Security Issues in Mobile Ad hoc Networks

Sudipto Das

BCSE – IV, Roll – 02892

Department of Computer Science & Engineering,

Jadavpur University,

Kolkata – 32

Seminar, April 3, 2006

Presentation Outline

- ***Mobile Ad hoc Networks - Overview***
- Challenges in Securing MANETs
- Ongoing Research in Securing MANETs
- Conclusion

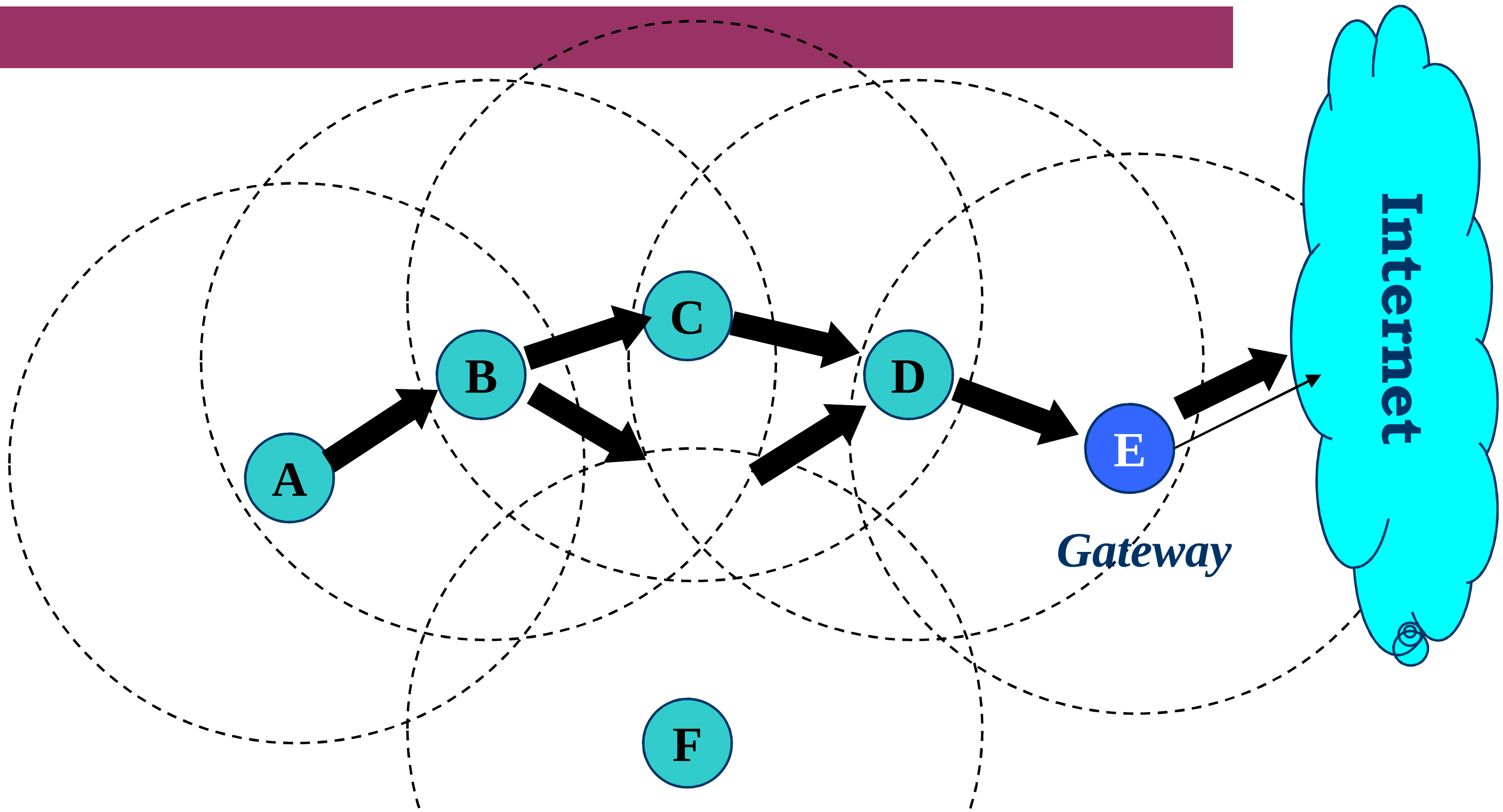
Mobile Ad hoc Networks (MANETs)
- Overview

- *MANET is a self-configuring network of mobile nodes connected by wireless links—the union of which form an arbitrary topology*
- *Individual nodes act as routers*

  - cooperate to forward both its own traffic as well as its neighbors traffic
- ***Minimal configuration** and **quick deployment** make ad hoc networks suitable for emergency situations like natural or human-induced disasters, military conflicts, emergency medical situations etc*
- *Such a network may operate in a standalone fashion, or may be connected to the larger Internet*

  - All these features have helped MANETs gain popularity in the last decade

MANETs: Operation



Stand-alone MANET

After one of the nodes is configured as a gateway, the entire network is connected to an external network like Internet

Presentation Outline

- Mobile Ad hoc Networks - Overview
- ***Challenges in Securing MANETs***
- Ongoing Research in Securing MANETs
- Conclusion

Challenges in Securing MANETs

- *The salient features of ad hoc networks pose both challenges and opportunities in achieving these security goals*

  - use of wireless links renders a MANET susceptible to link attacks ranging from ***passive eavesdropping*** *to* ***active impersonation***, ***message replay***, *and* ***message distortion***

  - to achieve high survivability, ad hoc networks should have a distributed architecture with no central entities

  - due to dynamic nature of MANETs, an a priori trust relationship between the nodes cannot be derived. It is desirable for the security mechanisms to adapt on-the-fly to these changes

  - a MANET may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network.

Challenges in Securing MANETs

- *Security in MANET is an essential component for basic network functions like packet forwarding and routing*

  - network operation can be easily jeopardized if countermeasures are not embedded into their design

- *To secure an ad hoc network, the following attributes may be considered:*

  - ***Availability***
  - ***Confidentiality***
  - ***Integrity***
  - ***Authentication***
  - ***Non-repudiation***

Challenges in Securing MANETs

- *Security exposures of ad hoc routing protocols are due to two different types of attacks:*

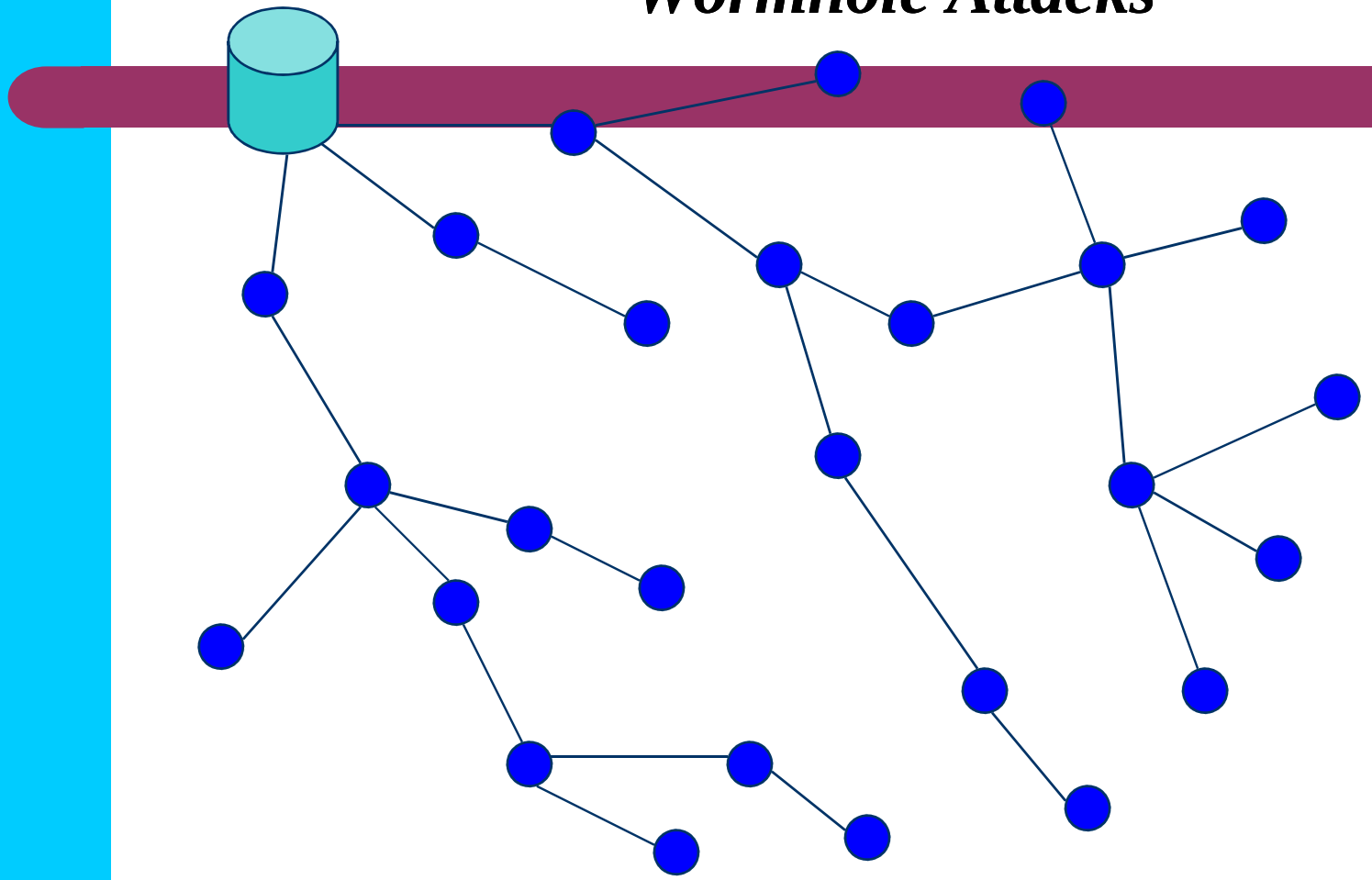
  *- **Active attacks** through which the misbehaving node has to bear some energy costs in order to perform some harmful operation, and*

  *- **Passive attacks** that mainly consist of lack of cooperation with the purpose of energy saving.*
- *Nodes that perform **active attacks** with the aim of damaging other nodes by causing network outage are considered to be **malicious**.*
- *Nodes that perform passive attacks with the aim of saving battery life for their own communications are considered to be **selfish***
- ***Selfish** nodes can severely degrade network performances and eventually partition the network*

Challenges in Securing MANETs
- Wormhole Attacks

- *In a wormhole attack a malicious node can record packets (or bits) at one location in the network and tunnel them to another location through a private network shared with a colluding malicious node.*
- *Most existing ad hoc routing protocols would be unable to find consistent routes to any destination*
- *When an attacker forwards only routing control messages and not data packets, communication may be severely damaged*

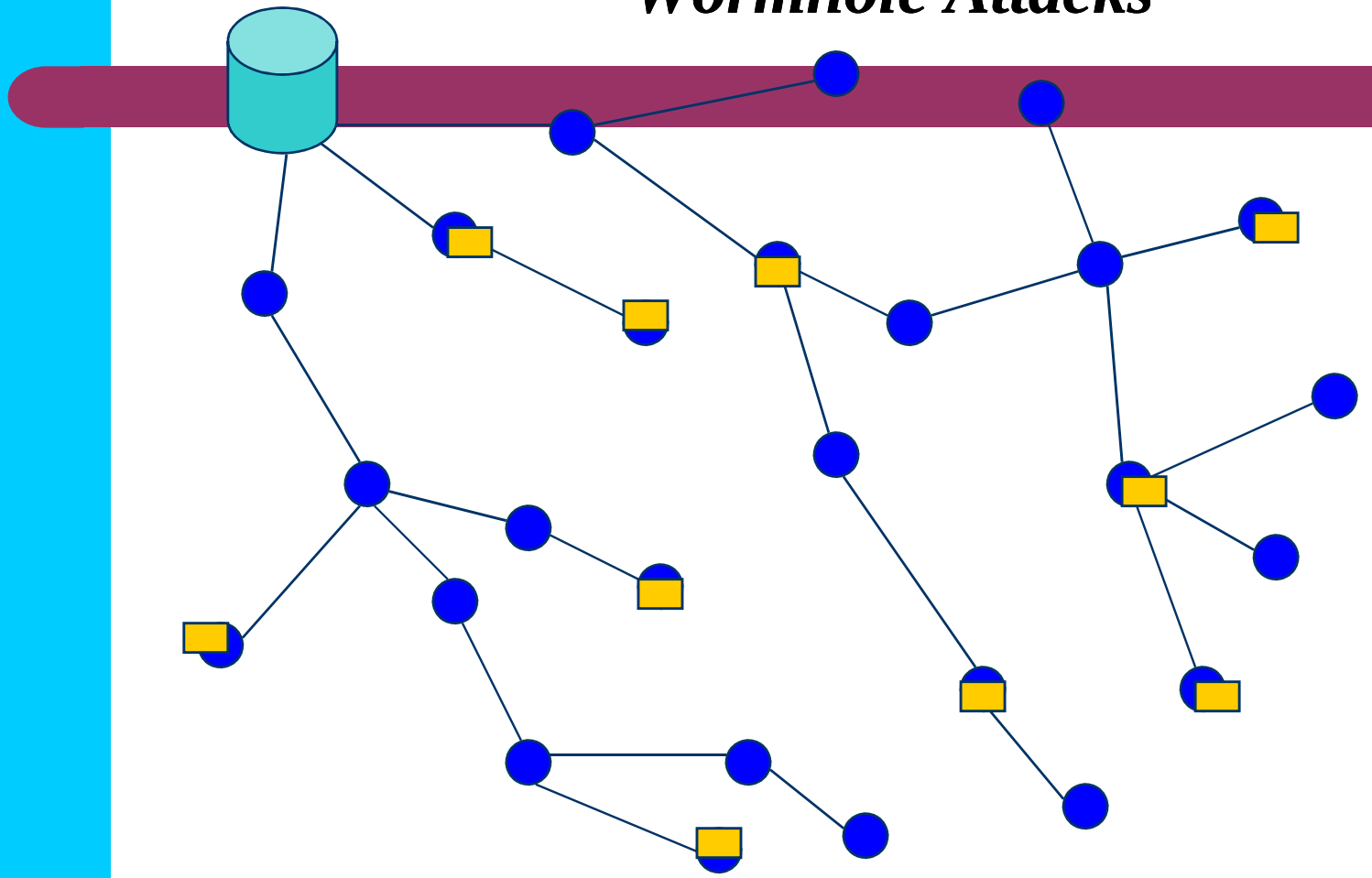
Challenges in Securing MANETs
- Wormhole Attacks



Initial Routing before attack

Adapted from Chris Karlof and David Wagner's WSNPA slides

Challenges in Securing MANETs
- Wormhole Attacks

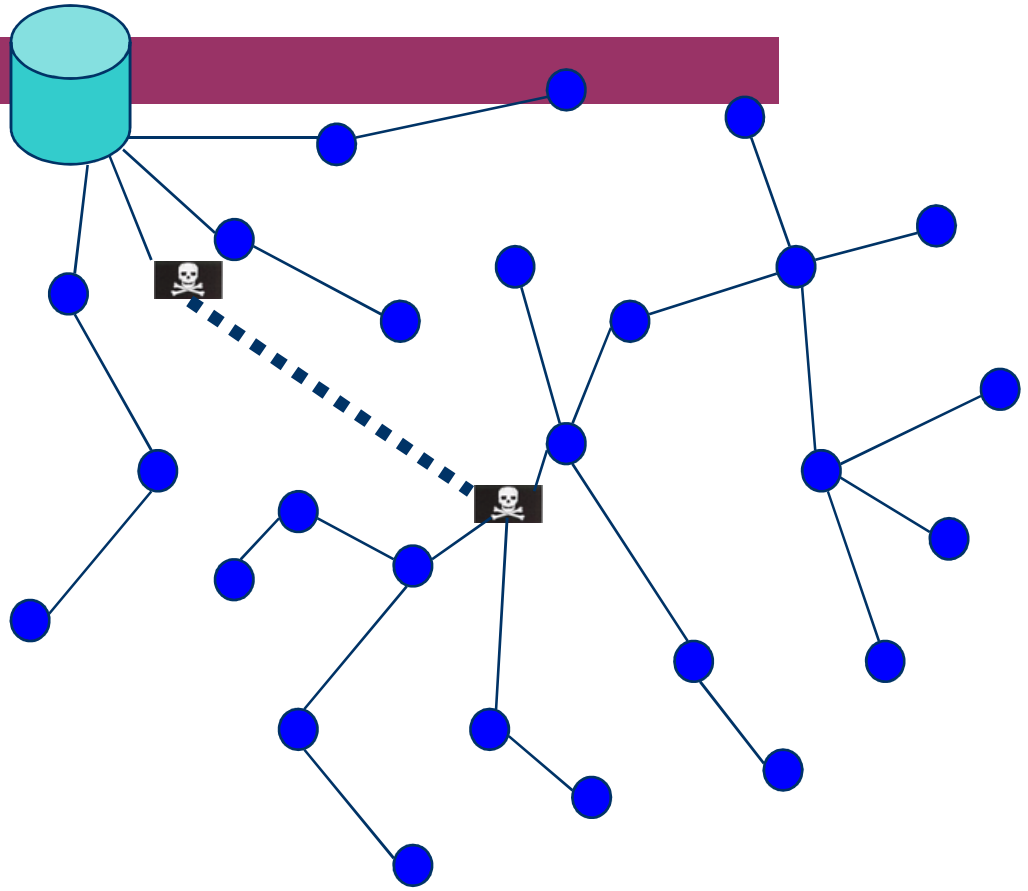


Initial Routing before attack

Adapted from Chris Karlof and David Wagner's WSNPA slides

Challenges in Securing MANETs
- Wormhole Attacks

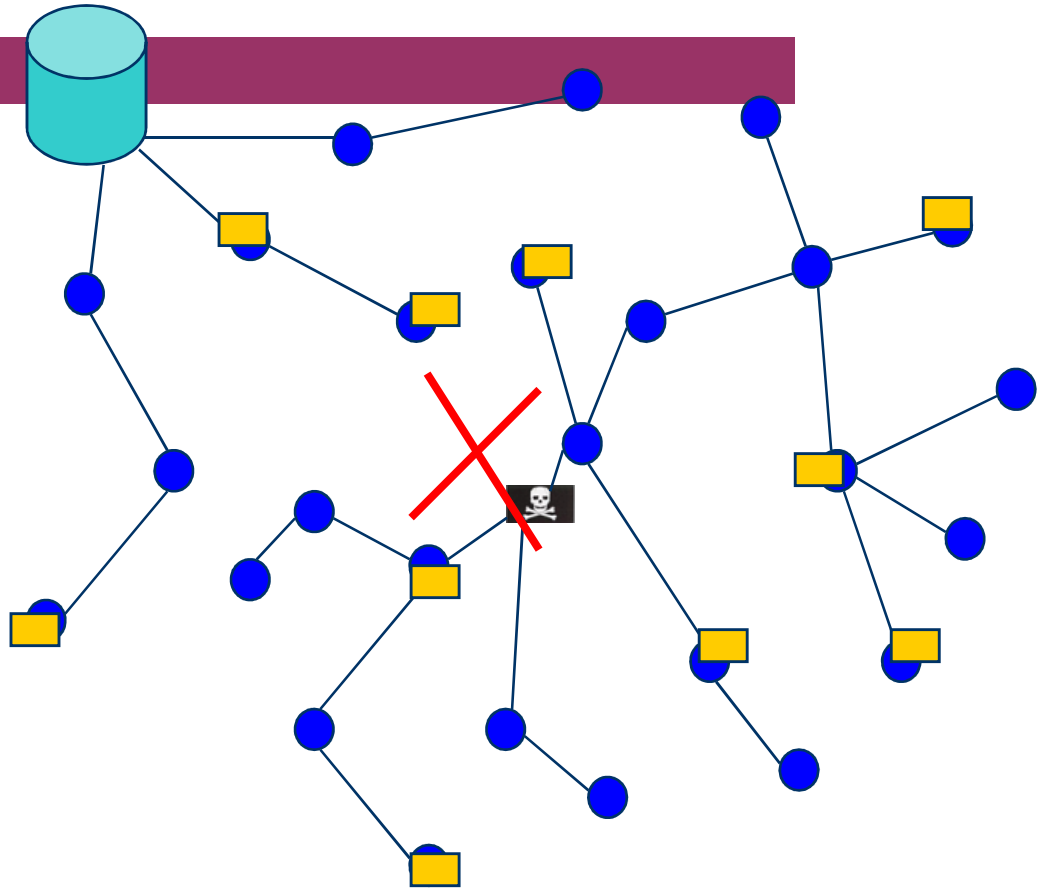
- *Tunnel packets received in one place of the network and replay them in another place*
- *The attacker can have no key material. All it requires is two transceivers and one high quality out-of-band channel*



Adapted from Chris Karlof and David Wagner's WSNPA slides

Challenges in Securing MANETs
- Wormhole Attacks

- *Most packets will be routed to the wormhole*
- *The wormhole can drop packets or more subtly, selectively forward packets to avoid detection*



Adapted from Chris Karlof and David Wagner's WSNPA slides

Presentation Outline

- Mobile Ad hoc Networks - Overview
- Challenges in Securing MANETs
- ***Ongoing Research in Securing MANETs***
- Conclusion

Ongoing Research in Securing MANETs
- Securing Routing in MANETs

- *The **Secure Routing Protocol** (SRP) is designed as an extension compatible with a variety of existing reactive routing protocols.*
- *SRP combats attacks that disrupt the route discovery process and guarantees the acquisition of correct topological information*
- ***ARIADNE** (a secure routing protocol based on DSR) guarantees that the target node of a route discovery process can authenticate the initiator*
- *the initiator can in turn authenticate each intermediate node on the path to the destination present in the RREP message*
- *no intermediate node can remove a previous node in the node list in the RREQ or RREP messages.*

Ongoing Research in Securing MANETs
- Securing Routing in MANETs

- ***ARAN*** *secure routing protocol (conceived as an on-demand routing protocol) that detects and protects against malicious actions carried out by third parties and peers in the ad hoc environment.*
- *It introduces* ***authentication, message integrity*** *and* ***non-repudiation*** *as part of a minimal security policy for the ad hoc environment*
- *Consists of a preliminary certification process, a mandatory end-to-end authentication stage and an optional second stage that provides secure shortest paths*

Ongoing Research in Securing MANETs
- Dealing with Selfish and Malicious Nodes

- ***CONFIDANT*** *(Cooperation Of Nodes, Fairness In Dynamic Ad-hoc NeTworks) aims at detecting malicious nodes by means of combined monitoring and reporting and establishes routes by avoiding misbehaving nodes*
- *It is designed as an extension to a routing protocol such as DSR.*
- *Another approach is a* ***Token based Cooperation Enforcement Scheme*** *that requires each node of the ad hoc network to hold a token in order to participate in the network operations*
- ***Tokens*** *are granted to a node collaboratively by its neighbors based on the monitoring of the node's contribution to packet forwarding and routing operations*
- *Upon expiration of the token, each node renews its token through a token renewal exchange with its neighbors.*

Ongoing Research in Securing MANETs
- Key Management and Node Authentication

- *A **Self-Organized Public-Key Management scheme** based on PGP has been proposed to support security of ad hoc network routing protocols*
- *Users issue certificates for each other based on their personal acquaintances*
- *In authentication based on **Polynomial Secret Sharing** public-key certificate of each node is cooperatively generated by a set of neighbors*

  - based on the behavior of the node as monitored by the neighbors
- *Using a group signature mechanism based on polynomial secret sharing, the secret digital signature key used to generate public-key certificates is distributed among several nodes*

The Secure Routing Protocol (SRP)

- ***SRP** allows the initiator of a route discovery to detect and discard bogus replies*
- *SRP relies on the availability of a **security association** (SA) between the source node (S) and the destination node (T).*
- *The SA could be established using a hybrid key distribution based on the public keys of the communicating parties.*
- *S and T can exchange a secret symmetric key ($K_{S,T}$) using the public keys of one another to establish a secure channel.*

The Secure Routing Protocol (SRP)

- *S and T can then further proceed to mutual authentication of one another and the authentication of routing messages.*
- *SRP suffers also from the lack of a validation mechanism for route maintenance messages: route error packets are not verified*
- *SRP is, however, not immune to the wormhole attack: two colluding malicious nodes can misroute the routing packets on a private network connection and alter the perception of the network topology by legitimate nodes*

ARIADNE

- *ARIADNE needs some mechanism to bootstrap authentic keys required by the protocol*
- *In particular, each node needs a shared secret key ($K_{S,D}$, is the shared key between a source S and a destination D) with each node it communicates with at a higher layer*
- *In ARIADNE, the basic RREQ mechanism is enhanced by eight additional fields used to provide authentication and integrity to the routing protocol as follows:*

  <ROUTE REQUEST, initiator, target, id, time interval, hash chain, node list, MAC list>

ARIADNE

- *When the target node receives the RREQ, it checks the validity of the request by determining that the keys from the time interval specified have not been disclosed yet, and that the hash chain field is equal to:*

  H [η_n , H [η_{n-1} , H [. . . , H [η_1 , MACKSD (initiator, target, id, time interval)] . . .]]]

  where η_i is the node address at position i of the node list in the request, and where n is the number of nodes in the node list
- *If the target node determines that the request is valid, it returns a RREP to the initiator, containing eight fields:*

  <ROUTE REPLY, target, initiator, time interval, node list, MAC list, target MAC, key list>
- *ARIADNE is protected also from a flood of RREQ packets that could lead to the cache poisoning attack.*

ARAN

- *ARAN requires the use of a trusted certificate server (T):*
- *The certificate contains the IP address of the node, its public key, a timestamp of when the certificate was created and a time at which the certificate expires along with the signature by T*
- *All nodes are supposed to maintain fresh certificates with the trusted server and must know T's public key*
- *The goal of the first stage of the ARAN protocol is for the source to verify that the intended destination was reached.*
- *In this stage, the source trusts the destination to choose the return path*

ARAN

- *The second stage of the ARAN protocol guarantees in a secure way that the path received by a source initiating a route discovery process is the shortest.*
- *The second stage of the ARAN protocol guarantees in a secure way that the path received by a source initiating a route discovery process is the shortest.*
- *The ARAN protocol protects against exploits using **modification, fabrication** and **impersonation** but the use of asymmetric cryptography makes it a very costly protocol to use in terms of CPU and energy usage.*
- *ARAN is not immune to the wormhole attack*

SEAD

- *In order to secure the DSDV-SQ routing protocol, SEAD makes use of efficient one-way hash chains rather than relaying on expensive asymmetric cryptography operations.*
- *SEAD assumes some mechanism for a node to distribute an authentic element of the hash chain that can be used to authenticate all the other elements of the chain.*
- *It suggests to ensure the key distribution relaying on a trusted entity that signs public key certificates for each node*
- *Each node can then use its public key to sign a hash chain element and distribute it*
- *The basic idea of SEAD is to authenticate the sequence number and metric of a routing table update message using hash chains elements.*
- *In addition, the receiver of SEAD routing information also authenticates the sender, ensuring that the routing information originates form the correct node.*

CONFIDANT
(Cooperation Of Nodes, Fairness In Dynamic Ad-hoc NeTworks)

- *CONFIDANT components in each node include*

  - a network monitor,

  - reputation records for first-hand and trusted second-hand observations about routing and forwarding behavior of other nodes,

  - trust records to control trust given to received warnings, and

  - a path manager to adapt the behavior of the local node according to reputation and to take action against malicious nodes.

- *The term **reputation** is used to evaluate routing and forwarding behavior according to the network protocol, whereas the term trust is used to evaluate participation in the CONFIDANT meta-protocol*

CONFIDANT

(Cooperation Of Nodes, Fairness In Dynamic Ad-hoc NeTworks)

- *The dynamic behavior of CONFIDANT is as follows.*

  - Nodes monitor their neighbors and change the reputation accordingly

  - If they have a reason to believe that a node misbehaves, they can take action in terms of their own routing and forwarding and they can decide to inform other nodes by sending an ALARM message.

  - When a node receives such an ALARM either directly or by promiscuously listening to the network, it evaluates how trustworthy the ALARM is based on the source of the ALARM and the accumulated ALARM messages about the node in question

  - It can then decide whether to take action against the misbehaved node in the form of excluding routes containing the misbehaved node, re-ranking paths in the path cache, reciprocating by non-cooperation, and forwarding an ALARM about the node.

Token-based cooperation enforcement

- *The token-based cooperation enforcement mechanism includes four interacting components:*

  - neighbor verification through which the local node verifies whether neighboring nodes are legitimate,

  - neighbor monitoring that allows the local node to monitor the behavior of each node in the network and to detect attacks from malicious nodes,

  - intrusion reaction that assures the generation of network alerts and the isolation of attackers, and

  - security enhanced routing protocol that consists of the ad hoc routing protocol including security extensions.

Self-Organized Public-Key Management based on PGP

- *In the proposed self-organizing public-key management system, each user maintains a local certificate repository*
- *When two users want to verify the public keys of each other, they merge their local certificate repositories and try to find appropriate certificate chains within the merged repository*
- *The success of this approach very much depends on the construction of the local certificate repositories and on the characteristics of the certificate graphs.*
- *The vertices of a certificate graph represent public-keys of the users and the edges represent public-key certificates issued by the users*

Authentication based on polynomial secret sharing

- *Using a group signature mechanism based on polynomial secret sharing, the secret digital signature key used to generate public-key certificates is distributed among several nodes*
- *Certification services like issuing, renewal and revocation of certificates thus are distributed among the nodes: a single node holds just a share of the complete certificate signature key.*
- *a **localized trust model** has been proposed to characterize the localized nature of security concerns in large ad hoc wireless networks.*
- *When applying such trust model, an entity is trusted if any k trusted entities claim so: these k trusted entities are typically the neighboring nodes of the entity.*
- *A locally trusted entity is globally accepted and a locally distrusted entity is regarded untrustworthy all over the network.*

Presentation Outline

- Mobile Ad hoc Networks - Overview
- Challenges in Securing MANETs
- Ongoing Research in Securing MANETs
- ***Conclusion***

Conclusion

- *Security of ad hoc networks has recently gained momentum in the research community*
- *Due to the open nature of ad hoc networks and their inherent lack of infrastructure, security exposures can be an impediment to basic network operation*
- *Security solutions for MANET have to cope with a challenging environment including scarce energy and computational resources and lack of persistent structure*

Conclusion

- *The solutions presented in this presentation only cover a subset of all threats and are far from providing a comprehensive answer to the security problem in ad hoc networks*
- *They often address isolated issues away from a global approach to security*
- *As the technology for ad hoc wireless networks gains maturity, comprehensive security solutions based on realistic trust models and addressing all prevalent issues like routing, key management and cooperation enforcement are expected to appear*

Questions?

Thank You

References

Networks", ... UCLA-CSD-TR-200030.
Distributed and Network-based Processing.