical and Applied Information Technology*, 99 (16), 2021.

[4] Khan ZA, Ullrich J, Voyiatzis AG, Herrmann P. A trust-based resilient routing mechanism for the internet of things. *In: Proceedings of the 12th International Conference on Availability, Reliability and Security*. ACM; 2017. p. 27.

[5] Airehrour D, Gutierrez JA, Ray SK. Sectrust-rpl: a secure trust-aware rpl routing protocol for internet of things. *Future Generation Computer System*, 2018.

[6] Airehrour D, Gutierrez J, Ray SK. "Securing rpl Routing Protocol from Black-Hole Attacks using a Trust-based Mechanism," *In: 2016 26th International Telecommunication Networks and Applications Conference (ITNAC)*. IEEE; 2016. p. 115–20.

[7] Hashemi SY, Aliee FS. Dynamic and comprehensive trust model for IOT and its integration into rpl. *Journal Super computer* 2018:1–30.

[8] Lahbib A, Toumi K, Elleuch S, Laouiti A, Martin S. Link reliable and trust aware rpl routing protocol for internet of things. *In: 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)*. IEEE; 2017. p. 1–5.

[9] Priya Sethuraman, P.; Kannan, N. Refined trust energy-Ad Hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET. *Wireless Networks* 2017, 23, 2227–2237.

[10] Ahmed, A.I.A.; Ab Hamid, S.H.; Gani, A.; Khan, S.; Khan, M.K. Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open research challenges. J. Netw. Comput. Appl. 2019, 145, 102409.

[11] Alamsyah, HeryPumomo, "Performance Comparative of AODV AOMDV and DSDV Routing Protocols in MANET Using NS2", 2018, 286-289.

[12] NirbhayChaubey, A. Jani, 2015, "Performance Analysis of TSDRP and AODV Routing Protocol under Black Hole Attacks in MANETs by Varying Network Size",pp. 320-324.

[13] Sridhar Subramanian, "Efficient Routing in Mobile Adhoc Networks Emphasizing Quality of Service by Trust & Energy based AODV ", 2015, 1-7.

[14] D. K Jha,S. Jain, "Network Performance Optimization based on AODV Routing in MANET", 2014, 1128-1132.

[15] Manjunath M "Spatial DSDV (S-DSDV) routing algorithm for mobile ad hoc network", 2015, 625-629.

[16] Julia Rahman, Md. Khaled Ben Islam, "Comparative analysis the performance of AODV, DSDV and DSR routing protocols in wireless sensor network", 2012, 283-286.

Received on 30.03.2023, Revised on 18.05.2023, Accepted on 26.05.2023.

[17] Alwi M, B. King, "Dynamic-power AODV routing protocol based on node density", 2012, 95-100.
[18] H.A. Esmaili, “Performance Analysis of AODV under Black Hole Attack through Use of OPNET Simulator”, 2011, 49-52.
[19] Jianwei Liu, Rashid Sangi, "AODV routing protocol under several routing attacks in MANETs", 2011, 614-618.
[20] A. Agarwal,N. Chaubey, “Performance Analysis ofAODV, DSDV and DSR in MANETs”, 2011, 167-177.

Received on 30.03.2023, Revised on 18.05.2023, Accepted on 26.05.2023.