ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 5 , May 2016

A Survey on Routing Protocols for Internet of Things

N. Jeba, V. Kamala

Assistant Professor, Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore, Tamilnadu, India.

Assistant Professor, Department of Computer Science and Engineering, KGiSL Institute of Technology,Coimbatore, Tamilnadu, India.

ABSTRACT: Internet of Things (IoT) is a wireless network of inter connected objects. It's a paradigm in which devices are embedded with sensors that will make them interact with other objects and humans as well. These objects are capable of capturing and transforming the information they receive from their environment. As IoT networks are self organizing and decentralized, the objects are transient and the network experiences dynamic changes in node position. Hence, routing has trivial importance where packets are transmitted between objects as a part of communication establishment and successful delivery of the packets should be ensured. Moreover due to its high dynamic nature route discovery incurs significant overhead and energy consumption. Thus there is a vital need to analyze the routing protocols for IoT. Popular routing protocols can be used in IoT, by intelligently considering the limited hardware available in devices, power consumption and their random behavior.

KEYWORDS: IoT, Routing Protocols.

I. INTRODUCTION

With the advent of the Internet, humans have been interconnected across geographical boundaries. IoT is a paradigm in which devices are embedded with sensors that will make them interact with other objects and humans as well. These objects are capable of capturing and transforming the information they receive from their environment. Advancement in sensing, computing and communication has brought in notable improvement in real time communication and decision making. Hence IoT aims to make the internet ubiquitous and pervasive in nature. The process of collecting, sharing and transmitting information will involve communication between nodes which act as both host and router with or without human intervention. In addition, the route discovery process incurs overhead due to beaconing, where the network is flooded with route request packets. Thus we have to quantify the energy and performance of each routing protocol. In addition, devices in IoT environment will be capable of location identification and notification and provide history of prior wireless connections. As billions of objects will be connected to the internet, it is vital to have an independent architecture that allows easy connection, communication and control. Interaction of these objects across platforms and times when they must be sharable and disjoint seems to be a challenge.

II. ROUTING PROTOCOLS FOR IOT

There exist lots of routing protocols each having a unique operating standard with significant performance for Wireless Sensor Networks that can be deployed for IoT with few modifications for bandwidth and power consumption. We discuss few of the broad categories of routing protocols in this section.

A.Naive Routing

The idea deployed in naïve routing is flooding. Each node can overhear its neighbors within its range. The source node floods the network with route request packets called as beacons. Destination nodes respond with a route reply message to the beacon and communication link is established between these nodes. Beaconing is typically utilized for location tracking, discovering routes to destinations and tracking neighbors through keep-alive requests. One of the most important factors that affect performance is the beacon interval in the route discovery process. If the beacon interval is too small, the number of beacons generated becomes huge. On the other hand, a higher beacon interval incurs a lesser number of generated beacons. Popular routing protocols such as DSR, DSDV and AODV fall under this category. However this flooding causes overhead in the network. By using steady state transition probability, we can derive the

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 5 , May 2016

power consumption for each node. This probability will give a clear picture of the individual node behavior and the overall network.

B.Hierarchical Routing:

Nodes form clusters based on polling. The cluster head is responsible for all communications on behalf of the members of the cluster. Group mobility can be achieved by the cluster head following some metric to devise the mobility pattern of the nodes in the cluster. LEACH is a common example, where the cluster head is rotated among the members to facilitate load balancing that can be deployed for IoT environments.

C.Query based Routing

The underlying principle of query based routing is data dissemination within the network. A querying node can retrieve data from any node in the network. Common examples are SPIN and Direct Diffusion.

D.Multipath routing

Protocols employing multipath routing seek to and use alternate paths towards every destination. This distributes the cost of forwarding packets among more nodes, saving the energy of individual, highly-frequented nodes.

E.Probabilistic routing

Routing decision is based on the calculated probabilistic value. A primitive method to compute these values is by gossiping. Data packets are flooded into the network like a rumor with a probability p. Unlike other flooding mechanisms, these packets are forwarded only once and thereby the traffic overhead is reduced. A highly structured approach is to refer the prior history of packet delivery and mobility pattern, based on this we can decide which nodes can form a route to the destination.

F.Ad-hoc On-Demand Distance Vector (AODV)

AODV computes a loop free single path on demand. A mobile node discovers and maintains a route to another node only when it needs to communicate. One observation of AODV is that, though the source actually discovers multiple paths during the route discovery process, it chooses only the best route and discards the rest. Also, frequent route breaks cause the intermediate nodes to drop packets because no alternate path to the destination is available. This reduces the overall throughput and the packet delivery ratio. Moreover, in high mobility scenarios, the average end-to-end delay can be significantly high due to frequent route discoveries. When route failures occur, the process of route discovery has to begin from scratch consuming more network resources and overhead [5].

G. Adhoc On-Demand Multipath Distance Vector (AOMDV)

In order to route with low overheads even under highly dynamic conditions, Adhoc On-Demand Multipath Distance Vector was introduced. AOMDV computes multiple loop free and link disjoint paths providing fault tolerance and efficient recovery from route failures. Each node maintains a list of its next hop neighbors that are sorted based on the hop count. When failures occurs during routing an alternate path is chosen, if there is no alternate path a route error message is given. The routing metric considered is the number of hops, thus paths with a small number of long hops are chosen. When paths with long hops are chosen, there is high probability for the occurrence of fading. Moreover the stability of the path is completely ignored as the alternate paths are not maintained. Thus the paths are stale and cannot be used on a failure. Therefore AOMDV is not adaptive to the dynamic changes in network topology [5].

H. Routing Protocol for Low Power and Lossy Networks (RPL)

RPL is based on IPv6 and is a link independent routing protocol which supports routing with minimal requirements by building a robust topology over lossy links. This routing protocol achieves multipoint-to-point, point-to-multipoint and point-to-point communication for simple and complex traffic models. The core of RPL is represented by a Destination

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 5 , May 2016

Oriented Directed Acyclic Graph (DODAG), which is a directed acyclic graph with a single root. Each node knows its parent but has no information about its related children. RPL maintains atleast one path for each node to the root along with a preferred parent to pursue a faster path establishment to increase the performance. In order to maintain the routing topology and to keep the routing information updated, RPL uses four types of control messages – DODAG Information Object (DIO), Destination Advertisement Object (DAO), DODAG Information Solicitation (DIS) and DAO Acknowledgment (DAS-ACK). The current rank of the node is stored in DIO, which determines the distance of each node to the root based on specific metrics and determines a unique parent path. The destination information is unicasted towards selected parents using DAO. RPL supports both upward and downward traffic. DIS is used to acquire DIO messages from a reachable adjacent node. DAO-ACK is a response to DAO message from a DAO parent node. DODAG is formed when the source nodes begins to send its location using DIO message to Low-power Lossy Network (LLN) levels. At each level the recipient routers register the paths for parent and participating nodes. As DIO messages propagate in the network, DODAG is built. After the construction of DODAG, a preferred parent establishes a default path with the root known as upward route. For downward routes, DAO message should be unicasted to the root through parents.

III. OPEN RESEARCH CHALLENGES

The gamut of research required to achieve successful routing in IoT raise few unique challenges that traditional routing protocols lack. This section addresses few of these challenges.

A. Security

The primary challenge that is prevalent in IoT and must be solved is dealing with security attacks. Minimal capacity of the devices, wireless communication and random failures – permanent or transient are major vulnerabilities that attackers exploit. To restore from an attack, the system must detect and diagnose the attack and deploy counter measures to heal from the same in a light weight manner due to the limited hardware resources. However routing must be safe amidst these attacks and there must be a mechanism to recover effectively from security attacks.

B. Interoperability

End to end interoperability is a challenge in IoT, as large number of heterogeneous devices which operate in different platforms should be effectively handled. So, there is a need for interoperation of the underlying technologies.

C. Mobility

Mobility is yet another challenge for IoT implementations since communication should be established with mobile users and service should be rendered even when the devices are in move. Interruption can occur when information transfers from one gateway to another. Successful communication can be achieved by caching and tunneling the services, which allow applications to access data even when resources are temporarily unavailable.

D. Energy

For successful communication, the quality of the link should be quantified based on certain metrics. The most commonly used technique is hop count, were the route with minimum number of hops are chosen. However this is not ideal, as some links might be error prone. A good choice would be to introduce energy awareness in the existing routing protocols. It’s apt to choose a node with more residual energy to prolong the life time of the link.

IV. CONCLUSION

In this paper we have described the routing protocols that can be used for communication in IoT and the open research challenges. Due to the lack of benchmarks, the protocols mentioned can only be evaluated based upon its features. These protocols must be simulated and tested in the target environment to reveal its potential implementation for Internet of Things.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 5 , May 2016

REFERENCES

[1] Chiara Buratti, Sebastino Milardo, “Testing Protocols for the Internet of Things on the EuWin Platform”, Journal of Internet of Things 2015.
[2] Oladayo Belloe, Sherali Zeadally, “Intelligent Device to Device Communication in the Internet of Things”, IEEE Systems Journal 2014
[3] Xianzhong Tian, Yi-Hua Zhu,Kaikai Chi, Jiajia Liu, Daqiang Zhang, “Reliable and Energy-Efficient Data Forwarding in Industrial Wireless Sensor Networks” IEEE Systems Journal 2015
[4] Andrea Zanella, Lorenzo Vangelista, “Internet of Things for Smart Cities”, IEEE Internet of Things Journal, Vol.1, No.1, February 2014.
[5] N. Jeba, “An Efficient and Optimal Adaptive Routing Technique for MANET with Fading Avoidance”, IJARCSMS, Volume 2, Issue 3, March 2014.
[6] Jose L Hernandez-Ramos, Jorge Bernal Bernabe, Antonio F Skarmeta, “ Managing Contex Information for Adaptive Security in IoT environments”, 29th Internation Conference on Advanced Information Networking and Applications Workshops, 2015.
[7] Sriram Sankaran, Ramalingam Sridhar, “Modeling and Analysis of Routing in IoT Networks”, CoCoNet’15.
[8] Masanori Ishino, Yuki Koizumi, Toru Hasegawa, “A Study on a Routing-based Mobility Management Architecture for IoT Devices”, International Conference on Network Protocols, 2015.
[9] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, Moussa Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols and Applications”, IEEE Communications Surveys & Tutorials 2015.
[10] Jinhyuk Yim, Woo-Sung Jung, Young-Bae Ko, “Link Quality Based Geographic Routing Resilient to Location Errors”, ICUFN 2015.
[11] Surapon Kraijak, Panwit Tuwanut, “A Survey on Internet of Things Architecture, Protocols, Possible Applications, Security, Privacy, Real-world Implementation and Future Trends”, ICCT 2015.
[12] Sudip Misra, P. Venkata Krishna, Anshima Gupta, Mohammad S Obaidat, “An Adaptive Learning Approach for Fault –Tolerant Routing in Internet of Things”, 2012 IEEE Wireless Communications and Networking Conference.