Mobile Ad-hoc and Wireless Sensor Networks

Lesson 06

Mobile Ad-hoc Network (MANET) Security

Confidentiality

- Only destined user must be able to read data
- Encryption of the data before transmission and deciphering it at the user end for ensuring confidentiality

Integrity

- Data integrity needs to be maintained or else the user receives a manipulated message
- System integrity needs to be maintained or else system can issue the message to wrong node

Pre-keying

- In order to decipher the encrypted messages, a key for deciphering is first exchanged between transmitter and receiver
- If a private key is used, key exchanges over wireless systems increase the risk of key trapping

Increased threat of eaves-dropping

- The probability that a MANET or sensor node transmits unsolicited messages while moving in the wireless region of two nodes is increased in ad-hoc networks
- Each node attempts to identify itself with a new node moving in its vicinity and during that process eavesdropping occurs

Unknown node caching the information

- An unknown node can move into the network and thus rigorous authentication is required before the node is accepted as a part of MANET

Authenticated node becoming hostile

- A previously authenticated device can be used for security attacks.

Availability

- Denial of service attack
- A source blocking the availability of data at the user end
- For example, the packets sent can be prevented from reaching the destination by some intermediate router misdirecting them due to the attack

Resource constraint

- Continuously irrelevant messages—exhaustion of device-memory due to caching and hoarding irrelevant data from the attacker
- Such an attack if occurs in between routers in the network, it seriously affects the whole network

Detection Power loss

- A mobile device may not detect the signals and therefore get data or message due to attack by jamming signals
- A solution is Frequency hopping of the modulation signal which has high background noise

Reconfiguration

- An attack can be on network configuration (e.g., manipulation of routing table)
- Network reconfiguration at different periods prevents such attacks

Spoofing (Impersonating address)

- A node can impersonate an address in a mobile ad hoc network
- A common node to several paths can lead to choking of all routes

Other Security problems

- Mobility risks– Changed location results in signals routing through paths, which cannot be relied upon

Solutions for the security problems in mobile and wireless computing systems

- The hash of a message— a set of bits obtained after applying the hash algorithm (or function)
- This set of bits is altered in case the data is modified during transmission
- It checks data integrity

Solutions for the security problems in mobile and wireless computing systems

- MAC (Message authentication code)– a combination of hash and secret key
- Encryption Public key and private key encryptions—DES, AES, and RSA cryptographic algorithms

SOLUTIONS FOR THE SECURITY PROBLEMS IN MOBILE AND WIRELESS COMPUTING SYSTEMS

- SHA and MD5
- Data encryption algorithms—DES and triple DES, and other encryptions
- Checksum and parity— are the primitive methods to check message integrity

Summary

- Continuously irrelevant messages—exhaustion of device-memory due to caching and hoarding irrelevant data from the attacker Hash
- A node impersonation or turning hostile
- A common node to several paths can lead to choking of all routes
- MAC, MD5, RSA and DES encryption

End of Lesson 06

Mobile Ad-hoc Network (MANET) Routing Security