ICS: Interoperable Communication System for Inter-Domain Routing in Internet-of-Things

Bhavana A[1]
Research Scholar, Department of Computer Science and Engineering, VTU, Belagavi, Karnataka, India

Nandha Kumar A N[2]
Professor, Department of Computer Science and Engineering, GSSS, Mysuru, Karnataka, India

***Abstract*—The Internet-of-Things consists of heterogeneous smart appliances connected by global network with self-configuring capabilities requiring interoperable communication schemes while performing inter-domain routing. A review of existing interoperable approaches shows that there is still a large scope of improving IoT interoperability. The proposed system introduces Interoperable Communication System (ICS) by developing a novel inter-domain routing in IoT using two schemes. Preemptive and Non-Preemptive Communication scheme targets mainly emergency-based routing, which demands faster transmission, and dedicated transmission, demanding accountability in communication. A simulation study carried out for the proposed system shows that it offers approximately 90% reduced delay, 57% increased packet delivery ratio, and 98% faster processing time when compared with existing approaches to accomplish interoperability in IoT.**

***Keywords*—Internet-of-Things (IoT); interoperability; heterogeneous; gateway protocol; inter-domain routing**

I. Introduction

The term Internet-of-Things (IoT) refers to technological advancement, which connects various virtual and physical things using the internet's existing infrastructure [1]. It consists of network infrastructure globally-connected, characterized by self-configuring capabilities considering interoperable communication systems [2]. IoT devices are generally considered smart appliances integrated with different platforms to assist in operating various applications, e.g., transportation, utilities, agriculture, healthcare, commerce, and industrial buildings [3]. In this aspect, the concept of interoperability is a much-discussed topic under the roof of research and development in IoT. If two IoT platforms are incompatible, then an application's operational features cannot be fully established [4]. The concept of IoT interoperability is perceived in the form of a platform, semantic, syntactic, networking, and device interoperability [5]. In the present time, the state of interoperability in IoT is managed using different approaches. The primary approach is to work on gateways and adapters that mechanizes intermediate software and tools to bridge the communication among the IoT devices with respect to different standards and data [6]. Existing gateway protocol in IoT offers one gateway to communicate with others. Still, it suffers from significant scalability issues, especially in multiple and massive smart appliances, which results in higher design complexity. The second approach uses overlay-based techniques to integrate the actuators/sensors with other IP-based objects to carry out seamless operation [7]. It can also be carried out using a virtual networking system that permits device-based communication with an end-to-end approach; however, it also suffers from scalability issues. The third approach uses different networking technologies using IP-based approaches, Software-defined approaches, network function virtualization, fog computing, etc. [8]-[10]. The fourth approach uses service-oriented architecture to offer syntactic interoperability among all smart appliances [11]. The fifth approach is to make use of semantic web technologies [12]. Apart from this, various other research work is being carried out to investigate interoperability issues in IoT. It is still in progress, and no definitive solution has yet arrived. There are various problems associated with interoperability from existing research trends which are as follows: i) existing trends of the solution is more inclined towards considering specific case study which is somewhat unpractical from practical IoT deployment, ii) in the presence of a large number of smart appliances, it is eventual that the communication has to be carried out using the application-domain approach, which is not considered much in existing trends of research, iii) although, all the major investigation towards interoperability of gateway node, they have ignored the consideration of amending the search and data translational services when gateway communicates with multiple application domains.

Existing studies in IoT towards interoperability focuses on specific communication environment without considering capabilities of devices included in it. This is a significant limitation of existing system. Therefore, this paper introduces a simple yet efficient inter-domain routing scheme in IoT that emphasizes achieving interoperability. The investigation contributes to evolving a new methodology where heterogeneous communication systems are considered while performing inter-domain routing. This paper's contribution is mainly to introduce a simplified framework that can support interoperability of communication systems in IoT, not current times. The organization of the paper is as follows: Section II discusses existing research approaches towards interoperability in IoT, Section III discusses identified research problems, Section IV discusses proposed research methodologies, Section V discusses system design along with algorithm discussion. Result analysis is carried out in Section VI, while the paper's conclusive remarks are provided in Section VII and future work description in Section VIII.

II. Existing Approaches

At present, various approaches have been implemented to address multiple ranges of issues in IoT [13]. This section

specifically discusses the issues about interoperability in IoT. The recent work carried out by Xu et al. [14] has presented a technique for improving throughput performance, specifically concerning industrial IoT systems using cognitive networks. The study has used a convex optimization process in order to address resource allocation issues in industrial IoT. The technique also considers scheduling of IoT devices in order to achieve better fairness control. A similar direction of study towards resource provisioning to achieve interoperability in IoT is also presented by Zhou et al. [15]. This approach makes use of the Lyapunov optimization scheme with delay awareness. Without having any form of dependencies towards predefined information of statistical data of cloud system, this technique reports provisioning of IoT application of different types. The approach finally claims a cost-effective operation considering practical world traces of traffic information. The current study also emphasizes security and interoperable conditions in IoT where signcryption is used for the multi-receiver system over the mobile system in IoT (Qiu et al. [16).

Another study carried out by Behera et al. [17] has developed an enhanced communication scheme focusing on the heterogeneous network in IoT. Considering the wireless sensor network case study, this implementation mainly deals with selecting cluster-head for performing data aggregation in the heterogeneous network in IoT. However, the scheme is restricted to addressing issues associated with energy efficiency only in IoT. Considering the case study of healthcare in IoT, the work carried out by Ray et al. [18] has used broker services for message queueing in order to perform service provisioning. A unique gateway testbed has been constructed, which includes various wireless networks for usage in translational services. The complete study has been carried out in prototyping form using real-time sensors. The work carried out by Diez et al. [19] has presented a validation framework in order to assess the fact of proper alignment of data with standards of the data model. It has also been seen that messaging protocols play an essential role in interoperability in IoT. Al-Masri [20] has discussed the dependency of multiple messaging protocols to establish proper communication among heterogeneous devices in IoT.

There is also dedicated research being carried out towards assessing the testbed of IoT. One such research work is carried out by Lanza et al. [21] where experimentation in the form of services has been presented for IoT. Existing studies have also been carried out towards assessing the trustworthiness of gateway systems in IoT, as seen in the work of Fraile et al. [22]. The approach discusses security architecture for device drivers along with faster visibility of the node. Yang et al. [23] have presented an optimization scheme towards industrial IoT operation where the Poisson process is used for developing the work distribution in IoT. The adoption of convex optimization principle is used for performing analysis. A combined study towards network security and quality of service is carried out by Sood et al. [24] in order to enhance the heterogeneity in the serviced rendered by Software Defined Network in IoT. The technique also performs transformation of the controllers of heterogeneous form to the homogeneous form using mathematical modelling. Heterogeneity is also studied with respect to security over physical layers in IoT as seen in work of Wang et al. [25]. The work carried out by Leu et al. [26] have emphasized over achieving stability in messaging services in IoT in order to enhance the heterogeneity in Service-Oriented Architecture. The technique makes use of shortest processing time in order to carry out scheduling of the IoT messages in web-based services.

Study carried out by Nguyen et al. [27] has used network codes in order to investigate the impact of energy consumption over IoT performance. In this study, the author has investigated the use of random linear network coding targeting to improve the throughput performance in IoT. A unique study presented by Wu et al. [28] discusses the use of tree concept in presenting sensor network over IoT considering case study of healthcare assessment. In this work, a unique tree structured is developed with indexing policies where a neural network is applied in order to perform feature engineering for facilitating interoperable operation in IoT. Such learning based approaches towards heterogeneous network are also witnessed in work of Yang et al. [29]. This approach makes use of radio frequency in order to cater up the QoS requirement using Markov decision process. The study also uses reinforcement learning scheme for further optimizing the outcome. Adoption of swarm intelligence is also reported to carry out optimization operation in IoT. Work of Ni et al. [30] have used dragonfly algorithm in order to plan the communication path considering multiple robotic system of heterogeneous form. An indepth investigation towards various optimization algorithm towards improving hardware architecture for heterogeneous IoT is carried out by Krishnamoorthy et al. [31]. Noori et al. [32] have carried out investigation towards slotted ALOHA protocol for improving the communication performance in heterogeneous IoT. Finally, Asad et al. [33] have improved the quality of service using provisioning of quality of service over multiple radio access technology using game theory concept. The idea is to offer a seamless access among heterogeneous devices in IoT.

Hence, it is seen that existing system mainly make use of heterogeneity concept in order to achieve better interoperability in IoT. Heterogeneity doesn't necessarily address interoperability issues in IoT. A closer look into existing system shows beneficial approaches and outcome when it comes to addresses considered problem. However, all the essential problems are not considered in generalized environment of IoT. The next section discusses about research problem.

III. Limitation of Existing Studies

After reviewing the existing approaches of interoperability in IoT, following research problems has been noticed:

- Although, there are certain degree of work being carried out towards addressing interoperability problem in IoT, but they are very much specific to singular environment of communication. However, practical application in IoT demands more towards inter-domain communication scheme, which unfortunately is very less. Existing solution are highly inclined towards either network layer or device level. This is not sufficient to deal with various emergency communication systems in IoT.

- Existing system offers minimal emphasis over capabilities of smart appliances or IoT devices while working on interoperability. There is a need of evolving up with standard of communication over IoT which are not present at this moment in order to cater up the demands of communication associated with the low end devices in IoT. It is essential to understand that a practical form of solution for interoperability should not be purely dependent on available network entity. Another biggest challenge is also associated with the existing gateway system in IoT which is not compatible with the changes when a new smart appliance is added or new services are edited. Apart from this, there is an emergent need of flexible interoperability within the gateway system for boosting up machine-to-machine communication system with higher range of scalability.
- The third challenge explored in existing studies is that they consider single of two platform in the form of application domain. In the practical concept of large scale scenario of IoT deployment, there are possibilities of multiple number of application domain and IoT nodes within this domain are required to establish communication process dynamically. A better and effective approach should be highly practical with facilitation of scalable operation over the multiple number of application domains. Adding of new domain should not affect the scalable performance of the gateway node.
- There are various routing scheme in IoT; however all the existing protocols suffers from the challenges associated with fault tolerance, context awareness, presence of multiple network standards, node deployment, intermittent connectivity, multihop communication scheme. Apart from this issue, existing routing scheme cannot actually differentiate dynamic demands of the large scale distributed communication system. It works in similar way for all kinds of communication demands. Interoperability is achieved by a predefined environment in IoT which is impractical.

Hence, the statement of problem is "It is challenging to develop scalable, interoperable routing scheme which justifies all forms of traffic demands in unbiased fashion in large scale IoT environment."

IV. Research Methodology

The proposed system adopts an analytical research methodology where the idea is to construct a framework which can jointly address the both preemptive and non-preemptive communication system in IoT. The novelty of the proposed methodology is that it offers higher degree of flexibility to achieve interoperability in achieving communication in IoT. The prime aim of the proposed study is to offer a significant range of interoperability among the heterogeneous smart appliances, also called as IoT nodes. It is a continuation of our prior implementation where scalability factor has been achieved [34]. Fig. 1 highlights the architecture implemented for this purpose to develop Interoperable Communication System (ICS).

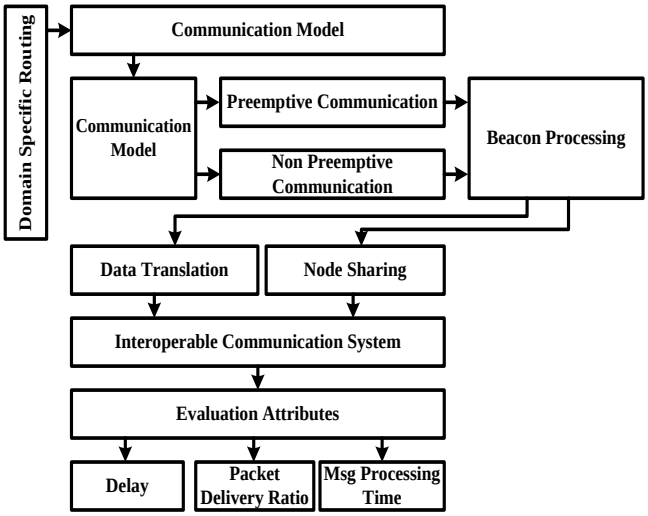

Fig. 1. Architecture of ICS.

Fig.1 highlights the composition of prominent block of operation of ICS. The first block of IoT Topology mainly incorporates IoT environment with presence of IoT nodes deployed in the form of group. The second block of Application Domain clusters all the IoT nodes within the IoT environment. The common block of IoT Routing considers the deployment of any communication protocol within application domain. Each domain is assumed to execute discrete IoT local routing. The next important block of operations is preemptive and non-preemptive communication scheme. The former scheme is used for processing emergency transmission while the later scheme is used for dedicated transmission in IoT. The idea is to develop a framework which can cater up communication demands of maximum situation in IoT. The next block of operation is Gateway Node Management which is mainly used for translational services for facilitating interoperability in the system. In case of preemptive approach, the gateway node performs data translation while in case of non-preemptive approach; addresses of the node are shared. The study outcome is finally. The further discussion of methodology of proposed system is illustrated in next section with respect to system design.

V. System Design

This part of the study illustrates about the system design as well as implementation being carried out towards developing Interoperable Communication System (ICS) in IoT. The complete implementation is carried out considering the practical environmental scenario of using different forms of smart appliances deployed in IoT environment. The study considers heterogeneity in the devices being connected where achieving interoperability in communication system is still an open-end problem. For this purpose, the complete ICS is designed considering two states of communication demands i.e. preemptive and non-preemptive stage. This section elaborates about the system design deployed for this purpose.

A. Preemptive Communication Scheme

The prime purpose of the preemptive communication scheme is to offer instantaneous communication establishment during any form of emergency circumstances (Fig. 2). It is based on the hypothesis that when a large number of heterogeneous smart appliances are connected in an IoT, either in small and large scale, achieving faster communication is quite a challenging aspect. Hence there is a need of preemptive mechanism which can ensure that an emergency communication always takes place irrespective of any situation of some of the IoT nodes owing to any reason. This scheme also considers that only few IoT nodes could possibly exhibit degradation in its performance of data forwarding either due to resource depletion or due to any miscellaneous reasons. Apart from this, it should also offer supportability of mobility condition of IoT nodes.

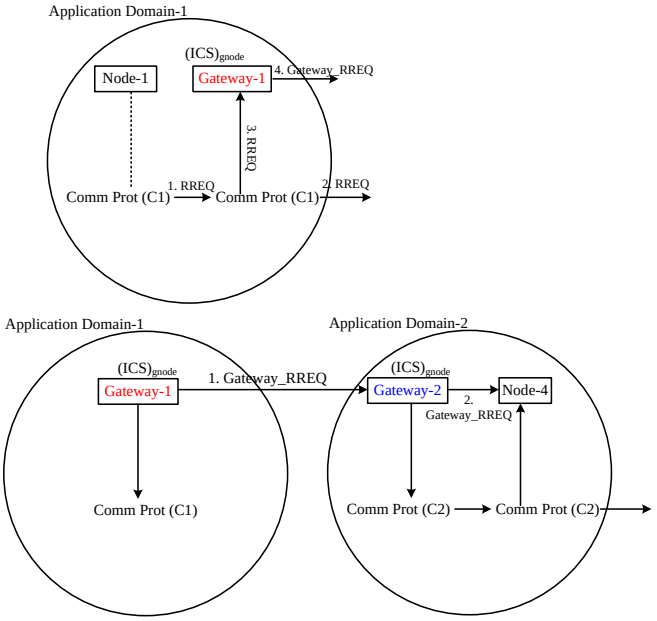

Fig. 2. Preemptive Routing Scheme in IoT.

Fig. 2 highlights a practical implementation environment where a smart appliance $node_1$ is a part of application domain α_1 which sensed an event-data and now it is required to transmit this data to $node_4$ that is part of different application domain α_2. The environment also considers usage of two different communication scheme β_1 and β_2 followed by all IoT nodes in domain α_1 and α_2 respectively. The transmitting $node_1$ broadcast the beacon for route discovery first considering the presence of an IoT gateway node γ. It should be noted that the study considers a single gateway node in one deployment zone γ which offers translation services for two application domain by offering two discrete sub-gateway services i.e. $\gamma=(\gamma_1, \gamma_2)$. This gateway node carries the addresses associated with identity and position of their respective registered smart appliances followed by establishment of connection. The proposed system constructs an algorithm which initiates processing of the request of data forwarding where gateway protocols assists in establishing preemptive routing. The algorithm implemented for this purpose is shown as follows:

Algorithm for Preemptive Communication Scheme

Input: *n*, *γ*, *β*, *Cv*, *f*
Output: *d*
Start
1. **For** i=1:*n*
2. Formulate α=1: *m*
3. $\alpha_i=[\alpha_1, \alpha_2, \ldots. \alpha_m | m<n]$
4. *alloc* $n_i \rightarrow \alpha_m$, $\gamma \rightarrow \alpha$
5. **For** α=1:*m*
6. n_{1i} forwards msg(C_{v1})
7. C_{v1} forwards msg(γ(α))
8. $\gamma(\alpha_i) \rightarrow msg_1(\gamma(\alpha_{i+1}))$
9. $\gamma(\alpha_{i+1}) \rightarrow f(C_{v2}) \rightarrow (d)n_{2j}$
10. **End**
11. **End**

The above mentioned algorithm takes the input of n (number of smart appliances), γ (gateway node), α (application domain), Cv (Communication vector), and f (function for data translation), which after processing leads to generation of d (transmitted data). The algorithm considers all the sensor nodes (Line-1) and formulates m number of application domain α (Line-2 and Line-3). It should be noted that number of application domain m is considerably less compare to number of IoT nodes. The algorithm further allocates specific number of sensors n_i to all m number of application domain (Line-4). Considering all the number of available application domain α (Line-5), the IoT node initially forwards the message in the form of communication vector C_v (Line-6). The variable msg will mean control message or beacon used for route discovery process (Line-6). This is carried out in the form of broadcasting and this information is then passed on primary gateway node γ of the parent application domain (Line-7). The parent domain accesses the information from the message to find out the location of the destination node within different application domain (Line-8). The implementation considers the fact that each application domain exercises a unique routing scheme where the gateway node assists in data translational services in cross-application domains. It is also assumed that each gateway node possess information of its respective IoT nodes. Therefore, when a request to forward data to a specific node arrives for a gateway node from different gateway node, there are two further possibilities viz. i) if the destination node is present than the data d is subjected to data translation using function f(x) (Line-9) and finally data is forwarded, and ii) if the destination node is not present than the gateway node passes the route request message to the next gateway node and this search continues until and unless the destination node is found. It should be also noted that all the gateway nodes performs an exchange of their information after a certain interval of time. This will reduce the search time as updated information will be always available.

B. Non-Preemptive Communication Scheme

This is another alternative of the routing scheme where the circumstances demands dedicated routing of the data among heterogeneous IoT devices.

This part of the implementation considers exactly the similar deployment of application domain, gateway node, and IoT devices. According to the representation shown in Fig. 3, the transmitting node $node_1$ transmits the control message for the purpose of route discovery process. When the parent gateway node receives this request, it is forwarded to neighboring gateway node of different application domain. This is done if the primary gateway node is located far from destination gateway node which has destination node. If the target gateway node is located near to primary gateway node than the message is forwarded directly to the destination gateway node. Different from preemptive communication scheme, this scheme basically emphasizes on the address information of all the nodes involved in communication process in order to offer more accountability in communication process. Another uniqueness of this technique is that it offers bidirectionality of the communication process. Apart from this, the study also contributes towards assisting in exchanging routing table information between the transmitting and destination node located in different application domain. This makes the process of updating routing operation quite faster.

The algorithm responsible for this purpose is as follow:

Algorithm for Non-Preemptive Communication Scheme

Input: n, γ, α, C_v, λ, τ.
Output: d
Start
1. **For** i=1:n
2. Formulate α=1: m
3. α_i=[α_1, α_2, …. α_m| m<n]
4. *alloc* $n_i \rightarrow \alpha_m$, $\gamma \rightarrow \alpha$
5. **For** α=1:m
6. n_{1i} forwards msg(C_{v1})
7. response of C_{v1} is forwarded to n_{1i}.
8. $C_{v1} \rightarrow \tau(\gamma(\alpha_i))$
9. $\gamma(\alpha_i) \rightarrow \tau_1(\tau(\gamma(\alpha_i)))$
10. $\gamma(\alpha_i) \rightarrow \lambda(C_{v2})$
11. $C_{v2} \rightarrow \tau(n_{1i})$
12. transmit d
13. **End**
14. **End**

The algorithm takes the input of n (IoT nodes), γ (gateway node), α (application domain), C_v (Communication vector), λ (process of sharing address), and τ (information of address), which after processing yields an outcome of the d (transmitted data). The unique aspect of this routing scheme is that it mechanizes a method which performs embedding of the routing information to the IoT devices present in the network. In order to facilitate a dedicated communication path, the proposed algorithm ensures that each communicating nodes should have an access to the address information of all the nodes involved in path establishment via different gateways. The gateway node is responsible for sharing the address information among each other. Therefore the non-preemptive process of communication differs from preemptive communication scheme by facilitating the gateway node to carry out mutual exchanging of positional information among each other. The preliminary steps of operation are nearly equivalent to preemptive operation. Considering all the IoT nodes and application domain involved in it (Line-1 and Line-2), the proposed system initiates it process when $node_i$ in domain α_i attempts to communicate with $node_j$ in application domain α_j. The IoT node nodei transmit its control message using communication vector C_v (Line-6). The respective response is forwarded to node $node_i$ and instantly transmits the information about the address along with it to $node_i$ via the gateway node γ_i in application domain α_i. The request for routing is not forwarded to the application domain but they only share information of its addresses. The gateway node associated with the α_j share its own information as well as adjacent IoT devices after it receives the information of address for the $node_i$ in the form of response. Once this information about address is received, the gateway node share the equivalent information with an assistance of communication vector C_v that make use of method of sharing address which is further forwarded to transmitting IoT node. One of the significant characteristic of this algorithm is that it is capable of generating maximum number of addresses of all connected IoT nodes with the gateway node. Therefore, there are minimal utilization of the network resources as well as there are lesser dependencies in processing this algorithm in contrast to preemptive routing scheme. Another potential contribution of this algorithm is that it facilitates inter-domain routing specific to those nodes which are registered under established entries in more secured manner. The proposed system also performs specific way to exchange the message. The proposed approach carries out forwarding of the beacon for collecting the associated information of the IoT nodes followed by sharing of the control message along with the gateway nodes. In this process, the sequence number as well as address of IoT node is used for formulating the structure of beacon used in proposed study. The proposed system considers IP address as the address of the IoT nodes while freshness of data is represented by the sequence number.

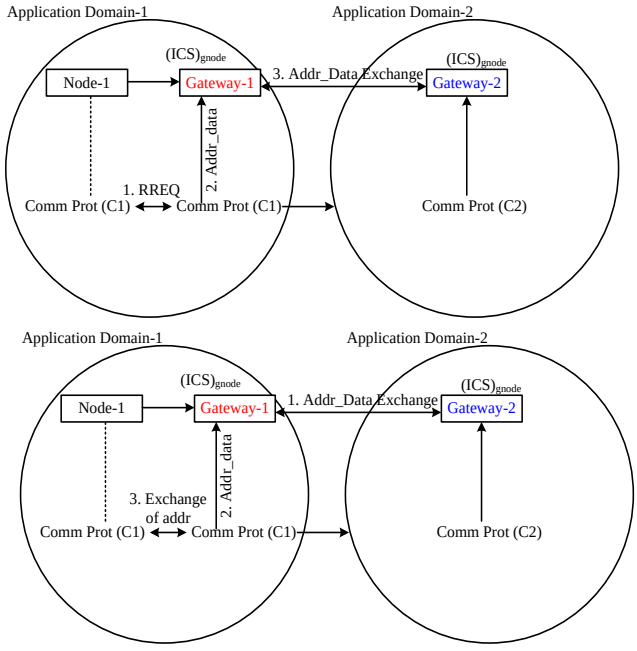

Fig. 3. Non-Preemptive Communication Scheme.

VI. Result Analysis

This section discusses about the outcome obtained after implementing the proposed ICS. The implementation of the proposed system is carried out considering 500 IoT nodes deployed in 1000 x 1000 m^2 simulation area where the transmission range is considered as 200m with assessment period of 1000s of iteration. As the proposed system mainly presents a modelling for communication scheme; therefore, it considers the equivalent standard performance parameters of delay, packet delivery ratio, and overall processing time. In order to perform a measurable assessment, the outcome of the proposed system is compared with the existing standards which are related to IoT. The first existing standard considered for processing is RFC 3221 which is responsible for performing inter-domain routing in IoT [35]. The second existing standards which are related to IoT is RFC 8352 which is responsible for implementing gateway scheme in IoT [36]. This section illustrates all outcome achieved.

A. Outcome of Delay

Delay is one of the prominent performance parameters to signify the communication effectiveness. Communication carried out in large scale scenario in presence of gateway and uneven traffic can significantly increase delay. Hence, the assessment of delay is carried out by forwarding 2500 bytes as experimental data. Fig. 4 highlights that the proposed system excels better outcome in contrast to existing approaches. The prime reason behind this is the underlying mechanism of message control in proposed ICS with availability of both the schemes. Presence of preemptive scheme always results in lower delay but at the same time, non-preemptive scheme too assists in reducing delay as once the path is set via accessing addresses, then data transmission becomes almost seamless in this dedicated path of inter-domain routing.

It is to be noted that the gateway node of proposed system contributes towards collecting individual address of the IoT devices and it performs periodic exchange of information with its adjacent gateway node. Therefore, proposed system can ascertain routing of maximum quantity of data over shorter range of time. Apart from this, the duration for obtaining information of communication vector from other IoT devices is also reduced. There is no potential overhead in the gateway as it only permits the exchange of the address information of IoT device. On the other hand, RFC 3221 offers overhead control in IoT, but there is no updating process towards the routing information in the memory of routing table. Apart from this, no information is shared with its adjacent nodes. The existing approach of RFC 8352 assists in performing gateway protocol implementation standard by opting for highly stabilized communication channel which is carried out using index of mobility criterion. It should be noted that gateway node is tracked via index of mobility to find out if they resides within the coverage of network. This calls for increasing search process which further increases the delay to a higher value. Therefore, the proposed system offers approximately 90% improved delay reduction when compared with existing standards of interdomain routing in IoT for targeting better interoperability.

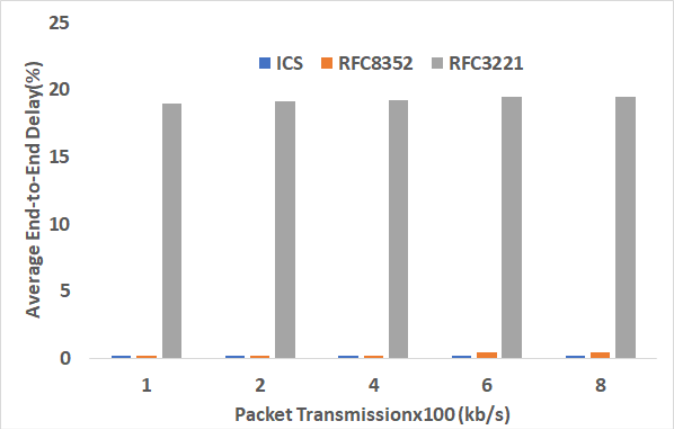

Fig. 4. Analyzed Outcome of Delay.

B. Outcome of Packet Delivery Ratio

Packet delivery ratio is considered another performance parameter which is assessed by considering amount of data which is already being forwarded to the amount of the data received by the recipient. Fig. 5 highlights that proposed system offers approximately 57% of improved packet delivery ratio in contrast to existing system of inter-domain routing. The prime reason behind this outcome is that it offers better form of data processing over the gateway node which makes the system characterized by higher interoperability. The routing tables are generated as well as updated by proposed data translational services into multiple structured which has solution to all the possible alternative communication path between transmitting and receiving IoT nodes.

Apart from this, preemptive scheme assists in node-by-node communication system where data is instantly forwarded to next node during route discovery process itself. Hence, it constructs a stabilized path whereas the path stability increases multifold when non-preemptive communication scheme is applied. However, no such operation takes place in existing system resulting in inferior packet delivery ratio.

C. Outcome of Processing Time

Processing time is one of the essential performance parameter to measure the computational complexity as well as to assess the overall response time of the system. It gives a fair idea of effectiveness of proposed model over practical network environment. The proposed evaluation considers processing time as the cumulative amount of time needed for the gateway node in order to perform processing of the data transmission from source node of one application domain to destination node of another application domain. Hence, there is higher feasibility of different ranges of processing time for different set of communicating IoT nodes. Considering multiple rounds of simulation, the assessment of the processing time is carried out to evaluate the effect of various traffic behaviour, its load, and variable data over the processing time.

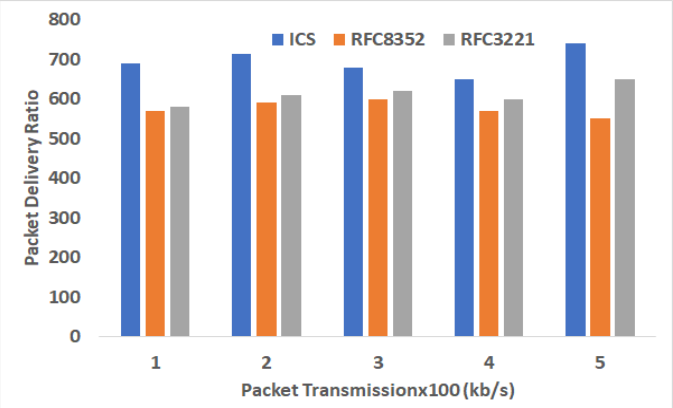

Fig. 5. Analyzed Outcome of Packet Delivery Ratio.

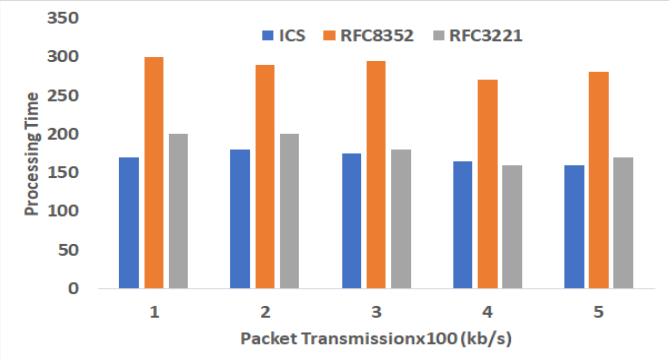

Fig. 6. Analyzed Outcome of Processing Time.

Fig.6 showcase that the proposed system accomplishes approximately 98% of reduced processing time in comparison to existing system. The justification behind this outcome is that the developed gateway system of ICS can cater up the demands of any form of dynamic environment. The proposed ICS solve the problem associated with intermittent breakage of link in dynamic topology of IoT. This is made possible when there is communication exchange between gateway nodes of different application domain. However, such forms of route management is not taken care of by existing standards in IoT. Another essential contribution of proposed system is that IoT nodes are freed from any form of duty towards strengthening the connectivity of IoT devices that is also the reason for faster response time.

VII. Conclusion

This paper presents a discussion about a novel framework of facilitating an inter-domain routing in IoT with core emphasis to accomplish full-fledge interoperability. The study uses an analytical approach where an IoT environment is deployed in such a way that the device-to-device (heterogeneous) communication is carried out using gateway. The protocol implemented is executed on gateway node where it facilities two forms of routing scheme apart from its data translation services. Preemptive scheme assists in emergency communication while non-preemptive scheme assists in offering dedicated line of communication in IoT. The study outcome shows better communication performance in contrast to existing schemes deployed in achieving interoperability. The definitive findings of the measure of its significance in the research community is that proposed system offers 90% reduced delay performance, 57% of more packet delivery ratio, and 98% of reduced processing time in comparison to existing system.

VIII. Future Work

The present research work will be continued towards achieving secure communication in data transmission in IoT in compliance of scalability and interoperability aspects too. It is necessary as the proposed system is capable of connecting a vast set of network with another network via a gateway system and hence massive number of data as well as services are exchanged. Hence, future work could be carried out using trust-based data integrity scheme along with privacy preservation.

References

[1] Alam, Sarfraz, Mohammad MR Chowdhury, and Josef Noll. "Interoperability of security-enabled internet of things." Wireless Personal Communications 61, no. 3 (2011): 567-586.

[2] Ahlgren, Bengt, Markus Hidell, and Edith C-H. Ngai. "Internet of things for smart cities: Interoperability and open data." IEEE Internet Computing 20, no. 6 (2016): 52-56.

[3] Elkhodr, Mahmoud, Seyed Shahrestani, and Hon Cheung. "The internet of things: new interoperability, management and security challenges." arXiv preprint arXiv:1604.04824 (2016).

[4] Di Martino, Beniamino, Massimiliano Rak, Massimo Ficco, Antonio Esposito, Salvatore Augusto Maisto, and Stefania Nacchia. "Internet of things reference architectures, security and interoperability: A survey." Internet of Things 1 (2018): 99-112.

[5] Ahmad, Awais, Salvatore Cuomo, Wei Wu, and Gwanggil Jeon. "Intelligent algorithms and standards for interoperability in Internet of Things." (2019): 1187-1191.

[6] Mukherjee, Saswati, and Susan Elias. "An applications interoperability model for heterogeneous internet of things environments." Computers & Electrical Engineering 64 (2017): 163-172.

[7] Jabbar, Sohail, Farhan Ullah, Shehzad Khalid, Murad Khan, and Kijun Han. "Semantic interoperability in heterogeneous IoT infrastructure for healthcare." Wireless Communications and Mobile Computing 2017 (2017).

[8] Qin, Zhijing, Grit Denker, Carlo Giannelli, Paolo Bellavista, and Nalini Venkatasubramanian. "A software defined networking architecture for the internet-of-things." In 2014 IEEE network operations and management symposium (NOMS), pp. 1-9. IEEE, 2014.

[9] Kalkan, Kubra, and Sherali Zeadally. "Securing internet of things with software defined networking." IEEE Communications Magazine 56, no. 9 (2017): 186-192.

[10] Babiceanu, Radu F., and Remzi Seker. "Cyber resilience protection for industrial internet of things: A software-defined networking approach." Computers in Industry 104 (2019): 47-58.

[11] Noura, Mahda, Mohammed Atiquzzaman, and Martin Gaedke. "Interoperability in internet of things: Taxonomies and open challenges." Mobile Networks and Applications 24, no. 3 (2019): 796-809.

[12] Rahman, Hafizur, and Md Iftekhar Hussain. "A comprehensive survey on semantic interoperability for Internet of Things: State-of-the-art and research challenges." Transactions on Emerging Telecommunications Technologies 31, no. 12 (2020): e3902.

[13] Bhavana, A., and AN Nandha Kumar. "An Analytical Modeling for Leveraging Scalable Communication in IoT for Inter-Domain Routing." In Proceedings of the Computational Methods in Systems and Software, pp. 1-11. Springer, Cham, 2018.

[14] L. Xu, W. Yin, X. Zhang and Y. Yang, "Fairness-Aware Throughput Maximization Over Cognitive Heterogeneous NOMA Networks for Industrial Cognitive IoT," in IEEE Transactions on Communications, vol. 68, no. 8, pp. 4723-4733, Aug. 2020, doi: 10.1109/TCOMM.2020.2992720

[15] Z. Zhou, S. Yu, W. Chen and X. Chen, "CE-IoT: Cost-Effective Cloud-Edge Resource Provisioning for Heterogeneous IoT Applications," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8600-8614, Sept. 2020, doi: 10.1109/JIOT.2020.2994308.

[16] J. Qiu, K. Fan, K. Zhang, Q. Pan, H. Li and Y. Yang, "An Efficient Multi-Message and Multi-Receiver Signcryption Scheme for Heterogeneous Smart Mobile IoT," in IEEE Access, vol. 7, pp. 180205-180217, 2019, doi: 10.1109/ACCESS.2019.2958089.

[17] T. M. Behera, S. K. Mohapatra, U. C. Samal, M. S. Khan, M. Daneshmand and A. H. Gandomi, "I-SEP: An Improved Routing Protocol for Heterogeneous WSN for IoT-Based Environmental Monitoring," in IEEE Internet of Things Journal, vol. 7, no. 1, pp. 710-717, Jan. 2020, doi: 10.1109/JIOT.2019.2940988.

[18] P. P. Ray, N. Thapa and D. Dash, "Implementation and Performance Analysis of Interoperable and Heterogeneous IoT-Edge Gateway for Pervasive Wellness Care," in IEEE Transactions on Consumer Electronics, vol. 65, no. 4, pp. 464-473, Nov. 2019, doi: 10.1109/TCE.2019.2939494.

[19] L. Diez, J. Choque, L. Sánchez and L. Muñoz, "Fostering IoT Service Replicability in Interoperable Urban Ecosystems," in IEEE Access, vol. 8, pp. 228480-228495, 2020, doi: 10.1109/ACCESS.2020.3046286.

[20] E. Al-Masri et al., "Investigating Messaging Protocols for the Internet of Things (IoT)," in IEEE Access, vol. 8, pp. 94880-94911, 2020, doi: 10.1109/ACCESS.2020.2993363.

[21] J. Lanza et al., "Experimentation as a Service Over Semantically Interoperable Internet of Things Testbeds," in IEEE Access, vol. 6, pp. 51607-51625, 2018, doi: 10.1109/ACCESS.2018.2867452.

[22] F. Fraile, T. Tagawa, R. Poler and A. Ortiz, "Trustworthy Industrial IoT Gateways for Interoperability Platforms and Ecosystems," in IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4506-4514, Dec. 2018, doi: 10.1109/JIOT.2018.2832041.

[23] J. Yang, C. Ma, B. Jiang, G. Ding, G. Zheng and H. Wang, "Joint Optimization in Cached-Enabled Heterogeneous Network for Efficient Industrial IoT," in IEEE Journal on Selected Areas in Communications, vol. 38, no. 5, pp. 831-844, May 2020, doi: 10.1109/JSAC.2020.2980907.

[24] K. Sood, K. K. Karmakar, S. Yu, V. Varadharajan, S. R. Pokhrel and Y. Xiang, "Alleviating Heterogeneity in SDN-IoT Networks to Maintain QoS and Enhance Security," in IEEE Internet of Things Journal, vol. 7, no. 7, pp. 5964-5975, July 2020, doi: 10.1109/JIOT.2019.2959025

[25] D. Wang, B. Bai, K. Lei, W. Zhao, Y. Yang and Z. Han, "Enhancing Information Security via Physical Layer Approaches in Heterogeneous IoT With Multiple Access Mobile Edge Computing in Smart City," in IEEE Access, vol. 7, pp. 54508-54521, 2019, doi: 10.1109/ACCESS.2019.2913438.

[26] J. Leu, C. Chen and K. Hsu, "Improving Heterogeneous SOA-Based IoT Message Stability by Shortest Processing Time Scheduling," in IEEE Transactions on Services Computing, vol. 7, no. 4, pp. 575-585, Oct.-Dec. 2014, doi: 10.1109/TSC.2013.30.

[27] V. Nguyen, J. A. Cabrera, G. T. Nguyen, D. You and F. H. P. Fitzek, "Versatile Network Codes: Energy Consumption in Heterogeneous IoT Devices," in IEEE Access, vol. 8, pp. 168219-168228, 2020, doi: 10.1109/ACCESS.2020.3023639.

[28] C. K. Wu et al., "An IoT Tree Health Indexing Method Using Heterogeneous Neural Network," in IEEE Access, vol. 7, pp. 66176-66184, 2019, doi: 10.1109/ACCESS.2019.2918060.

[29] H. Yang, A. Alphones, W. Zhong, C. Chen and X. Xie, "Learning-Based Energy-Efficient Resource Management by Heterogeneous RF/VLC for Ultra-Reliable Low-Latency Industrial IoT Networks," in IEEE Transactions on Industrial Informatics, vol. 16, no. 8, pp. 5565-5576, Aug. 2020, doi: 10.1109/TII.2019.2933867.

[30] J. Ni, X. Wang, M. Tang, W. Cao, P. Shi and S. X. Yang, "An Improved Real-Time Path Planning Method Based on Dragonfly Algorithm for Heterogeneous Multi-Robot System," in IEEE Access, vol. 8, pp. 140558-140568, 2020, doi: 10.1109/ACCESS.2020.3012886.

[31] R. Krishnamoorthy et al., "Systematic Approach for State-of-the-Art Architectures and System-on-Chip Selection for Heterogeneous IoT Applications," in IEEE Access, vol. 9, pp. 25594-25622, 2021, doi: 10.1109/ACCESS.2021.3055650.

[32] M. Noori, S. Rahimian and M. Ardakani, "Capacity Region of ALOHA Protocol for Heterogeneous IoT Networks," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8228-8236, Oct. 2019, doi: 10.1109/JIOT.2019.2920161.

[33] M. Asad, S. Qaisar and A. Basit, "Client-Centric Access Device Selection for Heterogeneous QoS Requirements in Beyond 5G IoT Networks," in IEEE Access, vol. 8, pp. 219820-219836, 2020, doi: 10.1109/ACCESS.2020.3042522.

[34] Bhavana, A., and AN Nandha Kumar. "An Analytical Modeling for Leveraging Scalable Communication in IoT for Inter-Domain Routing." In Proceedings of the Computational Methods in Systems and Software, pp. 1-11. Springer, Cham, 2018.

[35] Huston, Geoff. Commentary on inter-domain routing in the internet. RFC 3221, December, 2001.

[36] Gomez, Carles, M. Kovatsch, H. Tian, and Z. Cao. "Energy-Efficient features of internet of things protocols." draft-ietf-lwigenergy-efficient-06 (trabajo en curso) (2017).