SECURITY ISSUES IN DTN - A REVIEW

Pradosh Kumar Gantayat
Asst.Prof. Dept. of Computer Science,
DRIEMS, Odisha

Sambit Mohanty
PG Scholar Dept of Computer Science,
DRIEMS, Odisha

Sudeep Kumar Gochhayat
PG Scholar Dept of Computer Science,
DRIEMS, Odisha

Abstract - Delay tolerant network is a type of wireless adhoc network. In DTN nodes are mobile, self managed and intermittently connected with each other using wireless link. DTN are mostly used in that situation where that is no fixed infrastructure is present like in military operation, interplanetary communication, disaster rescue etc. Nodes in DTN has limited communicational capabilities and they communicate with each other when they are in transmission range of each other. Due no previous knowledge of route these type of network suffers from various types of security threats, these security attacks can disturb the normal operation of the network and increases the delay, packet dropping, message overhead, communication overhead, network congestion and decreases the overall all performance of the network. This paper discuss about such different types of security threats on DTN.

Keywords: DTN, security threat

1. Introduction:
DTN is a type of adhoc wireless network because it has no pre existing infrastructure and any node can be attached and leave the network any time. DTN is designed on the principle of store and forward technique to operate in the situation when there is no continuous connectivity among nodes.[1] Nodes communicates with each other when they come within their transmission range. As continuous communication is not available due to the mobile nature of node and limited transmission range of nodes so delay in data transmission occurs. As there is no predefined route is present in the network so it is the responsibility of the nodes to forward packets to destination. DTN depends on the temporary path created by nodes by finding their neighbors. Mobility of nodes, activation and deactivation of nodes, power consumption of node may change the network topology. so nodes have to track the network topology for packet transmission.[2] Some times sender has no direct path to destination so the network has to depend on the intermediate nodes for packet forwarding.[3] Sender node forwards the packet to its neighbor node in its range. By this the packet be comes closer to the destination, as the packet passes through several nodes so there is a possibility that one or more node to be malicious[4].These malicious node may hamper the packets and security of the network.

2. Classification of nodes in DTN:
There are basically two types of nodes other than normal nodes: Selfish node and Malicious node.

2.1 Selfish node:
In our daily life there are some persons which are selfish by nature. They only helps those people which can help them in achieving their goals. Similarly in DTN there are some nodes are present which...
intentionally drops some of the packet instead of forwarding them to other nodes. They behaves selfishly to preserve their battery power.[5]

2.2 Malicious node:
Malicious node does not forward any message to any other node, they simply drops all the packet received from other nodes. Malicious nodes attacks the whole network and reduces the performance of the network.[5]

3. Threats in DTN:
DTN suffers from variety of attacks but it is broadly divided in to two types Passive attack and Active attack[6][7]. Passive attack does not disturb the operation of the network. The attacker only tries to extract the important information from the network. It is difficult to detect because it does not disturb the network or modify the content of data packet.[8].
Active attack disturbs the operation of network and tries to modify the content of the data packets. It is further divided in to 2 types External attack and Internal attack. External attack are launch by the outsider nodes which are not the part of the network. It disturbs the network by introducing delays in routing. Internal attack are done by the insider nodes of the network. It is difficult to detect internal attack than external attack.[7]

3.1 Blackhole Attack:
Blackhole is a point in the space where energy and matters disappears due to gravitational energy.[8] a malicious node acts like blackhole when it starts dropping all the received packets. Nodes passes data packets to its neighbor node basing on some constraints, blackhole node declares itself as the best path for packet forwarding. So nodes forwards their packets to blackhole node. On getting the packets it starts dropping packets. In DTN communication is opportunistic so there is lack of confirmation of acknowledgment on packet delivery. So sender unables to know about the packet dropping.[5][9]

3.2 Grayhole Attack:
In this type of attack , the malicious node when receive a route request message from other node then it behaves normally by sending true route reply message. So the sending node treats the route is the best path and forwards the packets. Upon receiving the data packets the attacking nodes starts dropping them. After dropping packets it again starts behaving like normal node. So it is very much difficult to detect the grayhole nodes.[5][8][9]

3.3 Wormhole Attack:
In this type of attack , two attacking nodes creates a tunnel in between them, they shows the network that it is the optimal path for data transmission from any point to any point in the network. When the attacker node get the forwarded packet then it suddenly passes the data packet through the wormhole tunnel to the other attacking node. When the packet is received by the other attacking node then it re inject the data packet in to the network which causes network congestion and delay .[9][10][11]

3.4 Flooding Attack:
Flooding attack means sending unwanted packets into the network .An attacking node can do this by sending Route Request Message or useless data packets to this node.
In route request flooding method, attacker node sends an invalid route request message to all nodes or some of the nodes. So that the nodes in the network unable to answer route reply because the address does not belongs to the node or it may be an invalid address. In this way the attacker node repeatedly sends this kinds of route request message to the nodes so that the nodes faces network congestion and hampers the performance of the network.In data flooding method ,
attacker node sends useless data to the targeted nodes. So that the node is always busy in accepting the data packet. These useless data packet consumes the resources of nodes like memory, battery power etc.[9]

3.5 Jellyfish Attack:
In this type of attack, attacking node introduces delay in the network. During transmission process when the attacker node receives data packet from other node it stores in it’s memory for a period of time without forwarding it. After a finite period of time it starts transmitting it to it’s destination. So that a delay is introduced in the network which hampers the performance of the network. In some jelly fish attacks the attacking nodes receives data packets in a particular order but transmits the data packet in different orders which reduces the performance of flow control mechanism of the network. The receiving node gets data packet out of order.[9][12][13]

3.6 Modification Attack:
In DTN all the nodes are mobile. Communication between nodes takes place only when a node comes in the transmission range of other nodes. Network topology may changes due to activation and deactivation of nodes. So there is no fixed topology of the network. So at any time any node can be part of a network or leave a network. By using this advantage the attacker node becomes the part of the network. The node actively participate in the routing process. By using the irregularity of DTN like intermittent connectivity, delay etc. the attacker node performs the message modification attack. There are two main types of modification attacks are misrouting and impersonation [9].

3.7 Misrouting/silent route change Attack:
In this type of attack, first the attacking node becomes the part of routing process. Then it forwards the packet to as invalid or unknown destination. So that the data packet does not find it’s original destination. It travels through the network for a period of time by using the resources of network. Finally the network drops the packet.[9]. As this type of attack changes the route of the data packet unknowingly, so such type of attack some time known as silent route change attack.[5]

3.8 Impersonation Attack:
In a network every node has an unique identity to distinguish itself from other node. In DTN, a node can be identified by using it’s IP or MAC address. In this type of attack the attacker node thefts the identity of a normal node and shows that it is the actual node.[9][14] The attacker node takes the identity of legitimate node either to use the network resource or to disturb the normal operation of the network. There are different types of impersonation attack exist like Sybil attack,[14] trust attack, man in middle attack.[15]

3.9 Sybil Attack:
The term Sybil is derived from a case study of woman with multiple identity.[16] In DTN every node is uniquely identified using IP address or MAC address. When a single node exhibits more than one identity then such type of node is called as Sybil node. During data transmission process, a normal node when communicates with a Sybil node but believes that it communicates with multiple node. Actually there is only one physical node is present which exhibits multiple identity. In this way attacker node uses the network resources. It creates confusion and congestion in network.[17]

3.10 Man in Middle Attack:
It is a type of impersonation attack in which the attacker node first tries to become the part of the network. Then it sits between the two communicating node without the knowledge of both nodes. The communicating nodes believes that they are
communicating with each other but actually they are communicating with man in middle node.[12][14][15]

3.11 Sleep Deprivation Attack:
In DTN all the nodes are mobile and have to operate in limited resource. For the better performance of the network energy management is a key functionality. A node is active in DTN till it has battery power. In sleep deprivation torture attack the attacking node targets the nodes battery power rather than dropping packets. The attacking node sends a large number of unnecessary packets to the targeting node to make the node busy. Such that the battery power is consumed with each transaction. Attacker node sends data packet until the targeted node goes to sleep node. In this way the attacker node disturbs the whole network.[5][18][19]

3.12 Reply Attack:
In this type of attack the attacking node does not change the content of the packet but it re inject the previously captured original packet into the route. So that it creates a duplicate clone or replicate clone of the original packet. It injects it into traffic to create network congestion and delaying in transmission.[14][20]

3.13 Byzantine Attack:
It is a type of attack in which more than one node in the network attack the network to degrade the performance of the network .In this type of attack different attacking node collectively performs different type of misbehavior like creating loops in route, dropping packets selectively, forwarding packets in non optional paths. By creating loops in the network the packets faces congestion in the network so it introduces delay in the network.[14][15][21]

3.14 Rushing Attack:
In this type of attack, when a sender wants to forward message to other node then it sends a route request message to other node. Attacking node upon getting these route request message creates a malicious route request message of that node and floods it through out the network with very high speed. Other node receives these malicious route request message before receiving the actual message. Upon receiving the actual message they discard it as the duplicate copy of the first message. So the sending node always gets a route through the attacking node. It does not find a secure route without including the attacking node.[12][14][15].

3.15 Information Disclosure Attack:
In this type of attack, the attacking node first start monitoring the network traffic between the targeting node and other nodes. Then it understands the traffic pattern and other routing information. Then the attacking nodes discloses important information about the network like encryption technique, node status, password, optimal routes to target nodes, node location etc. these type of attack violates the network security principles like authentication, confidentiality etc.[12][14][15].

3.16 Timing Misbehavior Attack:
In this type of attack, the attacking node holds the packet for a period of time so that the packet is expired. In data packets there is a field TTL(time to live) is present that determines how long a data packet will exist. At each node in the path it decrements. When it reaches zero then the packet is expired and discarded by the network. the main aim of the attacking node is that the data packet should not reach its proper destination so it blocks the packet until the TTL becomes zero.[5].

3.17 White Washing Attack:
White washing attack is a type of Sybil attack. Here a Sybil node at a time uses only one identity and discards all other previous identity in which some
malicious activity has done. It is some how like changing a person’s identity to hide his previous criminal activity. The main purpose of discarding all earlier identity is to remove previous records of the attacking node. It shows the network that it joined as a fresh node.[17]

3.18 Route Salvaging Attack:
Due to the intermittent connectivity every data packets may not reach its proper destination. Due to such issue some selfish node performs route salvaging attack. To protect their data packets these selfish node retransmits them without informing other nodes. So the network suffers unnecessary congestion and intermediate nodes loses its battery power.[22]

3.19 HELLO Flood Attack:
In this type of attack the attacking node first sends a broadcast message to all nodes. So all nodes believe that the attacking node is neighbor to them so they transmits their data packets to it. This type of attack creates a confusion and network congestion and unnecessary consumption of bandwidth and wastage of energy of nodes.[23]

4. Conclusion:
In this paper we have tried to describe different types of attack on DTN. These various types of attack are carried out by the malicious nodes. So there is a need to detect these type of malicious node irrespective of routing protocol. This paper helps to know about various types of attack and their nature and helps to find solution for preventing them in future.

Reference:
paper presented at National Conference on Computational Instrumentation Chandigarh, India, 19-20 March 2010


