International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 07, Issue: 02 (March-April, 2021)

A Survey: Energy-Efficient Mobile Adhoc Network

Taruna Saxena, Bhanu Pratap Singh
Department of Computer Science and Engineering,
All Saint College of Technology, Bhopal
Tarunasaxena.india@mail.com

Abstract: - *In recent years, the technology of wireless networks has gained much importance. Wireless networks are a special case of ad-hoc wireless networks. A wireless network is a collection of sensor nodes that communicate through wireless links to work together to carry out functions. This paper gives a birds-eye over routing protocol of sensor network that concentrates over energy-efficient routing in other to longer survival of mobile Adhoc network.*

Keywords:- Wireless network, Mobile Adhoc network, Encryption, Energy-saving routing

I.INTRODUCTION

An ad-hoc wireless network is a distributed kind of wirelessly connected network. The ad-hoc nature demonstrates that it does not depend on a pre-existing infrastructure, like routers in wired networks. There is an access point in wired networks connected to all other devices in the network for communication. Instead, in the wireless network, each node contributes to routing by forwarding data to other nodes. Energy-saving is a major issue in ad-hoc wireless networks. In the ad-hoc wireless network, energy consumption is based on several data transmission. A greater number of transmissions is equal to more energy consumption, and a smaller number of transmissions is equal to less energy consumption. We studied that network coding uses less transmission, so that network coding can be used to reduce energy consumption in the ad-hoc wireless network. With network coding, energy can be reduced by encryption/decryption of data; due to encryption/decryption, data transmission more secure from external users, which create confusion to eavesdropper cannot detect the actual data. Data also contains redundant data and false data, which has to be eliminated or reduced to better the ad-hoc wireless network. We studied that Support Vector Machine (SVM) can detect and reduce these redundant data by using Locality Sensitive Hashing, which is based on the data similarity on each node and improved network performance with less energy consumption.

In addition to the classic routing, ad-hoc networks can use flooding for forwarding the data. Figure1 wireless ad-hoc network that communicates with a router and wireless access point that manage the wireless network.

An ad-hoc network denotes a set of networks where all devices have similar status and are free to connect with any other network device in a defined range. Ad-hoc network often denotes a mode of process of IEEE 802.11 wireless networks.

Figure 1 Wireless Ad-hoc Network

The earliest wireless ad-hoc networks were the PRNETs. Multiple devices connected by "links create an ad-hoc network". Links are subjective to the node's behavioural properties and resources, similarly link properties. The links are unstable by nature, and connectivity is affected at a network is dynamic, preferably in a way that is efficient, timely, robust, reliable, and scalable to cope with restructuring. The network must allow cooperative communication by forwarding the information through other nodes. So, a "path" is a sequence of several connected devices.

Wireless networks consist of local, metropolitan, wide and global areas. In most wireless ad-hoc networks, nodes participate to access a shared wireless channel, frequently causing collisions and packet drop. That improves immunity to snooping by having the sink node associate self-interference and a different node interference to enhance decoding of the preferred signal.

A mobile ad-hoc network is a wireless network that communicates from device to device. It means such devices can directly communicate with all other nodes within their radio range. All devices must communicate at a central administrative unit, the peer - to - peer communication methods can extend the range of wireless communication networks. One of the devices can be linked through wired or wireless to a service provider to access the services.

Ad-hoc wireless devices can detect the connection with neighbouring nodes or devices and identify their type and corresponding attributes. There is no need to use a fixed infrastructure. Ad-hoc mobile devices imply battery capacity of devices that can vary from device to device, and for forwarding the data packet, the Ad-hoc mobile network consumes power, so it is a crucial issue. There are some metrics proposed for power-aware routing:

1. Minimum energy consumed per packet
2. Maximum time to network partition
3. Minimum variance in node power level
4. Minimum, maximum node cost
5. Minimum cost per packet

II. Ad-hoc Routing Protocols

An ad-hoc routing protocol is a standard that regulates how nodes find the way to route packets among communicating devices in ad-hoc networks. In ad-hoc networks, initially, nodes do not figure out the topology of networks, therefore discovering it. The basic concept is that a new node may broadcast its presence and observe broadcast by its adjacent nodes. Each node acquires knowledge about nearby nodes and for the path to reach those.

A. Pro-active (table-driven) routing

Such kind of protocols manage fresh lists of destinations and their routes. That is performed by updating routing tables overall the network. The main difficulties of such algorithms are:

1. Maintenance such a large amount of data.
2. Deliberate reaction on rearrangement and failures.

B. Reactive (on-demand) Routing

This type of protocols routes is discovered on-demand basis using the flooding concept with Route Request packets. The main drawbacks of such algorithms are:

1. High latency time in route finding.
2. Excessive flooding can lead to network congestion

C. Flow-oriented Routing

This type of protocols discovers a route on-demand by considering the current flows. One opportunity is to sequentially unicast when forwarding data while supporting a new connection. The main drawbacks of such algorithms are:

1. It takes a long time when discovering new routes without a piece of previous knowledge.
2. May rise to existing traffic to reward for missing knowledge on routes.

D. Hybrid (both pro-active and reactive) Routing

This type of protocols hybridizes the benefits of pro-active and reactive routing. The routing is initially recognized with pro-actively mined routes and then obliges the demand from additional nodes using the reactive flooding technique. The selection of one of the different method involves pre-computation for complex cases. The main drawbacks of such algorithms are:

1. The benefit depends on the number of active nodes.
2. Traffic demand response gradient depending on traffic volume.

E. HIERARCHICAL ROUTING PROTOCOLS

The selection of pro-active and reactive routing is subject to the hierarchic. The routing is arranged by some pro-actively prospected routes and serves on-demand on the lower levels. The selection technique requires proper acknowledgement for particular levels. The main drawbacks of these algorithms are:

1. Advantage depends on the depth of nesting and addressing scheme
2. Reaction to traffic demand depends on meshing parameters

F. BACKPRESSURE ROUTING

This type of routing paths is pre-computed. It selects next-hops when a packet is in progress towards the destination. These judgments are based on the congestion of neighbour nodes. This routing is used with max-weight scheduling; this produces optimal throughput.

G. Host Specific Routing Protocols

This type of protocols needs administration to adopt the routing for certain network topology and a unique flow approach; the main difficulties of these algorithms are :

- Depending on the quality of the benefit plan administration addressed.
- The proper reaction to changes in topology demands reconsidering all parameters

H. POWER-AWARE ROUTING PROTOCOLS

The energy required for transmission of a signal is proportional to d^{α} where d is the distance between devices and $\alpha >= 2$ considered path loss exponent or attenuation factor that directly depends on the transmission channel. When $\alpha = 2$, transmitting a signal half the distance needs one-fourth of the energy. But, if a node in the middle wants to consume another fourth of

its energy for the second half, data would be transmitted for half of the energy than through direct transmission. The main disadvantages of such algorithms are:

1. This method induces a delay for each transmission.
2. No significance for energy network powered transmission functioned via sufficient repeater infrastructure.

III. RELATED WORK

Boniewicz [8] compare the algorithms proposed in the method of the wireless sensor network. Energy consumption is very important for self-powered radio nodes. But some energy applications balance is more important. Networks of wireless sensors used in large areas such as farmland or stores consist of hundreds of nodes. The conventional method of routing is directed to transmit a short time and low energy consumption. But consumption of unbalanced energy can often cause unpredictable failures due to lack of energy in frequent use nodes. Energy balance to avoid this dynamic behaviour by skipping nodes used. The document discloses examples of algorithms that may be used in the method of the wireless sensor network. This method aims to extend the network via a data path selection to minimize the network nodes' energy dispersion.

Hartwell [9] Understand energy consumption in a wireless sensor network is the most important of these networks inexpensive sensors deployed appearance. This role models and calculates the energy consumption of a network, such as an intrusion into a secure zone is followed. The network comprises a wireless sensor without randomly distributed, simulating several protocols to transmit information to the detection matrix. Increasing the number of heads of munitions range sensor and increasing the transmission range of individual nodes directly reduces the energy consumed while monitoring intrusion. However, increasing the precision of the sensor increases energy consumption while monitoring intrusion. Models created to simulate a network, its protocols and data transfers, and a penetrating agent, has proven to be an effective set of tools to test network conditions and determine the cost of energy.

Bala Krishna [7] Propose energy organized aware clustering protocol (SECC) for sensor networks wireless sensor network-based energy node and remote node groups. Suppose the node's energy is less than the threshold value, SECC self-organized clusters of forms and reorganize the sensor array. The nodes having less than the threshold value energy attributes are removed from the cluster network to maintain efficient energy sensors. Energy management in clusters SECC node function parameters (such as remote node, power node, the node density) and cluster parameters (such as cluster density, sensor nodes per group). Performance analysis and simulation results are given with variations in the number of clusters, the energy levels, and the node's distance.

Peng Zhang [11] Proposed a lightweight encryption scheme to provide confidentiality for network-coded MANETS in an energy-efficient way. P-Coding's basic idea is to let the source randomly permute each packet's symbols (which is prefixed with its coding vector) before performing network coding operations. Without knowing the permutation, eavesdroppers cannot locate coding vectors for correct decoding and cannot obtain any meaningful information.

This section of the report contains the observations and facts that help develop problem statements and solution.

Some recent works promised to improve the Energy Consumption and Security for increasing the routing protocol's performance. Common concepts are used the encryption/decryption technique and network coding, proving the secure data transmission in a smaller number of transmission networks. They defined that each node in the network has some attributes (like identity, threshold), based on these attributes can transmit from one node to their neighbour node. It includes the allowable overhearing of control messages from adjacent nodes and limiting the local repair for a small topological range of the link break; therefore, alternative routes to the sink node can be found quickly with optimum routing overheads—a range of threshold values for changing network scenarios, specifically for different network load conditions. Demonstrate a decision-making process for energy-saving and security technique that is flexible and adaptive for different network load conditions and leads to a performance improvement. A routeing table that is maintained by each node in the network contains the following information:

- Destination
- Next hop
- Number of hops
- Destination sequence number
- Active neighbours for this route
- Expiration time for the route table entry

After studied different research papers and article, some of the problems associated with the previous paper are investigated, and they are:

1. Dynamic topology is the main problem in previous work done.
2. When the density of network nodes increases, the throughput of the network decreases.
3. Dynamic multicast routing problem arises through the node moment independently with different speed in the network.
4. Dynamic topology creates the current issues such as data redundancy problem, a false data problem, lost data in routing, TSP problem, route break frequently problem, channel bit issues (BER) problem, and other real-time problems.
5. Dynamic topology also increases the packet drop ratio and end to end delay.

IV. CONCLUSION

Energy Consumption and Security for increasing the routing protocol's performance, a common concept is that encryption/decryption technique and network coding prove the secure data transmission in a smaller number of transmissions in the network. They defined that each node in the network has some attributes (like identity, threshold), based on these attributes can transmit from one node to their neighbour node. It includes the allowable overhearing of control messages from adjacent nodes and limiting the local repair for a small topological range of the link break; therefore, alternative routes to the sink node can be found quickly with optimum routing overheads.

REFERENCE

1. Zunnun Narmawala, Sanjay Srivastava, "Survey of Applications of Network Coding in Wired and 12.
Wireless Networks" in Proceedings of the 14th National Conference on Communications, pp. 153-157, February 2018.
2. Sheikh, R., Singh Chande, M. and Mishra, D.K., "Security issues in MANET: A review", IEEE 2019, pp 1-4.
3. Kannhavong, B., Nakayama, H., Nemoto, Y. and Kato, N., " A survey of routing attacks in mobile ad hoc networks" IEEE 2017, pp 85-91.
4. Verma, M.K. and Joshi, S.; Doohan, N.V. "A survey on An analysis of secure routing of volatile nodes in MANET", IEEE 2012, pp 1-3.
5. Mariannne. A. Azer, "Wormhole Attacks Mitigation in Ad Hoc Networks", IEEE 2018, pp 561-568.
6. Ren Yueqing, Xu Lixin A study on topological characteristics of wireless sensor network based on the complex network", IEEE 2017, pp 486 - 489
7. Bala Krishna, M., Doja, M.N., "Self-organized energy-conscious clustering protocol for wireless sensor networks", IEEE 2018, pp 521 - 526
8. Boniewicz, Miroslaw Toruń, Poland Kozlowska, Anna ; Zawadzka, Anna ; Lukasiak, Zbigniew ; Zielinski, Marek "Review of selected algorithms in the method energy evening algorithm in wireless sensor network", IEEE 2019, pp 1 – 4.
9. Hartwell, R., Wireless Sensor Network Energy Use While Tracking Secure Area Intrusions" IEEE 2019, pp 1696 – 1701
10. Baghyalakshmi, D.; Ebenezer, J.; SatyaMurty, S.A.V. "Low latency and energy-efficient routing protocols for wireless sensor networks", IEEE 2020, pp 1 – 6.
11. Peng Zhang, Chuang Lin "A Lightweight Encryption Scheme for Network-Coded Mobile Ad Hoc Networks" in IEEE Transactions on Parallel And Distributed Systems, 1045-9219, 2018 IEEE.