电子科技大学
University of Electronic Science and Technology of China

无线移动Ad hoc路由协议DSR的安全研究

电子科技大学
计算机科学与工程学院
张翔

www.uestc.edu.c

MANET路由

- Mobile Ad-hoc Network (MANET)
  - 由一系列配置有无线收发装置的移动节点构成的多跳临时自治系统。
    - 多跳性（Multi-hop）
    - 自组织（Self-organizing, No Infrastructure）
    - 拓扑变化频繁
    - 带宽有限
    - 资源受限（包括计算能力、存储能力和供电能力）

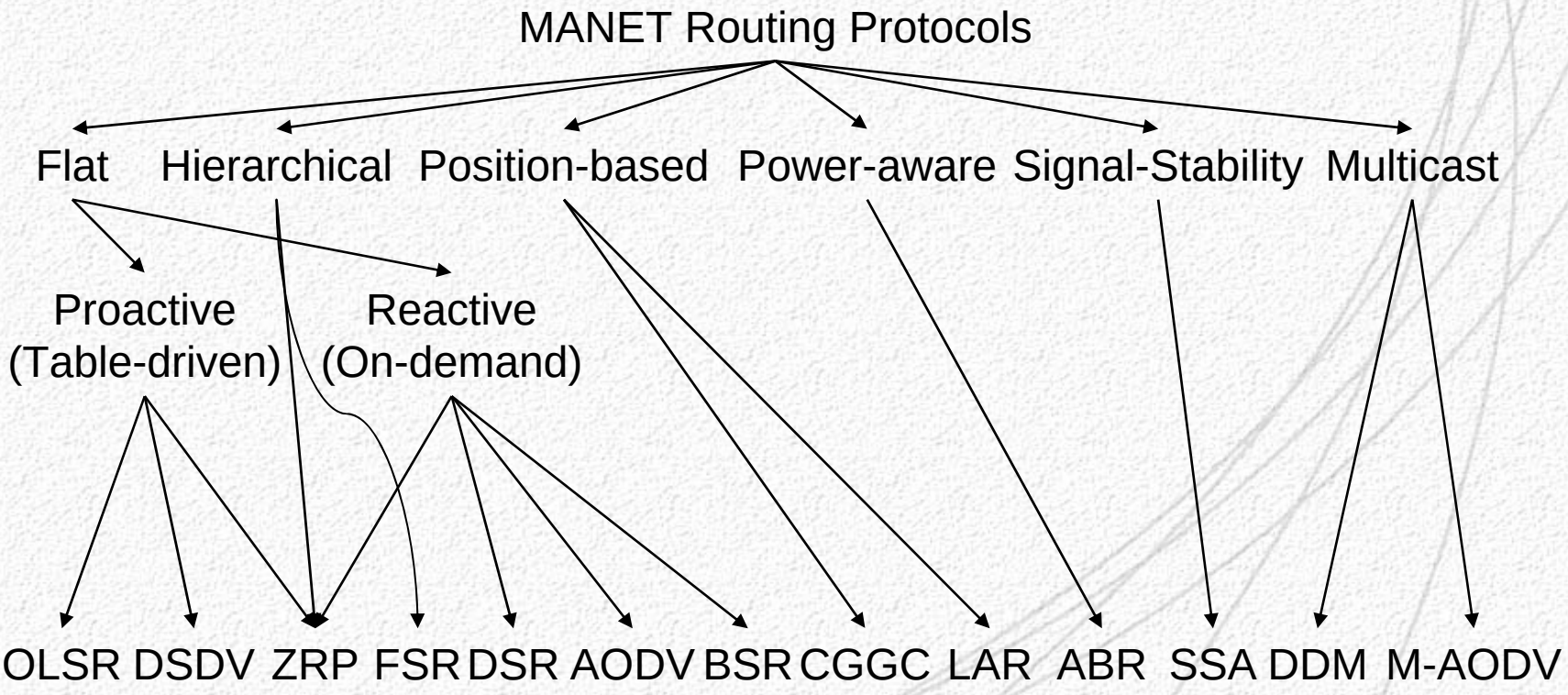
MANET路由

- Mobile Ad-hoc Network (MANET)
  - 主要应用
    - 军事战场、灾难救援、紧急场景等
    - 普适计算（Ubiquitous Computing）、传感器网络等

图片引自[Chris Ellis, 2004]

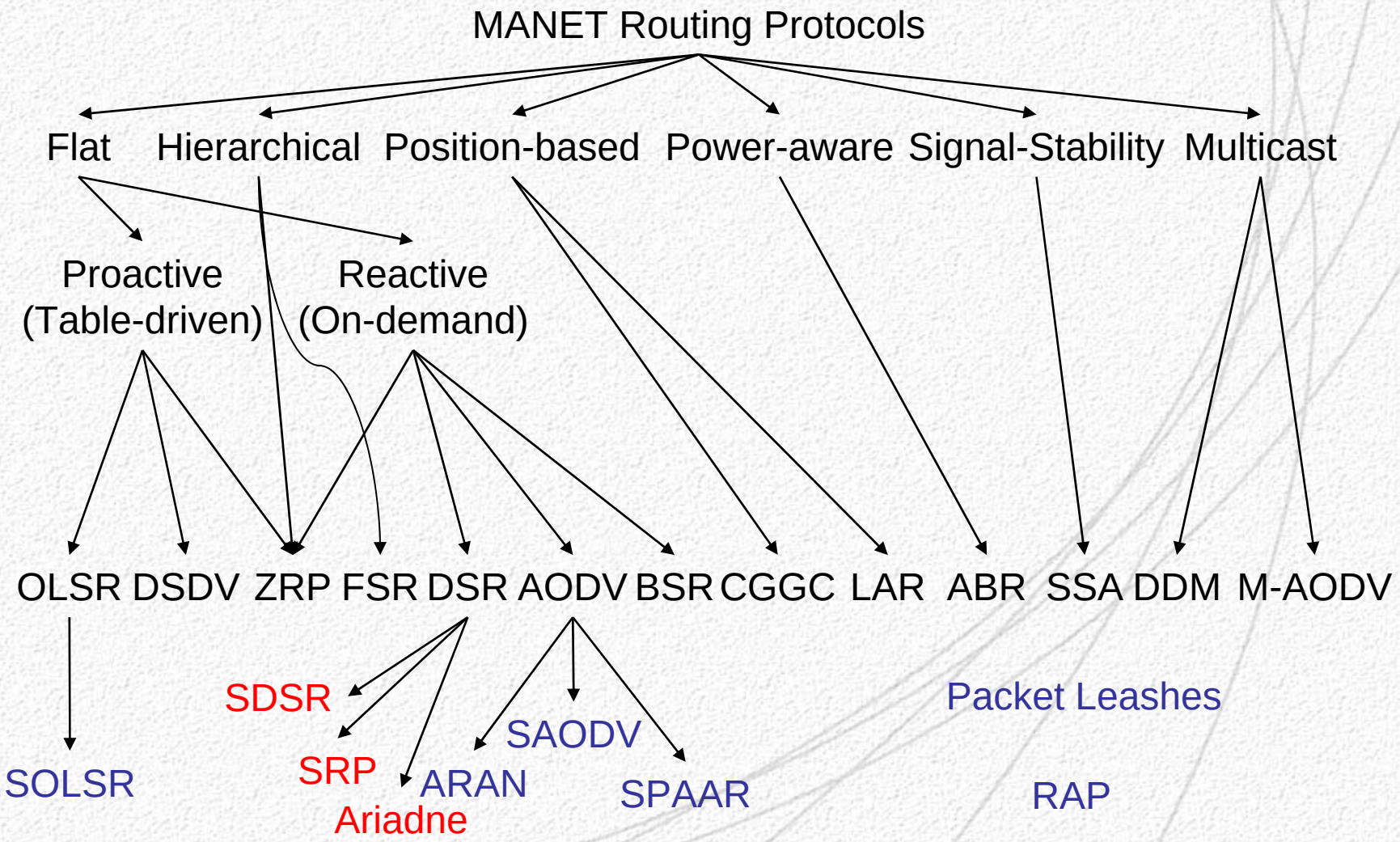
MANET路由

- 不同类别的MANET路由协议



图片引自[Frank Kargl , 2006]

MANET路由



图片引自[Frank Kargl , 2006]

MANET路由

- IETF MANET Working Group (Since 1997)
  - http://www.ietf.org/html.charters/manet-charter.html
- RFC 2501
  - Routing Protocol Issues and Evaluation Considerations
- RFCs for different routing protocols
  - AODV RFC3561 2003;
  - OLSR RFC3626 2003;
  - D S R RFC4728 2007;
- Newest Routing Protocol Draft
  - DYMO, draft-ietf-manet-dymo-14, 2008

MANET安全

- MANET安全期望
  - 机密性（Confidentiality ）
  - 真实性（Authenticity ）
  - 完整性（Integrity）
  - 可用性（Availability）
  - 不可抵赖（ Non-Repudiation）
  - 访问控制（ Access Control ）
  - 隐密性（Privacy）

MANET安全

- 影响MANET安全的固有因素:
  - 拓扑结构变换频繁
  - 无线信道易受攻击
  - 计算存储能力受限
- 直接导致：传统安全认证机制难以实施
  - 基于公钥基础结构(Public Key Infrastructures，PKI)的传统安全认证机制依赖于第三方可信机构(Certificate Authority，CA)的存在， MANET由于缺乏集中控制机制，难以通过特定节点提供CA服务。

MANET安全

- 常见攻击(目的):
  - 私自怠工 (Selfish Behavior)
    - 成因之一：本地资源受限(包括CPU、内存、带宽、能量等)
      - 为什么要本地浪费资源去支持其他节点的通信?
    - 可能产生的自私行为:
      - 拒绝加入路由发现
      - 决绝转发数具报文
      - 假装无法侦听邻居
  - 隐秘攻击 (Privacy Attack)
    - 定位跟踪等

MANET安全

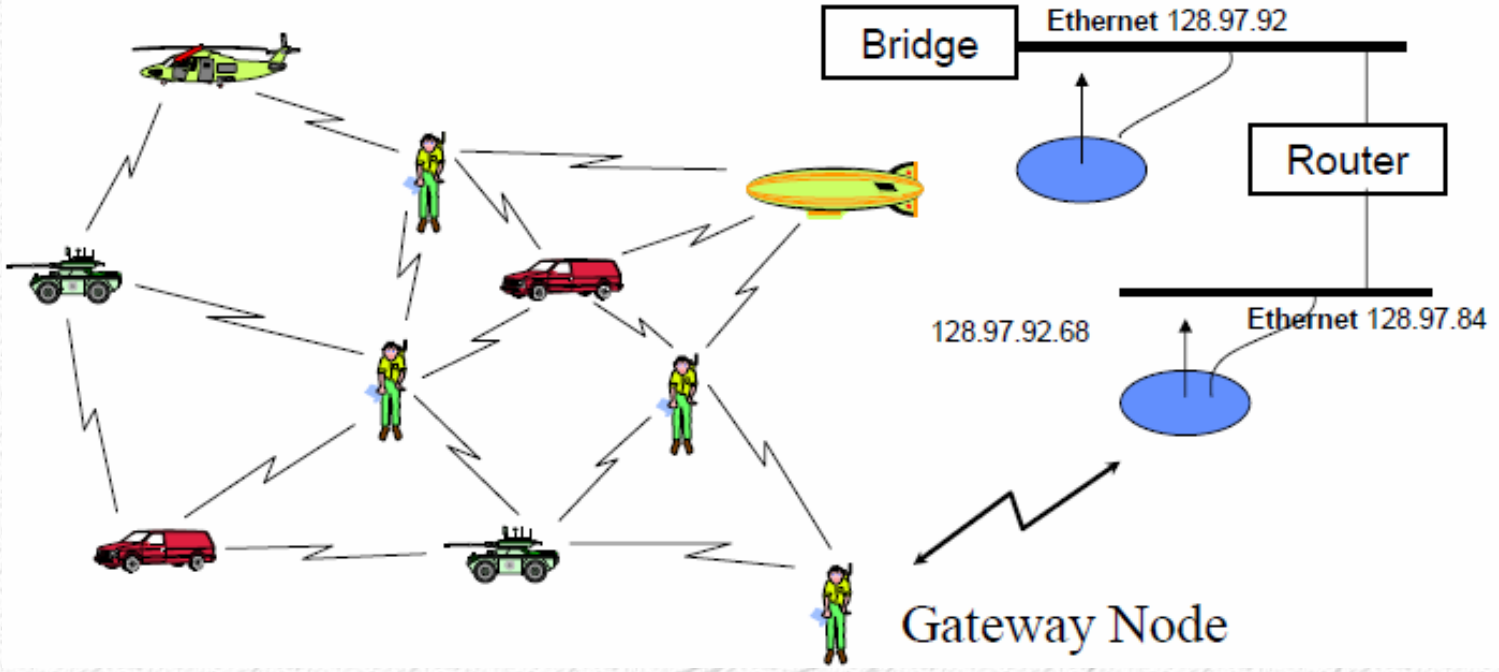
- 常见攻击(目的):
  - 拒绝服务式攻 (DoS, Denial of Service)
    - Sinkhole, Rushing, Wormhole Attack
    - Destroy Topology
    - Flooding / Overloading
  - 信息获取 (Information Access)
    - Sinkhole(do not drop), Rushing, Wormhole Attack
  - 信息篡改 (Information Modification)
    - Sinkhole(modify packets), Rushing, Wormhole Attack

动态源路由协议DSR

- Dynamic Source Routing Protocol (DSR)
  - 主要特点:
    - 允许节点根据发送需求动态寻找去往目的节点的路由信息（反应式路由，Reactive）
    - 传送报文在DSR选项头中携带有完整的从源到达目的的路径信息，有效避免路由环路
    - 中间节点可以通过提取旁听到的DSR报文所携带的源路由来扩充本地路由缓存，从而增强路由信息复用率，并为自动缩短等优化提供支持

动态源路由协议DSR

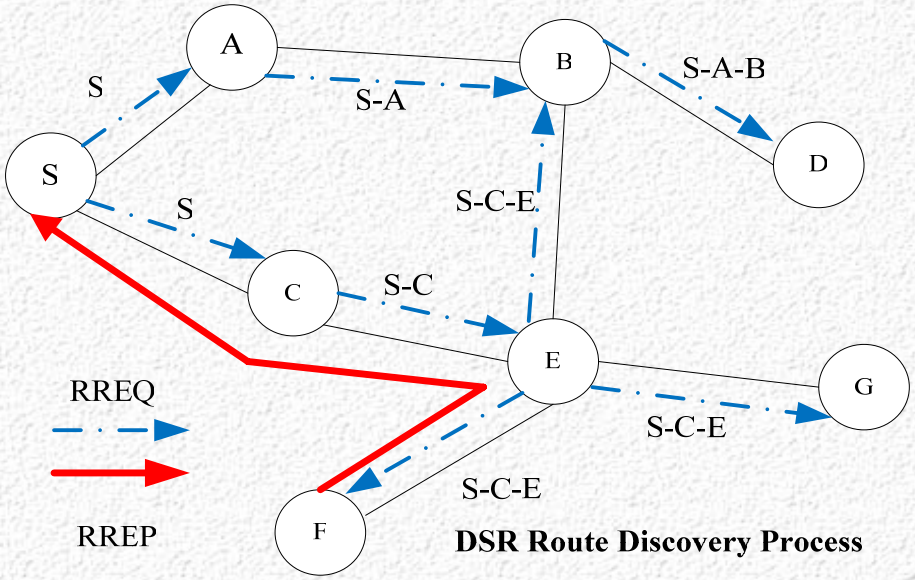
- Dynamic Source Routing Protocol (DSR)
  - 主要特点:
    - 可以很好的实现与既有网络(Internet)之间的无缝连接。



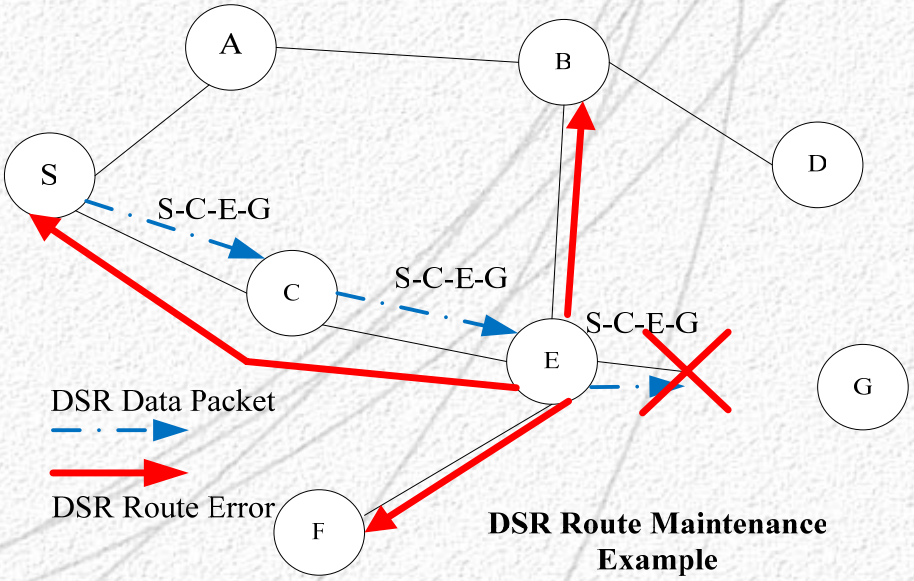
图片引自[吴晓光，2004]

动态源路由协议DSR

- Dynamic Source Routing Protocol (DSR)
  - 核心功能
    - 路由发现(Route Discovery)
    - 路由维护(Route Maintenance)



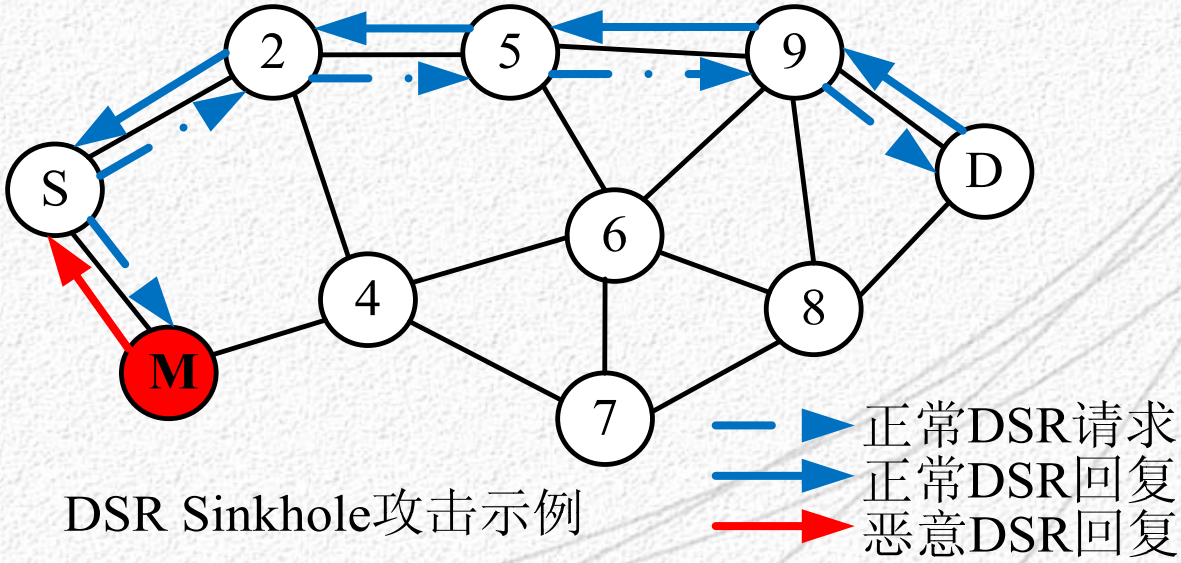
DSR Route Discovery Process



DSR Route Maintenance Example

DSR安全威胁

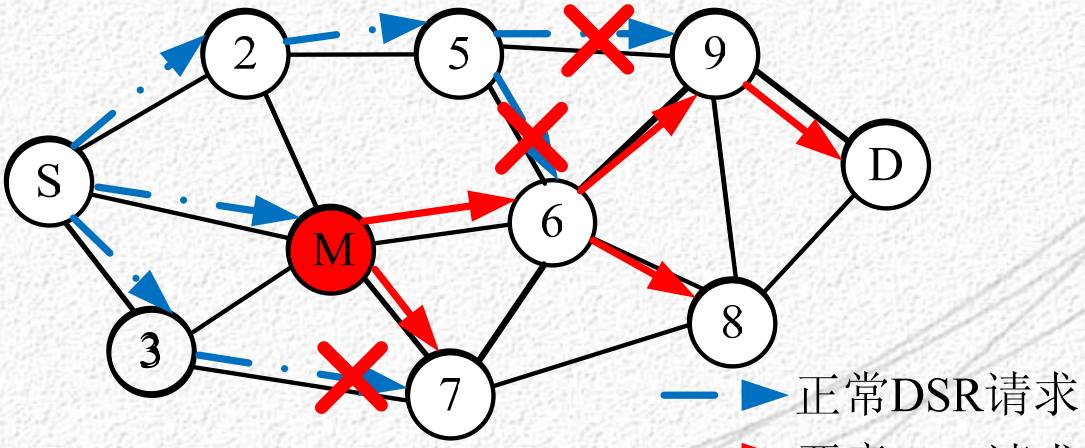
- DSR典型攻击-Sinkhole攻击 (Black hole攻击)
  - 攻击手段
    - 恶意节点M通过发送伪造的DSR路由请求或者回复信息，谎称自己拥有到达特定节点的路径，由此造成通往该特定节点的数据信息大量流向恶意节点，形成黑洞效应。



DSR Sinkhole攻击示例

DSR安全威胁

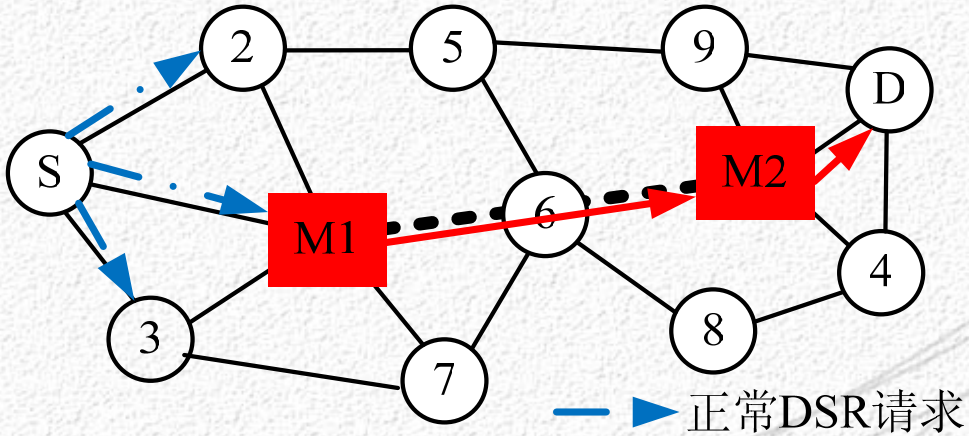
- DSR典型攻击-Rushing攻击
  - 攻击手段:
    - 利用DSR特性--即DSR中间节点仅会处理第一个到达的路由请求报文，而将后续相同的路由请求报文抛弃(以保证不出现环路，避免路由请求广播风暴)--攻击节点比其他其他中间节点更快地转发路由请求报文，增大源路由必然经过恶意节点的概率。



DSR Rushing攻击示例

DSR安全威胁

- DSR典型攻击- Wormhole攻击
  - 攻击手段:
    - 两个以上的多个恶意节点联手，相互构建跨越普通DSR网络层次的隧道通信(通常是高质量的私有链路)，隧道一端的恶意节点监听记录特定报文信息，通过隧道将该报文发送到位于隧道另一端的恶意节点处重放。



DSR Wormhole攻击示例

恶意节点使用隧道方式诱使试图寻找更短路径的DSR源节点落入陷阱

DSR安全协议

- DSR协议安全扩展
  - DSR攻击首要目标:
    - 为特定目标渗透、干扰、破坏**DSR**正常路由发现机制
  - DSR安全路由核心:
    - 高效可靠获取路由信息
  - 既有DSR安全协议:
    - SRP, Secure Routing Protocol. [Papadmitratos etc. 2002]
    - Ariadne. [Hu etc. 2002]
    - SRDP, Secure Route Discovery Protocol. [Kim etc. 2005]
    - SDSR, Secure DSR Protocol. [Yu etc. 2005, Ji etc. 2006]

DSR安全协议

- Secure Routing Protocol (SRP)
  - 基本假设:
    - 无线通信双向连接 (e.g. 802.11)
    - 源节点S和目的节点T间具有安全关联(Security Association)
    - 源节点S和目的节点T间可以协商共享密钥(Shared Secret Key)
  - 核心思路:
    - Query Sequence Number (32-bit)
      - 初始化于SA的建立阶段，用于Target判断Request的版本新旧，不允许重复滚动使用。
    - Query Identifier (32-bit)
      - 随机产生，不可预测，中间节点通过记录检查<SID, TID, QID>三元组预防传统DSR假冒攻击

DSR安全协议

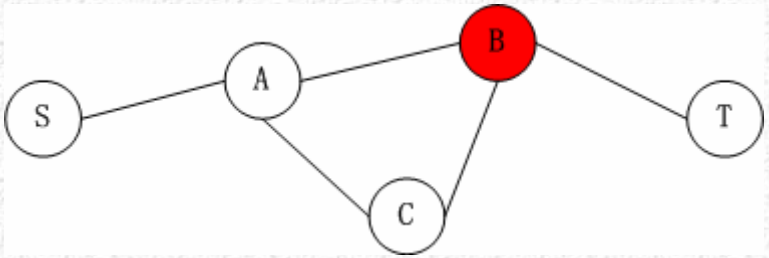
- Secure Routing Protocol (SRP)
  - SRP MAC (96-bit)
    - 通过S和T之间的共享密钥生成初始Request的MAC (不包含DSR路由请求过程中的Source Route List)
  - 优势缺陷:
    - 贡献:

      实现了S与T之间的相互验证，有效抵御Sinkhole攻击
    - 缺陷:

      S、T均没有和中间节点建立安全关联(SA)，使得Route Request过程中源路由节点链可以被随意篡改，对付不了Rushing攻击和Wormhole攻击

DSR安全协议

- Secure Routing Protocol (SRP)
  - 针对SRP的简单攻击示例



S-〉* (RREQ, S, T, Qid, Qsn, MACst)

A-〉* (RREQ, S, T, Qid, Qsn, MACst, A)

B-〉* (RREQ, S, T, Qid, Qsn, MACst, ACXB)

T-〉B (RREP, S, T, Qid, Qsn, ACXB, MACts)

B-〉A (RREP, S, T, Qid, Qsn, ACXB, MACts)

A-〉S (RREP, S, T, Qid, Qsn, ACXB, MACts)

DSR安全协议

- Ariadne
  - 基本假设:
    - 无线通信双向连接 (e.g. 802.11)
  - 三种方案:
    - 1、采用共享密钥
      - 假设全网任意两节点间均建立有共享密钥(Pairwise Shared Key)
    - 2、采用TESLA广播认证协议
      (Time Efficient Stream Loss-tolerant Authentication)
      - 假设仅通信两端(S和T)之间建立有共享密钥
    - 3、采用数字签名
      - 假设全网任意节点间均建立有公私密钥对

DSR安全协议

- Ariadne
  - 核心思路(应用TESLA广播认证协议):
    - 路由请求数据内容

      (RREQ, S, T, id, time interval, hash chain, node list, MAC list)
    - 路由回复数据内容

      (RREP, T, S, id, time interval, node list, MAC list, target MAC, key list)
    - 路由请求示例

      S: $h_0 = MAC_{K_{ST}}$(RREQ, S, T, id, ti)

      S-〉*: (RREQ, S, T, id, ti, h_0, (), ())

      A: $h_1 = H[A, h_0]$

      $M_A = MAC_{K_{Ati}}$(RREQ, S, T, id, ti, h_1, (A), ())

      A-〉*: (RREQ, S, T, id, ti, h_1, (A), (M_A))

DSR安全协议

B: $h_2 = H[B, h_1]$

$M_B = MAC_{K_{Bti}}(RREQ, S, T, id, ti, h_2, (A, B), (M_A))$

B-〉*: $(RREQ, S, T, id, ti, h2, (A, B), (M_A, M_B))$

C: $h_3 = H[C, h_2]$

$M_C = MAC_{K_{Cti}}(RREQ, S, T, id, ti, h_3, (A, B, C), (M_A, M_B))$

C-〉*: $MAC_{K_{Cti}}(RREQ, S, T, id, ti, h_3, (A, B, C), (M_A, M_B, M_c))$

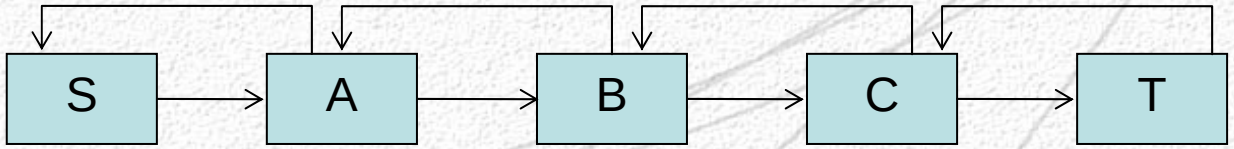
T: $M_T = MAC_{K_{TS}}(RREP, T, S, id, ti, (A, B, C), (M_A, M_B, M_c))$

T-〉C: $(RREP, T, S, id, ti, (A, B, C), (M_A, M_B, M_C), M_T, ())$

C-〉B: $(RREP, T, S, id, ti, (A, B, C), (M_A, M_B, M_C), M_T, (K_{Cti}))$

B-〉A: $(RREP, T, S, id, ti, (A, B, C), (M_A, M_B, M_C), M_T, (K_{Cti}, K_{Bti}))$

A-〉S: $(RREP, T, S, id, ti, (A, B, C), (M_A, M_B, M_C), M_T, (K_{Cti}, K_{Bti}, K_{Ati}))$



DSR安全协议

- Ariadne
  - 优势缺陷
    - 贡献

      在解决S与T相互验证基础上，提供了中间节点的验证

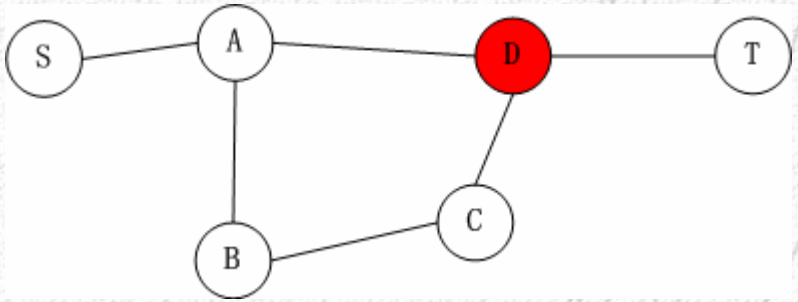
      – 采用TESLA广播认证协议或数字签名方式，由S验证中间节点有效性

      – 采用共享密钥方式，则是利用中间节点与T之间的安全关联，由T来验证中间节点的有效性，此时不再在RREP中回送MAC List和KEY List，M_r计算内容也不再包括MAC List。
    - 缺陷

      Ariadne提供了强大的安全机制，但也并非滴水不漏，一旦攻击节点掌握了用于中间节点单向散列计算的函数H，则可能发生危险，尽管这种事件不宜发生。

DSR安全协议

- Ariadne
  - 针对Ariadne的简单攻击示例



S: h0 = MAC$_{K_{ST}}$

S -〉 *: (RREQ, S, T, Qid, h0, (), ())

A: h1 = H[A, h0]

A -〉 *: (RREQ, S, T, Qid, h1, (A), Sig$_A$)

B : h2 = H[B, h1]

B -〉 *: (RREQ, S, T, Qid, h2, (A, B), (Sig$_A$, Sig$_B$))

C : h3 = H[C, h2]

C -〉 *: (RREQ, S, T, Qid, h3, (A, B, C), (Sig$_A$, Sig$_B$, Sig$_C$))

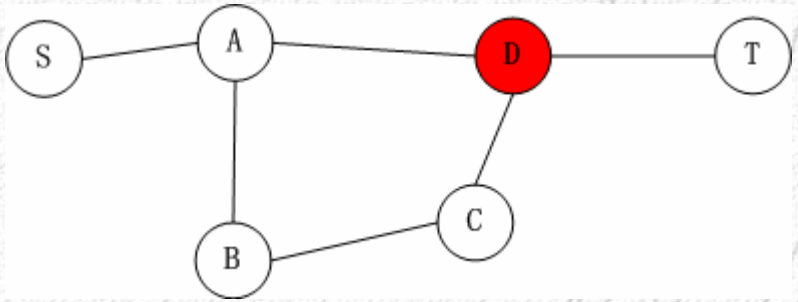
D : h' = H[D, h2]

D -〉 *: (RREQ, S, T, Qid, h3, (A, B, D), (Sig$_A$, Sig$_B$, Sig$_D$))

// 分别从A、C处获得的信息中提取到h1和Sig$_B$，并计算出h2

DSR安全协议

- Ariadne
  - 针对Ariadne的简单攻击示例



T: $M_T = MAC_{K_{TS}}$(RREP, T, S, Qid, (A, B, D), (Sig_A, Sig_B, Sig_D))

T -〉 D: (RREP, T, S, Qid, (A, B, D), (Sig_A, Sig_B, Sig_D), M_T)

D -〉 A: (RREP, T, S, Qid, (A, B, D), (Sig_A, Sig_B, Sig_D), M_T)

A -〉 S: (RREP, T, S, Qid, (A, B, D), (Sig_A, Sig_B, Sig_D), M_T)

DSR安全协议

- Secure Route Discovery Protocol (SRDP)
  - 提出后向验证(Backward Authentication)
  - 两种方案:
    - 共享秘钥
    - 数字签名

DSR安全协议

- Secure Route Discovery Protocol (SRDP)

S： 产生RREQ = <RREQ, S, D, SID, MAC_{SD}>

S->*: RREQ0 = <RREQ, ()>

B： 缓存RREQ0

B->*: RREQ1 = <RREQ, (B)>

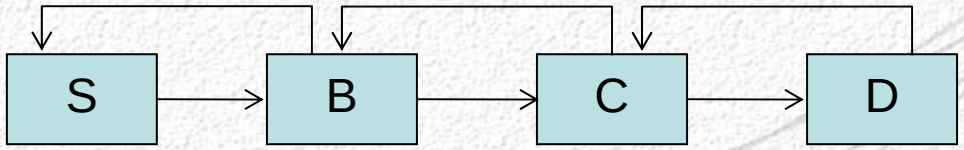
C： 缓存RREQ1

C->*: RREQ2 = <RREQ, (B, C) >

D： 缓存RREQ2，选择性验证MACsd

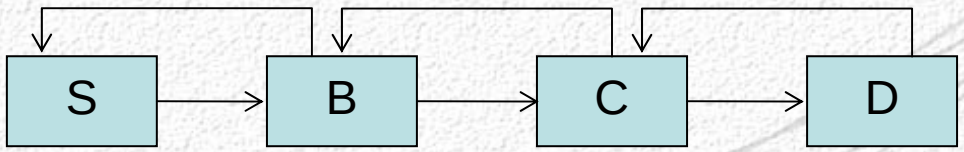
产生RREP = <RREP, D, S, SID , (B , C , D)>

计算 $\beta_D = MAC_{DS}$（RREP）



DSR安全协议

- Secure Route Discovery Protocol (SRDP)
  - D->C: RREP0 = <RREP, β_D>
  - C: 取出缓存的RREQ1，验证路由前缀和 β_D
    计算 $\beta_{DC} = MAC_{CS}$ (RREP0)
  - C->B: RREP1 = <RREP, β_{DC}>
  - B: 取出缓存的RREQ0，验证路由前缀和 β_{DC}
    计算 $\beta_{DCB} = MAC_{BS}$(RREP1)
  - B->S: RREP2 = <RREP, β_{DCB}>
  - S：验证 β_{DCB}是否等于MAC_{SB}(RREP, MAC_{SC} (RREP, MAC_{SD} (RREP)))



DSR安全协议

功能	Ariadne	SRP (old)	SDSR
密钥分发	前提	前提	集成
节点认证	全部	S和T	全部
安全RREQ	是	无	是
安全RREP	是	是	是
保证更新	是	是	是
会话秘钥交换	无	无	有
其他前提	时钟同步	无	无

DSR安全协议

- DSR密钥管理
  - 以上协议的共同特点:
    - 均基于**预先**建立的可信环境(Priori Trust)
    - 均将实体的可靠性作为前提
    - 缺陷:
      - 依赖于基础架构设施(Infrastructure)
      - 一旦密钥系统建立，将长时间存在，难以更改，不适应自组变化的DSR网络环境
  - 真实环境与需求:
    - 难以实施基础架构设施
    - 期望实现密钥自组织管理(Self-organized Key management)

DSR安全协议

- Secure DSR Protocol (SDSR)
  - 文献[16] [于良国等, 2005] 运用了基于身份的密码体制，提出了安全DSR协议（SDSR, Secure DSR）。
    - 假设组网时存在一个离线的可信机构，为每个节点分发一个与其身份对应的私钥(ID-based Crypto)
      - 身份信息作为公钥存在(PK = h(ID))，避免了证书的使用，从而在一定程度上减少了资源的消耗与管理的复杂度。
    - 选出多节点以门限分享机制共有可信机构私钥，用以为合法节点更新密钥。(Threshold-based Secret Share)
      - 通过本地节点私钥和通信对方的身份信息，即可有效计算初始共享密钥而无需信息交换，实现了SRDP中应用消息验证码方式的前提假设。

DSR安全协议

- 未来方向
  - 认证系统的自动初始化?
  - 私钥生成服务(Private Key Generation，PKG)的完全分布化?
  - 合法邻居节点的验证?
  - 在没有第三方可信机构的情况下新节点的准入机制?

谢谢大家!