Available online at www.elixirpublishers.com (Elixir International Journal)

Network Engineering

Elixir Network Engg. 80 (2015) 31285-31288

ISSN: 2229-712X

A Review: Characterizing an Analysis of Important Parameters for Infrastructure less Based Networks-MANETs

Kiran Kapalta and Ravinder Thakur

HPTU, Hamirpur,L.R.I.E.T,Solan, Himachal Pradesh, India.

ARTICLE INFO

Article history:

Received: 17 October 2014;

Received in revised form:

28 February 2015;

Accepted: 23 March 2015;

Keywords

MANET's,
Performance analysis,
Reliability,
Power saving,
Efficiency, Security.

ABSTRACT

Today in the world of computer networking, wireless networks are becoming one of the most popular, valuable, decisive & critical medium for communication. Among the wireless networks, MANET's i.e., Mobile Ad-hoc Networks are of their own importance. For the purpose of group communication, there are many applications of MANET's in the areas like as an automated battlefields, crowd control, disaster recovery, conference, search and rescue operations etc. An Ad-hoc Network is basically a wireless network comprising a set of mobile nodes in absence of any centralized access point or fixed infrastructure.In this paper, the necessary parameters which are required to characterize the MANET's have been presented. A kind of review is done upon these important parameters. The various parameters responsible for the routing strategies in MANETs are the parameters like as performance analysis, reliability, scalability, power saving, efficiency as well as security.By depicting these essential parameters for MANETs, we are able to make proper as well as efficient utilization of MANETs in various fields of communication such as conferencing, pollution monitoring, emergency services like battlefield, disaster recovery, vehicular networks, etc.

Introduction

An infrastructure-less (ad-hoc) network is one of the newly developing wireless networking technology that has been replaced almost all of the wired networks because of its several advantageous applications. This type of network is basically a collection of autonomous nodes that communicate with each other by forming a multi-hop radio network.

MANETs are basically the dynamic peer-to-peer networks, which employs multi-hop transfer of information without having any need of infrastructure to communicate. Wireless Network Topology is defined as the configuration in which a mobile terminal communicates with another terminal. Wireless Networks are broadly classified in two classes – infrastructure-based networks (WLAN) and infrastructure- less based (MANET) networks.

Infrastructure based network is a collection of nodes that communicate with each other through access points. In this network, access point acts like a hub or a base station, providing connectivity for the wireless computers. Each access point has a finite range within which a wireless connection can be maintained between clients. In order to communicate with a client beyond its radio range, access point acts as a router.

In the second category of wireless networks, the ad-hoc or an infrastructure- less based networks works without any pre-existing infrastructure. They are easy to deploy and set up at any place and time, hence it has decreased the dependence of the infrastructure. So ad-hoc networks became a very important technique these days because of its several advantageous features.

The various fields of MANETs applications like as disaster recovery, pollution monitoring, conferencing, etc requires group communication like as one-to-many & many-to-many. To make an efficient as well as effective use of MANETs, we need to emphasize upon the various essential parameters such as performance analysis, power saving, efficiency as well as security. By virtue of considering these important parameters in mind, the users are able to make communication efficiently & securely over the networks.

Characteristic Features of MANETs

There are several characteristic features of MANET's & these are as follows:

i. Autonomous and infrastructure-less
ii. Multi-hop routing
iii. Dynamic network topology
iv. Reduces delivery delay
v. Device heterogeneity
vi. Less power consumption.
vii. Reduces overhead
viii. Self-creation, self-organization and self-administration
ix. Performance & reliability
x. Network scalability

Literature Review

In this paper, a kind of review is done which basically emphasizes upon the necessary parameters which are responsible for an efficient & secure communication using MANETs.

These parameters are discussed in detail as follows:

- Performance Evaluation,
- Delay, Reliability & Trust,
- Security,
- Power Saving,
- Least Control Overhead.

Performance Evaluation

Mobile Ad Hoc Networks (MANETs) are multi hop wireless networks that result from the cooperative engagement of a collection of mobile hosts without any centralized access point and infra- structure. Mobile nodes that are within each

Tele:
E-mail addresses: kiran.063erkapalta@gmail.com

other's radio range communicate directly via wireless links, while those that are far apart, rely on the other nodes to relay messages i.e. act as routers or hops. Since the mobile nodes in the MANET dynamically establish routes among themselves to form their own network, such networks are also known as infrastructure less networks.

MANET is an excellent tool to handle the situations like disaster recovery, crowd control, search and rescue operation, and automated battlefields, etc. where no infrastructure exists at the time of occurrence of such events. The nodes move arbitrarily and its topology also changes frequently.

Factors Responsible For Performance Evaluation

A. Vertical and Horizontal Scalability

For the performance evaluation, a multicasting technique named Scalable overlay Multicasting (SOM) is used. [4] SOM supports both the scalability, vertical (bigger group size) as well as horizontal (more number of groups). Vertical scalability is achieved due to the fact that state maintenance is confined only to group members. SOM uses source based data delivery tree, therefore the data traffic of all the groups would be passed through the group members and the intermediate nodes fall on the path only. No core or specific group of nodes is responsible for the data traffic forwarding, therefore horizontal scalability is another achievement of the protocol.

Less Network Latency and Delay

By using source based tree, multicast traffic is transmitted directly to the receivers without going through the shared root. Thus, source based tree architecture reduces network latency and possible congestion at the shared root. The latency in updating the topology in case of nodes failure is also reduced by reconfiguring the routes using preventive approach before the failure of the node.Less delay is also achieved as at the lower layer the packet is forwarded using the location information of the child group member of the virtual tree.

Efficient Data Delivery

The mismatch between virtual and physical topology is minimized and this way the multicast tree is optimized which results in less consumption of energy power of nodes and bandwidth of the links. Efficient data delivery is achieved as end result.

Packet Delivery Ratio

It is the ratio of all the received data packets at destination to the number of data packets sent by all the sources. It is calculated by dividing the number of packets received by destination through the no. of packets originated from the source.

PDR = (Pr / Ps) * 100 Where, Pr is total packets received and Ps is total packets sent.

Uniform Load Distribution

By putting a constraint on the degree of a member node a uniform load distribution is assured.

Delay, Reliability & Trust

For ensuring the Quality of Service (QoS), a methodology for handling high mobility in wireless mobile ad hoc networks have been established. A novel design framework for the development of scalable ad hoc routing protocols that are capable of providing quality of service guarantees (delay, reliability as well as trust) in the high mobility has been analyzed.Firstly, the consideration is focused upon the problem of providing delay guarantees for ad hoc routing protocols under high mobility. The novel aspect of the work is the distribution of network and MAC layer congestion to space, which enables congestion-aware routing & provides delay guarantees over a much longer duration than that achieved by traditional ad hoc routing protocols. Over the duration during which the node density and the offered traffic pattern remain roughly constant, the spatial congestion of the network remains roughly invariant. [1]

To ensure the parameters like delay, reliability & trust, an accurate method of spatial delay estimation, named “path integration”, between distinct locations, & an upper bound for the estimation error has been analyzed.

In the second part, an attention has been turned to the problem of reliable & trustworthy routing in mobile ad hoc networks. The implications of applying spatial approach to improve routing reliability through difficult terrains with possibly untrustworthy regions in tactical mobile ad hoc networks have been considered.

The reviewed approach provides maps of spatial reliability and trust that reflect the probabilities for finding trustworthy routes between distinct locations.

Security

Computing nodes (usually wireless) in mobile ad hoc network act as routers to deliver messages between nodes that are not within their wireless communication range. Because of this unique capability, mobile ad hoc networks are envisioned in many critical applications (e.g., in battlefields). Therefore, these critical ad hoc networks should be sufficiently protected to achieve confidentiality, integrity, and availability. The dynamic and cooperative nature of MANETs presents substantial challenges in securing these networks. Unlike wired networks which have a higher level of security for gateways and routers, ad hoc networks have the characteristics such as dynamically changing topology, weak physical protection of nodes, the absence of centralized administration, and highly dependence on inherent node cooperation. As the topology keeping changing, these networks do not have a well-defined boundary, and thus, network-based access control mechanisms such as firewalls are not directly applicable. In addition, there is no centralized administration, making bootstrapping of crypto systems very difficult. It is extremely easy for a malicious node to bring down the whole network. As a result, ad hoc networks are vulnerable to various attacks including eavesdropping, spoofing, modification of packets and distributed denial-of-service attacks. Thus, we require to consider security issue as an essential parameter for having efficient and secure communication.

Security Requirements for MANETs

Security Requirements for the wireless communications are very similar to the wired counterparts but are treated differently because of the applications involved as well as potential for fraud. Different parts of the wireless network need security. Over the air security is usually associated with the privacy of voice conversations. This is changing with the increasing use of wireless data services. Message authentication, identification, authorization, and so on also become issues here. Wireless Networks are inherently insecure compared to their wired counterparts.

The broadcast nature of the channel makes it easier to be tapped. Analog telephones are extremely easy to tap, and conversations can be eavesdropped using an RF scanner. Digital systems such as TDMA and CDMA are much harder to tap, and RF scanners cannot do the trick anymore, but as the circuitry & chips are freely available, it is not hard for someone to break into the system.

Very little work has been done on optimizing security services for wireless systems and patchwork solutions have made wireless networks not very secure. As long as the deployment is sparse and potential for harm to the consumer

small, such measures can be sufficient. As more people use wireless access to the Internet and use wireless networks for e-commerce, credit-card transactions, and so on the potential for harm increases.

In this section, we try to address some security requirements that have been identified for wireless voice networks and some that are emerging for wireless data networks.

Privacy Requirements of Wireless Networks

Privacy Requirements are two fold in wireless networks like MANETs. There is also a fixed infrastructure for handling the registration of mobiles, billing, mobility, power control and other issues. There are privacy requirements for the air-interface and others for the messages transmitted over the wired infrastructure.

A variety of control information is transmitted over the air in addition to the actual voice or data. These include call setup information, user location, user ID (or telephone number) of both parties and so on. These should all be kept secure because there is potential for misusing such information. Calling patterns (traffic analysis) can yield valuable information under certain circumstances. A flurry of calls between the CEOs of two major companies may indicate certain trends if it was discovered, even if the actual information in the calls was secure. Hiding such information is also important.

Other Security Requirements in Wireless Networks

Although privacy and confidentiality continue to be important issue in wireless networks, other security requirements are becoming significant in recent times. There has been widespread fraud and impersonation of analog cellular telephones in the past.

Although this is more difficult with digital systems, it is not impossible. There is thus a need to correctly identify and authenticate a mobile terminal. This becomes more important for private wireless data networks. For example, an organization that has installed a wireless LAN within its premises discovers that the coverage area extends into a neighbouring street. With the reducing costs of wireless LAN PC-cards, anyone could buy a PC-card and access the organization's WLAN from the street. [4]

Miscellaneous Issues

Even though traditional wired security measures are being put in place for wireless networks like MANETs, wireless specific issues have been largely neglected. In addition to traditional security services such as privacy, authentication, message integrity, non repudiation, access control, and availability, some of the wireless devices need certain intermediate security services such as authorization, identification, & varying degrees or classes of security as well as privacy.

The potential security implications and interaction between security requirements and wireless network/device limitations are unclear. Wireless communication devices are expected to be mobile and have the additional requirement that they must consume as little power as possible while performing computations for encrypting or decrypting data to conserve battery power. Thus, it is very important to consider and analyze all these security issues for MANETs.

Power Saving

Wireless network is a growing new technology and has replaced approximately all wired network due to its heavy advantages. Mobile ad-hoc networks works without any pre-existing infrastructure. They are easy to deploy and set up at any place and time, hence it has decreased the dependence of the infrastructure. So ad-hoc networks became a very important technique these days because of its features. Quality of service is the ability to assign different priority to different applications, users, or information flows, or to ensure a certain level of performance to a data flow.

Routing is the main constraint within the working with ad-hoc network. Routing is the integral part of any kind of the network as it not only exchanges the data but also control the information in the form of packets with its respective connected nodes in its range. There are varieties of routing protocols available in the area of the mobile ad-hoc networks. Due to the popularity of these networks, it is important to improve the quality of service for these networks. There are many parameters on which the quality of service depends.

With rapid development of wireless technology, the Mobile Ad Hoc Network (MANET) has emerged as a new type of wireless network. MANET is a group of wireless mobile nodes (e.g. laptops) that dynamically function as a network without the use of any existing infrastructure and centralized administration. In MANETs each node operates not only as an end system but also as a router to forward packets for other nodes. [2], [8]

Since the nodes in MANET move around, the connections between them break and re-establish frequently. Most of mobile nodes are having limited resource in computing capability and battery power. In order to work with MANETs, there are some predefined routing strategies through which we can pursue our communication i.e. active routing (on demand), proactive routing (table driven). All these protocols have some wonderful features if we intermix the selected features, particularly offer additional stress on signal strength that acts as threshold and distance to define inter/intra cluster communication. We could found a routing path that is extremely efficient in terms of power conservation. [3]

Least Control Overhead

Using multicast instead of sending through multiple unicasts not only minimizes link consumption, but also reduces sender and router processing, communication costs and delivery delay. Group communication is important in Mobile Ad Hoc Networks (MANET). Many ad hoc network applications which require close association of the member nodes depends on group communication. In addition, many routing protocols for wireless MANETs need a broadcast/multicast as a communication primitive to update their states and maintain the routes between nodes.

Multicast network structures are fragile in nature, therefore need to be readjusted and repaired continuously as the connectivity changes. Multicast protocols have to produce multi-hop routes under bandwidth shortage, limited battery power and dynamic topology due to nodes' random mobility. Even in wired networks, building optimal multicast trees and maintaining group membership information is challenging which becomes predominantly puzzling in mobile ad hoc networks.

The protocol named effective multicast routing protocol for MANET with least control overhead, called EMPLO uses the concept of proactive zone and constructs a shared bi-directional multicast tree with back up root for its routing operations.

To search for an existing multicast tree outside the zone, constrained directional forwarding is used which ensure a good reduction in overhead in comparison to network wide flooding for search process. Performance and reliability in terms of reduced overhead, less consumption of power and bandwidth is improved using the local connectivity technique and protective route reconfiguration on the basis of the current status of the nodes.

Table 1. Comparing values for various cases

Attributes / Cases	No. of Hops	Malicious nodes	Inefficient nodes
Best Case	1	1	1
Average Case	8	9	11
Worst Case	12	14	10

These techniques also ensure good reduction in latency in case of link breakages and prevention of the network from splitting. [7]

To improve the problem of dependency on a core node, a backup root node along with the primary root node is used. To reduce overhead and power requirement, the constrained directional forwarding in the direction of the target using its location information employed in the protocol.

Simulation

We have used Network Stimulator 2 for carrying out simulation. As we already know that MANETs works on the principle of multi-hopping mechanism. For having an efficient communication, we require to get a secure, reliable as well as an efficient route from source to destination. So in this connection, an algorithm known as Farthest Reliable Efficient Node Selection Algorithm is being utilized for next node selection so as to enhance the quality of next node selection for MANETs.

MANETs Scenario

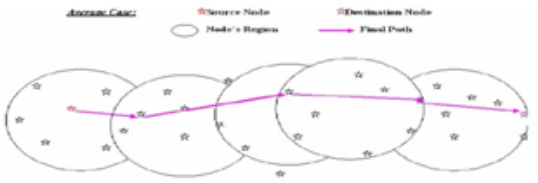

Fig 1. General Scenario of MANETs

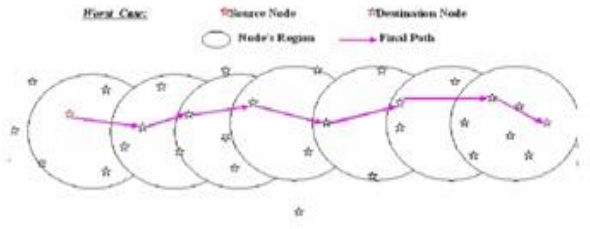

Fig 2. Best Case Illustration of communication between two nodes

In order to find the route from source to destination in terms of hops, we can consider three cases. We are having minimum number of hops in best case, an optimal number of hops in average case and maximum number of hops in the worst case.

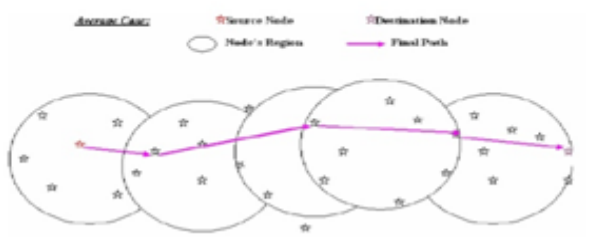

Fig 3. Average Case Illustration of communication between two nodes

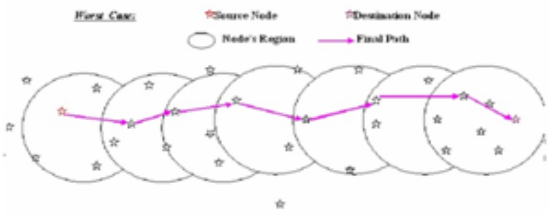

Fig 4. Worst Case Illustration of communication between two nodes

Conclusion

By having a depth analysis over the various necessary parameters responsible for an effective and efficient utilization of MANET's, we are able to make efficient group communication. Also, we are able to deal with various security issues as well as power saving issue in MANET's. Also the characteristics nature of MANET's may reduce the dynamic routing and reliable node selection may provide a good quality of service. By considering its various existing protocols, we are also able to make more improvements upon the functioning of MANET's. Thus, we can consider various other parameters for further enhancements over MANETs.

References

[1] Aminzadeh Gohari, Amir, - A Space Centric Approach to Routing, Dissertation Abstracts International , Vol. 73, No. 3, September 2012.

[2] Gaurav Banga and Ankur Singhal, - Performance Evaluation of Queuing Principles, International Journal of Applied Engineering Research, Vol.6, No. 18, Nov 2011.

[3] Gaurav Banga, Shakti Kumar and Amar Singh, - Enhanced Efficient Power Saving Adaptive Routing Algorithm for Mobile ad-hoc Networks, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 8, August 2013.

[4] Kaveh Pahlavan, Prashant Krishnamurthy, A Unified Approach-Principles of Wireless Networks

[5] Pariza Kamboj and A.K. Sharma, - Scalable Overlay Multicasting in Mobile Ad Hoc Networks, International Journal of Computer Science and Engineering, Vol. 02, No. 07, 2010

[6] Priyanka, Komal Kumar Bhatia and Nitin Goel, - Performance Analysis of FRENSA for Best, Average and Worst Case Scenarios in MANETs, International Journal of Advances in Computing and Information Technology, ISSN 2277-9140

[7] Vijay Kumar Tiwari and Rakesh Kumar , - An Effective Multicast Routing Protocol for MANET with Least Control Overhead, International Journal of Computer Networks and Wireless Communications, Vol. 2, No. 3, June 2012

[8]http://www.routingprotokolle.de/Routing/routing_sbr.htm