CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

Network Security [33] is the major concern of the internet and has become important to personal computer users, organizations and military applications. It is a subset of communication security, the protection of voice and data are the networking components [71]. It is becoming of great importance due to the intellectual property, which is easily acquired through the internet. The use of cryptographic algorithm in network protocol and network applications are covered in the network security [62].

The network security is analyzed by researching the following stages:

- History of security in networks
- Vulnerable security aspects of the Internet
- Types of attacks on the Internet and its methods
- Development of network security hardware and software

The Delay Tolerant Network (DTN) [13] is the smaller network, which accommodates longer disruptions and delay between and within the network. The DTN supports the interoperability of other networks and is considered to be the approach to the computer architecture, which seeks the technical issues in heterogeneous networks. The short range wireless communication is used for an infrared data [75]. It accommodates the mobility and limited power of evolving the wireless communication devices. It is the network, which enables the communication between the nodes and handles the issues such as sparse and intermittent connectivity, long and variable delay, high latency, high error rate, etc. The DTN consists of mobile
devices such as laptops, PDAs, smartphones connected due to the mobility and the low node density.

1.2 ATTACKS IN DTN

The network attack is usually defined as the intrusion in the network infrastructure, which analyzes the environment and collects the information to exploit the vulnerabilities.

Types of attacks

There are several major attacks in DTN, which is listed as follows:

- Passive attacks
- Active attacks
- Black hole attacks
- Worm Hole attacks
- Flooding attacks
- Identity Spoofing attacks
- Password based attack
- Man-in-the middle attack
- Compromised key attack
- Sniffer attack
- Application layer attacks
- Gray hole attacks
- Authenticity attacks
- Sink hole attacks
- Byzantine attacks, etc
1.2.1 Passive Attacks

The goal of the opponent in passive attack is to obtain the information, which is being transmitted. The passive attacks are in the nature of monitoring of, eavesdropping on the transmissions. An interception is a form of unauthorized access the attacker intercepts data and breaks confidentiality or prevents the data by others in this context interception is a passive attack [51]. There are two types of passive attacks such as and is depicted in Figure 1.1.

- Release of message contents
- Traffic analysis

The sensitive information or confidential information contained in a file during the telephonic conversation or electronic mail message is released to the opponent. The opponent should be prevented from learning the contents of the messages.

The traffic analysis is the passive attack and is the subtler. If the contents of the messages or other traffic information, so that the opponents even if they captured the message cannot extract the information from the message. The encryption is the common technique used for masking the contents. Passive attacks are very difficult to detect and it does not involve any alteration of the data.
1.2.2 Active Attacks

The active attacks are the type of attacks, which involves the modification of the data stream or the creation of the false stream. The active attacks are divided into four categories as shown below and the diagrammatic representation is shown in Figure 1.2.

- Masquerade
- Replay
- Modification of messages
- Denial of service

1.2.3 Masquerade

The masquerade is the type of attack when one entity pretends to be the different entity. The masquerade attack usually includes any one of the other forms. Examples of masquerade include the authentication sequences captured and replayed after a valid authentication sequence.
1.2.4 Replay

Replay attacks, captures the passive data unit and its subsequent retransmission to produce an unauthorized effect.

1.2.5 Modification of Messages

The opponent or the third party alters some portion of the legitimate message. The modification of messages simply means that the legitimate messages are altered, delayed or reordered for producing an unauthorized effect.

1.2.6 Denial of Service

This type of attack has a specific target and prevents the normal use of or management of the communication channel. The opponent suppresses all the messages directed to a particular destination. After gaining the access to the network, the attacker does the following:

- It randomizes the attention of the internal information systems staff so that the intrusion is not seen immediately, which allows to make the diversion during the attacks.
- Sends the invalid data to the applications or the network services.
Figure 1.2 Types of active attacks (a) Masquerade (b) Replay (c) Modification of messages (d) Denial of service
1.2.7 **Black Hole Attack**

The black hole attacks [29] are the types of attacks in which the malicious node waits for its neighbor node to send a Route Request (RREQ) packet. When the RREQ packet is received by the malicious node, it sends the forged Route Reply (RREP) to the source node with the sequence number modified. It is considered to be the well-known security threats in wireless ad hoc networks. The source node assumes the fresh route towards the destinations. The source node discards the RREP packets, when it receives from other nodes having a genuine route, which sends the data packets through the malicious nodes. The malicious nodes are responsible for taking the routes towards itself and it does not forward any packet and the attack is known as the black hole attack. The black hole attack is the type of attack, which absorbs everything but never leaves out any information. The black hole is the type of active insider attack and is characterized by two properties, namely the attacker consumes the intercepted packet without forwarding to the destination node. The malicious node announces itself as an accurate route to the destination node, but in reality it is not the accurate route.

![Figure 1.3 Black hole Attack](image-url)
1.2.8 Worm Hole Attack

The wormhole attack is the attack, which is commonly associated with the two remote malicious nodes shown as X and Y in the Figure 1.4. The X and Y nodes are both attached through the wormhole link and the target is to attack the source node S. The source node S broadcasts the RREQ packet during the path finding process to a destination node D. The node A and C are the neighbors of the source node S, it accepts the RREQ packet, and transmits the RREQ packet to their neighboring nodes. The malicious node X is responsible for receiving the RREQ packet, which it sent by A. The node X records and tunnels the RREQ through a high-speed wormhole link to its partner Y.

![Figure 1.4 Wormhole attack](image)

The Y is the malicious node and forwards the RREQ to its neighbor B. The node B forwards the packet to the destination D. The RREQ packet is forwarded via the two paths, namely S-A-X-Y-B-D and the S-C-H-E-F-G-D. The nodes X and Y are connected through the high speed bus and the RREQ packet from the path S-A-X-Y-B-D reaches first to the destination D. The node S chooses the S-A-B-D route to send the data, which passes through the malicious nodes X and Y. Thus, the wormhole attacks is not difficult to set up and immensely harmful for an ad-hoc network.
There are several techniques to detect the wormhole attacks and to secure the protocols against the ad-hoc network.

1.2.9 Flooding Attacks

The Flooding attack is the form of the Denial of Service attacks in which an attacker sends the packets to a particular destination in an attempt to consume enough server resources.

Defences Against Flooding Attacks

The following is the defenses against the packet flooding attacks such as:

- If the packets are received from the arbitrary ports then the packets are avoided.
- The traffic of an application under the flooding attack is used to protect the traffic of other applications.
- The traffic of the established connections are protected.
- The rate at which the new connections are opened are throttled.

1.2.10 Identity Spoofing

Most of the networks and operating systems use the IP address to identify the valid entity. The IP address can be falsely assumed in certain cases such as the identity spoofing attack. The attacker uses the special programs to construct the IP address, which originates from the valid address inside the corporate intranet. If the attacker gains access to the network with a valid IP address, the attacker is able to modify, reroute, or delete the data. It can also conduct other types of attacks.
1.2.11 Password Based Attacks

A common point in most operating system and network security is the password-based access control. The access rights to a computer and network resources are determined by the user name and the password. The applications that are older are not protected as it is passed through the network for validation, which allows the eavesdropper to gain the access to the network by posing it as a valid user.

If the attacker detects the valid user account, then the attacker has the same rights as the real user. If the user of the system has the administrator rights then the attacker creates the accounts, which is accessed at a later time.

If the network is accessed with a valid account, an attacker is responsible for the following:

- Obtains the lists of valid user and computer names and information about the network.
- It modifies the server, configurations of the network, which includes the access control and routing tables.
- Modifies, reroutes, or deletes the data in the network.

1.2.12 Man-in-the Middle Attack

Man-in-the middle attack occurs, when someone is monitoring, capturing, and controlling the communication transparently between the source and the destination of the communicating persons. The computers that are communicating at the low levels of the network layer, the computers are not able to determine with whom the data are exchanged. It is like someone assuming the identity in order to read the message. The person at the other end will believe that the message is coming from the source because the attacker actively replays the messages and exchanges to gain more
information. The man-in-the middle attack causes the same damage like the application layer.

1.2.13 Compromised Key Attack

A key is the secret code or the number, which is used to interpret the secret information. Obtaining the key is a difficult task and the resource-intensive process for an attacker. The key is said to be compromised if an attacker gains the access to the key. An attacker uses the compromised key to gain access to a secured communication without the sender and the receiver being aware of the attack. The attacker is able to decrypt or modify the data with the compromised key and tries to compute the additional keys. The additional keys are used to access other secured communications by the attacker.

1.2.14 Sniffer Attack

A sniffer is an application or device, which is used to read, monitor and capture the data exchanges and reads the network packets. The sniffer provides the full view of the data inside the packet if the packet is not encrypted. Even if the packets are tunneled or encapsulated is broken, open and read unless it is encrypted and the attacker does not have any access to the key.

The sniffer attack is responsible for the following attacks, such as:

- It analyses the network and gains the information to crash the network or to become corrupted.
- Reads the communication between the sender and the receiver.

1.2.15 Application-Layer Attack

An application-layer attacks are the attacks, which targets the application servers by causing a fault in a server’s operating system. The attacker bypasses
the normal access control of the network. The attacker has some advantage in gaining the control of the application system or network and has any one of the following:

- Reads, adds, deletes or modifies the data or the operating systems
- Introduces the viruses in the computer and software applications to copy the viruses throughout the network.
- Terminates the data applications or the operating systems abnormally.
- Disables the security controls to enable the future attacks.

1.2.16 Gray Hole Attack

Gray hole attack actually has two phases. In the initial phase a wicked node abuses other nodes in the network to publicize itself having a effective route to a target node with the aim of seizing packets though the path is forged.

![Gray hole attack diagram](image)

**Figure 1.5 Gray hole attack**

On the later phase, the node drops the captured packets with a definite probability. It is very much hard to discover the multi-behavior of this attack. Either it may send packets coming from definite nodes in the network while forwarding other packets to all other nodes. At times it may also work in a different way by dropping packets and later switch over to its normal behavior.
1.2.17 Authenticity Attack

Authenticity attack is a type of attack in which an attacker assumes others identity in an unauthorized manner. It generates and distribute packets under that pre assumed fake identity.

Figure 1.6 Authenticity attack

1.2.18 Sinkhole Attack

Sinkhole attack is a type of attack were bargained node tries to attract network traffic by presenting its fake routing information. Sinkhole attack influences other attacks like selective forwarding attack, acknowledge spoofing attack to be launched and drops or alter routing information.

Figure 1.7 Sinkhole attack

1.2.19 Byzantine Attack

Byzantine attack is generally known as spectrum sensing attack. Actually opponent have full control over authenticated devices and behave randomly to disturb the network on the whole. An Intermediate node or a set of Intermediate Nodes works in collusion and carry out attacks.
Attacker node creates routing loops, forwarding packets which results in disruption or degradation of the routing services.

1.3 ROUTING PROTOCOLS IN DTN

The DTN routing protocols are categorized into two broad categories as shown in Figure 1.8:

- Flooding based Routing Protocols
- Forwarding based Routing Protocols

![Routing Protocols Diagram]

**Figure 1.8 Routing Protocols in DTN**

1.3.1 Flooding Based Routing Protocols

The flooding based routing protocols are used, when the nodes have no knowledge about the nodes in the network. The epidemic routing algorithm is chosen in which the sender node replicates the message to other nodes. Better results are achieved based on the replication of the message, but it consumes more network
resources for a single message. The flooding based routing is classified into two types such as:

- Replication based
- Quota based

**Replication Based Routing**

The Replication based routing allows the network nodes to create the replicas of the received message. The number of replicas generated within the network for a particular message could be n-1, where n is the number of nodes in the network.

**Quota Based Routing**

Each and every message is assigned with some fixed quota such as the number of replicas for a particular message. In quota based routing the size of the message is limited.

The other types of Flooding based routing algorithms are listed below:

- Direct Contract
- Epidemic Routing
- Prioritized Epidemic Routing
- Two-Hop Relay
- Tree based Flooding
- Spray and wait
- Probabilistic Routing
- Reconfigurable Ubiquitous Networked Embedded Systems
**Direct Contract**

In this type of forwarding scheme the source node forwards the bundle of messages to the destination node. The source node is responsible for creating the bundle and waits for the destination node. Since, it does not require any information about the network these types of algorithm fall into flooding based routing.

**Epidemic Routing**

In the epidemic routing method, the node replicates the message to every other node. The summary vector is checked and then the message is replicated to other nodes. The summary vector is maintained at each and every node and stores the information regarding the messages, which are passed by the node or stored in its buffer.

**Prioritized Epidemic Routing**

The prioritized epidemic routing imposes the partial ordering on the message called the bundles. The priority functions of transmission and the deletion are used, which is based on the four inputs such as:

- Current cost to the destination
- Current cost from source
- Expiry time
- Generation time

**Two-Hop Relay**

The message is delivered to the destination node within two hops only. The source node is responsible for the message to be delivered to a large number of relay nodes. In this method, a large number of relay nodes are used for the delivery of the message.
Tree Based Flooding

The tree based algorithm works on the concept that the source node has a limited number of replicas. Each node has a maximum of two child nodes, so that the replicas are equally distributed between the nodes. After receiving phase, the nodes start off loading the message so that the message reaches the destination.

Spray and wait

The advanced version of the epidemic routing is the spray and wait algorithm. The nodes are not responsible for distributing the replicas to every node, but an optimal number of nodes are selected to relay the message to m nodes. In the spray phase, if the destination is not found, then the node stores the message and performs the direct transmission to the destination node.

Probabilistic Routing

In this routing method, when a message arrives at the node, it stores the message in the buffer until the node encounters with another node. The node receives the message, when its delivery probability exceeds the threshold.

Reconfigurable Ubiquitous Networked Embedded Systems (RUNES)

In RUNES, the new metric is named as “hop” [1]metric, where the value of m means how close the message is to the source and the value of n is how close the message is to its destination.

1.3.2 Forwarding Based Routing Protocols

If the nodes have some knowledge about the other nodes, then the forwarding based routing protocols are used. This type of routing protocols does not generate any
replicas of the message. The resource consumption is reduced or not permitted and used, when the resources are limited.

The following are the protocols used in forwarding based routing scheme:

- NECTAR
- Source Routing
- Per-Hop Routing
- Per-Contact Routing
- Hierarchical Forwarding and Cluster Control Routing
- Hierarchical routing

**NECTAR**

The NECTAR is the algorithm, which uses the concept of the neighborhood index table. The table is maintained at each and every node in the network. The node with the highest frequency is assigned a higher value. If a node needs to forward the message to the destination, it first chooses the relay node with highest index value.

**Source Routing**

The source routing method consists of the two phases such as the route discovery and the route maintenance phase. The control packet is sent towards the destination node and the route is discovered initially. The address is appended in the packet by the intermediate nodes. The routes are cached and maintained by the node over time. If the packet reaches the destination the entire route is appended to the data packet. If any failure occurs in the link, a link error message is sent by the source node.
Per-Hop Routing

Hop is actually a shifting of packet from source to the destination node. Hop occurs when a packet passes to other network device. Routing table contains the next hop IP address and each known destination address along the correct path.

Per-Contact Routing

The per-Contact routing information is the most updated information, when any intermediate node receives the message for a particular destination, then the node checks the current up contacts and selects the appropriate node for relaying the message.

Hierarchical Forwarding and Cluster Control Routing

This routing protocol introduced the concept of the clustering of the nodes on the basis of the property and the characteristics of the communication. A cluster head is selected depending on the criteria. The head of the cluster is selected based on the higher stability or the higher quality within the cluster node.

Hierarchical Routing

Hierarchical routing is the hop-by-hop routing, which is scalable for the localized traffic patterns, and does not need any information regarding the location. A method is needed to aggregate the time varying information and the contact information is time-variant.

Other Routing Protocols

The routing protocols are categorized into three based on the topology such as:

- Proactive Routing protocol
- Reactive Routing protocol
- Hybrid Routing protocol
**Proactive Routing Protocol**

The proactive routing protocol is the protocol in which each and every node keeps one or more tables representing the complete topology of the network. The tables are updated constantly for updating the routing information from each and every node. The routes in the network is available on request. These types of protocols arise from the traditional link state routing protocols. The Optimized Link State Routing Protocol (OLSR) is the example for the proactive routing protocol.

**Reactive Routing Protocol**

The Reactive routing protocol is the on demand routing protocols. These protocols does not have the correct routing information on all the nodes at all times. The routing information is collected, whenever required. These types of routing protocols have the fixed overhead data for routes, which is never consumed. Reactive search procedures adds the significant amount of control traffic in the network because of flooding. Due to the weakness reactive routing protocol is less applicable for the real time traffic.

**Hybrid Routing Protocol**

Wireless hybrid routing is based on the idea of organizing nodes in the group and allows the different functionalities inside and outside a group. The routing table size and the update packet size is reduced based on the network.

The DTN network is the part of the mobile ad hoc network and uses the same protocols as in the MANET [53]. A mobile Ad hoc network is a system of wireless mobile nodes that dynamically self organize in arbitrary and temporary network topologies [66]. The protocols in DTN are listed as follows based on the topology:

- Dynamic Source Routing (DSR)
Dynamic Source Routing (DSR)

The DSR is a reactive routing protocol, which discovers the routes and maintains the routes between the nodes. The first step is to discover the routes between the nodes by flooding the Route Request packet to the network. In the reactive protocol the node receiving the packet first adds the address to the packet and sends the packet to the next node. If the targeted node or a node, which has a route to the destination receives the Route request packet and replies with the route reply packet to the sender node. Each time if the packet follows an established route then each and every node has to ensure that the link is reliable between the sending node and the next node. The DSR routing protocol provides three successive steps in maintaining the route such as:

- Link layer Acknowledgement
- Passive Acknowledgement
- Network layer acknowledgement

If any error is detected, then the node sends the Route Error packet to the original sender.

Optimized Link State Routing (OLSR)

The OLSR is considered to be the table driven protocol, which stores the routes and updates the routes whenever needed. The route is provided without any initial delay in the network. In OLSR, the candidate nodes are called as the multipoint relays (MPR) that are selected and responsible to forward the packets during
the flooding process. The OLSR technique reduces the overhead of packet transmission, when compared to the flooding mechanism. The hop-by-hop routing is performed in the OLSR routing technique. In this technique, each node uses the most recent routing information to route the packets. The MPRs is selected based on the sensing information of the node with the control messages called the HELLO packets.

**Ad-Hoc on Demand Distance Vector Routing (AODV)**

The AODV is the on demand route discovery in ad hoc network. If the nodes need to send the data to the destination and the routing information is not found in the routing table then the route discovery process begins, which finds the routes from the source to the destination. The Route Request Packet (RREQ) is sent by the source node to the neighboring nodes. The RREQ packet is comprised of the broadcast ID, two sequences number, the source and the destination addresses, the hop count. If the intermediary node is not the destination means it performs the following two steps:

- It rebroadcasts the packet to the neighboring nodes.
- If it is the destination node, then it sends the unicast message as a reply.

Each and every node is associated with a sequence number and if any node wants to initiate the route discovery process then the node uses the sequence number and the fresh sequence number it has for its destination node. Every entry in the routing table is associated with the lifetime period. If the routes are not applied within the lifetime period, the routes are not expired and should be dropped from the table.
Gathering Based Routing Protocol (GRP)

The GRP scheme collects the network formation at the source node with small amount of control overheads. The source node finds the routes and continuously transmit the data even if the route is disconnected. This approach achieves fast transfer with less overhead of control messages. This method is called as the hybrid approach in routing. When a packet reaches the destination node, it broadcasts a Network Information Gathering (NIG) packet to its neighbors. The source node computes the best route according to the collected information and then starts to transmit the data packets.

1.4 TRUST MANAGEMENT IN DTN

Trust management is the basis for communicating policy among the system and demands the credential checking for all the virtual resources. The trust management is a popular method for implementing the information security, and the access control policies. There are several advantages in trust management, such as:

- The trust management in DTN is the basis for the communicating policy among the systems.
- There is no unified policy-based mechanism and other recovery mechanisms across a large distributed system.
- The trust management provides the unified approach in interpreting the security policies, credentials, and the relationships.

Trust Management Schemes

There are several trust management schemes used in DTN, such as:

- Erasure coding
- Checksum
- Hash Function
- MD5-MAC
- Bloom Filter (Authentication mechanism)
- Hierarchical Trust management Scheme

**Erasure Coding**

The erasure coding is the trust management protocol used in DTN and works by breaking the message into a set of message segments. A large subset of message segments of the original message is reconstructed. The erasure coding starts with the message size of M and the total size of the information \( I = M(1 + \epsilon) \) needed for the message recreation. \( \epsilon \) is the constant and is considered to be the smallest quantity, which depends on the exact encoding algorithm. The k is the minimum number of segments, which is selected such that I is divided evenly by k. The total number of segments, \( s > k \) is chosen and the encoded message is divided into many segments. When the erasure coding is used as the key aspect is the replication factor of r. The message is recreated by considering the \( s/r \) of the message segments at the destination.

**Checksum**

The checksum is the trust management mechanism, which is used to determine the trustworthiness of the neighbor nodes. If all the message segment arrived at the destination and recreated the complete message, then the trust of the neighboring nodes increases. If one or more segments in the messages are corrupted or if it is a malicious nodes, then bad actors are determined. The bad actors are determined by
appending the source node with the checksum to every message, which is sent prior to the erasure coding. The checksum scheme steps are listed as follows:

The node A sends the message m to the node B.

- The message m is segmented by adding the checksum, using the erasure coding such that k segments the message m.
- If k unique segments arrive at the node B, the message m is recreated.
- If the segmented message m has a valid checksum, then the node B has an increased trust for all the nodes by sending a valid segment.
- The node B waits for each additional segment until recreating the m, which produces a valid checksum.
- The receiving node waits for a time T and accepts the addition, segments for the message m. The validity of the each node is checked against the k-1 good segments and the trust are changed in the relevant path accordingly.

The checksum not only increases the delivery ratio of the packets but also to establish, update, and revoke the trust.

**Hash Function**

The hash function is used for verifying the intermediate nodes for trustiness. Based on the hash function the trust value is evaluated.

**MD5 Algorithm**

MD5 is the hash function proposed by Rivest and it is the strengthened version of MD4. The MD5 algorithm takes the arbitrary length message and a 128 bit value is generated. The input message M is padded and is represented by the $\overline{M}$ and it is the multiple of 512 bits. The length of the M bits is represented by l, and the bit 1 is appended to the end of the message. The end of the message is followed by the k 0
bits, where $k$ is the smallest non-negative integer. The smallest integer is calculated such that $l+1+k=448 \mod 512$. Then, the 64 bit block is appended, which is equal to the number $l$ expressed using a binary representation. The $\overline{M}$ is the padded message and is divided into the 512 bit message blocks. Each and every iteration invokes a compression function, which takes a 128 bit chaining value and a 512 bit message block as inputs and outputs a 128 bit hash value. The compression function has normally four rounds, each and every round has 16 steps and employs a round function. The hash function for $n$ iterations is performed for $\overline{M}$ with $n$ blocks.

**MAC algorithm**

A Message Access Control (MAC) algorithm is the hash function with secret key $K$ as the secondary input. HMAC (Hash Based Message Authentication Code) and the NMAC (Nested Message Authentication Code) are the two popular algorithms derived from the efficient hash functions. Three other MAC algorithms are constructed by the Secret Prefix Method, Secret Suffix Method, and the Envelope Method.

**MD5-MAC Algorithm**

The MD5-MAC algorithm is the security mechanism used in the DTN, which is first proposed by the Preneel and Van Oorschot. The MD5-MAC algorithm converts the MDx family hash functions into MAC algorithms. The key size is up to 128 bits and the underlying hash function is any of MD5, RIPEMD, SHA or other algorithms. The MD5 –MAC is obtained from MD5 with the following modifications such as:
- The MD5’s initial value is replaced by \( K_0 \).
- The \( K_i \) key is split into four 32-bit words denoted by \( K_i[i] \) which are added to the constants used in the round \( i \) of each MD5 iteration respectively.
- The padding and the appended length are defined in the block by using the MD5 algorithm.
- The left most \( m \) bits of the hash value is the MAC value.

**Bloom Filter (Authentication Filter)**

The Bloom Filter is the classifier, which is used for the authentication in the DTN. The Bloom Filter is a simple and the space efficient randomized data structure in order to support the membership queries. A bloom filter is used to check, whether the node belongs to a particular subset or not. All the phases in the bloom filter is set to 0 and uses the hash functions to map the items to a random integer. The bloom filter is used to assign the nodes probability of reaching every node in the network. To establish the probabilities in the network, the nodes periodically exchanges the bloom filters. If the neighbor node receives a filter from a neighbor, it uses the addition operation to merge the contents of the current topological information with the received filter. The nodes use the degradation operation to implement the probabilistic form of the state in which the information of the destination is lost. The bloom filter \( F \) is considered to be an array of \( m \) counters, which takes the values from the 0 to count. The insert operation is used to add the identity of the node in the network. The insert operation takes the filter \( F \) and the identifier of a node and returns a new filter, which contains the identity \( a \).

The degradation operation is a unary operation, which decrements the single unit of each counter with the probability \( p \). The degradation operation is used, where
the information contained in the filter is lost. The information from the filter is lost because of the growing stale or if the information is propagated away from the place of generation.

Hierarchical Trust management Scheme

Hierarchical trust management scheme derives multi-dimensional trust attributes from various communication and social networks to evaluate overall trust of the sensor node. General geographic routing trusts only the geographic information and results in low message delivery ratio but here both traditional geographic trust and QoS trust are gathered to imply a best routing.

1.5 MOTIVATION

In our day-to-day life all are using the Internet through wired or wireless medium. The Internet is vulnerable to many types of attacks and providing the security to the network is the challenging and interesting area of research. The DTN is an emerging technology in ad-hoc network, which facilitates the secure access to information. Since, the DTN is the ad-hoc network it is vulnerable to many types of attacks. In this research work mainly two attacks, namely the black hole and the wormhole attacks are detected and removed using the proposed Repetitive trust management and adversary detection techniques. Several secure routing mechanisms are also designed in the DTN to detect the black hole and the wormhole attacks. The proposed system is useful in detecting the black hole and the wormhole attacks in the DTN and forwarding the information in a secure manner to the destination node in an end-to-end routing scheme.
1.6 OBJECTIVES

The main objectives of the thesis include,

- To detect the Byzantine attacks an efficient trust management scheme such as the Repetitive Trust management (RTM) and the adversary detection schemes are used.
- To authenticate the user or the information in the Delay Tolerant Network the Bloom Filter is used.
- To prevent the black hole and the wormhole attacks, the secure routing mechanism such as the reactive routing protocols are designed.
- To enhance the trust in the DTN, the Privacy Preservation Mechanism is implemented.
- To secure the information and for preserving the privacy in the DTN, the MD5-MAC algorithm is used.

1.7 ORGANIZATION OF THESIS

The thesis is organized as follows,

**Chapter 1** discusses the basics of this research work, gives the basic knowledge regarding the objective, motivation behind the research and the justification of this relevance. Various types of attacks, routing protocols and security mechanisms are studied in this chapter.

**Chapter 2** describes the literature survey related to various attacks in the DTN. Various papers related to the DTN, trust management, black hole and wormhole detection techniques are surveyed.

**Chapter 3** describes an efficient approach namely, the Repetitive Trust Management and the adversary detection for handling the Byzantine attacks. The trust
management based classifier is also discussed for the effective authentication of the information. The performance of the trust management and adversary detection method is compared to the performance of the existing methods and depicted in the graph format.

**Chapter 4** describes the security mechanisms for preventing the black hole and the wormhole attacks. The MD5-MAC algorithm is also described in this chapter. The performance of the secure routing mechanism is compared to the performance of the existing methods and depicted in the graph format.

**Chapter 5** discusses the privacy preservation schemes for enhancing the trust in the DTN. The DTN formation, trust identification, and the preservation of privacy is discussed in this chapter. The performance of the privacy preservation mechanism is compared to the performance of the existing methods and depicted in the graph format.

**Chapter 6** concludes the research outcome of this thesis. It also provides suggestions for some possible research work that can be done in the future to extend the outcome of present research.

In this section, the basics of the DTN and the network security are described. Various types of attacks, which violates the security of the network are discussed such as the active attacks, passive attacks, black hole attacks, worm hole attacks, etc. The routing protocols such as the reactive, proactive and the hybrid protocols are discussed. Several routing protocols such as AODV, OLSR, and DSR used in the ad hoc network are also described. The security mechanisms for preventing the black hole and the wormhole attack in DTN are also described in detail. Then, the motivation, objective, and the organization of the thesis are explained. The rest of the chapters explain the brief overview of the research work.