ECE509
Cyber Security : Concept, Theory, and Practice

Lecture 6: Network Security part 1

Fall 2023

What will be covered in this class?

Application Security & Resilience

User and Web Applications	Mobile Platforms	Web Protocols
Encryption	Forensic Analysis	Insider Threats

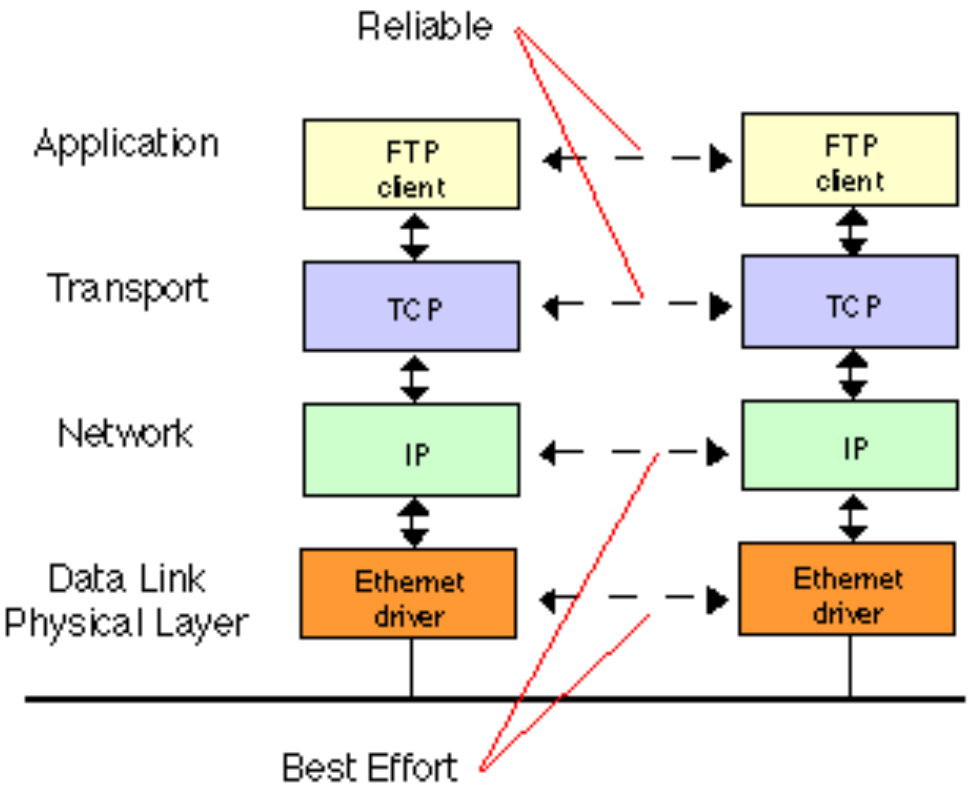
Operating System Security

Basic Control Hijacking	Rootkits, Isolation

Computer Networks and Protocols Security

Computer Networks		Communication Protocols	
Wireless	Wired	IP Based	Non IP Based

Relevant Network Layers



*From http://www.erg.abdn.ac.uk/users/gorry/course/images/ftp-tcp-enet.gif

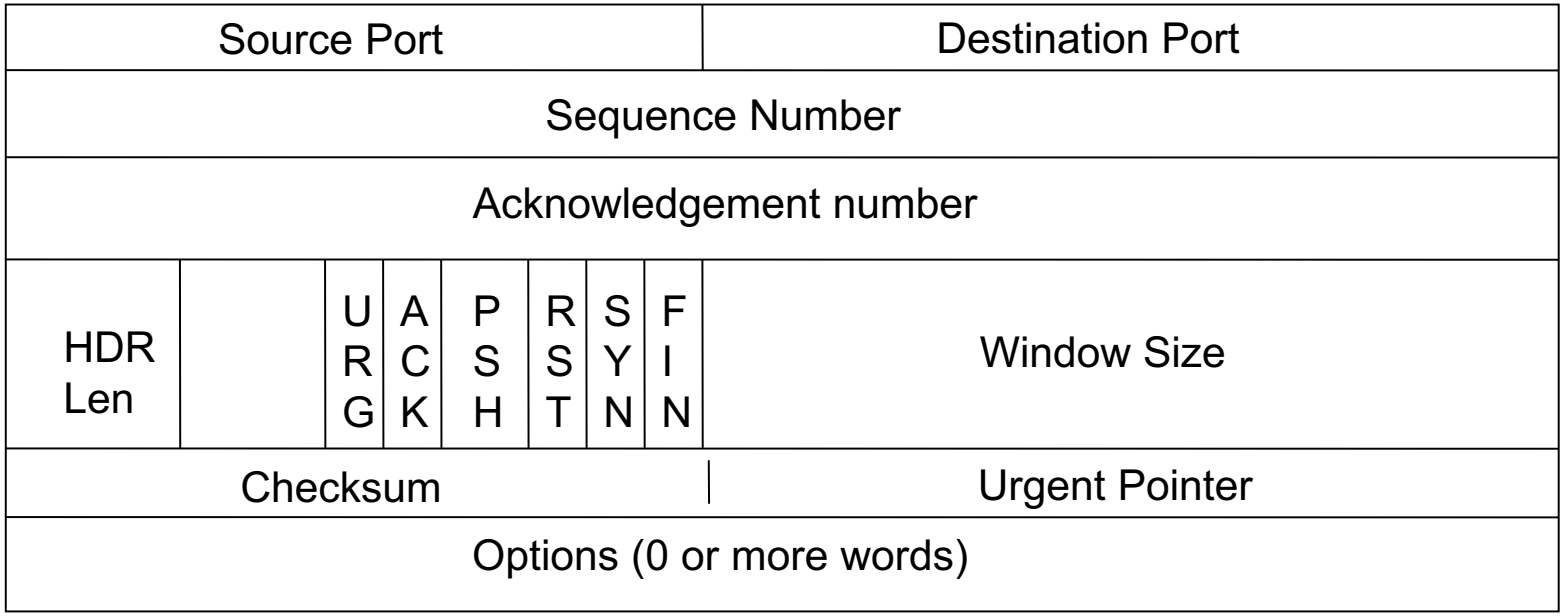
UDP Header

Source Port	Destination Port
UDP Length	UDP checksum

UDP Amplifier Attack

- Fraggle
  - Broadcast UDP packet sent to the "echo" service
  - All computers reply (amplification)
  - Source IP was spoofed, victim is overwhelmed

TCP Header

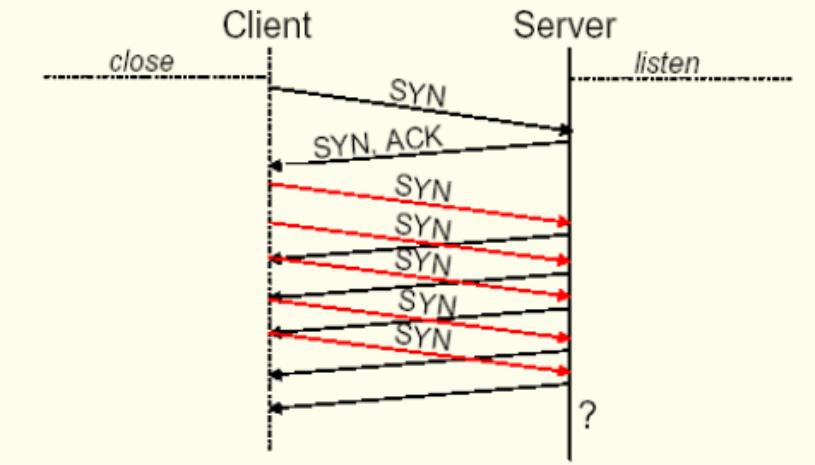

Source Port
Destination Port
Sequence Number
Acknowledgement number
HDR Len
URG
ACK
PSH
RST
SYN
FIN
Window Size
Checksum
Urgent Pointer
Options (0 or more words)

TCP Reliability

- A TCP connection is a *stream*
- Each TCP packet contains a *stream segment*
- A sequence number is associated to each byte
  - Packets have a single field for the sequence number
    - e.g., refers to the sequence number of a specific byte, according to a convention described in the RFC
- An ACK is required for each byte
  - If an ACK is not received in a certain amount of time, data is retransmitted
  - An ACK packet serves as an ACK for all bytes up to the byte indicated by the ACK's sequence number
- Receiver uses sequence numbers to correctly reorder segments and remove duplicates

SYN flood

- A resource DoS attack focused on the TCP three-way handshake
- Denial of service when an attacker sends many SYN packets to create multiple connections without ever sending an ACK to complete the connection, aka SYN flood.

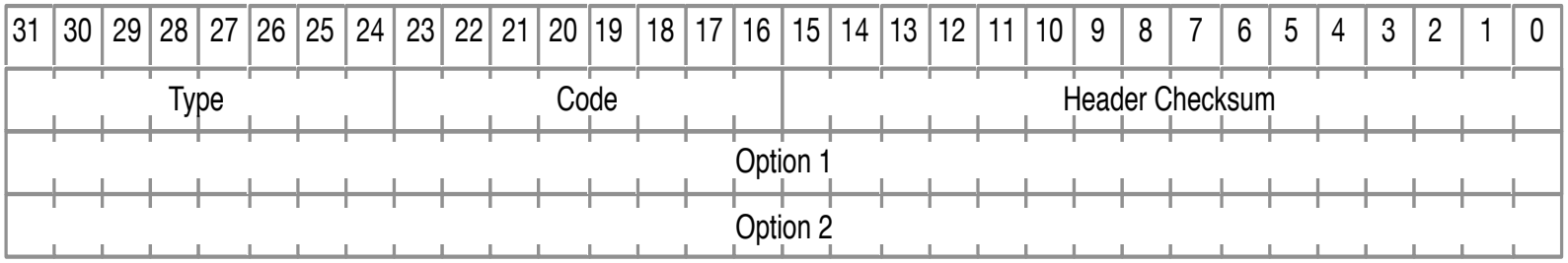


- This leaves B with a bunch of half open connections that are filling up memory
- Firewalls adapted by setting limits on the number of such half open connections.
  - Keeping track of each half-open connection takes up resources

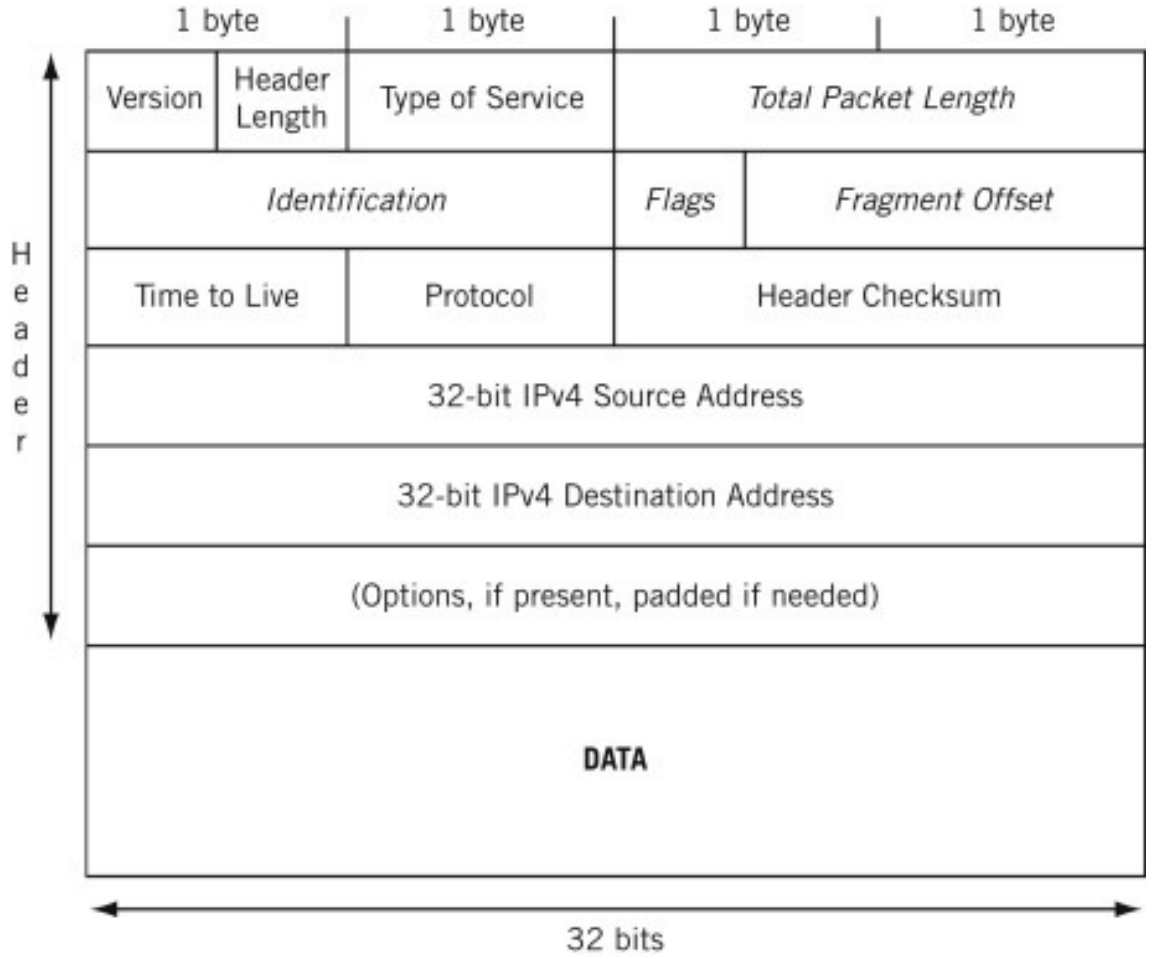
Application Protocols Security Issues: Internet Control Message Protocol (ICMP)

- RFC 792
- Used for diagnostics
  - Destination unreachable
  - Time exceeded, TTL hit 0
  - Parameter problem, bad header field
  - Source quench, throttling mechanism rarely used
  - Redirect, feedback on potential bad route
  - Echo Request and Echo reply, ping
  - Timestamp request and Timestamp reply, performance ping
- Can use information to help map out a network
  - Some people block ICMP from outside domain

ICMP Header



IP Header



PING OF DEATH

- ICMP echo with fragmented packets
  - Maximum legal size of an ICMP echo packet: 65535 - 20 - 8 = 65507
  - Fragmentation allows bypassing the maximum size:
    (offset + size) > 65535
- Reassembled packet would be larger than 65535 bytes
- OS crashes
- Really a problem with reassembly, ICMP just used for convenience
- Same attack with different IP protocols

Ping Flood

- Denial of Service attack
- Overwhelming the victim with ICMP Echo Request packets (ping)
- Attacker has more bandwidth
- How to defend?
  - Filter incoming ICMP Echo Request packets
  - filter large PING packets

Vulnerability of Routing Protocols

- Routing Protocols
  - RIP (Routing Information Protocol) – Distance Vector Protocol
  - OSPF – Open Short Path First Protocol – Link State Protocol
  - BGP – Border Gate Protocol – between Autonomous Systems
- ICMP
- Transport Layer
  - UDP
  - TCP
- Application Layer

IPv4 Routing Protocols

- Network routing requires switches and routers to be aware of the other devices in the network to know where to send packets.
- Each router shares its knowledge about the network with the other devices
- All routers have a basic understanding of the network and know how to forward packets.

Basic IPv4 Routing - Static routing.

- Used by hosts and some firewalls and routers.
  - Routing table consists of entries of
    - » Network, Next hop address, metric, interface
  - May have routing table per incoming interface
  - To route a packet, take the destination address and find the best match network in the table. In case of a tie look at the metric
    - » Use the corresponding next hop address and interface to send the packet on.
    - » The next hop address is on the same link as this device, so you use the next hop's data-link address, e.g. Ethernet MAC address
  - Decrement "time to live" field in IP header at each hop. Drop packet when it reaches 0
    - » Attempt to avoid routing loops
    - » As Internet got bigger, TTL fields got set bigger. 225 maximum

Dynamic Routing Protocols

- For scaling, discover topology and routing rather than statically constructing routing tables
  - RIP: Routing Information Protocol
  - Open Shortest Path First (OSPF): Used for routing within an administrative domain
  - Border Gateway Protocol (BGP): Used for routing between administrative domains. Can encode non-technical transit constraints, e.g. Domain X will only carry traffic of paying customers
    - Receives full paths from neighbours, so it avoids counts to infinity.

Attack Damages on Routing Protocols

- **starvation**: data traffic destined for a node is forwarded to a part of the network that cannot deliver it
- **network congestion**: more data traffic is forwarded through some portion of the network
- **blackhole**: large amounts of traffic are directed as to be forwarded through one router that cannot handle the increased level of traffic and drops many/most/all packets
- **delay**: data traffic destined for a node is forwarded along a path that is in some way inferior to the path it would otherwise take
- **looping**: data traffic is forwarded along a path that loops, so that the data is never delivered,
- **eavesdrop**: data traffic is forwarded through some router or network that would otherwise not see the traffic, giving an opportunity to see the data,

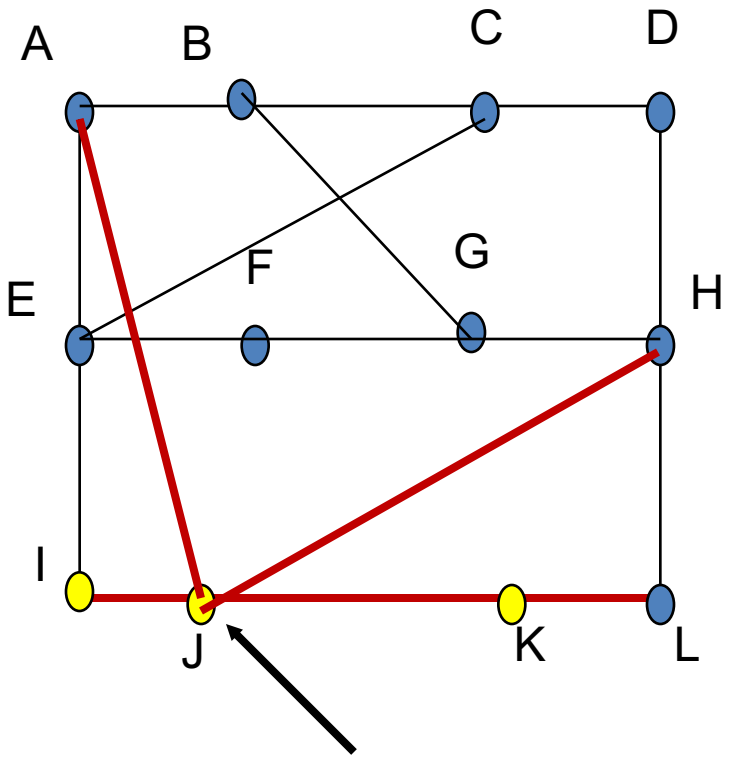
Attack Damages on Routing Protocols

- **partition**: some portion of the network believes that it is partitioned from the rest of the network when it is not,
- **cut**: some portion of the network believes that it has no route to some network that is in fact connected,
- **churn**: the forwarding in the network changes at a rapid pace, resulting in large variations in the data delivery patterns (and adversely affecting congestion control techniques),
- **instability**: routing protocol becomes unstable so that convergence on a global forwarding state is not achieved,
- **overload**: the routing protocol messages themselves become a significant portion of the traffic the network carries.
- **resource exhaustion**: the routing protocol messages themselves cause exhaustion of critical router resources, such as table space and queues.

RIP v1/v2

- Routing decisions are based on number of hops
- Works only within the AS
- Supports only 15 hops
- RIPv1 communicates only it's own information
  - RIPv2 can communicate other routers' information
- RIPv1 has no authentication
  - RIPv2 support up to 16 char password, but clear txt

Distance Vector Routing

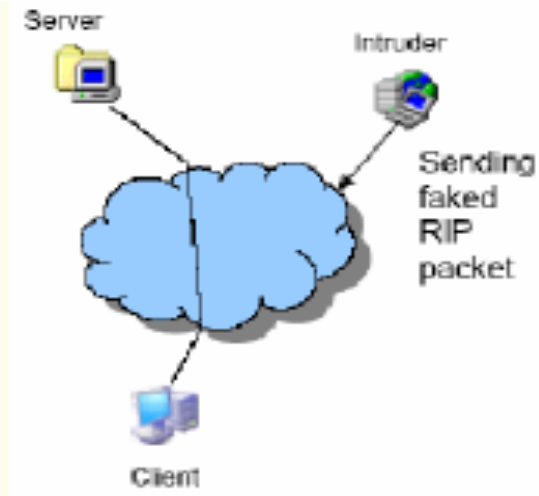


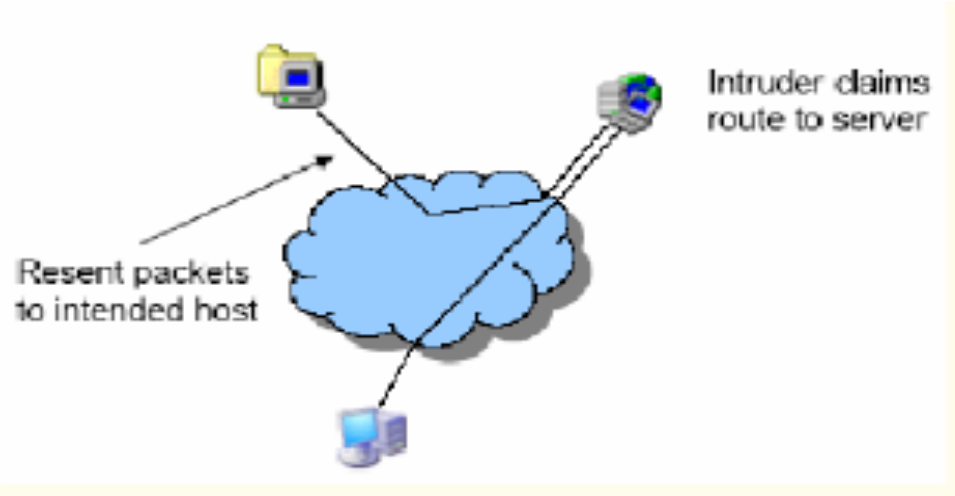
Router uses Echo packets
to estimate delays to neighbors

	DV A	DV I	DV H	DV K		
A	0	24	20	21	8	A
B	**12**	**36**	**31**	**28**	**20**	**A**
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	**18**	**31**	**6**	**31**	**18**	**H**
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	-
K	24	22	22	0	6	K
L	29	33	9	9	15	k
	JA	JI	JH	JK	new rout	
	8	10	12	6		

RIP Attack

- By sending wrong routing information the connection can be diverted to the intruder
- Identify RIP Router by performing a Scan
  - » nmap –v –sU –p 520
- Case: ***On April 27, 1997, a router from MAI Network services in Virginia absorbed*** about 50,000 network addresses which caused much of the internet to be disconnected from 20 minutes to 3 hours





OSPF

- OSPF stands for Open Shortest Path First
  - TCP/IP Internet routing protocol
  - Classified as an Interior Gateway Protocol (IGP) - distributes routing information between routers belonging to a single AS - intra-AS routing protocol
  - It is an authenticated link state protocol running directly on top of IP
  - Every node calculates the paths independently

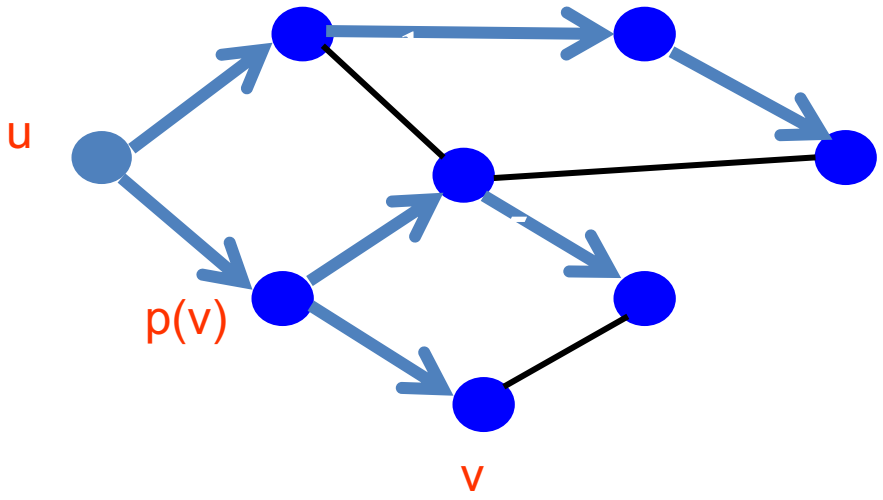
Link State Protocol

- Each router is responsible for meeting neighbours and learning their names
- Distance-vector routing protocol works by sharing its knowledge of the entire network with its neighbours, link-state routing works by having the routers tell every router on the network about its closest neighbours.
- Each router constructs a packet called a Link State Advertisement (LSA)
- LSAs are reliably "flooded" to all routers; everyone gets the same consistent information
  - The entire routing table is not distributed from any router, only the part of the table containing its neighbours.
- Each router computes the best routes on its own

  -- no need to trust your neighbour's calculations.

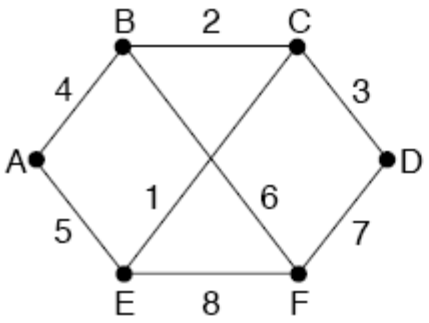
Shortest-Path Problem

- Given: network topology with link costs
  - **c(x,y)**: link cost from node x to node y
  - Infinity if x and y are not direct neighbors
- Compute: least-cost paths to all nodes
  - From a given source u to all other nodes
  - **p(v)**: predecessor node along path from source to v



Link-State Packets

- Packets to be distributed



Link State Packets

A	
Seq.	
Age	
B	4
E	5

B	
Seq.	
Age	
A	4
C	2
F	6

C	
Seq.	
Age	
B	2
D	3
E	1

D	
Seq.	
Age	
C	3
F	7

E	
Seq.	
Age	
A	5
C	1
F	8

F	
Seq.	
Age	
B	6
D	7
E	8

- Sequence number prevents nodes from using old messages
- Age determines a time to live for the packet (why do we need this?)

Areas

- A set of networks are grouped together into area (generalization of an IP subnetted network).
  - Each area runs a separate copy of link-state routing algorithm
  - Has its own link-state database
  - Area’ s topology unknown to outside and vice versa
  - Separated in order to reduce a routing traffic

Classification of Routers

- Internal Routers - routers with all directly connected networks belonging to the same area
- Area Border Routers - routers that are attaches to multiple areas
- AS Boundary routers - routers that exchange routing information with routers belonging to other AS

OSPF Packets

- **Hello Packet** - sent out on each functioning router interface. Used to discover and maintain neighbour relationships
- **Database Description Packet** - exchanged when an adjacency is being initialized. Describe the contents of the topological database

OSPF Packets (cont’d)

- Link State Packets
  - **The Link State Request packet** - after exchanging Database Description packets, may find that parts of its topological database are out of date. Request the pieces of the neighbour's database that are more up to date
  - **The Link State Update packet** - implement the flooding of link state advertisements
  - **Link State Acknowledgement Packets** - to make the flooding of link state advertisements reliable

Authentication

- All OSPF protocol exchanges are authenticated.
  - configurable on a per-interface basis.
- Authentication types 0, 1 and 2 are defined as follows:

AuType	**Description**
0	Null authentication
1	Simple password
2	Cryptographic authentication

OSPF Operation

- Determine neighbouring routers by transmitting “hello” packets
- When a router receives “hello” packet – “relationship” is established and information is exchanged
- When it is determined that more than 1 router is present within an area, DR and BDR are selected
- All other routers establish relationship with DR and BDR to exchange db information (OSPF request and response messages are used)
- Routers run shortest path algorithm
- Once network up and running, the routers periodically send “hello” packets to verify that all links are active

Attacks on OSPF

- **Eavesdropping**: The routing data carried in OSPF is carried in clear-text, so eavesdropping is a possible attack against routing data confidentiality.
- **Message Replay**: In general, OSPF with Cryptographic Authentication provides a sufficient mechanism for replay protection of its messages. Nonetheless, there are still some scenarios in which an outsider attacker can successfully replay OSPF messages;
- **Message Insertion**: OSPF with Cryptographic Authentication enabled is not vulnerable to message insertion from outsiders. In the case of an insider or in the absence of Cryptographic Authentication, message insertion becomes a trivial operation even for a remote attacker.

Attacks on OSPF (Cont'd)

- **Message Deletion**: OSPF provides a certain degree of protection against message deletion. The receiver itself cannot detect if a message has been deleted or not, but the sender will detect a deleted Link State Update (LSU) message since it will not receive any OSPF Link State Acknowledgment message for it. There is no acknowledging mechanism for Hello messages, but the deletion of some, generally four or more, consecutive Hello messages belonging to the same router will cause "adjacency breaking" and thus be easily detected by all the parties involved.
- **Message Modification**: OSPF with Cryptographic Authentication provides protection against modification of messages. In the case of an insider or in the absence of Cryptographic Authentication message modification becomes possible.

Attacks on OSPF (Cont'd)

- **Man-In-The-Middle**: OSPF with Cryptographic Authentication provides protection against man-in-the-middle attacks. In the case of an insider or in the absence of Cryptographic Authentication, the protocol becomes exposed to man-in-the-middle attacks through the lower network layers - such as ARP spoofing - on all OSPF peers that are one hop apart; while OSPF peers connected over virtual links are exposed to Layer 3 man-in-the-middle attacks too.
- **Denial-of-Service**: While bogus routing information data can represent a Denial of Service attack on the end systems that are trying to transmit data through the network and on the network infrastructure itself, certain bogus information can represent a more specific Denial of Service on the OSPF routing protocol itself. For example, it is possible to reach the limits of the Link State Database of a victim with External LSAs or with bogus LSA headers during the Link State Database Exchange phase.

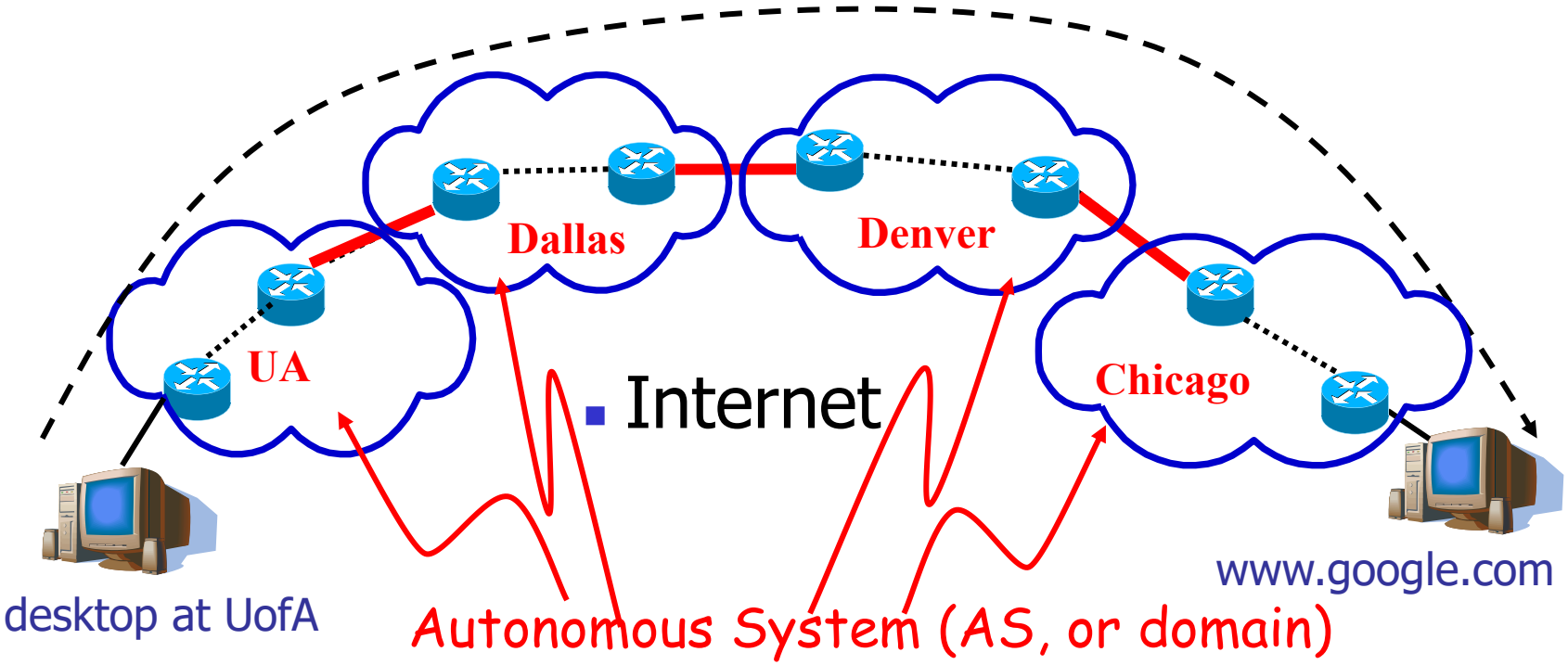
Attack Scenario 1

- **Max Age attack**
  - Attacker sends LSA packets with maxage set.
  - LSA flushed from all the routers reached by the flooding mechanism.
  - The original router that sent this LSA (owner) then contests the sudden change in age by generating a refresh message (age=0, higher sequence number) in a process called "fight-back".
  - Attacker continually interjects packets with the maxage value for a given routing entity which causes network confusion and may contribute to a DOS condition.

Attack Scenario 2

- **Sequence++ attack**
  - Attacker continually injects a larger LSA sequence number, which indicates to the network that it has a fresher route.
  - The original router contests this in the "fight back" process by sending it’ s own LSA with an even newer sequence number than the attackers sequence number.
  - Unstable network is created and could contribute to a DOS condition.

Inter-domain Routing Protocol: BGP



- Hierarchical Internet Routing:
  - Intra-domain: OSPF, IS-IS, EIGRP, and RIP
  - Inter-domain: BGP (Border Gateway Protocol)

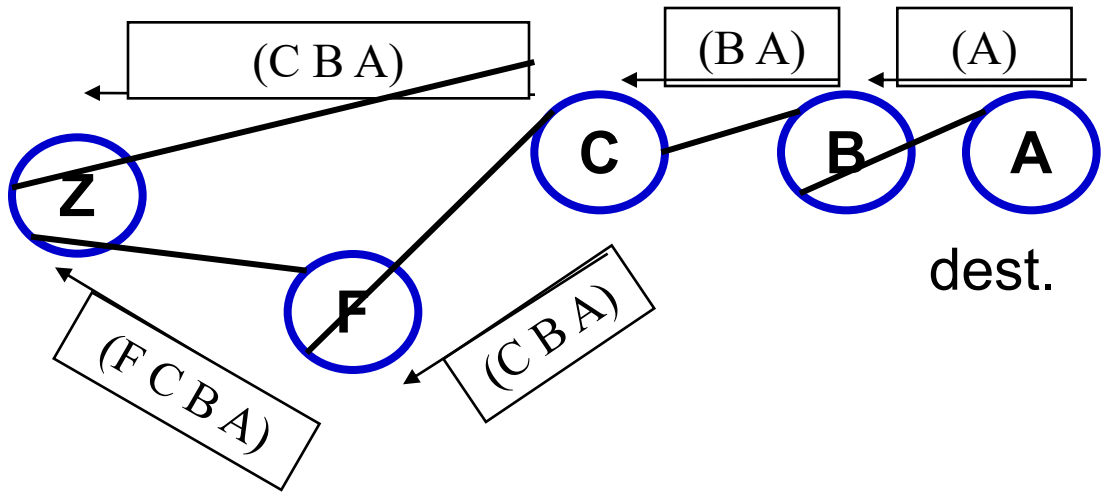
A Simplified Model of BGP

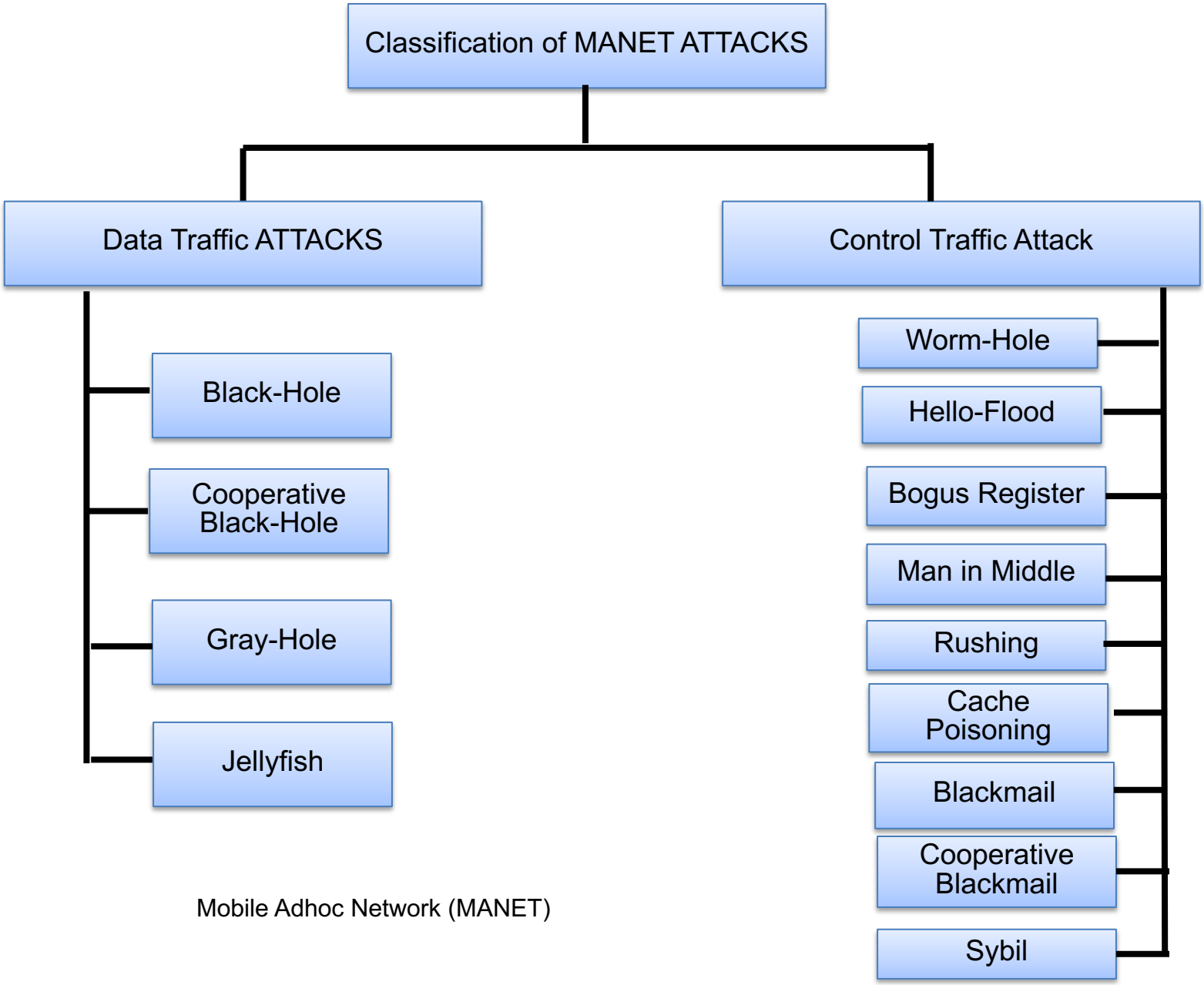
- Autonomous System: node
- Nodes exchange entire path information
- Messages are "triggered" by topology changes.

Z's route to A:

Route via C = (C B A)

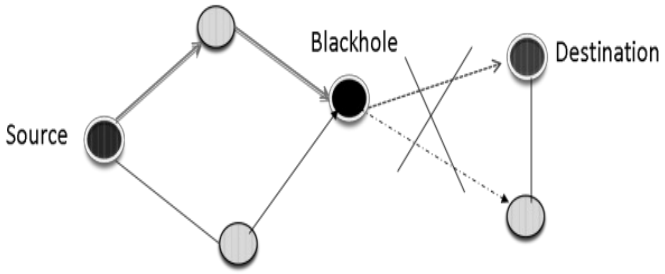
Route via F = (F C B A)




Classification of MANET ATTACKS
Data Traffic ATTACKS
Control Traffic Attack
Black-Hole
Cooperative Black-Hole
Gray-Hole
Jellyfish
Worm-Hole
Hello-Flood
Bogus Register
Man in Middle
Rushing
Cache Poisoning
Blackmail
Cooperative Blackmail
Sybil

Data Traffic Attacks: Black Hole Attack

In this attack, a malicious node acts like a Black hole, dropping all data packets passing through it



Few strategies to mitigate the problem:

(i) Collecting multiple RREP messages (from more than two nodes) and thus hoping multiple redundant paths to the destination node and then buffering the packets until a safe route is found.

(i) Maintaining a table in each node with previous sequence number in increasing order. Each node before forwarding packets increases the sequence number. The sender node broadcasts RREQ to its neighbors and once this RREQ reaches the destination, it replies with a RREP with last packet sequence number. If the intermediate node finds that RREP contains a wrong sequence number, it understands that somewhere something went wrong.

Data Traffic Attack- Gray Hole Attack

Gray-Hole attack has its own characteristic behavior. It too drops DATA packets, but node's malicious activity is limited to certain conditions or trigger. Two most common type of behavior:

(i) Node dependent attack – drops DATA packets destined towards a certain victim node or coming from certain node (fig 3), while for other nodes it behaves normally by routing DATA packets to the destination nodes correctly.

(i) Time dependent attack – drops DATA packets based on some predetermined/trigger time while behaving normally during the other instances. (fig. 4)

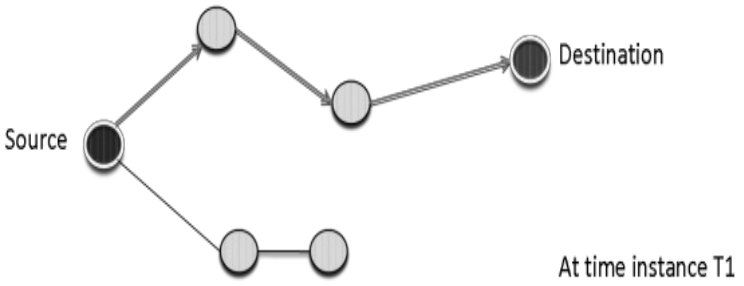


Figure 3: Gray-Hole – Node dependent attack

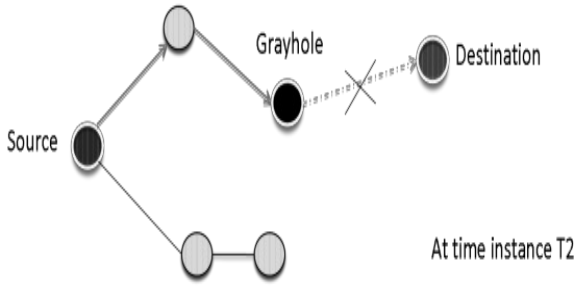
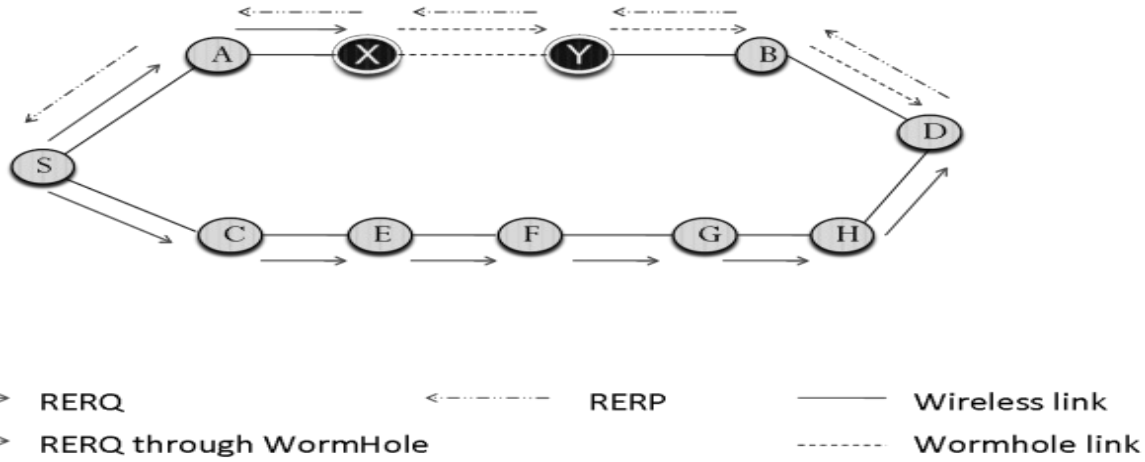


Figure 4: Gray-Hole – Time dependent attack

Control Traffic Attack- Wormhole

One or more attacking node can disrupt routing by short- circuiting the network, thereby disrupting usual flow of packets



There have been few proposals recently to protect networks from worm-hole attack:

(i) Geographical leashes & temporal leashes: A leash is added to each packet in order to restrict the distance the packets are allowed to travel. A leash is associated with each hop. Thus, each transmission of a packet requires a new leash.

(ii) Using directional antenna: Using directional antenna restricts the direction of signal propagation through air. This is one of the crude ways of limiting packet dispersion.

Control Traffic Attack- Bogus Registration

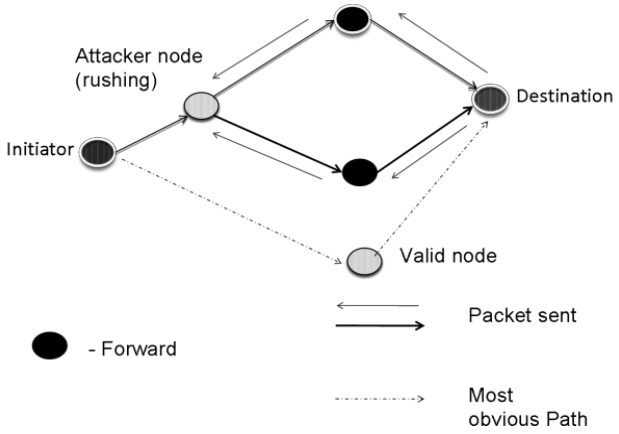
- It is an active attack in which an attacker disguises itself as another node either by sending stolen beacon or generating such false beacons to register himself with a node as a neighbor.
- Once registered, it can snoop transmitted packets or may disrupt the network altogether.
- Encrypting packets before sending and secure authentication in route discovery (SRDP, SND, SNRP, ARAN, etc) will limit the severity of attack to some extent as attacker node has no previous knowledge of encryption method.

Control Traffic Attack- HELLO Flood

- The attacker node floods the network with a high quality route with a powerful transmitter. So, every node can forward their packets towards this node hoping it to be a better route to destination.
- Some can forward packets for those destinations which are out of the reach of the attacker node.
- A single high power transmitter can convince that all the nodes are his neighbor.
- The attacker node need not generate a legitimate traffic; it can just perform a selective replay attack as its power overwhelms other transceivers

Control Traffic Attack- Rushing

- In AODV or related protocol, each node before transmitting its data, first establishes a valid route to destination.
- Sender node broadcasts a RREQ (route request) message in neighborhood and valid routes replies with RREP (route reply) with proper route information.
- Some of the protocols use duplicate suppression mechanism to limit the route request and reply chatter in the network.
- Rushing attack exploits this duplicate suppression mechanism. It quickly forwards with a malicious RREP on behalf of some other node.
- Due to duplicate suppression, actual valid RREP message from valid node will be discarded and the attacking node becomes part of the route.
- In rushing attack, attacker node does send packets to proper node after its own filtering is done, so from outside the network behaves normally as if nothing happened. But it might increase the delay in packet delivering to destination node



Control Traffic Attack- Cache Poisoning

- Each node keeps few of its most recent transmission routes until timeout occurs for each entry.
- If some malicious node performs a routing attack then they will stay in node's route table until timeout occurs or a better route is found.
- An attacker node can advertise a zero metric to all of its destinations. Such route will not be overwritten unless timeout occurs.
- Once it becomes a part of the route, the attacker node can perform its malicious activity.
- Effect of Cache poisoning can be limited by either adding boundary leashes or by token authentication. Also each node can maintain its friend-foe list based on historical statistics of neighboring nodes performance.

- Few of the mitigation methods proposed:

- (i) SAODV [29]: Secure AODV is an extension to AODV protocol that adds each node to exchange signed routing messages. Each node has its own public key which it uses to sign routing messages.
- (ii) ARAN [16][18][28] : Authenticated Routing protocol for Ad-hoc Networks uses similar techniques as SAODV. ARAN uses certificates issued by a third party certification authority.
- (iii) SNRP [16]: Secure Neighbor Routing protocol uses security enhanced Neighbor Lookup Protocol (NLP) to secure MANET routing. Newly added node uses public key to participate in MANET.