WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Energy Saving Load Balancing Approach to Boost AOMDV Routing in MANET And Data Security: A Survey

[1]Priyanka Choudhary, [2]Roshni Verma

[1]M.Tech Scholar, [2]Assistant Professor
[1,2]Dept. of Information Technology (Cyber Security)
Vikrant Institute of Technology and Management, Indore

ABSTRACT

A Mobile ad-hoc Network (MANETs) may be a multipath of devices or nodes that transmit across a wireless communication medium principally supported frequency with none mounted infrastructure or centralized management. The basic objective of such network infrastructure is to develop dependency of communication and establishment intelligence. Every mobile node is associated with transmitter and receiver for wireless communication and information exchange, tiny processor for computation purpose and processing, flush memory for storage along with battery to supply energy to all connected devices. It use connecting board to mound all such important components together. The complete phenomena make them self-configurable nodes to deploy into hostile and confrontational environment for temporary purpose. Due to a different nature of such network, it may become crucial part of performance of actual system like military or emergency services. Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. Unlike the wire line networks, the unique characteristics of mobile ad hoc networks pose a number of nontrivial.Challenges to security design, such as open peer-to-peer network architecture, shared wireless medium stringent resource constraints, and highly dynamic network topology.Mobile nodes may deploy into arbitrary topology without any planning and random selection. Here destination may be deployed for way from source and can be out of range from source node. Routing protocol is used to determine route among mobile nodes. It is set of rules used to decide path and help to transfer information. Various routing protocols are studied during this thesis work and classified on basis of path like single path and multipath algorithms. Multipath routing protocols gives better performance rather than single path during congestion and link failure. It carries multiple alternative routes from source to destination. So, in case of link failure or congestion state it may use alternative one to transfer information. This work considers AOMDV as the routing protocol to create ad-hoc networks.Consequently, a load balancer is a mechanism or device provides distribution and traffic handling facility with reliability. It improves the performance by virtually implements the logic of distribution. They improve the overall performance of applications by decreasing the burden on server associated with managing and maintaining application and network sessions, as well as by performing application specific tasks. Project works consider Energy Aware Load Balancing Multipath Routing (EALBM) as the base work and explore some possibilities of improvement.

Keywords: Cryptology, PK Round, Secret Number, Encryption Time, Decryption Time, Speedup, Energy Efficiency, Mobile Ad-hoc Networks, Network Lifetime, Routing Protocol, Wireless Sensor Networks.

1.0 INTRODUCTION

Wireless technology allows to access information and services electronically from everywhere. Wireless technology has become tremendously popular due to its usage in various new fields of applications in the domain of networking. The wireless communication revolution is fetching primary modify to data networking, telecommunication and is making networking and communications anytime, anywhere possible.

Wireless network technology advancements provide many benefits.

- Wireless networks are easy to structure and economical.
- Mobility and convenience of accessing the network resources from any location.
- Scalability.
- In expensive as wireless networks eliminate or reduce wiring costs.

1.1 Multi-hop Wireless Network

Wireless network refers to any variety of networks that wireless, and is generally related to telecommunication network whose interconnections between nodes are enforced but not these wires. Wireless telecommunication network are usually enforced with some variety of remote data gear that uses magnetism waves, like radio waves, meant for the carrier and this implementation sometimes takes place at the physical level of the network.

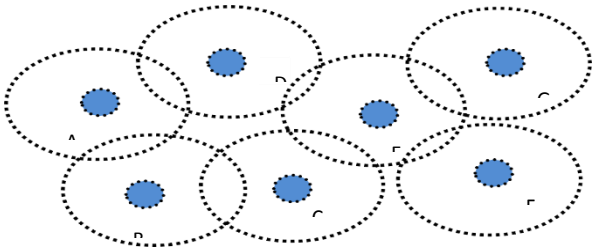


Figure1.1Multi-hop Wireless Network

This provides responsibility that the network won't stop functioning simply because one amongst the mobile nodes moves out of the vary others. Totally different nodes be purported to be able to enter and leave the network as they need. Owing to this restricted transmitted of then odes, varied hops are typically required to achieve different nodes.

1.2 Limitation

Mobile ad-hoc network (MANT) could be a localized autonomous network having options like self-configurability straight forward preparation structure communication via wireless suggests that, quality of nodes, dynamic topology, in stability, uneven links, interference, unreliable medium and route failure etc. Such networks area unit required in things wherever temporary network property is needed, like in tract, space of devastation and enormous meeting places.
These limitations are:

- Terribly restricted memory and cupboard space.
- Power limitation.
- UN reliable transferring of packets.
- Packet conflicting.

1.3 Motivation And Thesis Objective

Mobile ad-hoc network (MANET) could be a autonomous network having options
like self-configurability straight forward preparation, no mounted infrastructure communication via wireless suggests that, quality of nodes, dynamic to apology, instability, uneven links, interference, unreliable medium and route failure etc. Such networks however, DSDV in its gift type isn't compatible for mobile unintentional networks (MANETs).
Additionally to all or any links being wireless, frequent route failure esattri but able to quality produce serious issues to DSDV likewise. Route failures will cause packet drops at the intermediate nodes, which is able to be misconstrue as congestion loss. The development of DSDV performance was conjointly achieved with varied styles of networks with addition of latest DSDV variants referred to as AODV. Lots of analysis has been done on reliable network protocols for wireless networks. All the techniques projected rely heavily on the presence of wire-based station network, and thus can't be work for ad-hoc networks.

2.0 LITERATURE REVIEW

The legitimate purpose of packet sniffing is to monitor and analyses the network traffic and gain valuable insights about the network infrastructure and performance.
Depending on the type of network one is trying to sniff, packet sniffing can be categorized into
1) Active Sniffing 2) Passive Sniffing.

Active Sniffing
In Active sniffing the sniffer directly targets a point-to-point network device that regulates the flow of information between the ports. The active sniffer has to actively inject additional traffic into the LAN to capture the traffic.

Passive Sniffing

In passive sniffing, he sniffer is inserted into the hub that is connected with other devices via LAN. It means, the traffic that passes through the un-abridged network is seen by all the machines connected across the LAN and the sniffer has to wait for the data to be sent to every machine connected across the LAN. Internet Engineering Task Force (IETF) has painter unit (WG) that's devoted for developing information processing routing protocols. Routing protocols is one among the difficult and fascinating analysis areas. Several routing protocols are developed for MANETs e.g. AODV, OLSR, DSR etc.

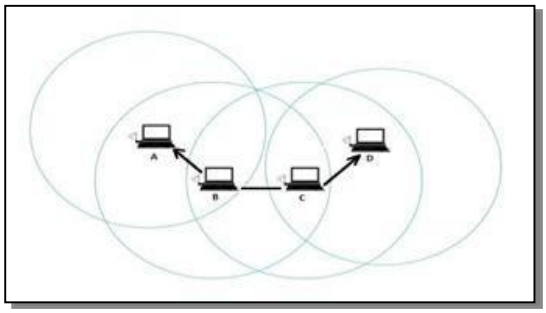


Figure 2.1 Mobile Ad-hoc Network

2.1 Routing Protocols

Information communication may be a necessary to follow in info Era's done by forwarding info from one node to a different node. Info forwarding task is finished with the assistance "Routing". Routing may be a difficult task since there's no central organizer, like base station, or mounted outers in alternative wireless networks that manage routing call. Every node act as a router/base station to forward the knowledge, therefore especial kind of routing protocol is important, there area in which unit ample range of routing protocols are developed for MANETs Routing protocols for Mobile im-promptu networks.

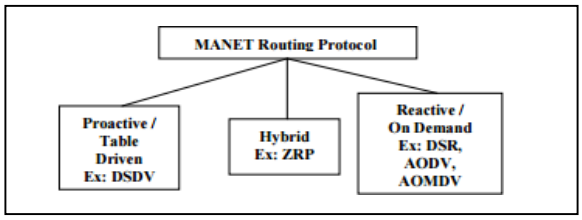


Figure 2.2 Routing protocol

2.2 Load Balancing

A load balancer is a device that acts as a reverse proxy and distributes network or application traffic across a number of servers. Load balancers are used to increase capacity (concurrent users) and reliability of applications. They improve the overall performance of applications by decreasing the burden on servers associated with managing and maintaing application and network sessions, as well as by performing application-specific tasks.
Load Balancers are generally grouped into two categories: Layer 4 and Layerb7. Layer 4 load balancers act upon data found in network and transport layer protocols (IP, TCP, FTP, UDP). Layer 7 load balancers distribute requests based upon data found in application layer protocols such as HTTP.
Requests are received by both types of load balancers and they are distributed to a particular server based on a configured algorithm. Some industry standard algorithms are:

- Round robin
- Weighted round robin
- Least connection
- Least response time

EALBM routing packets

- HELLO Packets
- RREQ Packet
- RREP Packet
- RERR Packet

A brief description of all relevant packet format and protocol services is cited below.

3.0 Problem disquisition

A lot of research work has been undertaking in wireless telecommunication technologies as well as low-price, low-power and multifunctional mobile nodes for conducting recent development. Ad-hoc networks suffer with couple of limitation which may be considers low processing, storage and battery life. Mobile nodes generally consider a limitation that they can't be allow to transfer energy from one node to another node. To achieve the objective, an optimized management of energy consumption is suggested. A well balanced network may help to avoid power draining to balanced load among all nodes. In homogeneous networks, the role of cluster head is usually periodically rotated among nodes to balance the energy dissipation.Packet sniffing is the act of gathering, collecting, and monitoring the data pieces (packets) that travel through a computer network or the internet.It means every packet that travels across the internet or a local network is gathered for a wide range of purpose such as-monitoring the traffic & bandwidth, maintains the networks, analyses the data collected by the device and so on.
Packet sniffing is used by ethical hackers, network admins, advertisers, ISPs, government institutions, etc for various ethical practices as below –

Network admins – Identify problems within the network and troubleshoot them.

System admin – Check employee's network usage.

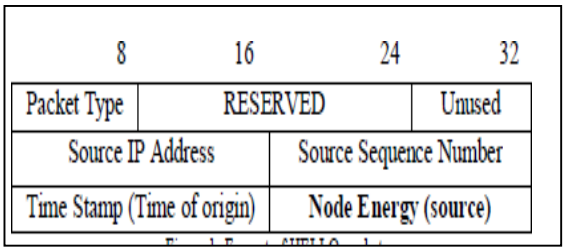
Advertisers – Show relevant ads to targeted users.

Data encryption standard (DSE) is one of the simplest method of data encryption decryption. Here the data to be encrypted is to be divided into 64 data blocks as shown in figure.

HELLO Packet

This is the implementation of ping request to find neighbors at regular interval. It is periodic packet forwarding may be done after milli second. All the neighbor nodes share the presence of their connectivity under the range of sender node.

Figure 2.3 Hello Packet Format



Packet Type: Specified the type of packet like RREQ or RREP.

Hop Count: Total number of hop count distance from source to destination.

Unused: Fitting for padding purpose only.

Source IP Address: Specify the IP address of sender.

Source Sequence Number: Unique number to maintain uniqueness.

Timestamp: To maintain time of origin and life time of packet.

Node Energy (Source): To specify the current remaining energy of source node.

RREQ Packet: It is an enquiry packet transmitted to discover route from source
destination. It can be state as he route discovery packet. Here, source node broadcasts route discovery packets to all connected nodes. It can be state as the initiative for route establishment and path discovery. Every packet carrier their own packet ID to maintain uniqueness and avoid packet unambiguously. A description of packet format attributes is cited below and shown in figure;

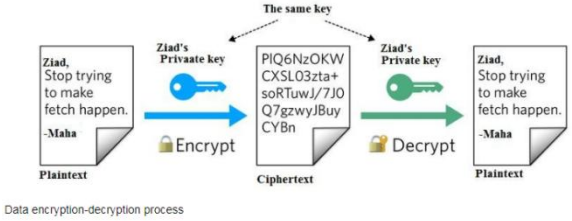


Figure 2.4 Data Encryption Decryption Process

Packet sniffing isn't just used only by the 'Good Guys'. Unethical hackers and cybercriminals use it to access insider information, login credentials, instant messages, bank account details, and other sensitive data. Sniffers are dangerous in the wrong hands and one should take necessary measures to prevent packet sniffing. Antivirus software, also known as malware helps you protect your device and network from worms, viruses, botnets, and other kind of malware.

Data cryptography means encrypting and decrypting data using a selected tool or method, encrypting the data means destroying the data to make it impossible to be understood or used by any other unauthorized party.

DES requires a small amount of time for encryption and decryption, but I is not secure and it can be easily hacked by third party person, because the length of the used PK is small

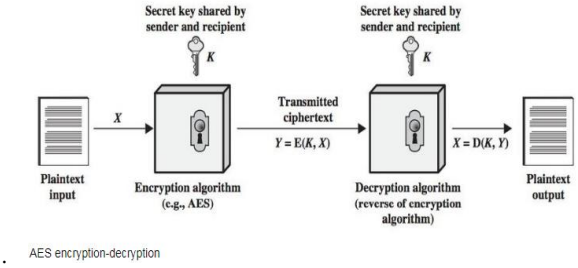


Figure 2.5 AES Encryption Decryption

Encrypted data, also known as cipher text, appears scrambled or unreadable to third party person or entity accessing without permission and without knowing the PK and the operations used for encryption.

Conclusions

This works consider AOMDV as the routing protocol to create ad-hoc networks.Consequently, a load balancer is a mechanism or device provides distribution traffic handling facility with reliability. It improves the performance by virtually implements the logic of distribution.They improve the overall performance of applications by decreasing the burden on servers associated with managing and maintaining application and network sessions, as well as by performing application-specific tasks. Project works consider Energy Aware Load Balancing Multipath Routing (EALBM) as the base work and explore some possibilities of improvement.

Following conclusion swer emade from above performance analysis.

- Throughput of proposed solution becomes high with 50 % than EALBM method and 60% with AOMDV method
- A slight slag has been happed with respect toPDR of proposed solution become 4 times than EALBM technique and AOMDV.
- It also observes that an enhancement into mobile nodes rapidly degrade the packet receiving.
- A poor performance has been observed into 30 node scenarios with respect to 10 nodes but still better than EALBM

REFRENCES

[1] Alotaibi, Naif D., and Elyas I. Assiri. "Enhancing MANET by Balanced and Energy Efficient Multipath Routing with Robust Transmission Mechanism with Using FF-AOMDV." *Communications and Network* 13.4 (2021): 131-142.

[2] Naseem, M., Ahamad, G., Sharma, S., & Abbasi, E. (2021). EE-LB-AOMDV: An efficient energy constraints-based load-balanced multipath routing protocol for MANETs. *International Journal of Communication Systems*, *34*(16), e4946.

[3] Sarhan, Shahenda, and Shadia Sarhan. "Elephant herding optimization Ad Hoc on-demand multipath distance vector routing protocol for MANET." *IEEE Access* 9 (2021): 39489-39499.

[4] Rani, B. Sandhya, and K. Shyamala. "Energy efficient load balancing approach for multipath routing protocol in ad hoc networks." *2019 Second International Conference on Advanced Computational and Communication Paradigms (ICACCP)*. IEEE, 2019.

[5] Singh, Sunil Kumar, and Jay Prakash. "Energy efficiency and load balancing in MANET: a survey." *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*. IEEE, 2020.

[6] Li, Peng, Lu Guo, and Fang Wang. "A multipath routing protocol with load balancing and energy constraining based on AOMDV in ad hoc network." *Mobile Networks and Applications* (2019): 1-10.

[7] Yazdinejad, Abbas, Sara Kavei, and Somayeh Razaghi Karizno. "Increasing the performance of reactive routing protocol using the load balancing and congestion control mechanism in MANET." *Computer and Knowledge Engineering* 2.1 (2019): 33-42. .

[8] Venkatachalapathy, K., and D. Sundaranarayana. "A Min-Max Scheduling Load Balanced Approach to Enhance Energy

[9] Efficiency and Performance of Mobile ADHOC Networks." *International Journal of Computer Networks & Communications (IJCNC) Vol* 11 (2019).

[10] Makwana, H., and Hitesh Patel. "Advancement in performance of wireless AdHoc network using AOMDV in MANET." *International Journal for Innovative Research in Science & Technology* 4.10 (2018): 16-20.

[11] Zaghal, Raid, Saeed Salah, and Mohammad Ismail. "An InfiniBand-based mechanism to enhance QoS in multipath routing protocols in MANETs." *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE, 2018.

[12] Venkatraman, Santhi, and Sai Kiran Sarvepalli. "Load balance technique with adaptive position updates (LAPU) for geographic routing in MANETs." *EURASIP Journal on Wireless Communications and Networking* 2018.1 (2018): 1-9.