

Mobile Computing non è SmartPhone: Sicurezza nei Sistemi Mobili

MANET

1

Contesto

- Sistemi di calcolo mobile sono tutti quei sistemi in cui qualche componente hw/sw è in grado di muoversi in uno specifico spazio
- È una definizione molto ampia che comprende sistemi molto eterogenei
- Ci concentreremo solo sui sistemi MANET

MANET

2

Definizione

- MANET (Mobile Ad-hoc NETwork) indica una tipologia di reti wireless che possono operare **senza la necessità di una infrastruttura fisica fissa**
- Permettono la comunicazione wireless tra host mobili

MANET

3

Host Mobili (1)

- In una MANET
 - le comunicazioni tra una sorgente e una destinazione sono **stabilite** e **mantenute** dalla **cooperazione** tra i vari host presenti nella rete
 - ogni host può agire
 - sia come **end-point** di una comunicazione (mittente/destinatario di msg)
 - che come **router** di pacchetti

MANET

4

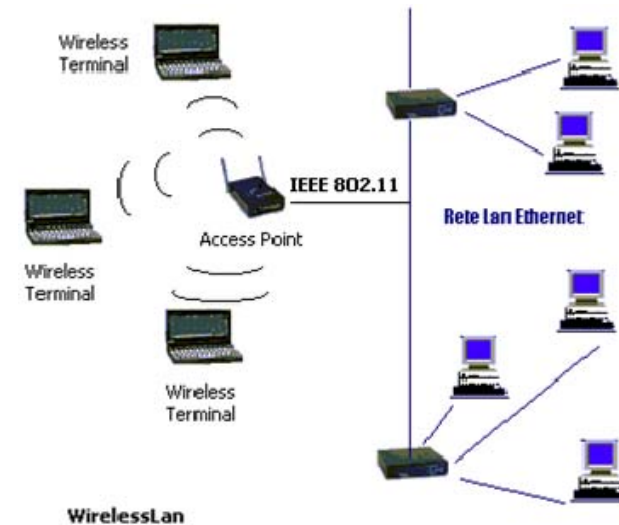
Host Mobili (2)

- Ogni host può muoversi a diverse **velocità**, in ogni **direzione** nello spazio della MANET
 - Durante la “vita” di ogni host in una MANET sia direzione che velocità cambiano continuamente
- Ogni host può comunicare direttamente solo con altri che sono all'interno di un predefinito **radio range**
 - Radio range è specifico per ogni host

MANET

5

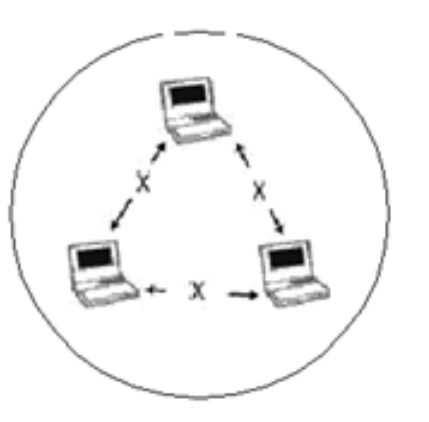
Reti Wireless con Infrastruttura



MANET

6

Reti Wireless senza Infrastruttura



MANET

7

Dinamicità in una MANET

- Le MANET sono sistemi altamente dinamici, a causa
 - del duplice ruolo ricoperto da ogni host
 - del continuo cambiamento nella topologia della rete,
- Due aspetti della dinamica:
 - dinamica della rete: cambiamento della posizione degli host
 - dinamica del comportamento computazionale di ogni host

MANET

8

Applicazioni

- Le MANET sono applicate per permettere la comunicazione quando non sono disponibili infrastrutture fisiche fisse
- Ad esempio
 - squadre di soccorso nel caso di disastri
 - navi durante traversate oceaniche
 - sistemi spaziali
 - reti di sensori per il monitoraggio (fauna selvatica, frane, robot, ...)
 - ...

MANET

9

Problemi

MANET

10

Problemi Tradizionali

- Le MANET richiedono di affrontare vari problemi **tradizionali**:
 - Il sw per l'uso e la gestione è molto complesso, spesso costituito da migliaia di moduli: sono tutti davvero necessari?
 - Esistono condizioni per eseguire tutte le componenti logiche di ogni algoritmo?
 - Esistono condizioni di deadlock/livelock?
 - Quali e quante risorse sono necessarie?
 - Cosa succede in caso di guasto?
 - Il sistema è completo? Quanto è complesso?

MANET ...

11

Problemi Specifici

- Le caratteristiche della MANET pongono vari problemi **specifici**:
 - Definizione e analisi delle prestazioni di protocolli di routing
 - Sincronizzazione, cooperazione e concorrenza tra le diverse componenti del sistema MANET
 - Quante comunicazioni possono essere contemporaneamente servite da un host inteso come router? Quante da un host inteso come end-point?

MANET
— ...

12

Soluzioni in Letteratura

- Tanti lavori in letteratura affrontano questi problemi
 - usando strumenti concettuali e computazionali derivati da altre discipline o specifici per questo caso
- Nella maggior parte dei casi lo studio fa uso di simulatori per valutare le prestazioni offerte dalla MANET

Simulatori

- Esistono diversi strumenti per simulare MANET
 - ns-2 MONARCH, OLSR, ...
- La maggior parte dei quali:
 - È basata su una logica **event-driven**
 - La sincronizzazione è imposta artificialmente da un **clock esterno**
 - Non permette di descrivere **formalmente** il sistema

Altre Soluzioni (1)

- L'approccio seguito da altri consiste nell'analisi della formalizzazione delle MANET allo scopo di indagarne il comportamento

Altre Soluzioni (2)

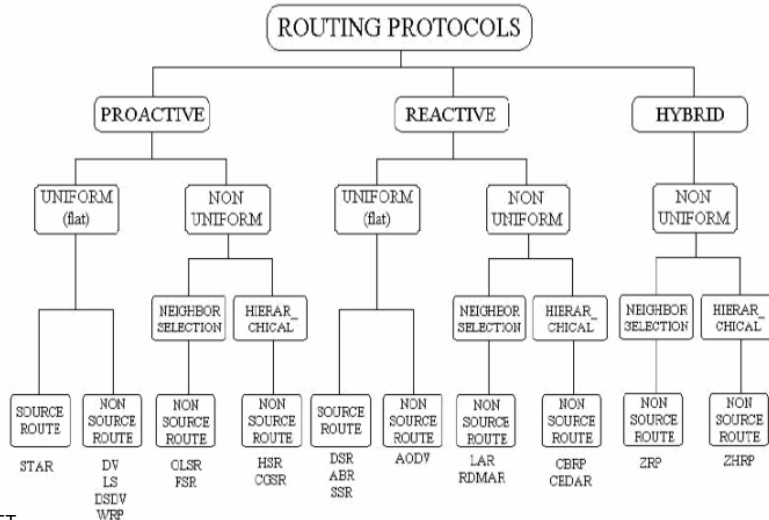
- Il gruppo di ricerca di Metodi Formali per Sistemi Distribuiti del dib affronta i problemi con un approccio ibrido
- Ha realizzato un ambiente che permette sia la **simulazione** che la **modellazione formale** delle MANET
 - in cui la sincronizzazione è stabilita dal comportamento degli host interni al sistema MANET
 - I modelli usati sono le PN (DEMONE) e le ASM (MOTION)

Protocolli di Routing per MANET

Premessa

- Esistono parecchi protocolli di routing specifici per MANET
- La principale caratteristica è la cooperazione dei vari nodi nell'instradamento di pacchetti verso la destinazione voluta
- Caratteristiche richieste ai protocolli:
 - Minimizzazione del numero di pacchetti inviati
 - Semplificazione delle attività computazionali
 - Conoscenza il più possibile aggiornata della topologia corrente della rete
- MANET Capacità di evitare cicli nell'invio dei pacchetti⁸

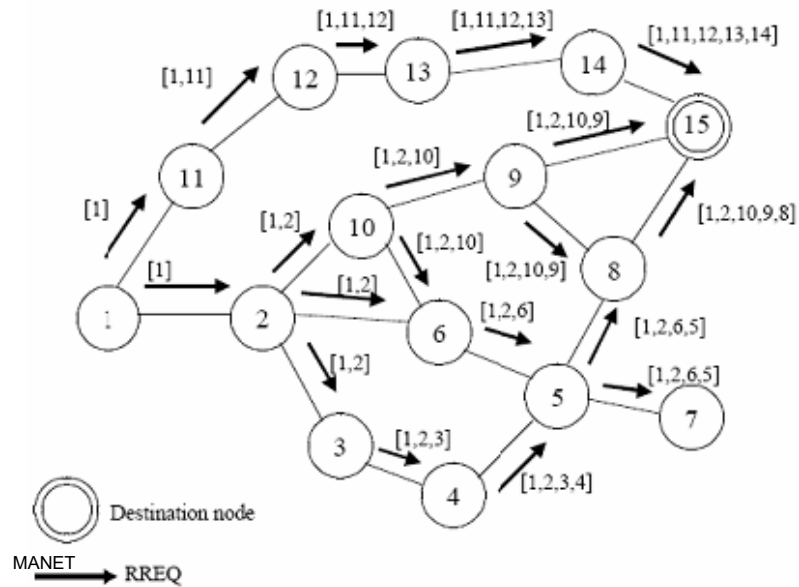
Tassonomia dei Protocolli di Routing



Dynamic Source Routing

- **Initiator** wants communicate with **Destination**
- If (Dest is a neighbour of Init) OR (a route to Dest is in Init's cache)
 - Communication can start
 - End Protocol
- Init broadcasts **RREQ** pck to neighbours
- Algorithm reiterated until route is found
 - **RREP** pck is sent back to Init

Route Discovery in DSR



21

Formato del Pacchetto RREQ

- Init address
- Dest address
- Request ID: integer number generated by Init – uniquely identifies RREQ
- Route record: list of visited hosts

MANET

22

Ad-hoc On-demand Distance Vector

- If a route to Dest is **not** in Init's cache AND Dest is **not** a neighbour of Init
 - RREQ pck is broadcasted to neighbours
 - If a node receiving RREQ is **not** Dest, neither knows a route to Dest, it
 - updates its info about route to Init
 - updates RREQ with its ID
 - broadcasts the updated RREQ
 - Else it
 - unicasts a RREP pck back to Init

MANET

23

Routing Table

- Ogni nodo possiede una propria routing table in cui ogni riga è associata a un nodo Dest conosciuto
- Per ogni riga sono registrate:
 - Dest IP address
 - Dest Sequence Number: stabilisce **quando** sono state ricevute le info su Dest
 - HopCount: distanza di Dest
 - NextHop: nodo successivo per raggiungere Dest

MANET

24

Formato del Pacchetto RREQ

- Contiene:
 - BroadcastID: numero intero associato ad ogni nodo
 - HopCount: inizialmente vale 0 ed è incrementato a ogni hop
 - DestIPAddress / InitIPAddress
 - DestSequenceNumber / InitSequenceNumber: I seq nums più aggiornati

Sicurezza nelle MANET

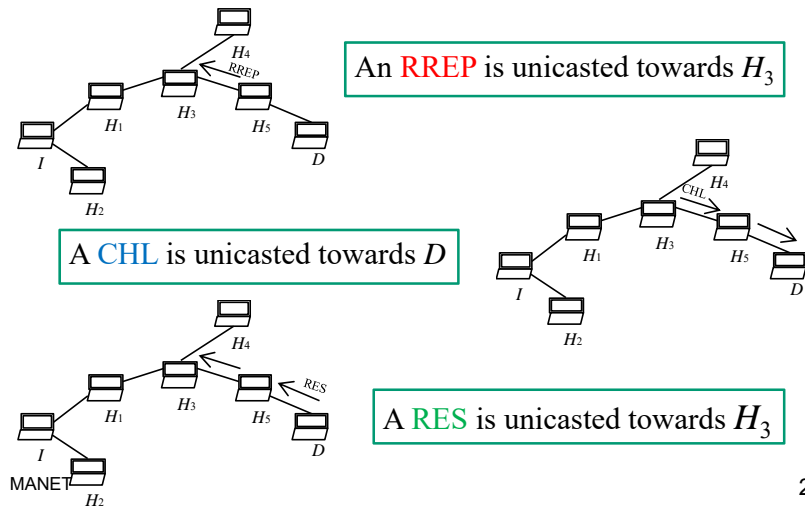
MANET = Open System

- Data la mobilità degli host e l'assenza di host di controllo è molto difficile implementare politiche di sicurezza
- MANET è molto sensibile a molti tipi di attacchi
- Ci concentreremo sull'esempio del BlackHole Attack

Concetto generale

- Nella sua versione più semplice, un attacco blackhole consiste dei seguenti passi:
 - Il **nodo malevolo** genera un **RREP fasullo**
 - Di solito, l'RREP fasullo ha grande numero di sequenza
 - L'iniziatore sceglie la route passate per il nodo malevolo per instradare pacchetti dati
 - Il nodo malevolo li **scarta** tutti
- Nella sua versione cooperativa, il nodo malevolo è supportato da **complici**

Blackhole-free AODV (B-AODV)



Meccanismi aggiuntivi

- Il protocollo fa uso di **chiavi pubbliche** per cifrare i pacchetti CHL e RES
- Fa inoltre uso di **tabelle di fiducia** e **livelli di fiducia** per stabilire la reputazione di ciascun nodo

MANET

30

Definizione formale di blackhole

- Una definizione formale e univoca di blackhole (e complice) **manca** in letteratura
- La nostra definizione:

Definition (forward neighbor). A *forward neighbor* f_n of a node n is the next hop of n in the route to reach destination d , i.e. n, f_n, \dots, d

Definition (blackhole). A *blackhole* is: (i) a main blackhole if it originates fake RREPs; or (ii) a colluder if its forward neighbor is a blackhole

MANET

31