International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 02 | Feb 2021 www.irjet.net p-ISSN: 2395-0072

An integrated approach to CCNX DATA networking for the Wireless Sensor Network using IOT and E-client data Aggregation

Sreeja.S.Nair[1], Nisha Mohan P.M[2]

[1]M Tech Student.APJ Abdul Kalam Technological University,Kerala,India
[2]Asst.Professor,Mount Zion College of Engineering,Kadammanitta,Kerala,India

---

Abstract - *In this project my idea is to develop integrating iot and content centric networking protocol with the help of e client data aggregation mechanism This paper aims to develop a new Internet architecture that can capitalize on strengths and address weaknesses of the Internet's current host-based, point-to-point communication architecture in order to naturally accommodate emerging patterns of communication. In this method named data networking pattern helps us to transforms data into first class entity which helps us the network to perform faster with enhanced security, and automatic caching facility helps us to reduce bandwidth by providing recent visited contents and most viewed contents in cache and also enabling this method in sensor networks which will give a perfect blend of technical solution to solve network issues like security, bandwidth etc. . . . . IOT act as throughput using hardware resources which cost less instead of using complex routers and another hardware resources which requires special attention, and using IoT updation of devices can be done in an easy manner and replacement is less costly compared to complex networking devices, this project concepts to work using the forwarding networking node mechanism service hands data to applications allow aggregation of data provides a faster reliable network methodology*

Key Words: **Content Centric Networking, Wireless Sensor network, Internet Of Things**

1.INTRODUCTION

The project mainly focus on the area Wireless Sensor Networks (WSN) and Content Centric Networking (CCN) WSN consist of spatially distributed often battery driven autonomous sensors to monitor physical or environmental conditions. They gather real world data in applications like habitat or industrial monitoring, or agriculture. Data is processed in the network and integrated information is provided to a gateway. Current technology use of IPv6 stacks on sensor nodes. The Internet Protocol IP addresses nodes via hierarchical addresses based on location. However, users are interested in content and Identify applicable funding agency here. If none, delete this. information instead of the location of data. To overcome this issue content centric networking (CCN) approaches have been developed in the recent past. CCN addresses data itself instead of the location where data is stored. Wireless communication technologies offer many advantages for applications and services which are deployed in various modern areas such as industry, healthcare, smart home, smart cities, etc. On the one hand, IP brings some advantages such as enabling the communication compatibility between devices in several domains. On the other hand, deploying IP in the IoT and its devices is challenging as introduced in more detail in III. However, IoT systems have application and device requirements such as scalability, robustness, power efficiency. The available solutions which are based on the host-to-host IP method influence the communication performance in current and future Internet. Using the IP means also using IP addresses for all devices connected to the Internet That leads to the need for new protocols and algorithms to match the requirements of the IoT and its devices. Additionally, the security of the end-to-end oriented devices is not entirely covered using the IP. The data are a self-identifying unit which can be requested by sending an Interest packet (NDN message type) from any authorized consumer using location independent and unique names. The NDN communication model has some features such as scalable naming scheme, lightweight configuration, management operations and simple communication model. Therefore, NDN has been suggested as a particularly promising solution for IoT systems . IoT systems run many applications in different domains on heterogeneous and constrained devices that may request the same data regardless of their provenance. In my concept I am trying to design an interface which designed and developed to meet IoT-NDN system will enable the research community, industry, and different sectors to contribute to the future Internet of Things with the Named Data Networking method which resolve the network issues by using this concept.

1.1 CACHING

Caching in Named Data Networking for the wireless Internet of Things Named Data Networking (NDN) is a promising Information-Centric future Internet architecture. Besides its recognized potentialities as a content retrieval solution in wired domains, NDN has been also recently considered as an enabling technology for the Internet of Things (IoT), thanks to its innovative features like named-based routing and in-network caching. In particular, the possibility of caching at intermediate nodes can be especially useful to reduce the retrieval delay, and limit the network traffic and the load on data producer. However, unlike traditional Internet

contents, IoT data are typically transient and periodically refreshed by the producer. At the same time, unlike Internet routers, IoT devices can be resource-constrained, with limitations in terms of energy, storage and processing capabilities. Therefore, caching algorithms designed for (intransient) Internet traffic and Internet routers do not well suit IoT domains. In this paper, we consider a wireless NDN-IoT network and propose a novel distributed probabilistic caching strategy that relies on the freshness of data and on potentially constrained capabilities of devices (energy level and storage capacity). The proposed solution has been evaluated through simulations with ndn SIM and results show that it outperforms traditional NDN caching mechanisms in terms of data retrieval and network energy efficiency

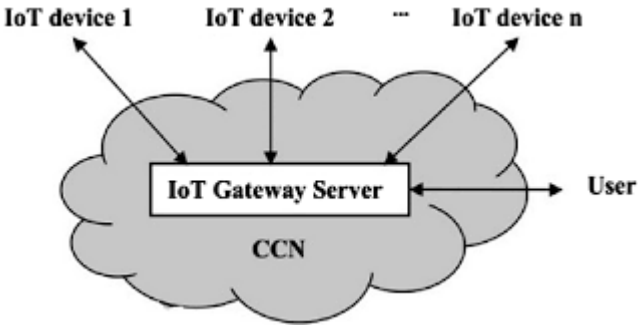

Fig -1: CCN Based IOT

1.2 NAMING AND SECURITY

Naming information plays an important role in the ICN concept. In today's Internet architecture, we mainly name the storage locations of information, e.g., we use Uniform Resource Locators (URLs) relating to a network node and file structure to name files, and Internet Protocol (IP) addresses to name the interfaces of the respective storage nodes. In information-centric networks, we name the information itself, i.e., we name Information Objects via location independent Object identifier (ID). Naming is closely related to security in several ICN architectures. In today's Internet architecture, security is an add-on to the original architecture that is mainly based on trusting the source of information via authentication and securing the data channel via encryption. In the ICN concept, security cannot be bound to the storage location as the network and/or user should benefit from any available copy. Consequently, new information-centric security concepts are required that base security on the information itself. A popular approach followed by several ICN architectures is to integrate security aspects with the naming concept, i.e., the object IDs. We define the following five general technical security goals in the ICN context: • Confidentiality: Only eligible entities (i.e., users or systems) can read secured information, i.e., IOs and corresponding metadata. • Data integrity: It is possible to identify accidental or intentional changes to IOs and the corresponding metadata. This is also referred to as self certification when closely integrated with the information itself. • Accountability: The owner/creator of information can be authenticated and/or identified. We explicitly differentiate between: – Owner authentication: Binds the information securely to a virtual entity, represented, e.g., by a pseudonym or a public/private key pair. – Owner identification: Binds the information securely to a real-world entity, e.g., a person's unique identity or an institution. • Availability: The IOs and corresponding metadata published in the network have to be available and accessible for (authorized) entities. • Controlled access: Access (i.e., read, write, execute) to IOs and/or corresponding metadata can be restricted to authorized entities

1.3. NAMING

The data in IoT-NDN are addressed by names. Requesting these data is based on hierarchically structured approach. The names contain human-friendly components and are location independent as shown in Fig. 2. Furthermore, IoT-NDN names describe a special task, an event or an application scenario. The architecture of IoT-NDN allows the applications to request specific data from producers or any device in the network using the naming mechanisms explained in this section. The marker component in IoT-NDN names is used to deliver further information about an application, service or devices resources. IoT-NDN Names could flexibly represent additional information about applications or specific events by adding them to the last component of the name. For example, the timestamps could be added as a last component to the Interest packet and can be used as a versioning component for all devices belongs to the wireless sensor network

1.4. DATA AGGREGATION

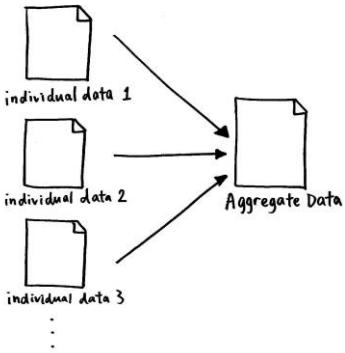

Fig -2: Data Aggregation Model

The aggregation, Forwarding Service, Unicast Faces and Intra Node Protocol (INP) components are explained in this section. Data aggregation in wireless networks is very important because of the device limitation in term of the memory size of CS and energy. For example, forwarding fewer Interests and Data packets saves a large quantity of energy. Furthermore, data which have the same meaning or

value could be aggregated in a Data packet and could be sent as an answer of the Interest packet to the consumer. NDN Integrated Data Centric services reachable from any device connected to the Internet, an IoT-NDN device runs as a gateway which has better performance in term of memory and energy. This gateway is developed to provide transition and services between the wired and wireless network. Furthermore, the gateway provides a protocol conversion from, e.g., the wired devices to the wireless devices such as in the IoT. Vice versa the application and service which are running on the devices using IoT-NDN should serve the requests and responses of other devices using this gateway.

1.5. DATA LIMITED FLOODING

IoT-NDN devices are often battery-powered and sometimes mobile and communicate through the unreliable broadcast shared medium in a multi-hop fashion. In such environments, the Forwarding Information Base (FIB) tables are usually not populated in advance by routing information. The Interest packets are broadcasted hop by-hop with controlled flooding mechanisms.

1.6. SENSOR NETWORK CACHING

The Content Store (CS) is the caching place for the Data packets in IoT-NDN devices (comparable with the buffer with routers in todays Internet Protocol). Routers with IP protocol also buffer Data packets but can not reuse it again after forwarding them, while IoTNDN devices are able to reuse the Data packets if they match the names of Interests. If an IoT-NDN device or router receives an Interest, it first looks in the CS for matching Data packets. The responsible algorithm of IoT-NDN checks the CS if a name of cached data is a prefix of the Interest name. If a match is found, then the Data packet is sent back to the consumer. In IoTNDN and other networks, different consumers are requesting the same data (multicast) which already requested before or could be lost during the transmission. Therefore, using the CS table can solve such problems. The dynamic data delivery can also benefit from caching the data in the CS.C

1.7. PACKET DATA FORWARDING

The forwarding strategy component in IoT-NDN system takes the task to select the forwarding paths from the FIB to forward Interest packets. This component could also be used to control the traffic by remembering the number of unsatisfied Interests. Also, the forwarding component chooses the faces which through the Interest packets could be forwarded using some performance metrics like delay or throughput. Such features are beneficial for the wireless network devices in term of select a specific forwarding or routing algorithm which matches better for the requirements of the constrained devices. IoT-NDN also supports the forwarding steps on devices and provides techniques for fast name Lookup

2. PROPOSED SYSTEM

In this project my idea is to develop integrating iot and content centric networking protocol with the help of e client data aggregation mechanism This paper aims to develop a new Internet architecture that can capitalize on strengths and address weaknesses of the Internet's current host-based, point-to point communication architecture in order to naturally accommodate emerging patterns of communication. In this method named data networking pattern helps us to transforms data into first class entity which helps us the network to perform faster with enhanced security, and automatic caching facility helps us to reduce bandwidth by providing recent visited contents and most viewed contents in cache and also enabling this method in sensor networks which will give a perfect blend of technical solution to solve network issues like security, bandwidth etcThe first part of this paper is analyzing the challenges of the IoT and discussed issues in IoT system using the current communication paradigm based on IP. The analyzed NDN protocol in this paper is related to the cache mechanisms, data aggregation and naming in wireless networks. Notably, building an IoT system based on the NDN is challenging again because NDN has not been developed for constrained devices which are limited with energy and memory.

3. SCOPE

In energy constrained sensor networks of large size, it is inefficient for sensors to transmit the data directly to the sink. In such scenarios, sensors can transmit data to a local aggregator or cluster head which aggregates data from all the sensors in its cluster and transmits the concise digest to the sink. This results in significant energy savings for the energy constrained sensors. Figure 2 shows a cluster based sensor network organization. The cluster heads can communicate with the sink directly via long range transmissions or multi hopping through other cluster heads. Recently, several cluster based network organization and data aggregation protocols have been proposed. In this section we discuss three such protocols. Security is another important issue in data aggregation applications and has been largely unexplored. Integrating security as an essential component of data aggregation protocols is an interesting problem for future research. Data aggregation in dynamic environments presents several challenges and is worth exploring in the future. Another interesting domain of research is the application of source coding theory for data gathering networks. The sensor data are usually highly correlated and energy efficiency can be achieved by joint source coding and data compression. Although some research has been pursued in this direction [20], there is significant scope for future work which will mainly focused on the development of an efficient routing mechanism for data aggregation. However,

the performance of the data aggregation protocol is strongly coupled with the infrastructure of the network. There has not been significant research on exploring the impact of heterogeneity and mode of communication (single hop versus multichip) on the performance of the data aggregation protocols. Although, many of the data aggregation techniques presented look promising, there is significant scope for future research. Combining aspects such as security, data latency and system lifetime in the context of data aggregation is worth exploring. A systematic study of the relation between energy efficiency and system lifetime is an avenue of future research. Analytical results on the bounds for lifetime of sensor networks is another area worth exploring. Existing work has provided bounds on lifetime for networks with specific network topologies and source behaviors. It would be interesting to extend this work to more general network topologies such as cluster based sensor networks The proposed framework enables secure data aggregation. However, simulations and experimental study are necessary to demonstrate the effectiveness of the approach. Although some discussion is included about the extension of the approach for hierarchical networks, a more detailed analysis is needed. In particular, functions such as median may not support hierarchical aggregation, Security in data transmission and aggregation is an important issue to be considered while designing sensor networks. In many applications, sensors are deployed in open environments and are susceptible to physical attacks which might compromise the sensor's cryptographic keys. Secure aggregation of information is a challenging task if the data aggregators and sensors are malicious. In this subsection, we describe some recent work which solve the secure data aggregation problem and also discuss some of the main issues involved in implementing security in sensor networks and these framework enables to integrate whole features with the help of iot to deal with less cost devices with more user friendly admin control

4. RELATED WORK

The Internet of Things (IoT) paves the way to interact with the smart objects namely sensors, hardware, circuits and software. Research in IoT ensures that collecting, processing and distributing the data needs to be improved to carryout data aggregation, processing and dissemination tasks of IoT data management. In the last few decades, various disaster management strategies have been proposed by the research community using different techniques, such as PUSH and PULL schemes, cloud infrastructure, and the Satisfied Interest Table (SIT). The focus is to minimize the communication time between mobile nodes, reduce memory consumption, improve the packet delivery ratio, and consume less energy. In this section, we present studies related to disaster scenarios. By identifying drawbacks from the major existing work as mentioned in Table 1, we introduce new IoT-based DMS architecture with the help of NDN architecture for a Smart Campus as shown in Figure 3.

Data Processing focuses on the characteristics Velocity, Volume, Variety, Variability, and Veracity. IoT Data Management may further be categorized as Communication, It depicts in Fig 1 Storage and Processing. Data communication involves data processing among objects, sensor data and hardware. To store the data, Cloud or distributed storage is used and processing involves filtering and analytics. Data dissemination distributes the processed data to end users. Message-delay in multi-hop massive IoT network is significantly optimized. This chapter enumerates the IoT data management frameworks, challenges and issues. Also, deployment of IoT Data management for smart home and smart city is described. According to a recent definition, data aggregation is the process of gathering and summarizing data from multiple sources. Aggregated data is normally found in a data warehouse. There, it can give answers to analytical questions and greatly reduce the time required to query large data sets. All things being equal, there is a need to identify suitable data aggregation techniques to collect and analyze incoming data. Typically, at this level, we differentiate between flat IoT data aggregation methods and a hierarchical approach to data aggregation. In flat wireless sensor networks, all sensors play an equal role—there is no hierarchical arrangement. Every sensor node serves the same purpose and all IoT sensor nodes are peers. One disadvantage of flat wireless sensor networks is that data aggregation takes place only in the sink node area. As a result, network delay can be high. Also, if the sink node fails, this negatively impacts the entire network. With the hierarchical approach to wireless sensor networks, there is a hierarchy among the individual nodes based on their capabilities. Roughly, these are divided into base stations, cluster heads, and sensor nodes. The sensor nodes within a given cluster communicate with each other and then communicate with the cluster head. More computing power and increased network transmission capabilities mean less battery life. So one of the main goals of this routing method is to achieve better energy efficiency for the sensors within a cluster. Cluster-based aggregation This is a hierarchical method best suited for large-scale energy-constrained sensor environments. In such scenarios, it is not efficient for the sensors to transmit the IoT data directly to the sink node (base station). Rather, sensors transmit data to a local aggregator, also known as a cluster head. The cluster head aggregates data from all the sensors in its cluster and transmits it to the sink node. The cluster heads can communicate with the sink node directly via long-range transmissions. They can also do multi-hopping through other cluster heads. The typical protocols here include clustered diffusion with dynamic data aggregation (CLUDDA), Low Energy Adaptive Clustering Hierarchy (LEACH), and Hybrid Energy-Efficient Distributed Clustering Approach (HEED). The main rationale behind data aggregation is that it minimizes energy depletion and the required network bandwidth. The use of different IoT data aggregation methods eliminates redundant data. This reduces network traffic by significantly minimizing the number of sent data

packages. IoT sensor nodes can also eliminate redundancies in the data received from neighboring nodes before transferring the final data packages. Another aspect to consider is the tradeoff between bandwidth and distance. For example, with Sigfox or LoRa, you can only send 2 bytes every 10 minutes but over very long distances. Questions of sustainability are also part of the discussion. Since sensor nodes are powered by batteries, saving energy and extending battery life is essential to the IoT data collection effort. Data aggregation is considered an energy-aware data collection technique and is preferred in scenarios where extending battery life is crucial. It is even known to increase the lifespan of WSNs. Energy aware data aggregation methods include clustered aggregation, tree-based aggregation, in-network aggregation, as well as centralized data aggregation that specifically considers the energy consumption of sensor nodes.

5. CONCLUSION

We have presented a comprehensive survey of data aggregation algorithms in wireless sensor networks. All of them focus on optimizing important performance measures such as network lifetime, data latency, data accuracy and energy consumption. Efficient organization, routing and data aggregation tree construction are the three main focus areas of data aggregation algorithms. We have described the main features, the advantages and disadvantages of each data aggregation algorithm. We have also discussed special features of data aggregation such as security and source coding. The trade-offs between energy efficiency, data accuracy and latency have been highlighted. Most of the existing IoT systems have application and device requirements such as scalability, robustness, power efficiency. The available solutions which are based on the host to-host IP method influence the communication performance in current and future Internet. Using the IP means also using IP addresses for all devices connected to the Internet That leads to the need for new protocols and algorithms to match the requirements of the IoT and its devices. Additionally, the security of the end-to-end oriented devices is not entirely covered using the IP. The data are a self-identifying unit which can be requested by sending an Interest packet (NDN message type) from any authorized consumer using location independent and unique names. The NDN communication model has some features such as scalable naming scheme, lightweight configuration, management operations and simple communication model. Therefore, NDN has been suggested as a particularly promising solution for IoT systems . IoT systems run many applications in different domains on heterogeneous and constrained devices that may request the same data regardless of their provenance. In my concept I am trying to design an interface which designed and developed to meet IoT-NDN system will enable the research community, industry, and different sectors to contribute to the future Internet of Things with the Named Data Networking method which resolve the network issues by using this concept.

REFERENCES

[1] Pourpeighambar, S. B., Aminian, M., & Sabaei, M. (2011). Energy efficient data aggregation of moving object in wireless sensor networks. In *Australasian telecommunication networks and applications conference* (pp. 1–8).M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[2] Krishnamachari, L., Estrin, D., & Wicker, S. (2002). The impact of data aggregation in wireless sensor networks. In *Proceedings of 22nd international conference of distributed computing system work* (pp. 575–578).K. Elissa, "Title of paper if known," unpublished.

[3] Cayirci, E. (2003). Data aggregation and dilution by modulus addressing in wireless sensor networks. *IEEE Communication Letters, 7*(8), 355–357.

[4] Madden, S., Franklin, M. J. Hellerstein, J. M., & Hong, W. (2002). TAG: A tiny aggregation service for ad hoc sensor networks. In *Proceedings of 5th symposium operating systems design implementation* (Vol. 36, no. SI, pp. 131–146).

[5] Al-Karaki, I. N., UI-Mustafa, R., & Kamal, A. E. (2004). Data aggregation in wireless sensor networks—Exact and approximate algorithms. In *Work. High performance switching and routing*, 2004. HPSR (pp. 241–245).

[6] Jesus, P., Baquero, C., & Almeida, P. S. (2015). A survey of distributed data aggregation algorithms. *IEEE Communications Surveys & Tutorials, 17*(1), 381–404.

[7] Li, W., Bandai, M., & Watanabe, T. (2010). Tradeoffs among delay, energy and accuracy of partial data aggregation in wireless sensor networks. In *Proceedings of IEEE international conference advanced information networking and applications AINA* (pp. 917–924).

[8] Shan, M., Chen, G., Luo, D., Zhu, X., & Wu, X. (2014). Building maximum lifetime shortest path data aggregation trees in wireless sensor networks. *ACM Transactions on Sensor Networks, 11*(1), 11–18.

[9] Din, I.U.; Almogren, A.; Guizani, M.; Zuair, M. A decade of Internet of Things: Analysis in the light of healthcare applications. IEEE Access 2019, 7, 89967–89979. [CrossRef]

[10] Tayyaba, S.K.; Khattak, H.A.; Almogren, A.; Shah, M.A.; Din, I.U.; Alkhalifa, I.; Guizani, M. 5G Vehicular Network Resource Management for Improving Radio Access Through Machine Learning. IEEE Access 2020, 8, 6792–6800

[11] Alghamdi, A.; Shetty, S. Survey toward a smart campus using the internet of things. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 22–24 August 2016; pp. 235–239.

[12] Haseeb, K.; Islam, N.; Almogren, A.; Din, I.U. Intrusion Prevention Framework for Secure Routing in WSN-Based Mobile Internet of Things. IEEE Access 2019, 7, 185496–185505. [CrossRef]

[13] Xylomenos, G.; Ververidis, C.N.; Siris, V.A.; Fotiou, N.; Tsilopoulos, C.; Vasilakos, X.; Katsaros, K.V.; Polyzos, G.C. A survey of information-centric networking research. IEEE Commun. Surv. Tutor. 2013, 16, 1024–1049. [CrossRef]

BIOGRAPHIES

Sreeja.S.Nair received the B.Tech degree in Computer Science and Engineering from Mahatma Gandhi University, Kerala, India in 2012. She is currently pursuing M.Tech degree in Computer Science and Engineering from APJ Abdul Kalam Technological University, Kerala, India at Mount Zion College of Engineering,Kadammanitta,Kerala, India. Her primary research interests are in Networking,IOT, data mining,AI, and Cyber Security

Nisha Mohan P.M. received the M.Tech degree in Communication and Networking from MS University, Tirunelveli, India in 2013. She is currently working as Assistant Professor in the Department of Computer science and Engineering at Mount Zion College of Engineering, Kadammanitta, Kerala, India. Her primary research interests are in Cloud Computing, Image Processing, Cyber Security and Artificial Intelligence (Machine Learning oriented programming).