

Efficient Power Utilization with Reactive Routing Protocols in Mobile Ad-Hoc Networks under the influence of Application layer Attack

Neha Shinde Holkar

ME Scholar
Department of IT
MIST, Indore

Latika Mehrora

Assistant Professor
Department of CSE
MIST, Indore

ABSTRACT

One of the majority vital issues in mobile ad hoc network(MANET) is collecting and processing data apparent from the atmosphere and sending that data to be processed and evaluated. Routing in MANETs is a challenging task due to the unpredictable changes in the network topology. MANETs are a heterogeneous mix of different wireless and mobile devices, ranging from little hand-held devices to laptops that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. A Mobile Ad hoc Networks (MANET) represents a system of wireless mobile nodes that can freely and dynamically self-organize in to arbitrary and temporary network topologies, allowing people and devices to seamlessly communicate without any pre-existing communication architecture. One of the main issues in MANET routing protocols is development of energy efficient protocols due to limited bandwidth and battery life. In this paper we will discuss about few energy-efficient routing protocols which will help in reducing power consumption while introducing application layer attack as MANET is typically based on battery power.

Keywords

Application Layer attacks, Received power, Packet received, Throughput, Delay, OPNET

1. INTRODUCTION

Recent advances in computer networking have introduced a new technology for future wireless communication, a mobile ad hoc network (MANET). This technology, which is the combination of peer-to-

peer techniques, wireless communications, and mobile computing, provides convenient infrastructure-less communications and could be very useful to provide communications for many applications especially when the infrastructure networks is not feasible. MANET could be used to overcome geographical constraints in a military operation. As it is easy to deploy, it may also very useful to assist in the disaster relief operations where temporary network infrastructure is immediately needed to replace the

damaged infrastructure networks. Mobile ad-hoc networks or "short live" networks operate in the absence of fixed infrastructure. They offer quick and easy network deployment in situations where it is not possible otherwise. Ad-hoc is a Latin word, which means "for this or for this only." Mobile ad-hoc network is an autonomous system of mobile nodes connected by wireless links; each node operates as an end system and a router for all other nodes in the network.

The mobile ad hoc network has the following typical features [1]:

1. Unreliability of wireless links between nodes. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.

2. Constantly changing topology. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes.

3. Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol.

The main factors of routing protocols consume maximum power are as following: [4]

- The topology of the network changed rapidly, which will lead to the lost of packets.
- Modification every node's routing table that within the communication distance of the rapid-passing node that will consumed a lot of the bandwidth and the overhead of the networks.
- Delay of the data sending to the rapid-moving node.
- Transmission between two hosts over a wireless network does not necessarily work equally well in both directions. Thus, some routes determined by some routing protocols may not work in some environments.
 - Decrease the routing updates as well as increase the whole networks overhead.
 - Periodically sending routing tables will waste network bandwidth. When the topology changes slowly, sending routing messages will greatly waste the bandwidth of Wireless Ad-hoc Networks.
 - Periodically sending routing tables also waste the battery power. Energy consumption is also a critical factor which prevents Wireless Ad-hoc Networks to be a non-flowed architecture.

1.1 Routing Protocol

Protocols

This section presents the most common routing protocols in mobile ad-hoc networks. There are basically three types of routing protocols which are discussed below:

1.1.1 Table Driven Routing Protocol

In table driven routing protocols each node in the network maintains the updated routing table information by frequent exchanging the information among the nodes. This reduces the delay time of sending data or information from one node to another because nodes will spend no time in discovering the route. This type of routing protocols approximately works the same way as the wired network routing protocol works. The table driven protocols are DSDV and WRP.

1.1.2 On Demand Routing Protocols

In on demand routing protocols, a node simply maintains routes information to get destination that it needs to send required data packets. The routes to get their desire destinations will expire automatically after some time of idleness, while the network is not being used. These routing protocols are AODV, DSR and TORA.

1.1.3 Hybrid routing Protocols

In this type of routing protocol is the combination of the above two categories. In which nodes belonging to a particular geographical area or within a certain detachment from an anxious node are said to be in routing area and uses table driven routing protocol. Communication between nodes in different areas will rely on the source initiated or on-demand routing protocols. This routing protocol include ZRP.

We select the most popular routing protocols, which is On-Demand routing protocols according the these routing protocols they are used when they are need and also in this routing protocols a node simply maintains routes information to get destination that it needs to send required data packets. The routes to get their desire destinations will expire automatically after some time of idleness, while the network is not being used,

which give less load on the network and that's why it's very hard to attack on such routing protocols.

1.1.1 AODV

AODV using a classical distance vector routing algorithm. It is also shares DSR's on-demand discovers routes. During repairing link breakages AODV use to provide loop free routes. It does not add any overhead to the packets, whenever a route is available from source to destination. Due to this way it reduces the effects of stale routes and also need for route maintenance for unused routes. One of the best features of AODV is to provide broadcast, unicast, and multicast communication. During route discovery algorithm AODV uses a broadcast and for reply it uses unicast.

1.1.2 DSR

The DSR is an on-demand routing protocol that is based on source routing. It uses no periodic routing messages like AODV, and due to this way it reduces network bandwidth overhead, and also avoids large routing updates as well as it also reduces conserves battery power. In order to identify link layer failure DSR needs support from the MAC layer. It is consist of the two network processes, Route Discovery and Route Maintenance. Both of neither AODV nor DSR guarantees shortest path.

2 APPLICATION LAYER ATTACKS

Applications layer need to be designed to handle frequent disconnection and reconnection with peer applications as well as widely varying delay and packet loss characteristics [3]. Like other layers application layer also vulnerable and attractive layer for the attacker to attack. Because this layer contains user data that supports many protocols such as SMTP, HTTP, TELNET and FTP which have many vulnerabilities and access points for attackers. The main attacks in application layer are malicious code attacks and repudiation attacks.

2.1 Malicious Code Attack

Various malicious codes such as virus, worm, spy-wares and Trojan horse attack both operating systems and user applications that cause the computer system and network to slow down or even damaged. An attacker can produce this type of attacks in MANET and can seek their desire information [4].

2.2 Repudiation Attack

The solution that taken to solve authentication or non-repudiation attacks in network layer or in transport layer is not enough. Because, repudiation refers to a denial of participation in the communication. Example of repudiation attack on a commercial system: a selfish person could deny conducting an operation on a credit card purchase or deny any on-line transaction [4].

Table1. Security attacks at each layer in MANET

Layer	Attack
Application Layer	Repudiation attack, Malicious code attack
Transport Layer	Session Hijacking, SYN flooding
Network Layer	Wormhole, blackhole, Byzantine, flooding, resource consumption, location disclosure attacks
Data Link Layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP Weakness
Physical Layer	Jamming, interceptions, eavesdropping

3. SIMULATION ENVIRONEMNT

In this paper we have explained the investigative result obtained from the simulation of different scenarios using OPNET Modeller 14.5. There are four different network scenario which we implement in OPNET and they are given below:

- 1.MANET using DSR protocol without attack.
- 2.MANET using AODV protocol without attack.
- 3.MANET using DSR protocol with Malicious code attack.
4. MANET using AODV protocol with Malicious code attack.

We compare the above scenarios by taking Delay and Throughput as performance parameter.

5.1 Network Scenario Description

In the simulation of mobile ad-hoc networks through OPNET we use 6 MANET stations, Jammer node, Profile configuration, Application configuration & Mobility configuration. Attributes of MANET stations are used as below:

Parameter	Value
Simulator	OPNET
Simulation time	300 seconds
Simulation area	300 m x 300 m
Buffer size (bits)	256000
Packet size (packets)	Infinity
Number of Mobile nodes	6
Addressing mode	IP V4
MAC Type	Mac/802.11

Transmit power	0.005
Bandwidth	10 Mbps

Application configuration model is used in the network topology. The application config node can be used for the following specification.

1. ACE Tiers information
2. Application specification
3. Voice encoder schemes

Profile configuration model is used in the network topology. The profile config node can be used to create user profiles. These user profiles can then be specified on different nodes in the network to generate application layers traffic. Mobility configuration is used to define the mobility of wireless stations.

3.2 Implementation of Repudiation attack

As discussed earlier, repudiation attack denies the participation in communication. We found two ways to create a repudiation attack by either fail a node or by creating a misbehavior node by changing the attributes of

a MANET node so that it behaves differently from the other nodes. By failing the node we mean completely denying a node to communicate, but it is likely to have one less MANET node in the network. Therefore we have

used second option to create a Misbehavior node by changing the following tabulated attributes.

Table 2: Comparison of MANET node attributes with Misbehavior node attributes

S No	Attributes	Value (MANET node)	Value (Misbehavior node)
1	Trajectory	Vector	None

2	Transmit Power (W)	0.005	0.001
3	Data Rate	11mbps	2Mbps
4	Large Packet processing	Drop	Fragment

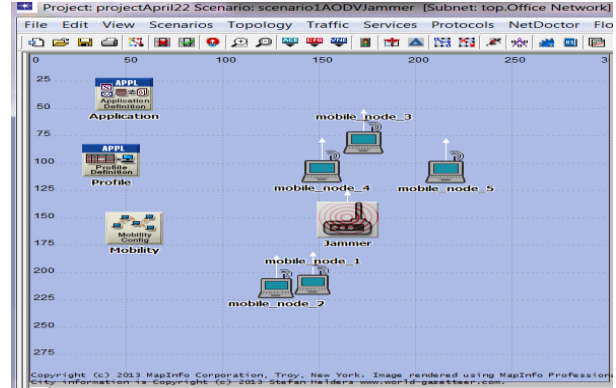


Fig 1 : Network Scenario with Jammer node

4 SIMULATION RESULT & ANALYSIS

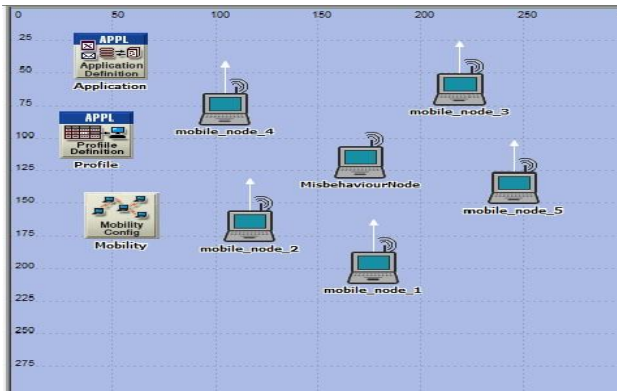


Figure 1 Scenario representing misbehavior node

Implementation of Malicious code attack:

In our simulation we use a Jammer node to create a Malicious code attack. We use mobile jam pulsed node. A jam pulsed node represents a jammer which can be deployed as a fixed, mobile or satellite node. The jammer provides transmission on a fixed single fixed frequency band which is masked by periodic pulse train in time. We use low power jammer node (.0001W) to show the effect of Jammer even when it transmit low power.

A network scenario with 6 mobile nodes and a jammer node is shown below.

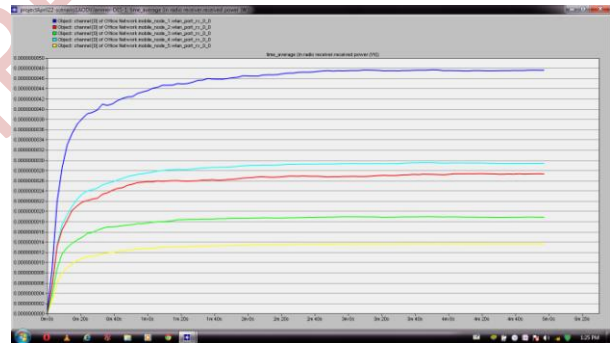


Fig 2: Total Received Power by AODV protocol

Above graph shows power received by each packet in each node. We have simulated six scenarios to calculate received by each packet in each node. We calculate the efficiency of power using below numeric methods:

$$\text{Total power received in each scenario} = \sum p_i * r_i * 300$$

Where,
 p_i = number of packets at each node per second
 r_i = power received by each packet in each node
 300 = simulation time in seconds

$$\text{Efficiency of power utilization} = \frac{\sum p_i * r_i * 300}{\text{Total power transmitted}} * 100$$

5. CONCLUSION

After this simulation result we can conclude the following:

1. Under the Malicious code attack, AODV protocol consumes less power.
2. Under the Repudiation attack, AODV protocol consumes less power but consumes more than with malicious code attack.
3. DSR protocol utilize less power when there is no attack in the network.

6. REFERENCES

- [1] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.
- [2] Dr. Shahriar Mohammadi and Hossein Jadidoleslami, "A COMPARISON OF LINK LAYER ATTACKS ON WIRELESS SENSOR NETWORKS", March 2011
- [3] R. Ramanathan, J. Redi and BBN Technologies, "A brief overview of ad hoc networks: challenges and directions," IEEE Communication Magazine, May 2002, Volume: 40, page(s): 20-22, ISSN: 0163-6804
- [4] B. Wu, J. Chen, J. Wu, M. Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Department of Computer Science and Engineering, Florida Atlantic University
- [5] Renu Mishr, Sanjeev Sharma, Rajeev Agrawal, IEEE 2010, Vulnerabilities and Security of Ad-hoc Networks.
- [6] N. Meghanathan, "A Simulation-based Performance Analysis of Multicast Routing in Mobile Ad hoc Networks," International Journal of Information Processing and Management (IJIPM), Vol. 1, No. 1, pp. 4-14, July 2010.
- [7] Shuyao Yu, Youkun Zhang, Chuck Song, and Kai Chen. A security architecture for Mobile Ad Hoc Networks.