An Optimized AOMDV based Upon RERMR and AMDMM

Priyanka Misra, Taranjit Singh Aulakh
Bhai Gurdas Institute of Engineering and Technology, Sangrur, Punjab, India

DOI: 10.23956/ijarcsse/V7I6/0120

Abstract— In the current research the enhancement of the secured MANET routing protocol is done. The protocol chosen for enhancement is AOMDV based upon RERMR and AMDMM due to the low QOS in the existing AOMDV. Encryption is quite an important parameter in the MANET. To make RERMR more secure 3d cryptography technique is implemented in it for secure transmission. By applying the encryption technique in the RERMR, some times the overheads are introduced in it. To overcome the problem of data dropped, load and encryption overheads in the network, an optimization technique called Adaptive ACO are used. Using the above mentioned optimization technique the data dropped and the losses in the network are reduced to some extent. The above defined results have shown the parameters that are improved using a network simulator called MATLAB. The existing protocol generates much load on the network and the packets start delayed in network. This problem is reduced in the proposed approach using an optimization technique which makes multiple paths to the packets that are sent to the destination. By using the exactly reciprocal path the network can send data through multiple paths and the load in the network can be reduced.

Keywords— Manet Routing, Energy Efficiency, EPAR, Cryptography

I. INTRODUCTION

A mobile ad-hoc network may be an assortment of mobile nodes forming associate ad-hoc network without the help of any centralized structures. These networks introduced a replacement art of network institution and may be suited to associate setting wherever either the infrastructure is lost or wherever deploy associate infrastructure isn't terribly value effective. MANET is associate IEEE 802.11 framework. Mobile Ad hoc Networks can be set up at any place and time. Mobile ad-hoc networks will operate in a very standalone fashion or might probably be connected to a bigger network like the net. They provide information and services regardless of geographic position. It's an interconnected assortment of wireless nodes where there is no networking infrastructure within the sort of base stations, devices don't got to be at intervals every other’s communication vary to speak, the end-users devices additionally act as routers, nodes will enter and leave over time, information packets area unit forwarded by intermediate nodes to their final destination. Mobile ad hoc network nodes are furnished with wireless transmitters and receivers using antennas, which may be highly directional (point-to-point), omni directional (broadcast), probably steer able, or some combination there of [1]. At a given point in time, depending on positions of nodes, their transmitter and receiver coverage patterns, communication power levels and co-channel interference levels, a wireless connectivity in the form of a random, multihop graph or “ad hoc” network exists among the nodes. This ad hoc topology may modify with time as the nodes move or adjust their transmission and reception parameters.

The characteristics of these networks are summarized as follows:
1. Communication via wireless means
2. Nodes can perform the roles of both hosts and routers
3. Bandwidth-constrained, variable capacity links
4. Energy-constrained Operation
5. Limited Physical Security
6. Dynamic network topology
7. Frequent routing updates

II. ROUTING PROTOCOL IN MANET

Mobile Ad-hoc networks are self-organizing and self-configuring multihop wireless networks, where the structure of the network changes dynamically. This can be chiefly thanks to the quality of the nodes [3]. Nodes in these networks utilize identical random access wireless channel, cooperating in an intimate manner to partaking themselves in multihop forwarding. The node within the network not solely acts as hosts however additionally as routers that route knowledge to/from alternative nodes in network [6]. In mobile ad-hoc networks there is no infrastructure support as is the
case with wireless networks, and since a destination node can be out of vary of a supply node transferring packets; therefore there is need of a routing procedure that can perpetually able to notice a path therefore on forward the packets fittingly between the supply and also the destination at intervals in a cell, a base station will reach all mobile nodes while not routing via broadcast in common wireless networks within the case of ad-hoc networks, every node should be ready to forward knowledge for alternative nodes. This creates extra issues besides the issues of dynamic topology that is unpredictable property changes [8].

Classification of routing protocols in mobile accidental network will be wiped out some ways; however most of those are done reckoning on routing strategy and network structure [2] [3] [10]. The routing protocols will be categorized as flat routing, gradable routing and geographic position power-assisted routing whereas reckoning on the network structure. The routing strategy routing protocols will be classified as Table-driven and supply initiated. The classification of routing protocols is shown within the Figure 2.

![Classification of Routing Protocols in Mobile Ad-hoc Networks](image)

**Fig 1: Classification of Routing Protocols in Mobile Ad-hoc Networks**

### III. ISSUES

1. **Uneven links:** Most of the wired networks think about the even links that are perpetually fastened. However this can be not a case with ad-hoc networks because the nodes are mobile and perpetually ever-changing their position at intervals.

2. **Routing Overhead:** In wireless accidental networks, nodes usually modify their location at intervals. So, some stale routes are generated within the routing table that results in supernumerary routing overhead.

3. **Interference:** This can be the main downside with mobile ad-hoc networks as links return and go reckoning on the transmission characteristics, one transmission may interfere with another one and node may hear transmissions of alternative nodes and may corrupt the entire transmission.

4. **Dynamic Topology:** Since the topology isn’t constant; that the mobile node may move or medium characteristics may modify. In ad-hoc networks, routing tables should somehow replicate these changes in topology and routing algorithms have to be compelled to be custom-made. As an example in a much fastened network routing table change takes place for each 30sec. This change frequency can be terribly low for ad-hoc networks.

5. **Packet Forwarding Attacks:** Attackers in MANET environment affect the data forwarding during transmission phase. This makes slow packet transmission, duplicate data forwarding and forwarding packets to the unknown destination.

6. **Path Instability.** In ad hoc environment, nodes are moving randomly and communicate with wireless links. Sometimes low Signal to Noise Ratio (SNR) leads to the path instability.

### IV. DEFINITION OF ENERGY EFFICIENCY

Cooperation is the core of MANETs. A Mobile Ad-hoc network is only successful if there is cooperation between nodes. High cooperation is expected between the nodes while packet transmission. But as far the commercial MANET is concerned it is difficult to encourage the cooperative behaviour between the nodes. In Commercial MANET Power consumption and power saving is a concern with every individual node. In order to save power for its own usage some nodes stops forwarding packets. Intermediate nodes want to conserve their limited resources like energy and bandwidth. This leads to selfish behaviour of nodes in MANETs. These non-cooperative nodes don’t cooperate or participate in forwarding packets for other nodes or finding routing path for them. This is a serious concern & devising ways to detain or minimize selfish behaviour is an open research challenge in this domain. In contrast to simply establishing correct and efficient routes between pair of nodes, one important goal of a routing protocol is to keep the network functioning as long as possible. As discussed in the Introduction, this goal can be accomplished by minimizing mobile nodes’ energy not only during active communication but also when they are inactive. Transmission power control and load distribution are two approaches to minimize the active communication energy, and sleep/ power-down mode is used to minimize energy during inactivity. Before presenting protocols that belong to each of the three approaches, energy-related metrics that have been used to determine energy efficient routing path instead of the shortest one are discussed. They are [4]
1. Energy consumed/packet;
2. Time to network partition;
3. Variance in node power levels;
4. Cost/packet; and
5. Maximum node cost.

The first metric is useful to provide the min-power path through which the overall energy consumption for delivering a packet is minimized. Here, each wireless link is annotated with the link cost in terms of transmission energy over the link and the minpower path is the one that minimizes the sum of the link costs along the path. However, a routing algorithm using this metric may result in unbalanced energy spending among mobile nodes. When some particular mobile nodes are unfairly burdened to support many packet-relaying functions, they consume more battery energy and stop running earlier than other nodes disrupting the overall functionality of the ad hoc network. Thus, maximizing the network lifetime (the second metric shown above) is a more fundamental goal of an energy efficient routing algorithm: given alternative routing paths, select the one that will result in the longest network operation time.

V. ENCRYPTION IN MANET

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors. The purpose of encryption is to ensure that only somebody who is authorized to access data (e.g. a text message or a file), will be able to read it, using the decryption key. Somebody who is not authorized can be excluded, because he or she does not have the required key, without which it is impossible to read the encrypted information. Encryption, by itself, can protect the confidentiality of messages, but other techniques are still needed to protect the integrity and authenticity of a message; for example, verification of a message authentication code (MAC) or a digital signature. Encryption has long been used by military and governments to facilitate secret communication. It is now commonly used in protecting in formation within many kinds of civilian systems. For example, the Computer Security Institute reported that in 2007, 71% of companies surveyed utilized encryption for some of their data in transit, and 53% utilized encryption for some of their data in storage.[6] Encryption can be used to protect data “at rest”, such as information stored on computers and storage devices (e.g. USB flash drives). In recent years there have been numerous reports of confidential data such as customers’ personal records being exposed through loss or theft of laptops or backup drives. Encrypting such files at rest helps protect them should physical security measures fail. Digital rights management systems, which prevent unauthorized use or reproduction of copyrighted material and protects of are against reverse engineering, is another some what different example of using encryption on data at rest.[7] Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic tellermachines. There have been numerous reports of data in transit being intercepted in recent years. [8] Data should also been encrypted when transmitted across networks in order to protect against eaves dropping of network traffic by unauthorized users.

VI. RESEARCH GAPS

A mobile ad hoc network (MANET) consists of one or more autonomous mobile nodes, each of which communicates directly or indirectly with the neighbor nodes within its radio range. The field of MANET is rapidly growing due to varied advantage and applications. Energy efficiency is a challenge faced especially in designing a routing protocol. A single routing protocol is hard to satisfy all requirements, i.e., one routing protocol cannot be a solution for all energy efficient protocol that is designed to provide the maximum possible requirements, according to certain required scenarios.

1. There is not any alternative path for downlinks.
2. Data packets are dropped due to downlinks.
3. Decrease in throughput.
4. In case of link failure repeat rescan of network decreases the efficiency and reduce power of battery.
5. No improvement for increased delay.
6. Maximize the increased network lifetime.
7. In-secure transmission in routing protocols.

So we’ll formulate secure and energy efficient RERMR Protocol due to insecure transmission of packets which is big problem that adversely affects the secure transmission other parameters like throughput, data dropped, power of battery etc [1].
VII. PROPOSED APPROACH

Figure 2: Flow Chart for implementation

VIII. RESULTS AND DISCUSSION

In current chapter with the help of comparative study, we can draw all the pros and cons of the above defined scheduling schemes. In this scenario a comparison is made between hybrid routing schemes by taking 25 subscriber stations which is shown below.

![Average Load(kbits*10^3)](image)

Figure 4: Load
The load in two MANET protocols called existing and proposed upto 20 nodes. From the above graph it is shown that the load in proposed approach is less.

Delay in existing and proposed approach in MANET in 20 nodes. From the graph it can easily depicted that the delay in proposed approach is less than that of existing protocol.

Throughput in proposed and existing approach in MANET in 20 nodes. From the graph it can easily depicted that the throughput in proposed protocol is more than that of existing protocol. Throughput in case of proposed case is approx 110 packets and in existing case it is approx 100 packets.

The encryption overheads in two MANET protocols called existing and proposed upto 20 nodes. From the above graph it is shown that the load in proposed approach is less.
MANETs are the adhoc network that don’t have any fixed topology and can easily send data from source to destination in wireless mode through some routing protocol. In the current research the enhancement of the secured MANET routing protocol is done. The protocol chosen for enhancement is RERMR due to the low QOS in the existing RERMR. Encryption is quite an important parameter in the MANET. To make RERMR more secure 3d cryptography technique is implemented in it for secure transmission. By applying the encryption technique in the RERMR, some times the overheads are introduced in it. To overcome the problem of data dropped, load and encryption overheads in the network, an optimization technique called Adaptive ACO are used. Using the above mentioned optimization technique the data dropped and the losses in the network are reduced to some extent. The above defined results have shown the parameters that are improved using a network simulator called MATLAB. The RERMR generates much load on the network and the packets start delayed in network. This problem is reduced in the proposed approach using an optimization technique which makes multiple paths to the packets that are sent to the destination. By using the exactly reciprocal path the network can send data through multiple paths and the load in the network can be reduced.

In the future scope the scalability can be improved by reducing the time delay and the load in this research as the load may increase in case of scalability in the network. Apart from this the mitigation and detection techniques may be included in this algorithm for attack prevention.

REFERENCES


