Intelligent Addressing and Routing Strategy for Smart Devices on Interactive Internet of Everything Platforms

Dr.Pradheep Kumar .K
Assistant Professor,
Dept of CSE, BITS Pilani
pradjourn@gmail.com

Dr. Srinivasan. N.
Professor, Department of CSE
Rajalakshmi Engineering College, Chennai 602105
srinivasan.n@rajalakshmi.edu.in

Dr.Murali Bhaskaran
Professor, Dept. of CSE
Rajalakshmi Engineering College, Chennai 602105
muralibhaskaran.v@rajalakshmi.edu.in

Abstract **- In this work a unique addressing scheme to identify smart devices on IoT platforms has been proposed. These devices are interconnected by minimizing the hop count distance. In an interactive environment where devices need to communicate only when required and exchange information is essential to ensure high reliability. The routing strategy also prevents hacking attacks by malicious access to the devices. The Interactive Internet of Everything (IIoE) routing strategy improves reliability and reduces communication cost by 29% and 25% respectively, compared to the conventional routing protocol strategy.**

Keywords – Qubits, Quantum Communication, Quantum Encoder, Sequence Analyser, Crosspoint, Crossbar router, OMNet++

I. INTRODUCTION

In today's digital world with the advancement of technology it becomes essential to have reliable addressing scheme for all devices to ensure that no unauthorized communication between devices takes place. Further such a communication strategy incurs high communication costs. In order to reduce this, cost we need to have a proper communication scheme. In real world there are several smart embedded devices ranging from mobile phones to cars, household appliances like washing machines, Air conditioners, etc. To ensure connectivity among these devices and prevent malicious access by hackers is essential to ensure high reliability.

In case of a failure of a particular communication link a rerouting strategy would be essential to ensure timely communication. When a malicious access is made a Quantum Communication mechanism verifies if it is a legitimate request.

The Quantum Communication mechanism compares the qubit sequence orientation of the user input generated with the sequence provided by a Quantum Encoder. The qubit has an orientation. When the orientation matches the sequence of the quantum encoder access is granted else it is denied. If a malicious access is made the orientation of the consecutive qubit would not follow the sequence generated by the quantum encoder which would deny access and intimate the administrator. When the request is not legitimate the Communication circuit declines access to the device.

The devices may be located geographically over a large area which may confine to a particular city, across cities and across countries. In such conditions an appropriate wireless mechanism would be required to ensure high reliability of the system.

The devices need to be registered with a routing mechanism which grants legitimate access to a device. In case of a malicious access being made the same needs to be intimated to the user revealing the source of the access. Such identifications are made by using Honeypots which act as traps to the intruder and relay the location coordinates of the intruder to the system administrator.

This could be identified by using qubits which have a particular orientation. When an intruder raises a qubit alert the orientation sequence is disturbed and the entire transaction request gets aborted. The IIoE routing strategy improves reliability and reduces communication cost by 29% and 25% respectively, compared to the conventional routing protocol strategy.

The Paper is organized as follows: Section 2 conducts a survey on the existing approaches for IoT devices. Section 3 proposes the communication model for Interactive Internet of Everything platform. Section 4 explains the simulation environment and discusses the results in detail. Section 5 concludes the work and Section 6 explains the scope of future work in this regard.

2. LITERATURE REVIEW

The Integration of different routing algorithms were discussed by Mishra et al in [1]. The optimization of Network strategies were also discussed. An optimization of energy was attempted by Fakher et al in [2]. The different assumption on homogeneity were also discussed. The different distance and cluster based routing strategies were explained by Shende et el in [3]. Content based routing strategies were also highlighted. The concept of blockchain and smart contract and the required optimisations in the network were also discussed by Sahay et al in [4]. A heterogeneous network model and its associated optimisations were also discussed by Shafique et al in [5]. The link efficiency for each node and the sensors were analysed by Dawood et al in [6]. The routing strategy optimization were analysed and the critical path was determined by Fathallah et al in [7]. Intrusion avoidance was demonstrated by analyzing malicious nodes by Haseeb et al in [8]. This information was obtained by Radio Frequency tags. A threat assessment

was carried out by computing an objective function for the routing strategy by Yasser and Shams in [9].

Maximising data collection and energy optimization was carried out by Ashfaq et al in [10]. The simulation of routing topology in nodes was carried out using OMNet++ as discussed by Varga in [11]. The optimization of discrete energy levels were explained by Varga in [12].

III. Proposed Work:

The Interactive Internet of Everything Platform consists of 2 Modules as shown in Fig 1.

- Authentication Module
- Communication Module

A. Authentication Module:

The function of the authentication module is to ensure the authenticity of the users request. As illustrated in Fig 2, When a user raises a request the same is converted to a set of qubits. The qubits are generated by a quantum encoder. The generated qubits are combined in the received order by a qubit aggregator and this is sent to a sequence analyser. Each qubit has an orientation. When the orientation sequence is correct the request is sent to the communication module. When a malicious user raises a request the orientation of the generated would not match with the sequence of the last qubit generated by the quantum encoder and the sequence analyser would start tracking the source of the requestor. It would then transmit this information to the administrator.

B. Communication Module:

The devices are interconnected as shown in the fig 3 using a crossbar topology. Each device is connected by a cross point switch. The cross point switches are controlled by a cross bar router. The total number of cross points depend on the number of devices. When the sequence analyser sends a request to the crossbar router the concerned cross point is enabled and a handshake signal is sent to the concerned device and data is sent to the device. At any point of time only a minimal number of cross points are enabled to prevent blocking in the network.

Fig 1. Block Diagram of Interactive Internet of Everything Platform

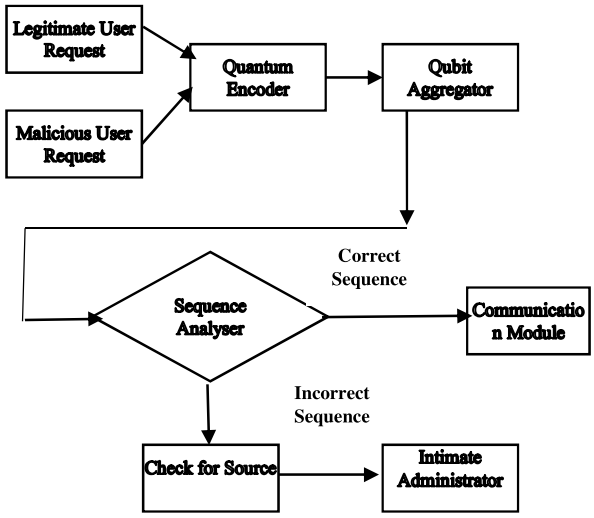

Fig 2. Block Diagram of Authentication Module

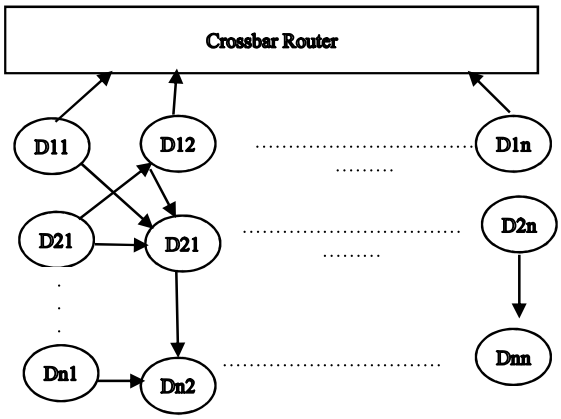

Fig 3 . Block Diagram of Communication Module

Each device is identified by a Smart IP address as shown in Fig 4 which has the following fields

Device Type	Device ID	Location Coordinates

Fig 4. Smart IP Address format

The Device Type identifies the device category of the IoT device which could be an appliance. The Device ID is the unique identifier which identifies its position in the communication network. The location coordinates identifies the location where the device or appliance is available.

The Communication module also maintains a routing table which has configured routes connecting each device and the associated communication cost for each route.

IV. Simulation Results:

The communication module has been simulated using OMNet++ simulator. The number of devices were varied upto 90 and number of requests were varied upto 170. The performance has been assessed based on the following metrics:

- Reliability
- Communication Overhead

The crossbar network was simulated using OMNet++ and the screenshot of the same has been shown in Fig 5.

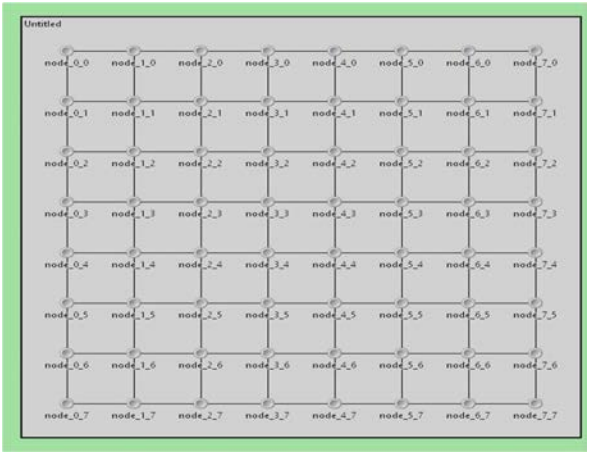

Fig 5. Output Screenshot on Simulation using OMNet++

A. Reliability:

The reliability is measured as the number of legitimate requests being granted by the communication module

TABLE I.
COMPARISON OF RELIABILITY (CONVENTIONAL ROUTING VS IIOE)

S.No.	Number of Devices	Total Number of Requests	Reliability		Improvement (%)
			Conventional Routing Topology	IIoE Platform topology	
1	10	10	7	9	28.57
2	15	20	13	17	30.77
3	20	30	22	28	27.27
4	25	40	29	39	34.48
5	30	50	37	48	29.73
6	35	60	44	58	31.82
7	40	70	52	68	30.77
8	45	80	59	78	32.20
9	50	90	69	88	27.54
10	55	100	78	98	25.64
11	60	110	83	108	30.12
12	65	120	90	118	31.11
13	70	130	101	128	26.73
14	75	140	110	139	26.36
15	80	150	116	148	27.59
16	85	160	123	158	28.46
17	90	170	132	168	27.27
18	95	180	141	176	24.82
19	100	190	148	188	27.03
Average	55	100	77	98	28.86

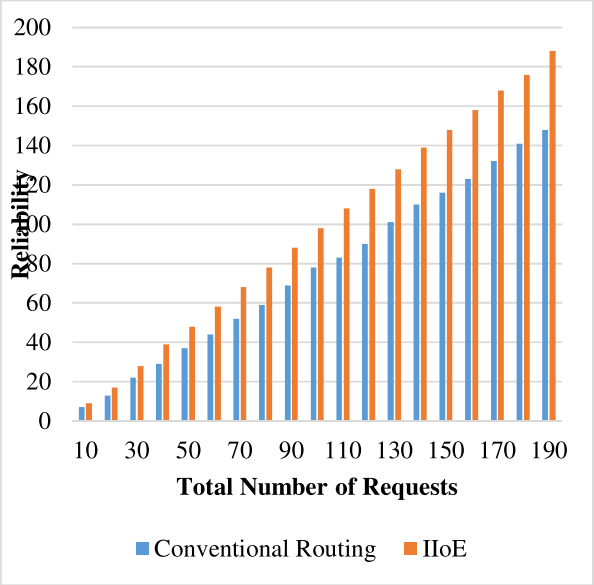

Fig 6. Plot comparing the Reliability (Conventional Routing Vs IIoE)

It could be observed from table 1, fig 6 and fig 7, for an average of 55 devices and 100 requests the improvement in reliability is around 29%. The reliability obtained using the IIoE platforms is 98 requests, compared to the conventional routing strategy which is 77 requests. A maximum of 188 requests are handled using the IIoE platform, compared to the conventional routing strategy which is 148 requests.

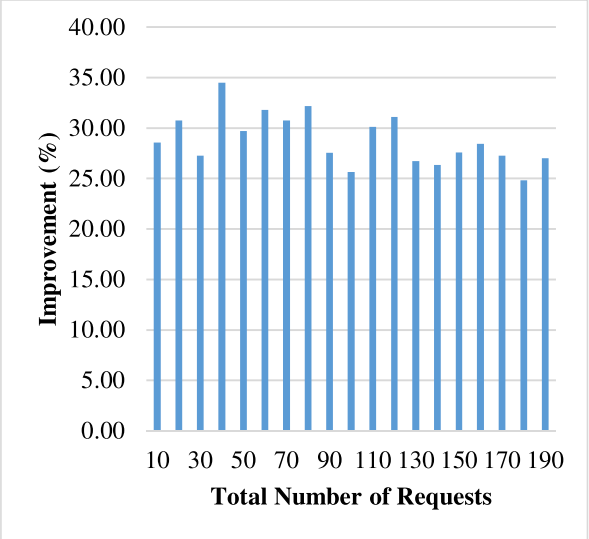

Fig 7. Plot showing improvement in Reliability for IIoE platforms

B. Communication Overhead:

It is the measured as the overhead incurred by the crossbar router to provide access to the required devices

TABLE II.
COMPARISON OF COMMUNICATION COST (CONVENTIONAL ROUTING VS IIOE)

S.No.	**Number of Devices**	**Communication Cost**		**Reduction(%)**
		Conventional Routing	**IIoE Platform**	

		Topology	topology	
1	10	18	8	10.00
2	15	23	11	12.00
3	20	35	13	22.00
4	25	43	18	25.00
5	30	47	23	24.00
6	35	51	29	22.00
7	40	58	35	23.00
8	45	61	39	22.00
9	50	69	42	27.00
10	55	74	48	26.00
11	60	79	54	25.00
12	65	81	57	24.00
13	70	95	63	32.00
14	75	105	73	32.00
15	80	115	81	34.00
16	85	124	95	29.00
17	90	134	110	24.00
18	95	146	119	27.00
19	100	154	123	31.00
Average	55	80	55	24.79

It could be observed from table 2, fig 8 and fig 9, for an average of 55 devices the reduction in communication cost is around 25%. The communication cost obtained using the IIoE platforms is 55 units, compared to the conventional routing strategy which is 80 units. A maximum of 123 units are utilized towards communication cost while using the IIoE platform, compared to the utilization of 154 units towards communication cost for the conventional routing strategy.

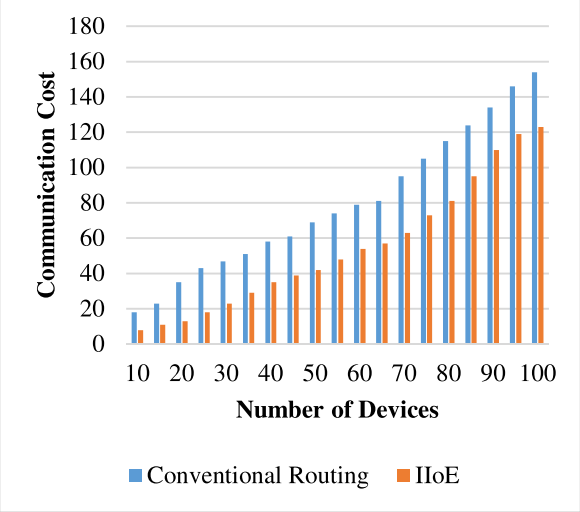

Fig 8. Plot comparing the Communication Cost (Conventional Routing Vs IIoE)

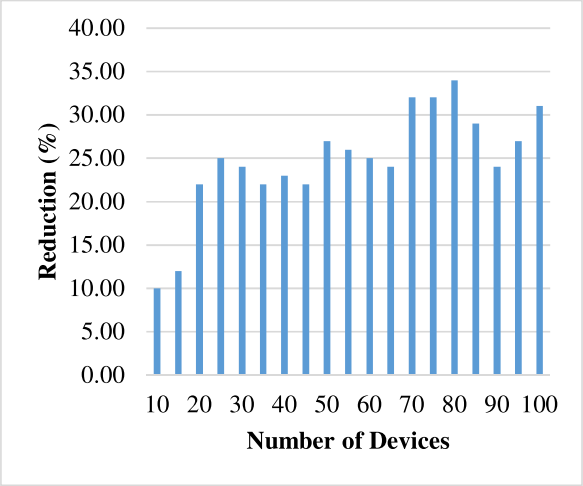

Fig 9. Plot showing Reduction in Communication Cost for IIoE platforms

V. Conclusion

In this work an Intelligent addressing and routing strategy has been proposed for the Interactive Internet of Everything platforms to interconnect smart gadgets and prevent malicious access of the devices.

The reliability which is based on the number of legitimate requests has been improved significantly with a reduction in communication cost with increase in devices.

VI. Future Work

The work could be extended to design protocols for adaptive routing based on dynamic workload and optimizing the performance for the same. The features of load balancing and load sharing could be incorporated on the crossbar router with an arbitration logic.

References

[1] Mukesh Mishra, Gourab Sen Gupta and Xiang Gui. "Network Lifetime Improvement through Energy-Efficient Hybrid Routing Protocol for IoT Applications", Sensors 2021, pp 1-26, 2021

[2] Hayder Fakher Jassim, Mohammed A. Twafeeq and Sawsan M. Mahmoud. "Overlapped hierarchical clusters routing protocol for improving quality of service", TELKOMNIKA Telecommunication, pp 705-715, 2021.

[3] Dipali K.Shende, Yogesh Angal and Sonavane.S.S. "A Comprehensive Survey of the Routing Schemes for IoT Applications", Scalable Computing: Practice and Experience, pp 203-216, 2020.

[4] Rashmi Sahay, Geethakumari.G. and Barsha Mitra. "A novel blockchain based framework to secure IoT-LLN's against routing attacks", Springer, Verlag, pp 2445-2470, 2020.

[5] Ayesha Shafique, Guo Cao, Muhammad Aslam, Muhammad Asad, Dengpan Ye. "Application-Aware SDN-Based Iterative Reconfigurable Routing Protocol for Internet of Things (IoT)", Sensors 2020, pp 1-22, 2020

[6] Muhammad Dawood Khan, Zahid Ullah, Arshad Ahmad, Bashir Hayat, Ahmad Almogren, Kyong Hoon Kim, Muhammad Illayas and Mohammad Ali. "Energy harvested and cooperative enabled efficient routing protocol (EHCRP) for IoT-WBAN", Sensors 2020, pp 1-23, 2020.

[7] Karim Fathallah, Mohamed Amine Abid and Nejib Hadj-Alouane. "Enhancing Energy Saving in Smart Farming through Aggregation and Partition Aware IoT Routing Protocol", Sensors 2020, pp 1-28, 2020.

[8] Khalid Haseeb, Ahmad Almogren, Naveed Islam, Ikram Ud Din and Zahoor Jan. "An Energy-Efficient and Secure Routing protocol

for Intrusion Avoidance in IoT based WSN", Energies 2019, pp 1-18, 2019.

[9] Seyyed Yasser Hashemi and Fereidom Shams Aliee. "Dynamic and Comprehensive trust model for IoT and its integration into RPL", Journal of Supercomputing, pp 3555-3584, 2018.

[10] Suhail Ashfaq Butt, Kamalrulnizham Abu Bakar, Nadeem Javaid, Niayesh Ghazrei, Farruh Ishmanov, Muhammad Khalil Afzal, Muhammad Khalid Mehmood and Muhammad Akram Mujahid. " Exploiting Layered Multi-Path Routing Protocols to Avoid Void Hole Regions for Reliable Data Delivery and Efficient Energy Management for IoT-Enabled Underwater WSN's", Sensors 2019, pp 1-28, 2019.

[11] Andras Varga. "OMNet++ IDE Customisation Guide", Opensim Ltd, pp 35-37, 2014.

[12] Andras Varga. "The OMNET++ Discrete Event Simulation System", Researchgate, pp 1-8, 2014.