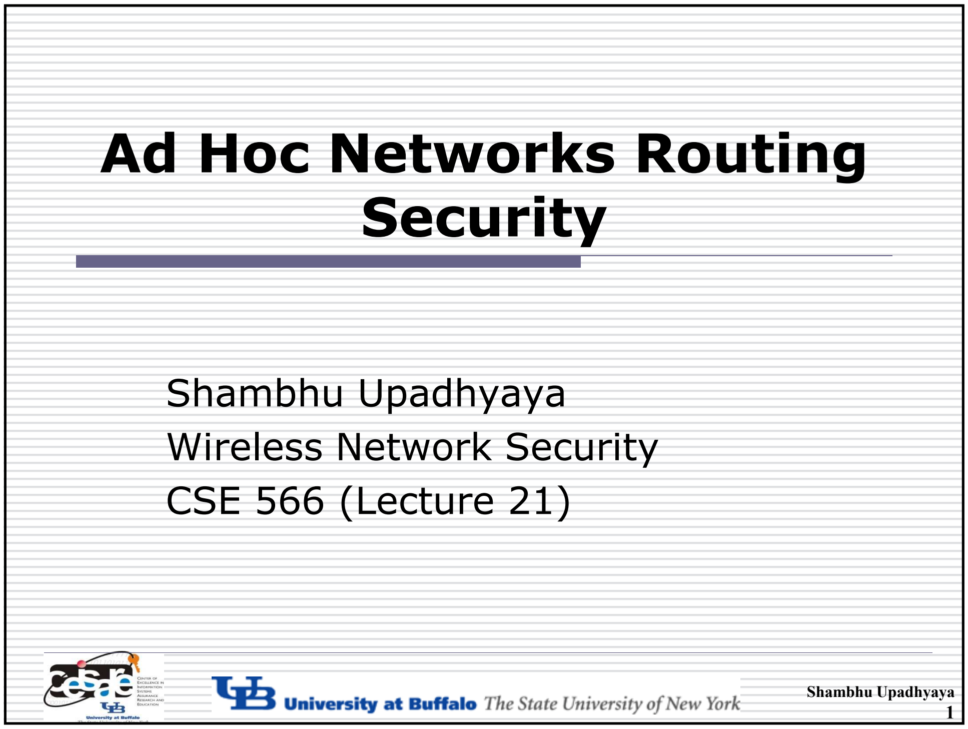
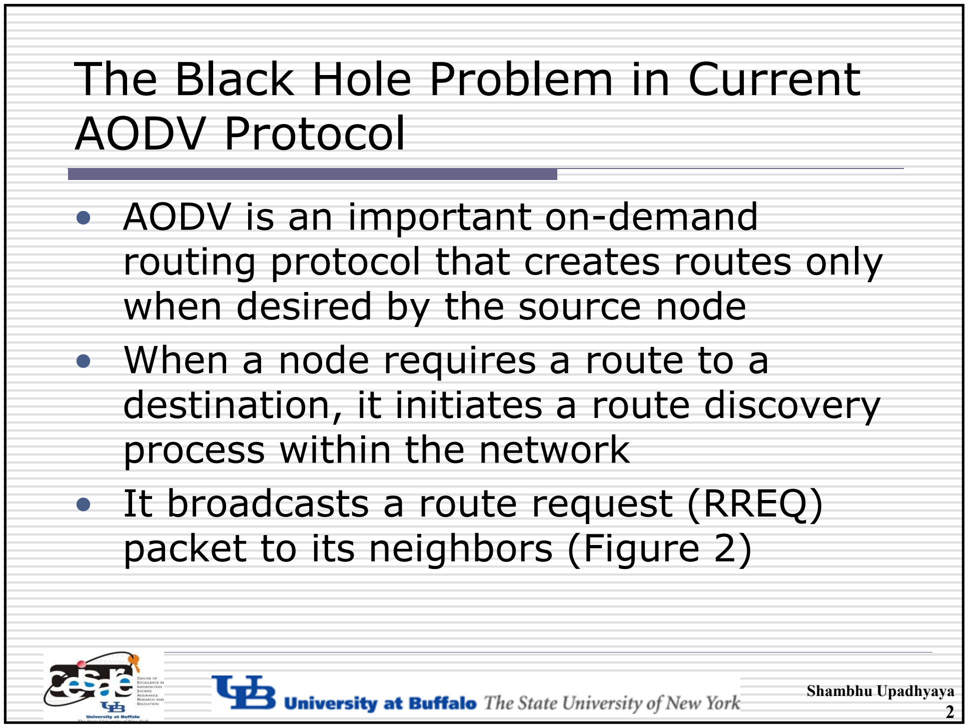


Ad Hoc Networks Routing Security

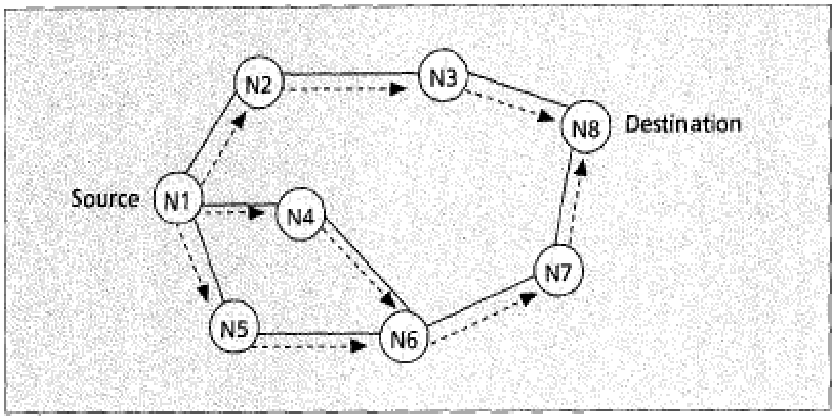
Shambhu Upadhyaya
Wireless Network Security
CSE 566 (Lecture 21)



The Black Hole Problem in Current AODV Protocol

- AODV is an important on-demand routing protocol that creates routes only when desired by the source node
- When a node requires a route to a destination, it initiates a route discovery process within the network
- It broadcasts a route request (RREQ) packet to its neighbors (Figure 2)

The Black Hole Problem in Current AODV Protocol (cont.)

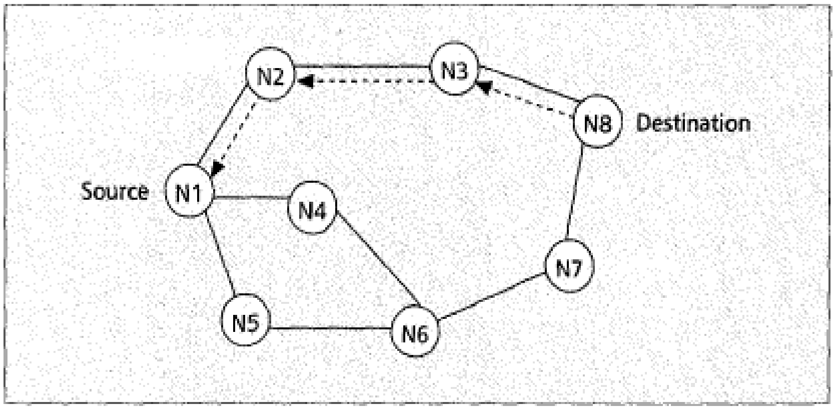


■ **Figure 2.** *Propagation of RREQ.*

The Black Hole Problem in Current AODV Protocol (cont.)

- Once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination or intermediate node responds by unicasting a route reply (RREP) packet (Figure 3) back to the neighbor from which it first received the RREQ

The Black Hole Problem in Current AODV Protocol (cont.)

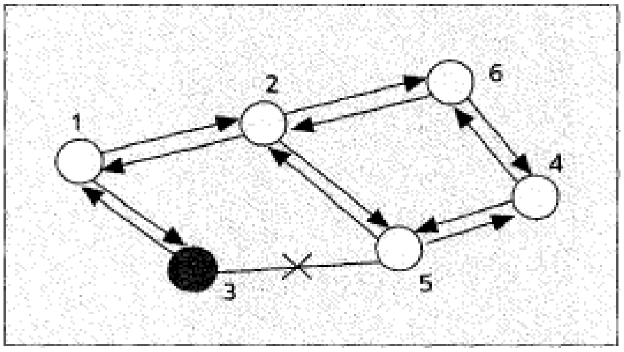


■ **Figure 3.** *The path of a routing reply.*

The Black Hole Problem in Current AODV Protocol (cont.)

- Any intermediate node may respond to the RREQ message if it has a fresh enough route
- The malicious node can easily disrupt the correct functioning of the routing protocol and make at least part of the network crash

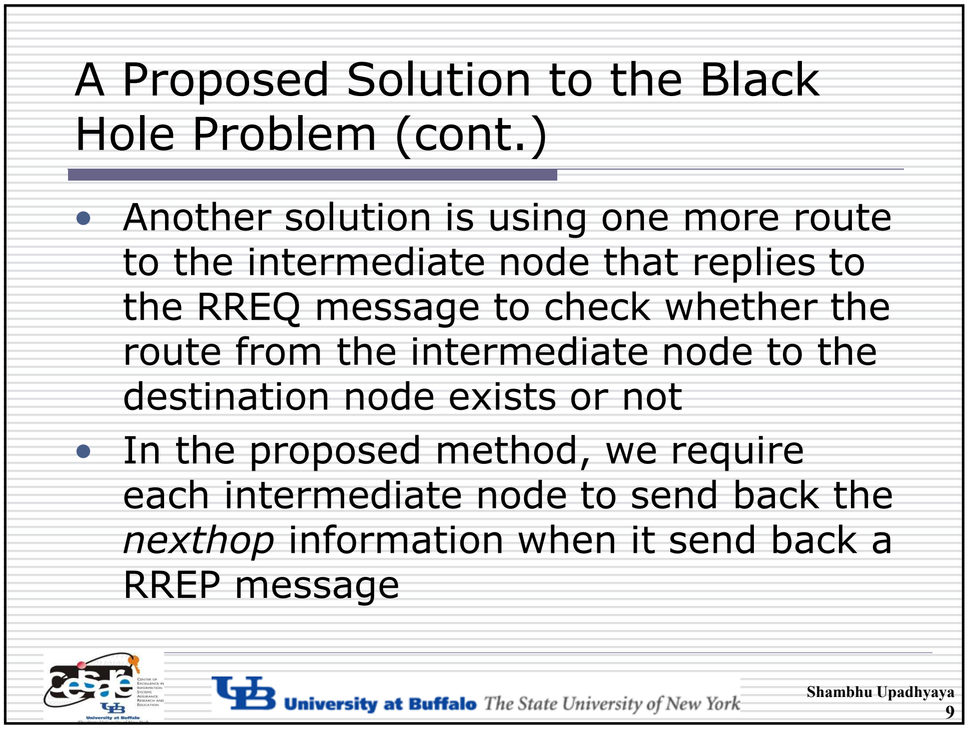
The Black Hole Problem in Current AODV Protocol (cont.)



■ **Figure 4.** *The black hole problem.*

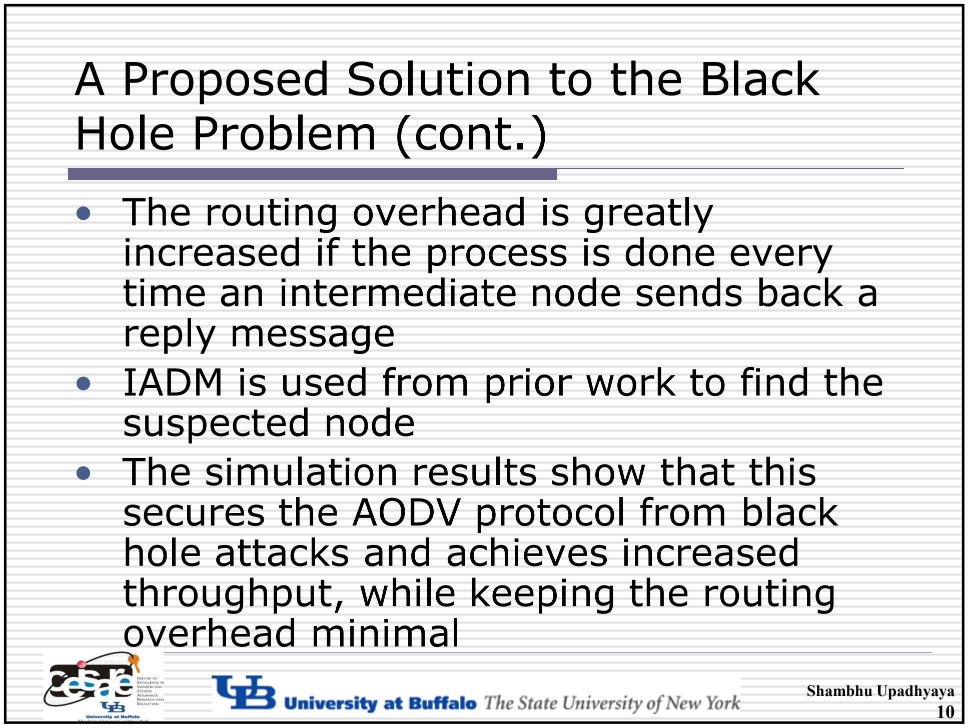
A Proposed Solution to the Black Hole Problem

- One possible solution to the black hole problem is to disable the ability to reply in a message of an intermediate node, so all reply messages should be sent out only by the destination node
- But there are some disadvantages in this method



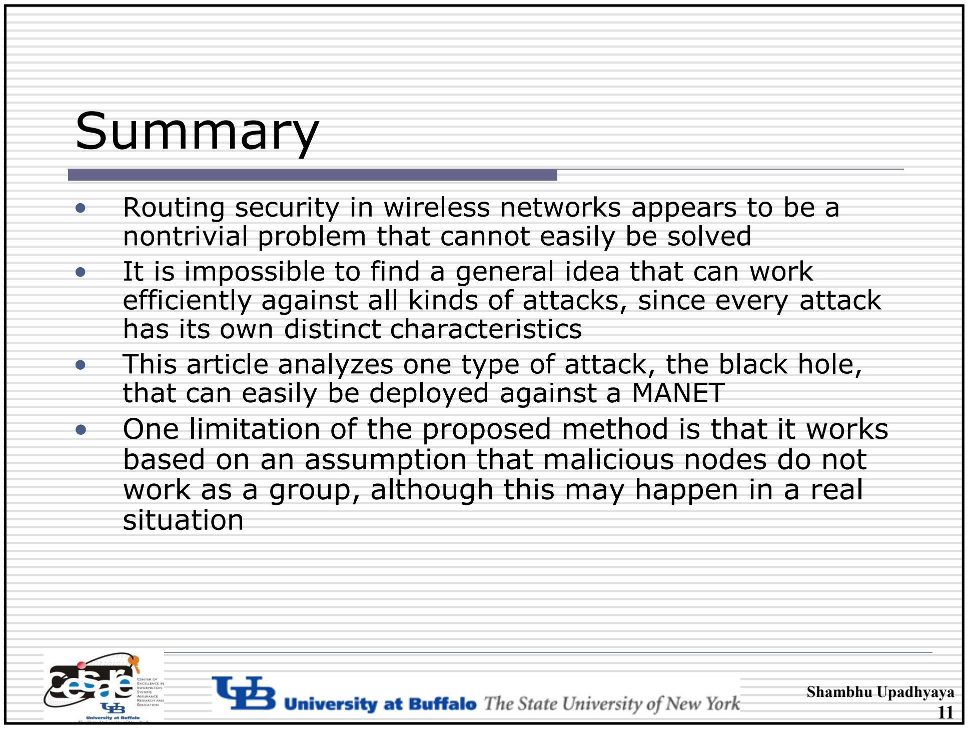
A Proposed Solution to the Black Hole Problem (cont.)

- Another solution is using one more route to the intermediate node that replies to the RREQ message to check whether the route from the intermediate node to the destination node exists or not
- In the proposed method, we require each intermediate node to send back the *nexthop* information when it send back a RREP message



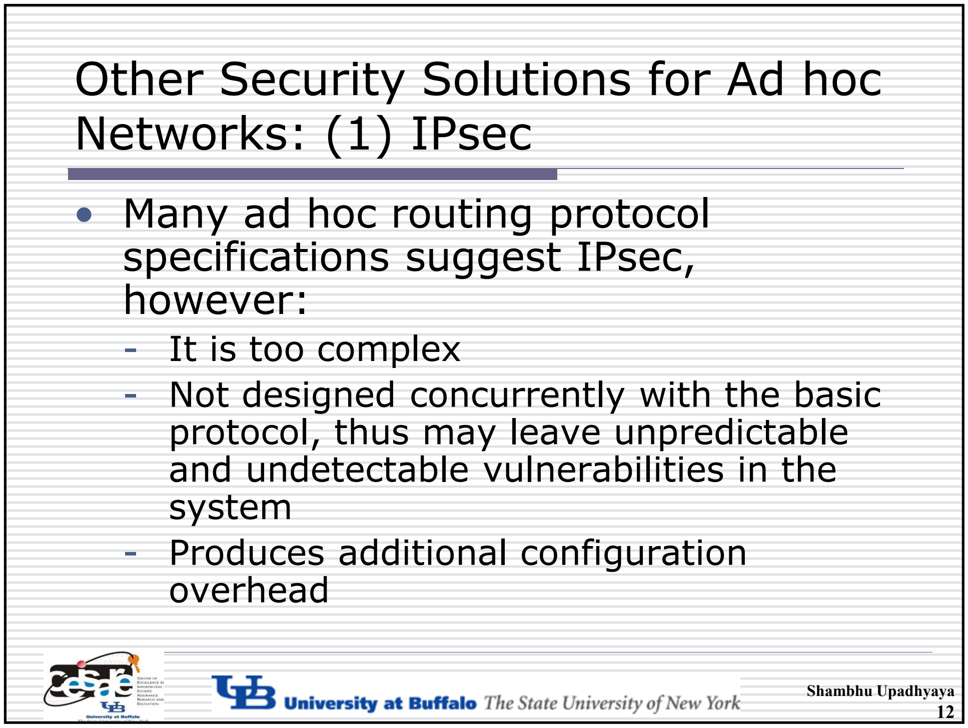
A Proposed Solution to the Black Hole Problem (cont.)

- The routing overhead is greatly increased if the process is done every time an intermediate node sends back a reply message
- IADM is used from prior work to find the suspected node
- The simulation results show that this secures the AODV protocol from black hole attacks and achieves increased throughput, while keeping the routing overhead minimal



Summary

- Routing security in wireless networks appears to be a nontrivial problem that cannot easily be solved
- It is impossible to find a general idea that can work efficiently against all kinds of attacks, since every attack has its own distinct characteristics
- This article analyzes one type of attack, the black hole, that can easily be deployed against a MANET
- One limitation of the proposed method is that it works based on an assumption that malicious nodes do not work as a group, although this may happen in a real situation



Other Security Solutions for Ad hoc Networks: (1) IPsec

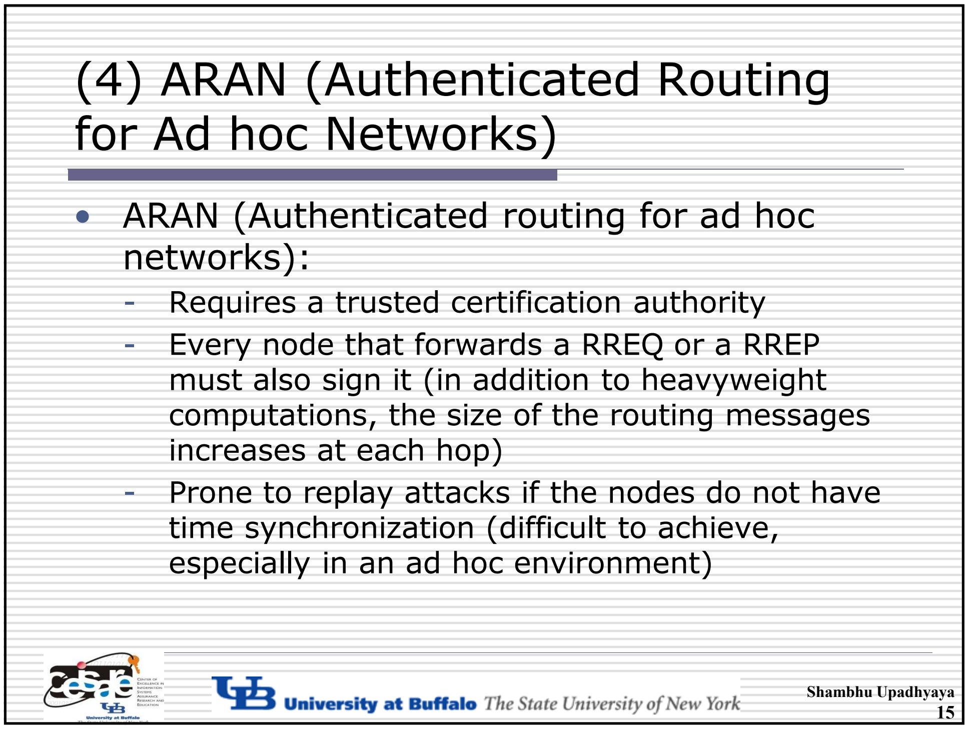
- Many ad hoc routing protocol specifications suggest IPsec, however:
  - It is too complex
  - Not designed concurrently with the basic protocol, thus may leave unpredictable and undetectable vulnerabilities in the system
  - Produces additional configuration overhead

(2) TIARA (Techniques for Intrusion Resistant Ad hoc Routing Protocols)

- TIARA (Techniques for intrusion resistant ad hoc routing protocols): a set of design techniques mainly against denial-of-service attacks
  - Multi path routing: discover and maintain all routes for data flow
  - Each node has a policy that defines the list of authorized flows that can be forwarded by the node
  - Sequence numbers: provide a countermeasure for replay attacks
  - Fast authentication instead of IPsec, but no guidelines on how to realize it

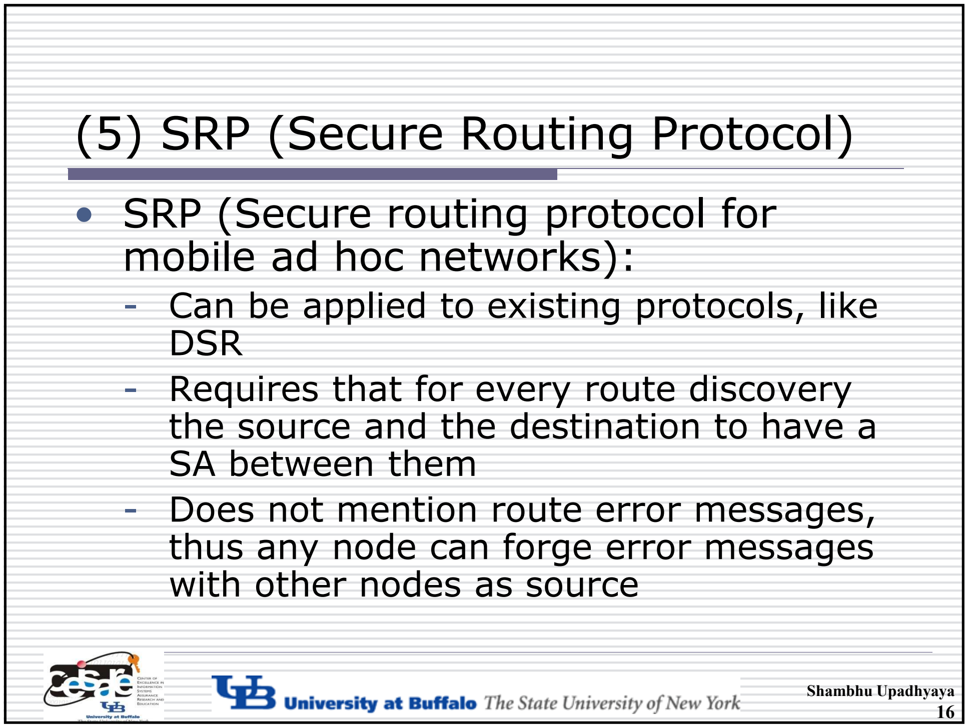
(3) SAR (Security Aware Ad hoc Routing)

- SAR (Security aware ad hoc routing):
  - Introduces a negotiable metric to discover secure routes
  - Security properties like time stamp, sequence number, authentication, integrity, etc. have a cost and performance penalty, thus affect the secure route discovery
  - The security metric is embedded into RREQ packets
  - A RREQ can be processed or forwarded only if the node can provide the required security (or has the required authorization)



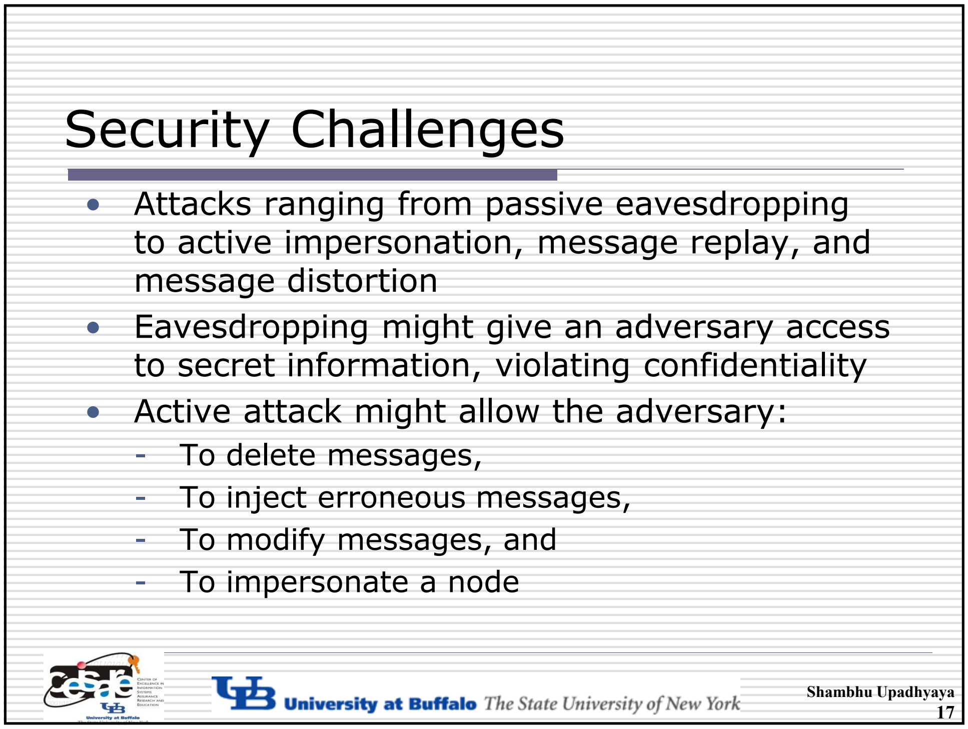
(4) ARAN (Authenticated Routing for Ad hoc Networks)

- ARAN (Authenticated routing for ad hoc networks):
  - Requires a trusted certification authority
  - Every node that forwards a RREQ or a RREP must also sign it (in addition to heavyweight computations, the size of the routing messages increases at each hop)
  - Prone to replay attacks if the nodes do not have time synchronization (difficult to achieve, especially in an ad hoc environment)



(5) SRP (Secure Routing Protocol)

- SRP (Secure routing protocol for mobile ad hoc networks):
  - Can be applied to existing protocols, like DSR
  - Requires that for every route discovery the source and the destination to have a SA between them
  - Does not mention route error messages, thus any node can forge error messages with other nodes as source

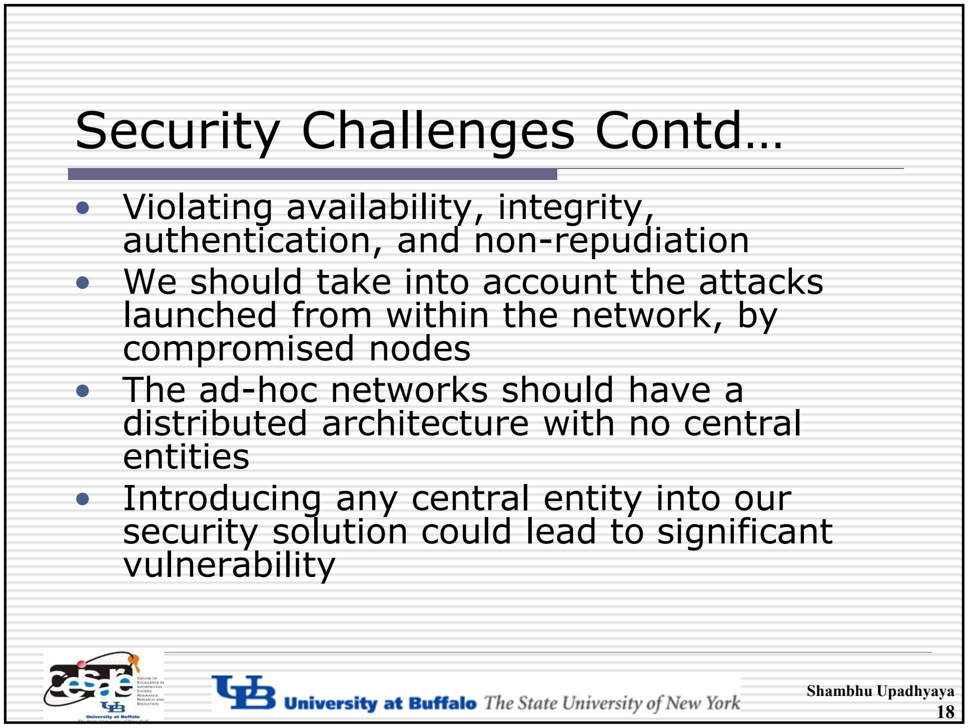


Security Challenges

- Attacks ranging from passive eavesdropping to active impersonation, message replay, and message distortion
- Eavesdropping might give an adversary access to secret information, violating confidentiality
- Active attack might allow the adversary:
  - To delete messages,
  - To inject erroneous messages,
  - To modify messages, and
  - To impersonate a node

University at Buffalo *The State University of New York*

Shambhu Upadhyaya
17

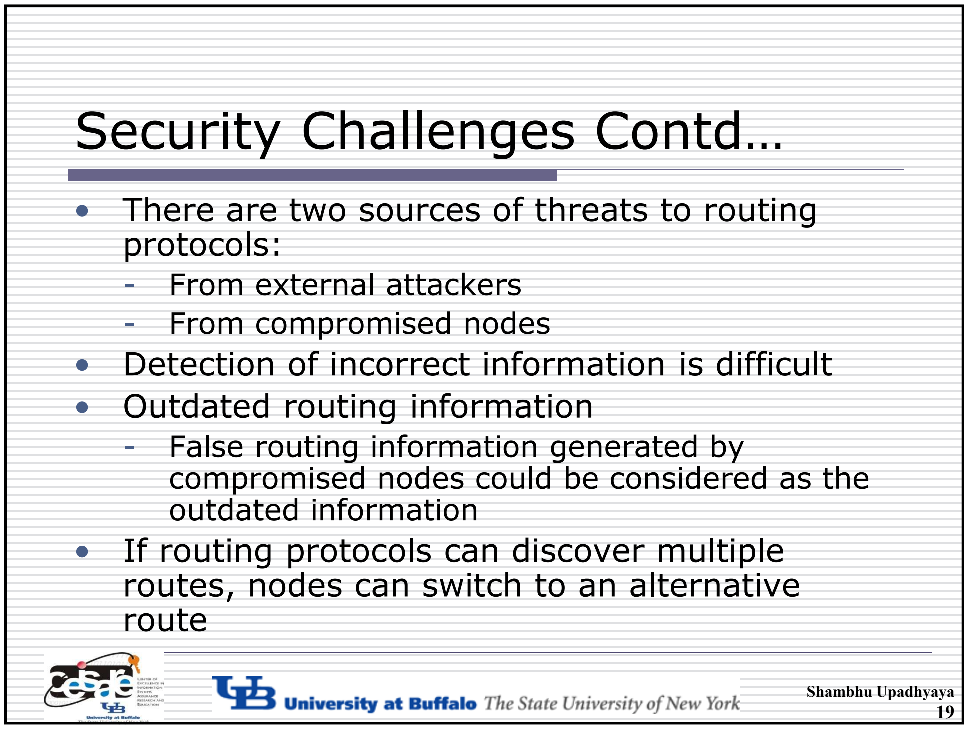


Security Challenges Contd…

- Violating availability, integrity, authentication, and non-repudiation
- We should take into account the attacks launched from within the network, by compromised nodes
- The ad-hoc networks should have a distributed architecture with no central entities
- Introducing any central entity into our security solution could lead to significant vulnerability

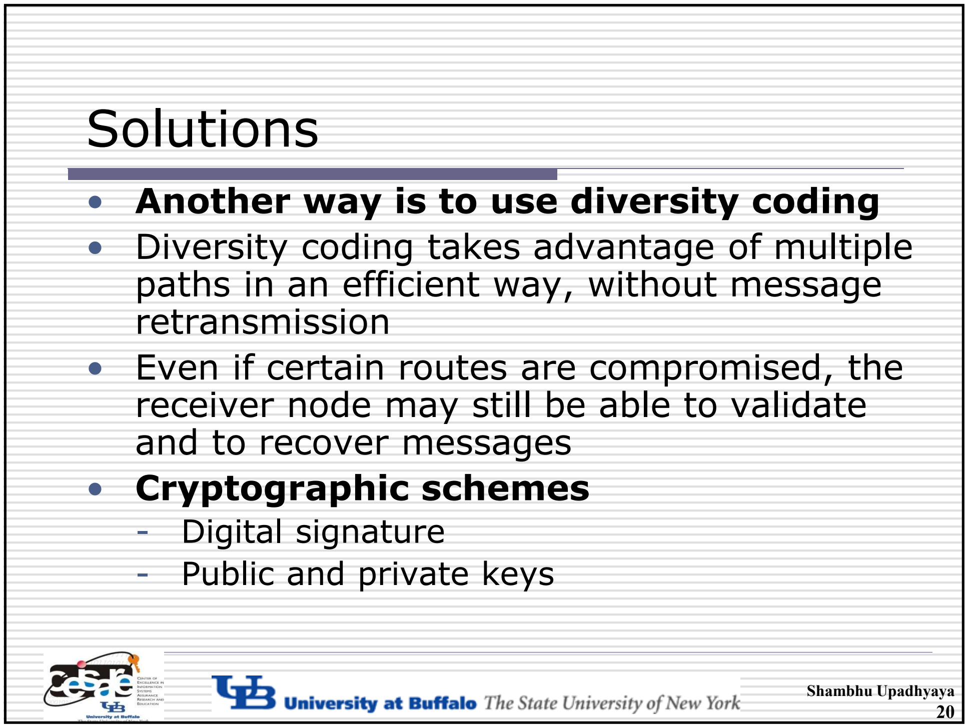
University at Buffalo *The State University of New York*

Shambhu Upadhyaya
18



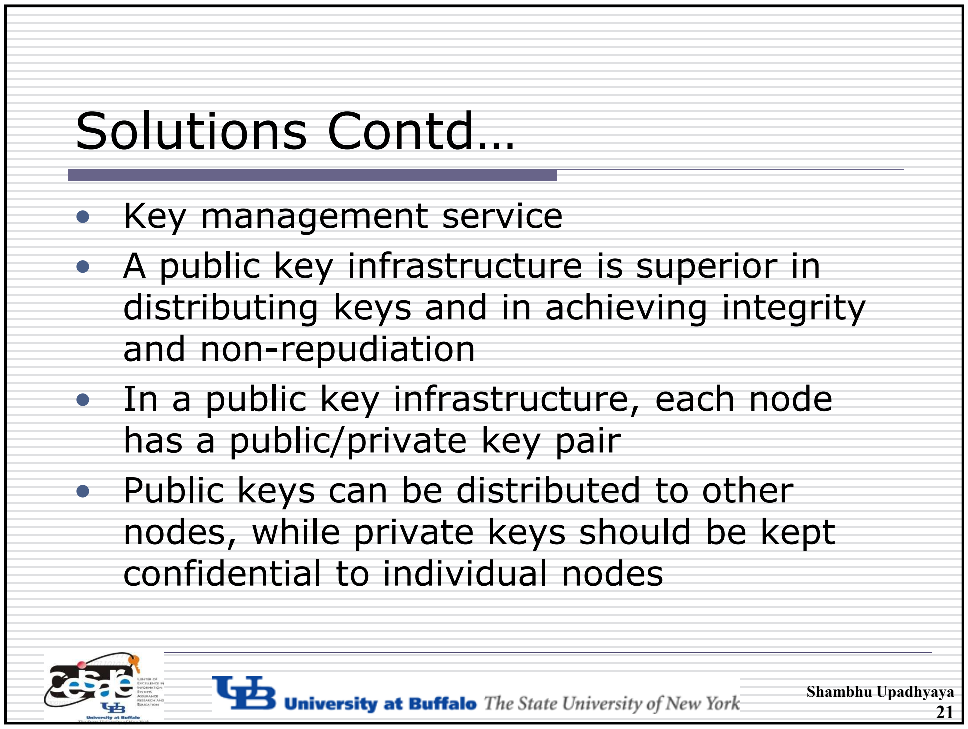
Security Challenges Contd…

- There are two sources of threats to routing protocols:
  - From external attackers
  - From compromised nodes
- Detection of incorrect information is difficult
- Outdated routing information
  - False routing information generated by compromised nodes could be considered as the outdated information
- If routing protocols can discover multiple routes, nodes can switch to an alternative route



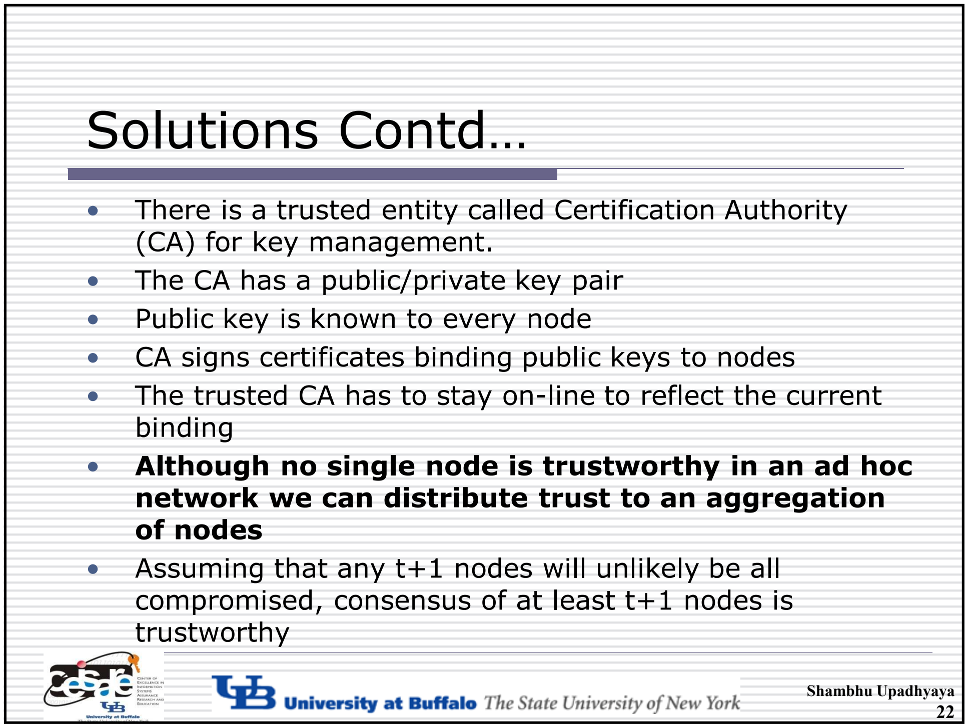
Solutions

- **Another way is to use diversity coding**
- Diversity coding takes advantage of multiple paths in an efficient way, without message retransmission
- Even if certain routes are compromised, the receiver node may still be able to validate and to recover messages
- **Cryptographic schemes**
  - Digital signature
  - Public and private keys



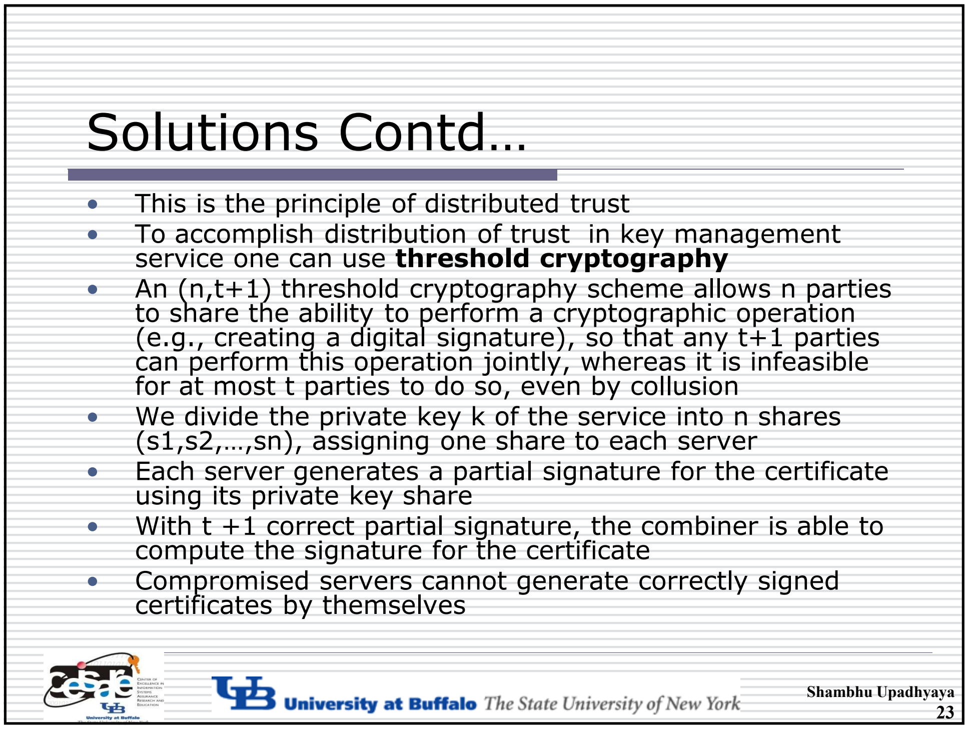
Solutions Contd…

- Key management service
- A public key infrastructure is superior in distributing keys and in achieving integrity and non-repudiation
- In a public key infrastructure, each node has a public/private key pair
- Public keys can be distributed to other nodes, while private keys should be kept confidential to individual nodes



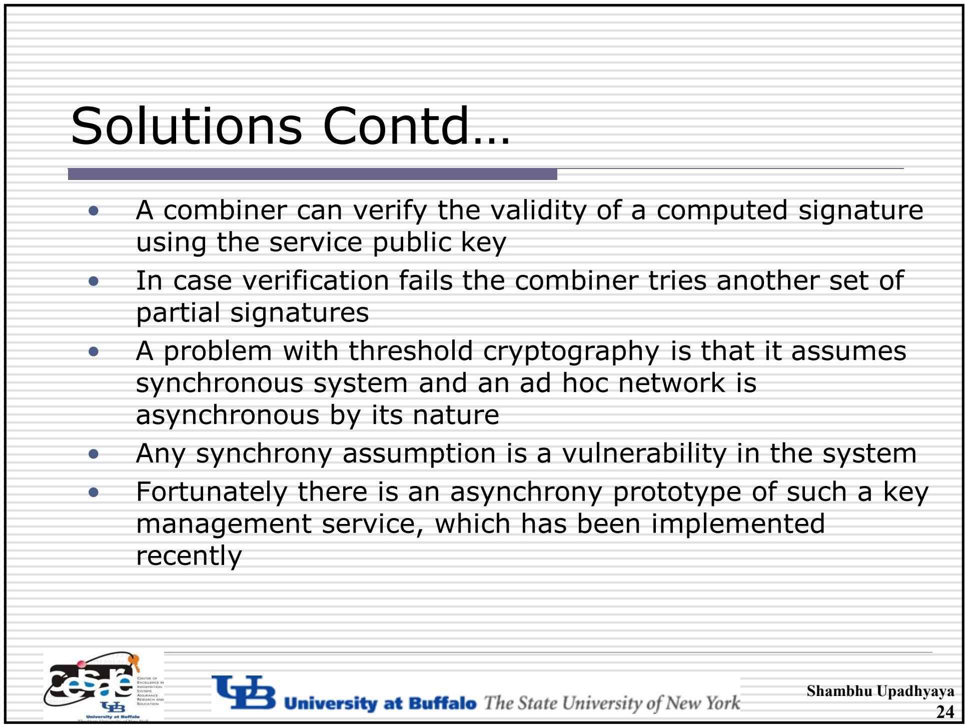
Solutions Contd…

- There is a trusted entity called Certification Authority (CA) for key management.
- The CA has a public/private key pair
- Public key is known to every node
- CA signs certificates binding public keys to nodes
- The trusted CA has to stay on-line to reflect the current binding
- **Although no single node is trustworthy in an ad hoc network we can distribute trust to an aggregation of nodes**
- Assuming that any t+1 nodes will unlikely be all compromised, consensus of at least t+1 nodes is trustworthy



Solutions Contd…

- This is the principle of distributed trust
- To accomplish distribution of trust in key management service one can use **threshold cryptography**
- An (n,t+1) threshold cryptography scheme allows n parties to share the ability to perform a cryptographic operation (e.g., creating a digital signature), so that any t+1 parties can perform this operation jointly, whereas it is infeasible for at most t parties to do so, even by collusion
- We divide the private key k of the service into n shares (s1,s2,…,sn), assigning one share to each server
- Each server generates a partial signature for the certificate using its private key share
- With t +1 correct partial signature, the combiner is able to compute the signature for the certificate
- Compromised servers cannot generate correctly signed certificates by themselves



Solutions Contd…

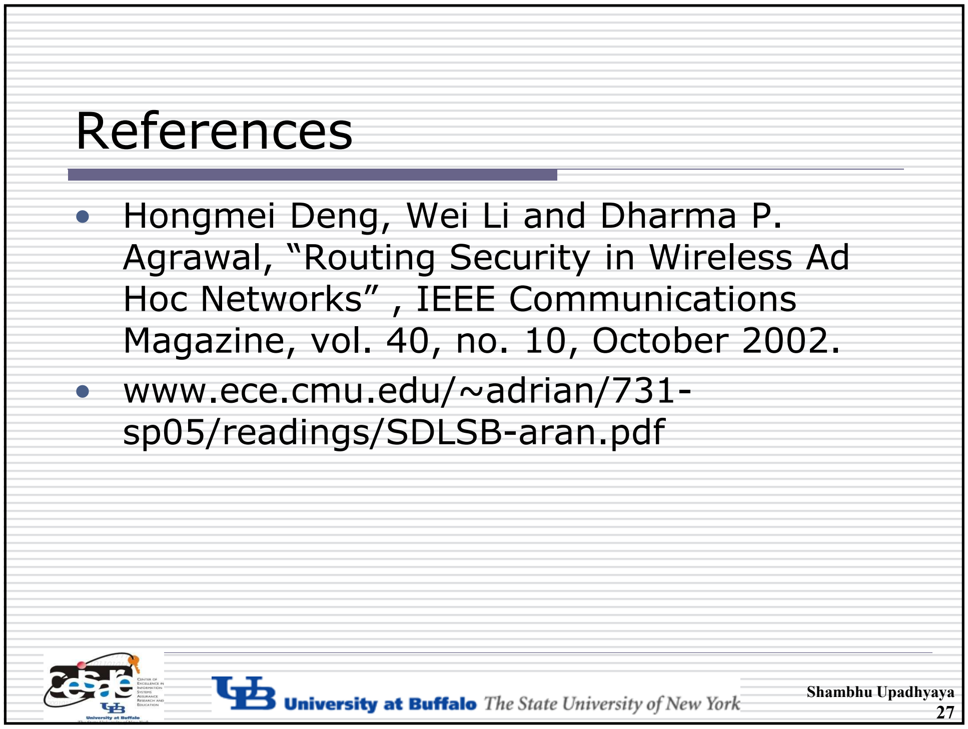
- A combiner can verify the validity of a computed signature using the service public key
- In case verification fails the combiner tries another set of partial signatures
- A problem with threshold cryptography is that it assumes synchronous system and an ad hoc network is asynchronous by its nature
- Any synchrony assumption is a vulnerability in the system
- Fortunately there is an asynchrony prototype of such a key management service, which has been implemented recently

Other Proposed Solutions

- SEAD (Secure efficient distance vector routing for mobile ad hoc networks): Employs hash chains to authenticate hop counts and sequence numbers
- Ariadne: same operational principles as SEAD, but based on DSR
- Both require clock synchronization between the participating nodes which is an unrealistic requirement for ad hoc environments

Summary

- If there is no security in the routing protocol active attackers can easily exploit, even completely disable, an ad hoc network
- Current ad hoc routing protocols are completely insecure
- Existing secure routing mechanisms are either too expensive or have unrealistic requirements
- It is difficult to find a general idea that can provide security against all kinds of attacks



References

- Hongmei Deng, Wei Li and Dharma P. Agrawal, “Routing Security in Wireless Ad Hoc Networks” , IEEE Communications Magazine, vol. 40, no. 10, October 2002.
- www.ece.cmu.edu/~adrian/731-sp05/readings/SDLSB-aran.pdf