An Analysis on Routing Protocols for Internet of Things

Dr. Ajay Jangra
UIET, Kurukshetra University, Kurukshetra, Haryana, India

Menakshi
UIET, Kurukshetra University, Kurukshetra, Haryana, India

DOI: 10.23956/ijarcsse/V7I5/0117

Abstract-- IoT provides interconnectivity between various devices crossover in sparse or dense areas. Devices may transfer data with each other through different routing protocols. A device movement can be controlled by movement model so it is clear that movement of nodes may effect on routing process. In this paper challenges in IoT routing protocols of IoT has been discussed in detail. After that comparative analysis of these routing protocols with various performance metrics like latency, route optimization and energy consumption has been done.

Keywords-- Internet of Things (IoT), Routing, AODV, DSR and Sensor.

I. INTRODUCTION

With the appearance of the Internet, people have been interconnected crosswise over geological limits. IoT is a worldview in which devices are installed with sensors that will make them interface with different articles and people also. These articles are fit for catching and changing the data they get from their condition. Headway in detecting, figuring and correspondence has acquired prominent change continuously correspondence and basic leadership [1]. Subsequently IoT expects to make the web universal and unavoidable in nature. The way toward gathering, sharing and transmitting data will include correspondence between nodes which go about as both host and router with or, on the other hand without human intercession. Also, the route disclosure prepare brings about overhead because of beaconing, where the network is overflowed with route ask for parcels. Subsequently we need to measure the energy and execution of each routing convention. Also, devices in IoT condition will be fit for area recognizable proof and warning and give history of earlier wireless associations. As billions of items will be associated with the web, it is essential to have an autonomous design that permits simple association, correspondence and control [2]. Association of these articles over stages and times when they should be sharable and disjoint is by all accounts a test. Internet of Things (IoT) is a wireless network of bury associated objects. It’s a worldview in which devices are inserted with sensors that will make them collaborate with different items and people also. These items are fit for catching and changing the data they get from their condition [3]. As IoT networks are self arranging and decentralized, the items are transient and the network encounters dynamic changes in node position. Subsequently, routing has minor significance where bundles are transmitted between articles as a piece of correspondence foundation and effective conveyance of the bundles ought to be guaranteed. In addition because of its high dynamic nature route disclosure brings about critical overhead and energy utilization.

A. Challenges in IoT: In IoT environment there are some open challenges like energy, mobility and many more. In this section these challenges are discussed [4].

- Security: The essential test that is common in IoT and must be settled is managing security attacks. Insignificant limit of the gadgets, wireless correspondence and arbitrary disappointments – changeless or transient are real vulnerabilities that aggressors misuse. To reestablish from an assault, the framework must distinguish and analyze the assault and send counter measures to mend from the same in a light weight way because of the constrained equipment assets. However routing must be sheltered in the midst of these attacks and there must be a system to recuperate adequately from security attacks.
- Interoperability: End to end interoperability is a test in IoT, as vast number of heterogeneous devices which work in various stages ought to be adequately dealt with. Along these lines, there is a requirement for interoperation of the basic advancements.
- Mobility: Mobility is yet another test for IoT usage since correspondence ought to be built up with versatile clients and administration ought to be rendered notwithstanding when the devices are in move. Interference can happen when data exchanges starting with one portal then onto the next. Effective correspondence can be accomplished by storing and burrowing the administrations, which enable applications to get to information notwithstanding when assets are briefly inaccessible.
- Energy: For effective correspondence, the nature of the connection ought to be measured in light of specific measurements. The most usually utilized method is jump tally, were the route with least number of bounces are picked. However this is definitely not perfect, as a few connections may be mistake inclined. A decent decision is present energy mindfulness in the current routing conventions. It's well-suited to pick a node with more leftover energy to drag out the life time of the connection.
B. Routing in IoT: In this section, standard routing protocols of IoT have been discussed. These are as follows:

- **Ad Hoc On-Demand Distance Vector Routing**
  
  At the point when a source node needs to make an impression on some destination nodes, it communicates route ask for message (RREQ) to its neighbors. The neighbors thus will communicate the message to their own neighbors. Amid the way toward sending the RREQ, a node advances a route ask for message to its neighbors, and it likewise records in its routing tables the source node from which the main duplicate of the demand came. The routing table is utilized to develop the switch way for the route answer message. Once the RREQ achieves the destination, the destination node reacts by unicasting a route answer message (RREP) back to the neighbor from which it initially got the RREQ. At the point when the route answer message (RREP) crosses back to the source, the nodes along the way enter the forward route tables which indicate the node from which the RREP came [5].

- **Dynamic Source Routing**
  
  Dynamic source routing has two noteworthy segments: (i) route revelation and (ii) route support. Route disclosure: When a source node needs to make an impression on some destination nodes, it initially finds its route store to decide whether it as of now has a route to the destination. On the off chance that a substantial route to the destination found, the source node will utilize this route to send the message. On the off chance that a legitimate route does not exist, it will begin the route revelation handle by communicating a route asks for message [6]. Route upkeep: The node produces a route blunder message when it experiences a deadly transmission issue at its information interface layer. In the event that a node gets a route blunder message, it will expel the bounce in mistake from its route reserve. All routes that contain the bounce in blunder will be truncated by then as well. Affirmation parcels are constantly used to confirm the right operation of the route joins.

- **Optimized Link State Routing**
  
  In OLSR the nodes need to trade data between each other occasionally to refresh and assemble their own particular system topology through disseminated figuring. A few nodes are chosen as Multi-Point Relay (MPR) and are utilized as routing node and the MPR selector does not take an interest in routing calculation [7].

II. RELATED WORK

Chengming et. al.[8] proposed SINS/WSN coordinated with movement state rectification technique in GPS-denied conditions.

Newell and Vejarano [9] a transmission control convention for remote body region networks that limits control utilization was produced, executed, and assessed tentatively.

Jianlong et. al.[10] proposed an IoV (Internet of Vehicle) platform, aimed to support the development of BEV (Battery Electric Vehicles). With the help of charging station, there are three main functions of this platform.

Fangchun et al. [11] proposed an abstract network model of the IoV, discussed the technologies required to create the IoV, presented different applications based on certain currently existing technologies, provides several open research challenges and describes essential future research in the area of IoV.

III. COMPARATIVE ANALYSIS

In this section comparison of various existing routing protocols of IoT with performance parameters like latency, energy consumption, redundancy elimination and route optimization has been shown.

- **Latency**: It indicates time delay occurred starting from message creation to message delivery.
- **Energy Consumption**: It shows how many energy is consumed during message transmission from source to destination.
- **Redundancy Elimination**: It shows how much duplicate data will be removed by routing algorithm.
- **Route Optimization**: It shows an optimal route must be chosen for message transmission.

<table>
<thead>
<tr>
<th>Routing Protocols</th>
<th>Latency</th>
<th>Energy consumption</th>
<th>Redundancy elimination</th>
<th>Route optimization</th>
</tr>
</thead>
<tbody>
<tr>
<td>AODV</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>DSR</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>OLSR</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
</tr>
</tbody>
</table>

IV. PROPAGATION MODELS

The propagation models are used to compute the received power. When a packet is received, the propagation model determines the attenuation between transmitter and receiver and computes the received signal strength. If the signal strength is lower than the Carrier Sensing Threshold, then packet is discarded by the physical layer. If the level is higher than this threshold, the signal strength is then compared with the receiver threshold. This threshold determines if the packet is received successfully or with errors; in the first case the packet is passed to the MAC layer, in the second case the packet is marked as erroneous and passed to the MAC layer that will provide to discard it.

Erroneous packets are delivered to the MAC layer so that it can detect a packet collision where multi-packets are received simultaneously. In this case the MAC layer determines the ratio between the strongest received signal strength and the sum of the other signal levels. The ratio is then compared with the CPThresh threshold that determines if the packet has been destroyed by a collision or it captured the channel.
The Free space model is the simplest one. It assumes ideal propagation conditions and a single line-of-sight path between the transmitter and receiver. The Two-ray ground reflection model considers both the direct path and a ground reflection path. As with the free space model, both transmitter and receiver node are assumed to be in line of sight. It has been shown that this model is more accurate than free space model in case of long distance line of sight path. Both the Free space model and the Two-ray model predict the received power as a deterministic function of the distance between the transmitter and receiver. A more realistic model is the Shadowing model. It adds to the deterministic path loss, a random component to the received power that attempts to reproduce random variability typical of wireless links (e.g. fading). The shadowing model consists, in fact, of two parts: the first one is the deterministic path loss that predicts the received power from the distance between the receiver and transmitter nodes; the second part of the shadowing model reflects the variation of the received power at certain distance.

V. CONCLUSION

Routing plays important role while data is transmitted between devices. There are number of routing protocols available such as AODV, DSR and OLSR. In this paper IoT and its technical challenges has been discussed. After that comparison between different routing protocols with different performance parameters has been presented. Comparative analysis shows that AODV is best suited routing protocols for IoT data transmission. In future try to enhance existing AODV routing protocols with better route optimization less and message delay etc.

REFERENCES