ISSN: 2321-8169
4210 - 4222

Scattered Dropping Attack on TCP-Based Mobile Ad-Hoc Networks

Priyanka Gaur
Computer Science & Engineering
Marudhar Engineering College
Bikaner, Rajasthan, India
er.priyankagaur@gmail.com

Neha Goswami
Assistant Professor, Computer Science & Engineering
Marudhar Engineering College
Bikaner, Rajasthan, India
er.neha28@gmail.com

Abstract**—**Scattered Dropping Attack (SDA) is a simple yet very powerful denial of service (DoS) attack that is effective on both TCP and UDP based MANETs. The simulation results clearly show the impact of proposed attack on the network throughput, bandwidth wastage and received data quality. It has also been observed that even though the TCP congestion control is adaptable to the packet losses but in case of the dropping attack it is fully unable to detect whether the packet drop is the result of the attacker misbehaving or it is due to the congestion or other wireless environmental problem.

Keywords*- MANET, SDA, DoS, TCP.*

*****

I. Introduction

Mobile ad-hoc network [1] is a dynamic network formed by independent system of randomly moving mobile nodes. Nodes are connected through wireless links without utilizing the existing network infrastructure or any form of centralized administration. Each node is able to communicate directly with nodes in its transmission range. For nodes outside communication range, intermediate nodes are used to relay the message hop by hop. Hence, such networks are called “multi-hop” networks.

In an ad-hoc network, it is required that a node forwards or routes data packets on behalf of other nodes. Each node, therefore, acts as a host and a router, necessitating use of routing protocols to make routing decisions. Many routing protocols have been proposed by the researchers. The biggest challenge for routing protocols is to establish and re-establish routes in the face of dynamically varying network topology and network partitions due to node mobility. Depending on how the mobile nodes acquire and maintain routing information, MANET routing protocols can be classified as either reactive or proactive.

A. MANET Challenges

MANET characteristics impose many challenges related to routing, security, dynamic topology and node cooperation. Some of the challenges are:

- Routing: MANETs are characterized by frequent, rapid and unpredictable topological changes. This causes mobile nodes to establish dynamic and multi-hop routing among themselves as they move from one place to another. Issue of developing efficient routing protocols to set up inter node communication paths in wake of power and bandwidth constraints is a challenge in MANETs.
- Security: MANETs have an open peer to peer architecture. Nodes communicate with each other through wireless channel. Wireless medium is vulnerable to eavesdropping and numerous other security attacks as it is accessible to both legitimate and malicious users [2] [3]. Issue of developing security solutions is a big challenge in the face of MANET constraints.
- Dynamic Topology: The network topology has a dynamic nature as nodes freely roam in the network and frequently leave or join the network. This causes frequent packet losses and possibly network partitions. In addition, a user may require access to fixed public network while operating within the ad hoc network. MANETs should not only be able to adjust to mobility patterns of the nodes but also to traffic and propagation conditions.
- Node Cooperation: Nodes in MANET cooperate with each other to establish the functionality of ad hoc network. Intermediate nodes route data on behalf of nodes outside each other’s transmission range. This intrinsically exposes the network to many security challenges.

B. Threats to MANET

Threats to MANETs can broadly be divided into two categories:

i. Compromise in routing logic: Incorrect routing packets are injected into the network to disrupt routing logic.
ii. Distortion in traffic: Compromised nodes in the network may block, distort or replay data messages and hinder data transfer from source to destination.

Quick and easy deployment of wireless network, in the absence of fixed supporting structure is the need of the hour. MANETs are prone to attacks from inside and outside the network. The power of MANETs can only be harnessed if secure solutions are provided to protect the system from attacks. To design good security solutions, it is first necessary to study how vulnerabilities in routing protocols are can be exploited to launch attacks.

C. Motivation

Due to its wireless channel wireless networks are vulnerable to various kinds of attacks. As MANETs are also an application of wireless networks same is truth for these networks as well. In addition to the open accessible wireless channel the another problem with the MANETs are that the routing between the source-destination pairs that are apart from each other more one hop has to rely on the intermediate nodes for data communication. Due to this the intermediate nodes get the opportunities to work as a malicious node and perform the various types of attacks on the route [4].

It is imperative to secure networks - wired or wireless for its proper functioning. Wireless ad hoc network is more vulnerable to security threats than wired network due to inherent characteristics and system constraints. The nodes are free to join, move and leave the network making it susceptible to attacks - both from inside or outside the network. The attacks can be launched by nodes within radio range or through compromised nodes. The compromised nodes exploit the flaws and inconsistencies present in routing protocol to destroy normal routing operation of the network [5]. A compromised node may advertise nonexistent or fake links or flood honest nodes with routing traffic causing Denial of Service (DoS) attacks [6] that may severely degrade network performance. Thus we see that routing protocols are one of the main areas of vulnerability. There is a need to study the vulnerabilities in routing protocols that may be exploited by malicious nodes to launch attacks. This provides a test bed for designing secure routing protocols.

Therefore, it is very important to understand the impacts of such attacks caused by the intermediate malicious nodes and discover solutions to detect and avoid them during the communication process. Some attacks are easier to detect than others like black-hole attack while in some attacks one can detect the attack but it's very difficult of either avoid it or prevent it from happening in the future like Jellyfish attack. These attacks if not detected and their impact is not analyzed properly may cause serious problems for the communication system on wireless networks. Due to this a large array of researchers are working on the field where various attacks are analyzed and tries to find solutions for their avoidance and prevention.

D. Contribution

In this section, we will provide the overview of the contributions that we have given in this thesis. We have performed a detailed literature survey on attacks on MANETs. This contains different types of attacks performed on various routing protocols and the attacks that are performed on both TCP-based [7] as well as UDP-based data communications. Furthermore, we have also study the current state of the art related to the attacks on mobile ad-hoc networks and their proposed solutions.

In addition to this, in our thesis we have created and implemented a new kind of attack which mainly exploit the behavior of TCP congestion control algorithm and causes some serious problems during the data transmission process. In the proposed attack the intermediate attacker nodes drops some packets over a random fraction of time and then again start the normal transmission process. The attack is implemented using a network simulator and its effects on various scenarios are analyzed to find a solution for its detection.

II. WIRELESS MOBILE AD HOC NETWORKS

Wireless Mobile Ad hoc networks are typically decentralized in nature. "Ad-hoc" is basically a Latin term meaning "for this purpose". They are ad-hoc since they are independent of any pre existing centralized infrastructure. Instead, for routing and forwarding functions, each node acts as a router itself.

MANETs have now become quite an active research area since last couple of decades. This is mainly due to the advent of laptops and growth of 802.11/Wi-Fi wireless networking. MANETs usually have a networking environment that is routable on top of link layer network.

Several efforts have been made towards designing efficient routing protocol for multi-hop ad-hoc networks based on diverse set of assumptions. Application set of MANETs is quite diversified, from small, power constrained static network to large, highly mobile and dynamic networks. Majority of these protocols are usually designed for medium sized networks of 10 to 100 nodes. These protocols are evaluated on the basis of various performance metrics like end to end delays, network throughput, packet drop rate, routing protocol overheads etc.

A. Mobile Ad-Hoc Network

A Mobile Ad-hoc Network is a network consisting of a number of mobile hosts, also called MANET nodes, which communicate with each other over wireless channels without the need of base stations or any other centralized authority.

The interest in this field of research has been growing hugely over the last 20 years. MANETs provide wireless communication that is highly mobile, spontaneous and robust in scenarios where it's not possible or quite difficult to provide centralized infrastructure, for example, Vehicle to vehicle networks (VANETs), battlefield communications, disaster recovery operations etc [8] [9]. MANET nodes are characterized by limited resources like limited battery, processing ability, memory, constrained bandwidth etc. Hence, designing a reliable routing strategy that efficiently uses these confined resources is quite a difficult task.

MANET hosts can move freely in the network, thereby causing frequent network topological changes. MANET nodes have the ability to configure them and can be deployed easily and urgently without any fixed configured network. They need not have any centralized authority or base station to assist in routing mechanism or data transmission. Hence, MANETs score an edge over other traditional wireless networks.

In these networks, all nodes themselves act as routers and are responsible for forwarding and routing operations.

1) Characteristics

Mobile Ad-hoc Networks are mainly characterized by:

i) *Scant Resources*

The wireless channels between MANET nodes have lower capacities compared to those in wired networks. Also, due to signal fading, noise and interference, the link capacity available is often lower than the total capacity of channel. Therefore, network congestions are more common phenomenon in these networks compared to fixed networks.

Also, MANET routing strategies needs to be competent enough to deal with the issue of limited battery life so as to optimize resource usage.

Consequently, signaling protocols in Mobile Ad-hoc Networks are quite challenging to draft due to such resource constraints.

ii) Decentralized Architecture

Due to dynamic nature of MANETs, hosts are organized in a decentralized manner. Any central node or base stations that are usually responsible for controlling routing, forwarding and discovery functions are completely absent. Such architecture presents its usefulness by increasing ability to recover in case of breakdown and at the same time posing harder challenges in designing capable and effective protocols.

iii) Continuous changing Topologies

MANET hosts can freely move and due to their arbitrary movement, their topology will be changed frequently and repeatedly.

Also, the nodes might run out of battery power and gets switched off or restarted, thereby causing random changes in network topology. Hence, MANET protocols need to be robust enough to deal with these recurrent changes in topology.

Other general features of Mobile Ad-hoc Networks can be summarized as follows:

- Wireless mode of communication
- Dual functional nodes, i.e. as hosts and as routers
- Bandwidth constrained
- Power constrained
- Higher frequency of routing updates

2) *Applications*

Mobile Ad-hoc Networks can be used in scenarios where either no already available infrastructure is present or is quite difficult to deploy due to factors like convenience or cost [10]. Examples of similar scenarios can be in disaster recovery or military applications where usual infrastructure has either been destroyed or is unavailable.

Another application can be in file sharing at conferences or any informal gathering or group of students interacting during a lesson or a presentation.

In brief, some major applications areas of Mobile Ad-hoc Networks can be summarized as follows [11]:

- Defense exercises (in battlefields)
- Disaster relief operations
- Mining sites
- Business or informal gatherings
- Vehicular networks (VANETs)

3) *Advantages of MANETs*

For Mobile Ad-hoc Networks, following advantages can be identified:

- High mobility and portability irrespective of geographic position
- MANETs are easily deployable at any place and time

4) *Disadvantages of MANETs*

- Resource constrained
- Lesser physical security
- Decentralized infrastructure (lack of authorization)
- Compatibility issues

B. Issues and Challenges for Routing in Mobile Ad-hoc Networks

Routing has always been a popular and active topic for research. In the last two decades, there have been continuous efforts in designing correct and effective routing protocols for MANETs that can also deal with various constraints associated with these networks.

Before describing the types of routing protocols, it is worth mentioning the development goals for a MANET routing protocol so that certain limitations specific to Mobile Ad-hoc Networks can be dealt with accordingly.

As has already been stated in previous sections of this thesis, some characteristics that define ad hoc networks includes resource constrained devices, limited battery power and bandwidth, security concerns and dynamic topologies. Therefore, exemplary design goals can be summarized for routing protocols for ad hoc networks:

i) *Minimal overheads*

Control messages exchanged during route discovery and other operations introduces unnecessary overheads by consuming battery power and bandwidth. Since these resources are critical and limited, routing operations should involve exchanging the minimum number of control messages between the nodes. This can help in conserving battery power [12]. Similarly, processing overheads are also introduced in the ad hoc networks due to algorithms that are computationally complex. This results in using up more resources and hence more battery power is consumed.

Therefore, research studies shows that it is advisable to implement protocols that are lightweight and involve minimal processing cycles so that battery power can be reserved for other useful tasks.

ii) *Multi-hop routing*

Because of limited transmission range of devices, it is required to use multiple hops to exchange data between source and destination hosts in a Mobile Ad-hoc Network since there is high possibility of them not being within each others' direct transmission range [13].

Therefore, for communication to be possible in the network, routing protocol must effectively be able to detect multi-hop routes.

iii) *Dealing with dynamic topologies*

In Mobile Ad-hoc Networks, route breakages are quite common due to unrestricted movement of nodes causing network topology to change continuously. Also, links can break due to devices getting switched off or restarted. So a path must be sustained during the movement of intermediate as well as end nodes.

Since a single channel is shared among multiple nodes, breakages must be treated rapidly with minimum delay and overhead.

iv) *Prevention of loops*

Generating loops that are free from loops is one of the substantial properties of a routing protocol. Protocols must also provide guarantees to produce fresh routes that consume fewer resources.

When a data packet encounters a loop while transmission, it may have to traverse the same path again and again. This leads to wastage of already scarce resources like bandwidth and battery power and also results in packet loss in the network, hence making the forwarding process quite expensive. Therefore, loops must be avoided in MANETs since they are highly wasteful of resources.

v) *QOS guarantee*

In recent times, majority of focus has been shifted to providing QOS guarantees in MANET routing since MANETs are capable of supporting multimedia applications as well as real time traffic. For such application, certain QOS parameters like delay, energy, bandwidth etc. needs to be taken into account. None of the traditional routing protocols deal with these characteristics in their implementation, but a lot of research is now being centered on extending these protocols with more functionality and is still under expansion. The primary goal of these QOS enabled routing protocols is to find the best QOS aware route from source to destination, not just the "shortest" one.

C. MANET Routing Taxonomy

With these goals in mind, several strategies for routing have been designed for Mobile Ad-hoc Networks. The proposed routing protocols fall into three broad categories:

i) Reactive (On demand) approach
ii) Proactive (table driven) approach
iii) Hybrid approach

i) *Reactive protocols*

Reactive protocols determine routes only when a source node has data to send to a destination node. If the route from the source to required destination is not already available, the source node initiates a route discovery operation to find the needed routes. In route discovery operation, a request message is flooded throughout the network resulting in reply messages from a subset of nodes. The most optimum route out of the search results is used for connection establishment and transmission till the chosen path is being used or till it becomes invalid or gets unavailable or broken.

DSR [14] and AODV [15] are the most widely used routing protocols based on On-Demand strategy. The most peculiar advantage of reactive routing approaches is their ability to immediately present a route when needed, thus eliminating any extra overheads in maintaining static routing tables.

Protocols belonging to this category discover the routes when required or demanded, hence also called as On-demand protocols.

Reactive protocols do not consume any bandwidth when any node is not sending data packet, which means, bandwidth is only consumed when the node has some data to transmit to a destination. They considerably reduce network bandwidth overhead and battery power since no routing advertisement or update messages are exchanged in the network.

ii) Proactive protocols

The proactive routing approaches for Mobile Ad-hoc Networks have originated from the distance vector and link state protocols for wired networks.

In proactive protocols, a route is always available between every two nodes in the network. Periodic route update messages are propagated in the network for the purpose of route creation and maintenance. Periodic updates are exchanged between nodes at specific intervals irrespective of traffic state and mobility of nodes. On the other hand, event triggered updates occurs only when some specific event like link breakage or addition takes place. Since an increase in node mobility has a direct impact on link changes, hence frequency of event triggered updates also increases.

In this category of protocols, routing information is maintained in number of routing tables. These tables are updated in the manner as discussed as above, therefore also called as Table-driven routing protocols.

The primary advantage of proactive protocols is the availability of consistent and up-to-date routes in routing tables between all nodes at all times in the network. However, a major disadvantage is in terms of large overheads incurred in creation, updation and maintenance of these routing table since table updation can become quite frequent in case of high mobility.

The most widely used proactive routing protocols in Mobile Ad-hoc Networks are:

a) Destination-Sequenced Distance Vector (DSDV) [16]
b) Optimized Link State Routing (OLSR) [17]

iii) Hybrid routing protocols

A routing scheme that is purely proactive is not suitable for MANET environment due to large overheads associated with routing tables. In the same way, a pure reactive protocol cannot be completely successful in MANETs due to its associated disadvantages. Hence, certain characteristics of both these approaches can be integrated to form an enhanced class of ad-hoc networking routing protocols, called as Hybrid protocols. These protocols demonstrate reactive behavior in some instances and proactive one in other set of circumstances; hence they allow flexibility and scalability in the MANET environment by assuming the entire network as being partitioned into zones.

Examples of Hybrid routing protocols are:

a) Zone Routing Protocol (ZRP)
b) Zone-Based Hierarchical Link State Routing Protocol (ZHLS)

This paper will mainly concentrate on one of the most popular and widely used reactive routing protocol, AODV and the way in which it can be enhanced to provide some degree of support to some Quality Of Service (QOS) metric. Therefore, this literature will focus mainly on AODV and the operations associated with this protocol for route discovery and establishment.

D. Ad-hoc On-demand Distance Vector (AODV) routing protocol

The Ad-hoc On-demand Distance Vector protocol is an ad-hoc network routing protocol that is purely reactive in nature because no routing tables are needed by the nodes to maintain any routing information. AODV is based upon DSDV and DSR routing protocols. Being an on-demand protocol, AODV maintains information only “active” routes.

In AODV, a node can either be a source or a destination or an intermediate node. If a source node has some data to send to a destination, it checks its routing table to decide whether it has an already available “working” route [6]. In case no such route exists, it performs a route discovery operation to find the needed path. The route discovery process is dynamic and is accomplished in MANETs through various control messages. If there isn’t any transmission ever between a pair of nodes, they need not to maintain a path between each other, hence saving on resources that otherwise would have been wasted in maintaining a path between them.

AODV inherits and enhances some of the typical features of DSDV protocol like periodic beaconing, multihop routing between participating nodes and sequence numbers. AODV ensures freshness of routes through sequence numbers. Periodic beaconing is the time to time exchange of Hello messages in the network used for identifying the neighboring nodes.

AODV accomplishes the complete process of routing through the following two mechanisms:

i) Route Discovery
ii) Route Maintenance

i) Route Discovery

AODV uses a combination of two messages for accomplishing route discovery in Mobile Ad-hoc Networks:

a) Route Request (RREQ)
b) Route Reply (RREP)

When a source node wants to establish a connection with a destination for data transmission, it sends the RREQ message to all its immediate neighbors. RREQ contains the IP address of the source and the destination, a pair of fields related to sequence numbers and a hop count field initialized to zero. Each RREQ message is uniquely identified by a RREQ ID which goes on increasing with each newly generated RREQ in the network. If a node receives an already processed RREQ via some other neighbor node, it is discarded. The source broadcasts this RREQ to its immediate neighbors. The neighbor nodes on receiving the RREQ, generates a backward route to the initiating source. Also, the hop count (distance from source node) in RREQ message format is increased by one.

The node receiving the RREQ checks its route table for the availability of fresh route(s) to the required destination. If it does not have any such route, it simply rebroadcast the RREQ further to its immediate neighbors with the previous hop count value being incremented. Hence, to search a valid route to a destination, RREQ packet is flooded in the network.

On the other hand, if the node receiving the RREQ is itself the destination or it does have an unexpired route to the required destination with the sequence number of the path to that destination (indicated in node's routing table) greater than or equal to the sequence number mentioned in the RREQ message, the node creates a Route Reply (RREP) message and transmit that on the backward route it created towards the node that sent RREQ. Hence, the backward node that was created during RREQ broadcast from source is now utilized for sending RREP back to the source node.

RREP packet contains the source and destination IP addresses, the sequence number of the path to the destination as indicated in the node's route table and the hop count field set equal to the distance between the node and the destination. The hop count is zero if the destination is creating and sending the RREP itself.

As soon as the source node receives an RREP from the destination, the source start utilizing the discovered path for transmission of data packets, till it expires or the topology changes.

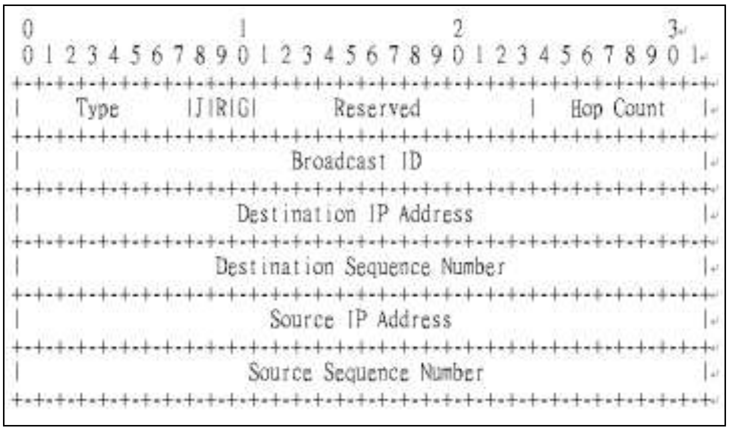
ii) Route Maintenance

After establishment, a route is maintained as long as it is "actively" in use. A path is said to be "active" if it is being used for the transmission of data packets. After the ongoing transmission along the path from source to destination stops, the link will eventually expire and will be removed from the routing tables of neighbor nodes. Another possibility may occur when the link breakage occurs while it is still active. This may happen as a result of sudden topological changes due to mobility of nodes. Link breakages along an active path must be repaired as soon as possible to avoid packet drops and decrease in overall throughput of the network. In such cases, the node upstream of the point of link break creates a Route Error (RRER) message and propagates it towards the source node via its upstream neighbors that were using that link. The RRER message is used for invalidating the broken paths. The source node, after receiving the RRER, can either repair the route or can initiate a new route discovery operation. If the source initiates the route repair, it is termed as a Global repair strategy. In AODV, a route repair process can also be carried out locally. A local route repair is where the intermediate nodes themselves try to repair the route locally instead of sending an RRER message to the source. The major advantage of the local route repair is the fact that since the route is repaired sooner compared to the global approach, hence lesser number of data packets will be dropped. If local repair is unsuccessful, the repair can be executed globally as described.

1) AODV Messages

i) Route Request (RREQ)

The broadcast of RREQ message is initiated by the source node that wish to communicate with another node in the network. A time to live (TTL) value is associated with every RREQ message that indicates the number of hops till RREQ can be transmitted. If the source node has no route in its routing table for the required destination for data transmission, it initiates route search by broadcasting RREQ to its adjoining neighbors. Two separate counters are maintained at every node, node sequence number and broadcast ID of source node.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |J|R|G|      Reserved       |   Hop Count   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Broadcast ID                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination IP Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Destination Sequence Number                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source IP Address                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Source Sequence Number                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1. Packet format: RREQ

The RREQ message format, as shown above, comprises of the following fields:

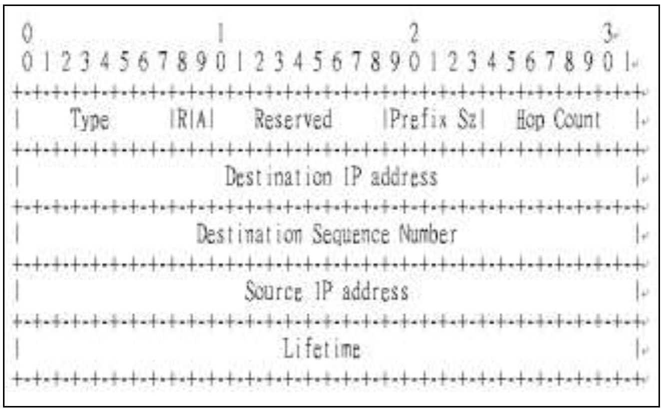
TABLE 1
FIELDS IN RREQ MESSAGE FORMAT

Fields/flags	Meaning
J	Join, reserved for multicast
R	Repair, reserved for multicast
G	Gratuitous, denotes whether a gratuitous RREP should be unicast to the IP address
D	Destination only, specifies that only the destination can respond to this RREQ
U	Unknown sequence number, shows that the sequence number of the destination is
Type	1
Reserved	Contains zero while sending which is ignored on reaching destination
Hop Count	Distance (in hops) from the source to the node handling the RREQ message
RREQ ID	A sequence number that uniquely identifies the RREQ message in combination with the
Destination IP address	IP address of the destination for which the path is required
Destination sequence	The last sequence number received by the source for any path towards the needed
Source IP address	IP address of the node that initiated the route request
Source sequence number	Current sequence number to be used in the route entry indicating towards the RREQ

ii) Route Reply (RREP)

The destination node or any intermediate node that has a path to the requested destination sends an RREP message back to the source after receiving RREQ.

The RREP messages are transmitted on the backward routes set up by the intermediate nodes while broadcast of RREQ during route discovery.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |R|A|    Reserved     |Prefix Sz|   Hop Count   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Destination IP address                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Destination Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source IP address                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Lifetime                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2. Packet format: RREP

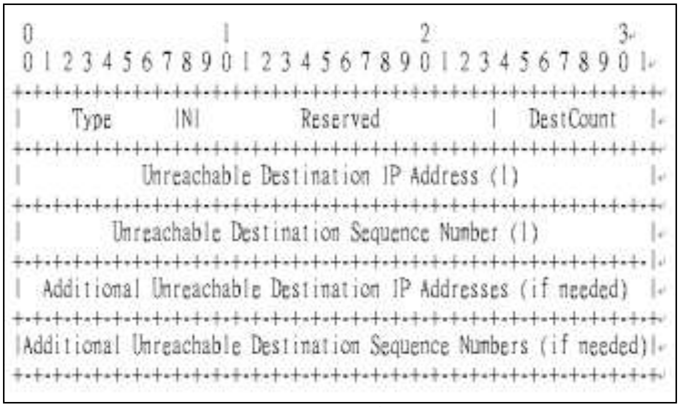
TABLE 2
FIELDS IN RREP MESSAGE FORMAT

Fields/flags	Meaning
Type	2
R	Repair, reserved for multicast
A	Acknowledgement required
Reserved	Contains zero while sending which is ignored on reaching destination
Prefix size	Is a non zero value. This 5-bit field means that next hop can be used for any node with the same routing prefix as the required destination
Hop Count	Distance (in hops) between the source IP address and the destination IP address
Destination IP address	IP address of the destination for which the route is being provided
Destination Sequence number	The sequence number associated with the route towards the destination
Source IP address	IP address of the node that initiated the RREQ propagation
Lifetime	Time (in milliseconds) for which the route will be considered valid by the nodes receiving the RREP

iii) Route Error (RERR)

Apart from the primary messages for route establishment, RREQ and RREP, an additional message is exclusively meant for route maintenance, i.e. RERR.

RERR message is sent to initiate route repair in case of link breakage.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |N|          Reserved           |   DestCount   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Unreachable Destination IP Address (1)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Unreachable Destination Sequence Number (1)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
|  Additional Unreachable Destination IP Addresses (if needed)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Additional Unreachable Destination Sequence Numbers (if needed)|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 3. Packet format: RERR

As shown above, the message format of the RERR packet contains the following fields.

TABLE 3
FIELDS IN RERR MESSAGE FORMAT

Fields/flags	Meaning
Type	3
N	No delete; this flag is set when the link has been repaired and used to indicate to upstream nodes that the link is functional and should not be deleted
Reserved	Contains zero while sending which is ignored on reaching destination
Dest. Count	The total number of unreachable destinations; must be at least 1
Unreachable destination IP address	The IP address of the destination that has become unreachable due to link breakage
Unreachable destination sequence number	The sequence number in the routing table entry of the unreachable destination whose IP address was mentioned in the “Unreachable Destination IP address” field of RERR message

The RERR message is transmitted in the network when one or more destinations become unreachable as a result of link breakage.

2) Characteristics of AODV

- Multiple mode of communication: Unicast, Broadcast and Multicast.
- Route establishment is On-Demand.
- Effective link repair strategies in case of breakages: Global or Local repair.
- Generation of loop-free and fresh routes with the help of sequence numbers.
- Keeps track of only next hop instead of the entire route, hence reducing the overheads considerably.
- Exchange of periodic beacon messages to trace and identify neighbor nodes.
- Reduced number of routing messages in the network.

3) *Limitations of AODV*

- The delay involved while establishing the route is quite large as compared to other reactive routing protocols
- More overheads, with respect to bandwidth and energy, required to maintain the routing table in case of high node mobility
- In case of Global repair, the throughput of the network reduces since more and more packets are dropped till the time RERR reaches the source which then initiates the repair
- Periodic exchange of beacon messages and generation of multiple RREP messages in response to a single RREQ message can cause unnecessary wastage of bandwidth and generate control overheads
- If the source sequence number is not updated from a long time and the intermediate nodes do not have the latest sequence number of the destination, this can lead to inconsistent routes since they will have stale entries in their route tables.

III. Proposed Scattered Dropping Attack on TCP-based Mobile Ad-hoc Networks

In this, we present the details of our proposed attack and also analyze the results that are generated after various simulation processes. The attack that we are implementing in this thesis is named as scattered dropping attack. This is because the attackers are randomly dropping few packets from the packets they receive for forwarding towards the destination node. We measure the effects of this attack on closed loop protocols such as TCP as well as user datagram protocol (UDP) to find out the impact factor of this attack on network throughput, end-to-end delay and number of retransmissions.

A. *Network Modeling*

In the network modeling, we will present the model of the mobile ad-hoc network that we have used for the implementation on which our proposed attack method is implemented and evaluated. The network scenario contains mobile nodes and each node is configured by assigning the required protocols of each layer of the TCP/IP stack. In this section we will present the models of five components of the network that are used to create a mobile ad-hoc network. The components are as follows:

a) Node model
b) Application layer model
c) Mobility model
d) Network Layer model
e) MAC layer model

1) *Node Model*

A node is an entity in the wireless network that is also known as other synonyms such as host, sink, router, source, destination etc. In MANETs due to the dual role of a node it is referred as host as well as router. The node can act as host if it is either source or destination of the data transmission and it has to act as router if it is on the route that is used for the data transmission.

A wireless node consists of the various components required for data communication as shown in Figure 4. As from figure 4 it can be seen that a wireless node mainly consists of five components. The first component is the processing subsystem that is used for processing of received packets such as processing a control packet and updates its routing table, processing a data packet and forwards it towards the destination node or processing the data for aggregation such as used in wireless sensor networks. This subsystem is designed with the help of micro processers and embedded chips that are able to process large data even with its small size and do this processing in energy and power efficient manner.

The second component of the node is communication subsystem which is used for the data communication by using the subsystems that are used for receiving and transmitting signal in the network. This communication subsystem can be a used to use in the different types of the wireless network such a mesh networks, Wimax, sensor networks, MANETs and many more depending upon their implementation details.

The third component is the memory subsystem which is used for the permanent and temporary data storage. Various tables required for routing data packets and storing data related to network topology. Due to the small size of the mobile devices the memory should be managed in an efficient way for efficient transmission.

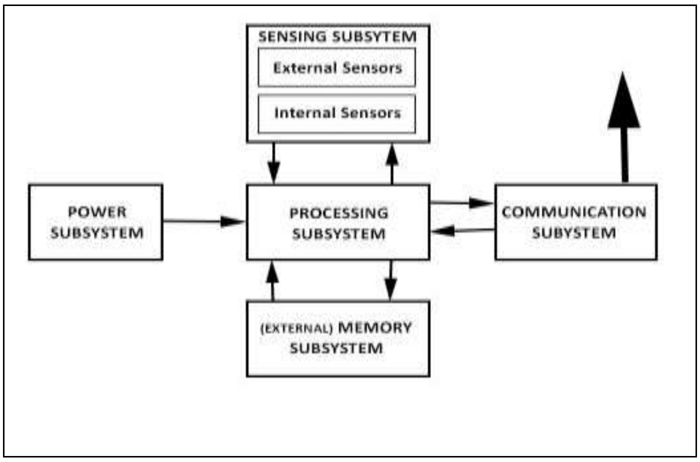


Figure 4. Wireless node architecture

The fourth and fifth components are the sensing subsystem and power subsystem. Again due to the size constraints the power management is the biggest issue due to the small size of the battery used in the mobile nodes. The sensing component is required for many wireless networks in which the wireless sensor networks are the most popular. The sensing units sense the area and provide the details to the sink.

2) *Application Layer Model*

The data communication in the network can either be unicast or multicast depending upon the source and destinations in the communication process. In a communication process, a node is acting as source which sends data to the other node in the network acting as the destination. Application layer processes are used for data generation from the source node. The data can be generated in various ways like it can be a constant stream of traffic with fixed sized data packets or it can be a variable size with variable inter-packet time between the consecutive data packets of a stream.

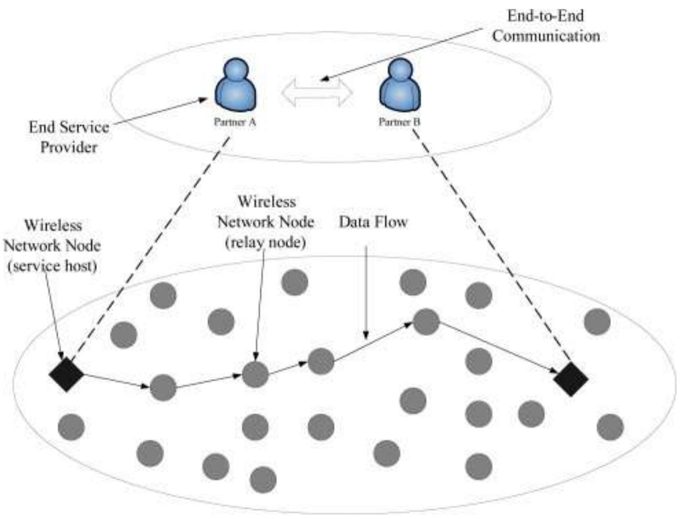


Figure 5. Applications communicating through wireless network

Figure 5 shows the complete process of communication between two applications through a multi-hop wireless network. The multi-hop communication is required in cases where source and destination nodes are not in each other's direct transmission range.

3) Mobility Model

The mobility model is used in the wireless networks to configure a mobility pattern on individual nodes or on the whole network. Based on the configuration details of the mobility model the nodes will move from one position to another in the network. The most commonly used mobility model in the MANETs is the random way-point mobility model. This model shows very close mobility behavior with respect to the real world mobility. Figure 6 shows how the nodes moves in the random way point mobility model inside a given network size.

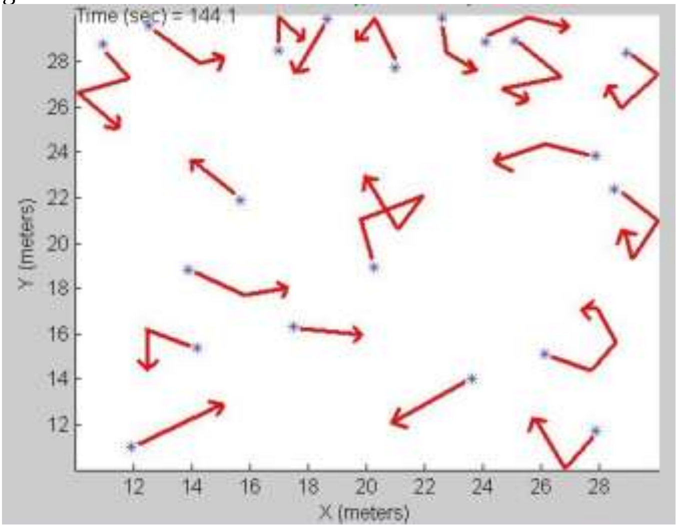


Figure 6. Random Way Point Mobility Model

In random way-point model, three parameters are used to configure the node mobility pattern. The parameters are as follows: a) Pause time, b) Minimum velocity, and c) Maximum velocity. Initially a node is placed a co-ordinate let's say (x1, y1). The node randomly selects another co-ordinate say (x2, y2) within the given network dimensions. Then the node selects a random velocity between the given Maximum and Minimum velocities in the mobility model. The node then moves towards the co-ordinate (x2, y2) with the velocity selected between the specified range and keep on moving until it reaches the selected co-ordinates. Once the node is reached to the selected co-ordinates it waits there for the time equal to the Pause time period given in the mobility model and when this time is over the node again started to the whole process described above.

4) Network Layer model

In the network layer model, the network layer protocols are configured in each node. We used the TCP/IP protocol stack; therefore, we configured the IP v4 protocol for the addressing of nodes. As the routing protocols are required for the communication process each node is running a routing protocol to create and update its routing tables. In wireless networks two types of routing protocols are mainly used for routing process.

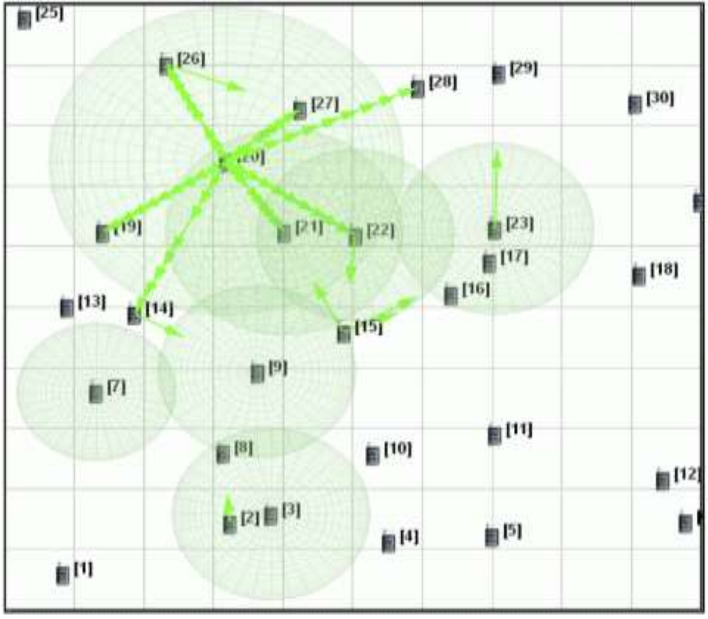


Figure 7. Routing in MANETs

We have used a reactive routing protocol called Ad-hoc on-demand distance vector routing protocol. For communication between two nodes the nodes should use the same routing protocol otherwise the communication is not possible between them. The network layer model may communicate with the MAC or application layer models using a cross-layer communication approach to perform efficient routing based on certain metrics. The network layer is the most important layer in the distributed communication scenarios such as MANETs. A network scenario with the routing between a source-destination pair is shown in Figure 7.

5) MAC layer model

Media access control (MAC) is used to coordinate the access on the shared medium used for data communication process. The MAC layer specifications used for the wireless networks are termed as IEEE 802.11. This standard uses the carrier sensing media access with collision avoidance (CSMA/CA) to avoid collisions and coordinate the channel access between the various contending nodes. In our network scenario, we use the 802.11b PHY layer specification for the transmission process and the data rate of the network is set to 11 Mbps.

In our work we use 802.11b PHY layer protocol with its maximum supportable data rate which is 11 Mbps to configure the nodes in the network. The transmission range is set to 160 meters while the carrier sensing range is nearly 300 meters in this PHY layer protocol.

B. Scattered Dropping Attack on TCP-based Mobile Ad-hoc Networks

In proposed scattered dropping attack an attacker node drops some packets randomly or selectively during the data communication process. The attacker node should be one of the intermediate nodes on the route between the source destination pair to effectively perform this attack. The attacker can perform the proposed dropping attack in one of the following two ways:

a) The attacker can drop a percentage of the total number of packets it receives in a fixed amount of time. For example, the attacker can drop 200 data packets from every 1000 data packets it receives for the forwarding towards the destination.

b) The second way in which the attacker node can perform the drop attack is by dropping all data packets that are arrived for a fixed period of time each time from a fixed amount of time. For example, the attacker node will start dropping all the packets it receives in the first 50 milliseconds of every second.

When the above mentioned packet dropping attack is performed on a data communication session that is transmitting data packets using the TCP protocol. The following can be result: due to the data packets drop at intermediate nodes the retransmission time out of lost data packets triggers their retransmissions at the source node either due to the reception of three duplicate acknowledgment packets or due to the time out of the RTO used by the TCP.

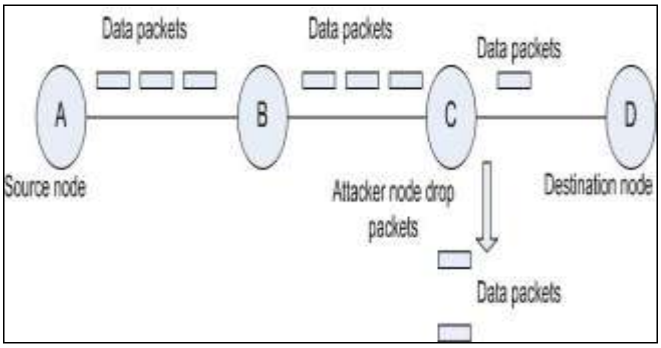


Figure 8. Packet dropping attack

Figure 8 shows how an attacker node drops data packets that are sent from source to destination using the attacker as an intermediate node. In the Figure 4.6 node A and node D are source destination pairs and data is communicated between these using the intermediate node's B and C. If the node C is an attacker node it will receive data packets from node B but it will drop some packets intestinally using one of the two dropping method described above.

In conjunction with the TCP-based MANETs it is interesting to analyze the effect of scattered dropping attack on UDP-based MANETs. Therefore, during the simulation process we have also used the UDP-based MANET scenarios for the impact analysis of our proposed attack.

Algorithm 1 Attacker processing for a data packet received for forwarding

```
Variable used:
//////////////////////////////////
S = Source node
D = Destination node
A = Attacker node
I = Intermediate node
T_total = Total time from which attack time is selected (we set it one second)
T_attack = Attack period
////////////////////////////////
IF1 (I got a data packet)
I check its AODV routing table
IF2 (Route is present in the routing table)
IF3 (I != A)
I forward the data packet towards D
ELSE
A checks whether the current time (Curr_time) is within the T_attack time
IF4 (Curr_time belongs to T_attack)
A drops the data packet
ELSE
A forwards the data packet
ENDIF4
ENDIF3
ENDIF2
ENDIF1
```

The scattered dropping attack is implemented in the trial version of the simulator that we have used for our work (i.e., Exata v2.0). The algorithm used for the implementation process of the proposed attack is given in the Algorithm 1. As we can see in the given algorithm that when an intermediate node gets a data packet for the forwarding purpose it checks its AODV routing table and forward the data packet to the next hop towards destination node. This is done by the intermediate node in the normal scenarios that is when no attacker is present on the communication route. But, when an intermediate node, which receives data packet, is also an attacker node than it checks its attack duration period which is the part of a one second period. The attacker chooses a fixed period which is some percentage of the one second period and the attacker drops all the data packets that it has been received during this chosen attack period. If the current time at which the data packet is received at an attacker node belong to the attack duration than the attacker will drop the data packet instead of forwarding it towards the destination node.

Three TCP variants namely TCP-Lite, TCP-Reno and TCP-NewReno [18] [19] are analyzed against the proposed dropping attack over MANET scenarios. The congestion avoidance phase of all the above three TCP variants uses different approach when congestion in the underlying network during the data communication process is detected.

- TCP-Reno: When three duplicate acknowledgment packets are received by the TCP source (that is 4 acknowledgment packets acknowledging the data packet which is same and also these acknowledgments are not piggybacked as a free ride on data packets. Furthermore, these acknowledgment are not changing the receiver's advertised congestion window), TCP-Reno sets its congestion window to the half of the current size and then the slow start threshold value is set equal to the congestion window. The TCP-Reno then performs a fast retransmit phase by entering in a phase known as Fast Recovery. If during the fast recovery phase an acknowledgment packet times out, slow start phase is started as it is with the traditional TCP. In the Fast Recovery phase, TCP protocol retransmits the data packets for which it has received the duplicate ACKs in the past that was signaled it by three duplicate acknowledgments that it has been received in the recent past. Once sent the missing data packets through retransmission process the waits for the acknowledgment of the whole transmit window before it returns to congestion avoidance phase. When no ACKs are received and again the timeout occurs again TCP-Reno enters into the slow-start phase.

- TCP-NewReno: TCP-NewReno which is defined by RFC 3782 is an improvement over the TCP-Reno described above. TCP-NewReno improves the number of retransmission done when the TCP-Reno uses the fast-recovery process. During the fast recovery phase, for every duplicate ACK that is returned to TCP New Reno, the transmit window is always kept full by sending an unsent data packet from the congestion window upon each arrival of the duplicate acknowledgment packet. Also, whenever there is a partial progress in the congestion windows sequence space the TCP sender assumes that it can now fill a new hole and it immediately transmits a new data packet which belongs to the window beyond the sequence numbers that are already acknowledged.

As the retransmission timeout timer is reset whenever a progress is there in the transmit window of the TCP sender, due to this TCP-NewReno is able to fill large holes and even multiple holes in the transmit window sequence space - something like TCP-SACK. Due to the reason that the TCP-NewReno can transmit new data packets at the end of the congestion window during its fast recovery phase it is able to maintain high throughput during the empty sequence filling process, even in the cases when there are more than one hole each consists of multiple packets. TCP-NewReno returns to the congestion avoidance phase when it gets acknowledgements for the highest unacknowledged sequence number. Problem which occurs with the TCP-NewReno is in the cases where more than 3 data packets are reordered instead of dropped when this happens TCP-NewReno enters in fast recovery phase mistakenly. This is because when those reordered packet is finally reached at the destination node. On the other hand, at the source TCP ACK sequence-number progress occurs in the transmit window and the NewReno sent duplicate and not required retransmissions which are immediately acknowledged by the receiver.

- TCP-Lite: This variant of TCP uses an hybrid approach of congestion avoidance which consists of the above two variants of the TCP (i.e. TCP-Reno and TCP-NewReno).

·

IV. Simulation Results and Performance Analysis

In this section, we present the detailed performance analysis and impact analysis of the proposed Scattered Dropping Attack (SDA) on different variants of TCP protocol over mobile ad-hoc networks. The network scenarios used in the simulation process are designed in such a way so that the effects of the wireless channel and environment can be mitigated. This is done to discover the exact impact of dropping attack on the TCP-based MANETs. Therefore, we ignore the congestion and mobility induced situation from the network scenarios used for simulation process. As already mentioned above that the network simulator used for the simulation process is the trail version of the well knows network simulator called EXata [20]. The source destination pairs in the simulated network are chosen in the way it is required to ensure the full network connectivity and lowest possible environmental effects. The other network parameters used for the scenario creation with their values used during the simulation are given in Table 4 given below. All the results presented in this thesis are the average of 10 simulation runs calculated using different seed values.

TABLE 4
SIMULATION PARAMETERS

Parameters	Values
Simulator	EXata
Network Size	600 x 600 meter square
Simulation time	500 Seconds
Application Layer Process	File transfer protocol (FTP)
Transport Layer Protocols	TCP (Lite, Reno, NewReno) and UDP
Routing protocol	AODV
Number of Nodes	25
Mobility model	None
MAC specification	IEEE 802.11
Network Bandwidth	11 Mbps
Performance Metrics	Network Throughput, Packet Delivery Ratio and Number of Retransmissions
PHY Specification	802.11b

As shown in Table 4 that the MAC specification used is the standard 802.11 which is used to create the MANETs. The PHY specification is 802.11 which has the highest data rate supported is 11 Mbps. The proposed attack effects are measured on both TCP as well as UDP based networks. Furthermore, the performance measurement metrics used are as follows:

A. The performance measurement metrics

1) Network throughput

The network throughput is defined as the ratio of the total number of data bytes received to the total duration of the communication process i.e., the difference between the data session start time and data session end time.

Network Throughput (NT) = Total number of bytes received / (Data transmission end-time – Data transmission start-time).

2) Packet delivery ratio (PDR)

The ratio of the application data packets that are received without any error at destination nodes to the total data packets generated by the CBR sources are called Packet delivery ratio (PDR) of the network. Let’s assume that S is the total number of packets send from source node and R represents the total number of packets received successfully at each destination node than the PDR is defined as follow:

PDR = R/S.

3) Number of retransmission (NOR)

This is the important evaluation metric as we are using TCP-based MANETs. In TCP a data packet is re-transmitted when its retransmission timer expires or the TCP receives the three acknowledgment packets for the same data packet. These retransmissions waste network bandwidth and lead to lower network throughput. The number of retransmissions in our case includes the number of data packets that are retransmitted by the TCP source as a fast retransmits as well as number of duplicate data packets transmitted as a slow re-transmit process.

B. Effects of increase in percentage drop

In figure 9, we have shown the effects on network throughput for three variants of TCP protocol when the attacker increases its percentage drop time. As it can be seen from Figure 5.1 that the throughput of the network decreases with the increase in the percentage drop time because as the drop period within every second of the data communication increases the number of data packets dropped instead of forwarding by the attacker also increases. Due to this the number of re-transmissions on the source TCP increases which decreases the network throughput. The TCP source is sending more duplicate data packets through the re-transmission which does not contributed in the send data and decreases the network throughput.

As it can also be seen from the figure 9 that the throughput of all the TCP variants are decreasing with increase in the drop percentage but the TCP-NewReno is still performing better than the other two variants compared. This is due to its fast recovery process that only performs poorly when the data packets are re-ordered instead of the dropped which is not the case here.

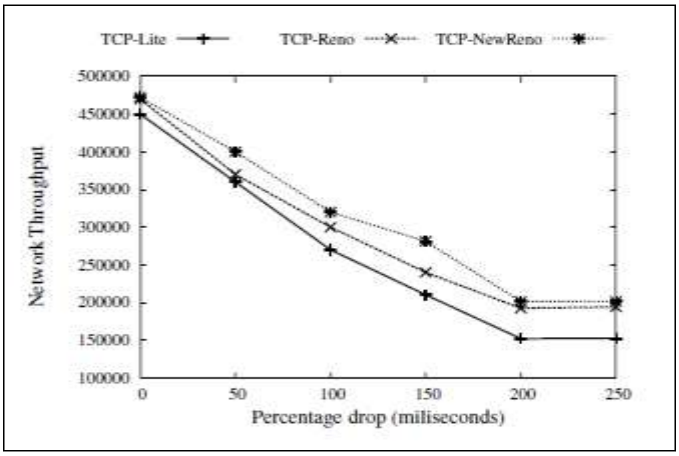


Figure 9. Throughput with increase in percentage drop time of attackers (TCP-based MANET scenario)

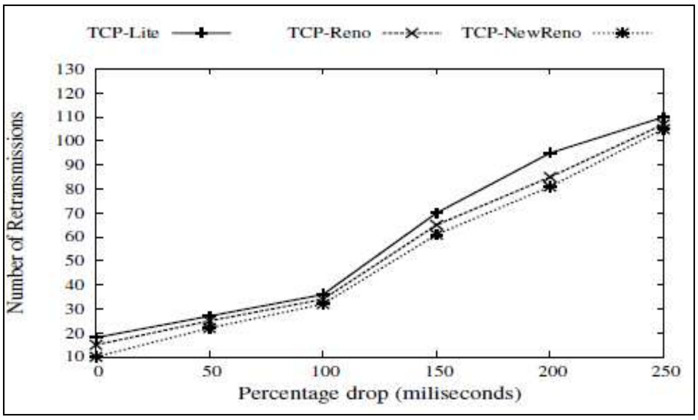


Figure 10. Number of retransmissions with increase in percentage drop time of attackers (TCP-based MANET scenario)

The numbers of retransmission for all the three comparing TCP variants are with increase in the percentage drop time are shown in Figure 10. In the Figure 10 it can be seen that the number of retransmissions both fast and slow increases as the packets from the communicating flow are dropped by the attackers. As the time of the attack increases the attacker is able to drop more data packets which lead to more retransmission either by the duplicate ACKs or when the re-transmission timer at the TCP source associated with the dropped data packet is expired. Finally, it can be summarize from the figures 9 and 10 that due to the hybrid congestion control algorithm the TCP-Lite outperforms the TCP-Reno and TCP-NewReno.

In Figure 11 we have presented the effect on network throughput when the three comparing versions of TCP are used with the increasing number of attackers on the communication route. In this evaluation method the drop percentage of the attackers varies between 50 to 250 milliseconds over a one second period. As it can be seen from Figure 5.3 as the number of attacker's increases the throughput of the network starts decreases this is because with the more number of attackers on the communication route the possibility that a data packet is dropped before it reaches to the destination is increases proportionally with the number of attackers on the route.

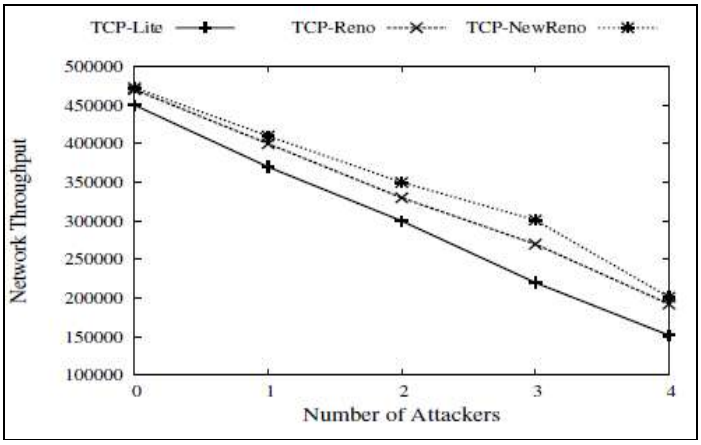


Figure 11. Throughput with increase in number of attackers on the route (TCP-based MANET scenario)

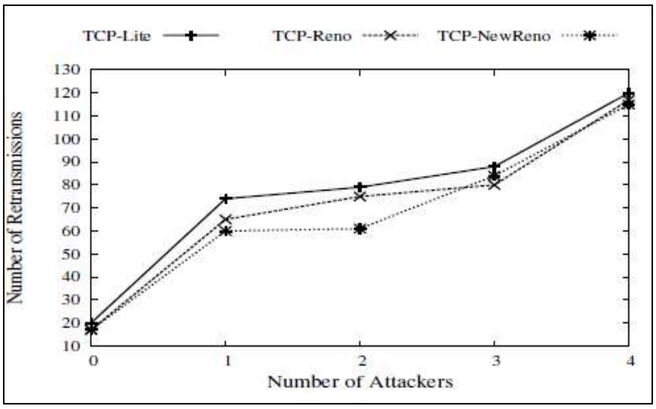


Figure 12. Number of retransmissions with increase in number of attackers on the route (TCP-based MANET scenario)

Figure 12 shows the number of retransmission performed by the TCP-Lite, TCP-NewReno and TCP-Reno when the numbers of attackers are increased on the active route. As the number of attackers increases the numbers of duplicate ACKs are increases as there are more missing data packets in the sequence of data packets that are expected by the destination node. In the TCP-Lite the retransmissions are lower as compared to other two TCP-variants used for comparison. This is because in TCP-Lite the lost packets are acknowledged regularly during the fast recovery and the number of retransmission are decreased due to the intelligent congestion control algorithm used by TCP-Lite.

To analyze the effects of packet drop attack on UDP based MANETs we have also done the simulations that includes scenarios in which the source-destination pair uses the UDP as the transport layer protocol. In the case of UDP based MANETs the proposed packet dropping attack drop the packets and because the UDP does not uses any ACK process for data packets theses dropped packets not only decreases the network throughput but also decreases the packet delivery ratio of the data flow which causes the drop in the quality of the received traffic. In case of video streaming application where a client first download the whole video and then watch that downloaded video offline. In such an application the TCP-based MANET routing will not be affected by the dropping attack because the dropped packets are delivered latter. But on the other hand the UDP-based routing will cause the loss of video frames that causes the decreases in the received video data.

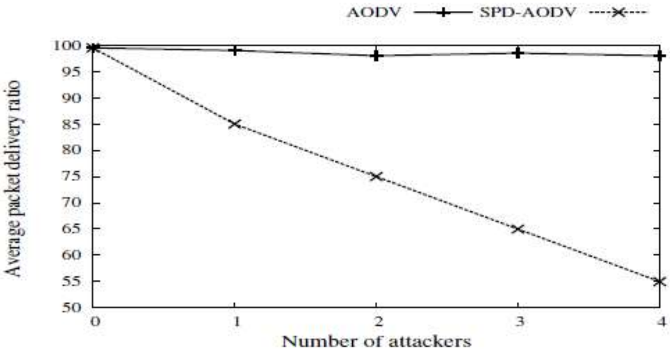


Figure 13. Packet delivery ratio (PDR) with increase in number of attacker nodes on an active route (UDP-based MANET scenario)

In Figure 13, we present the packet delivery ratio (PDR) of a data flow that is using the UDP-based MANET scenario. We compare the PDR when there is no attack on the AODV routing protocol that is represented by AODV in the graph and when there is the scattered packet dropping on the active route (i.e., denoted by SPD-AODV). As it can be seen from the above Figure 5.5 that the PDR of the network decreases greatly with the increase in the number of attackers because the number of data packets dropped on the route increases with the increase in the number of attackers. In this case due to the lack of ACKs the sender will never know about these packets losses. Figure 5.5 clearly shows the effectiveness and success of the proposed attack on a UDP-based MANET.

V. CONCLUSION AND FUTURE WORK

To perform the work proposed in this paper we start with the basics of the mobile ad-hoc networks. We have studied about the MANETs and its characteristics and its challenges and issues that are faced by the researchers when performing the routing over these networks. After the in-depth introduction of MANETs we started the related work which is similar to our proposed work in this thesis. For this we have studied all forms of existing attacks over Mobile ad-hoc networks. As it can be easily seen from the work presented in Chapter 4 that the proposed Scattered Dropping Attack (SDA) is a simple yet very powerful denial of service (DoS) attack that is effective on both TCP and UDP based MANETs. The simulation results clearly show the impact of proposed attack on the network throughput, bandwidth wastage and received data quality. It has also been observed that even though the TCP congestion control is adaptable to the packet losses but in case of the dropping attack it is fully unable to detect whether the packet drop is the result of the attacker misbehaving or it is due to the congestion or other wireless environmental problem.

The simulation results presented in the previous chapter shows that the proposed attack is successful and it will cause the various forms of problems during the data communication process. We have checked the impact of the proposed attack on three different variants of the TCP protocol (i.e., TCP-Lite, TCP-Reno and TCP-NewReno) and it has been found that almost all the variants of the TCP are performing poor under the attack situations. Although, if compared with each other than the TCP-Lite will outperform the other two compared versions of the TCP protocol. This is because the TCP-Lite uses the approach which uses a hybrid congestion avoidance mechanism which recovers faster when data packets are lost due to the congestion. Therefore, TCP-Lite is also able to handle the packet drops caused by the attacker in the more efficient way as compared to the TCP-Reno and TCP-NewReno.

REFERENCES

[1] James A. Freebersyser and Barry Leiner. “Ad Hoc Networking“ A DoD perspective on Mobile Ad hoc networks, 29–51. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2001.

[2] Aad I, Hubaux J-P, Knightly EW. Denial of service resilience in ad hoc networks. In: Proceedings of the 10th Annual International Conference on Mobile Computing and Networking, MobiCom '04, pp. 202-15, 2004.

[3] Aad I, Hubaux J-P, Knightly E. Impact of denial of service attacks on ad hoc networks. IEEE/ACM Trans. Netw, 16(4), pp. 791-802, 2008.

[4] Abdelaziz A, Nafaa M, Salim G. Survey of routing attacks and countermeasures in Mobile ad hoc networks. In: 15th International Conference on Computer Modelling and Simulation (UKSim); 2013.

[5] Abbas S, Merabti M, Llewellyn-Jones D, Kifayat K. Lightweight sybil attack detection in MANETs. IEEE Syst J, 7(2), pp. 236-48, 2013.

[6] Nguyen HL, Nguyen UT. A study of different types of attacks in mobile ad hoc networks. In: 25th IEEE Canadian Conference on Electrical Computer Engineering (CCECE); 2012.

[7] Floyd S, Mathis M, Romanow A. TCP selective acknowledgements options. In: IETF RFC 2018; 1996.

[8] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, and Piet Demeester, "An overview of mobile ad hoc networks: Applications and challenges", Journal of the Communications Network, pp 6066, July 2004.

[9] Cisco Systems Cisco Visual Networking Index: Forecast and Methodology, 20122016. Technical Report, Cisco Systems. 2009.

[10] Morten Lindeberg, Stein Kristiansen, Thomas Plagemann, and Vera Goebel. "Challenges and techniques for video streaming over mobile ad hoc networks", Multimedia Systems, pp. 51–82, 2011.

[11] George Hoffman, Yoko Ono, Akiko Kawakami, Kenichi Kusano, and Takashi Manabe "Japan Communications 2012 Top 10 Predictions" http://www.idc.com/getdoc.jsp?containerId=JP1376002U.

[12] Grossglauser, M., and D. N. C. Tse."Mobility increases the capacity of ad hoc wireless networks", Networking, IEEE/ACM Transactions, pp. 477-486, Aug 2002.

[13] Neely, M. J., and E. Modiano. "Capacity and delay tradeoffs for ad hoc mobile networks", Information Theory, IEEE Transactions 51, pp. 1917-1937, 2005.

[14] C.E. Perkins and E.M. Royer. "Ad–hoc on–demand distance vector routing" Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop, pp 90 –100, Feb. 1999.

[15] Perkins C, Royer E. Ad hoc on-demand distance vector routing. 1999.

[16] Perkins, Charles E. and Bhagwat, Pravin, "Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers", Proceed- ings of the conference on Communications architectures, protocols and ap- plications SIGCOMM" vol 24, pp. 234-244 Oct 1994.

[17] http://tools.ietf.org/html/draft-ietf-manet-olsrv2-11.

[18] Socolofsky T, Kale C. A TCP/IP tutorial. In: IETF RFC 1180; 1991. Stevens W. TCP slow start, congestion avoidance, fast retransmit, and fast recovery algorithms. In: IETF RFC 2001; 1997.

[19] Wazid M, Katal A, Sachan R, Goudar R. E-TCP for efficient performance of MANET under JF delay variance attack. In: IEEE Conference on Information Communication Technologies, pp. 145-50, 2013.

[20] http://www.scalable-networks.com/products/exata/.