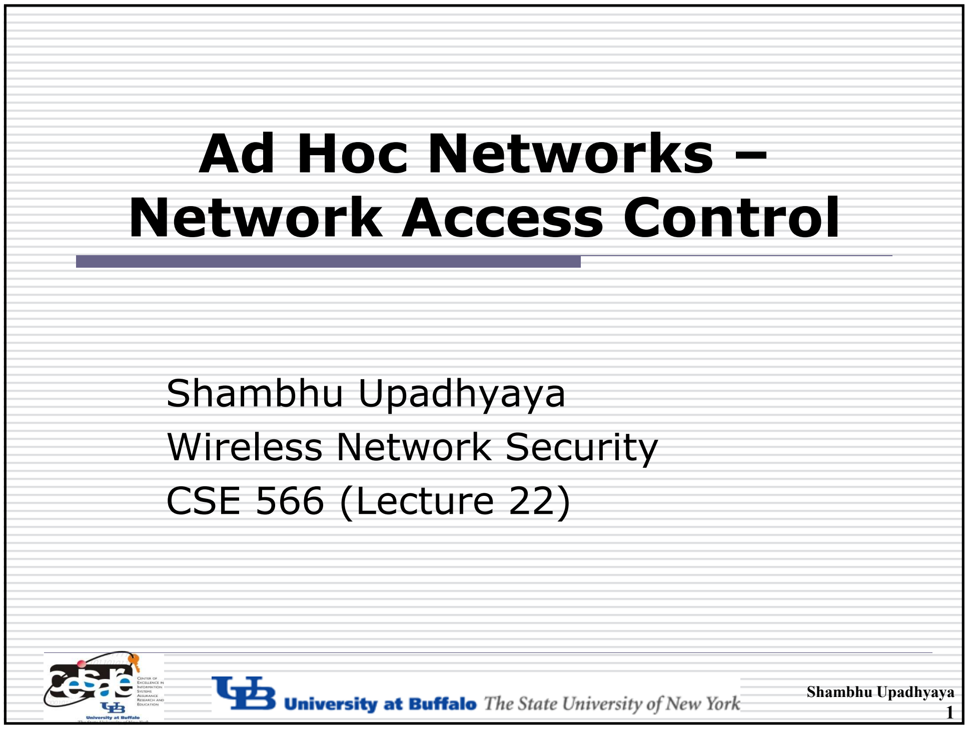
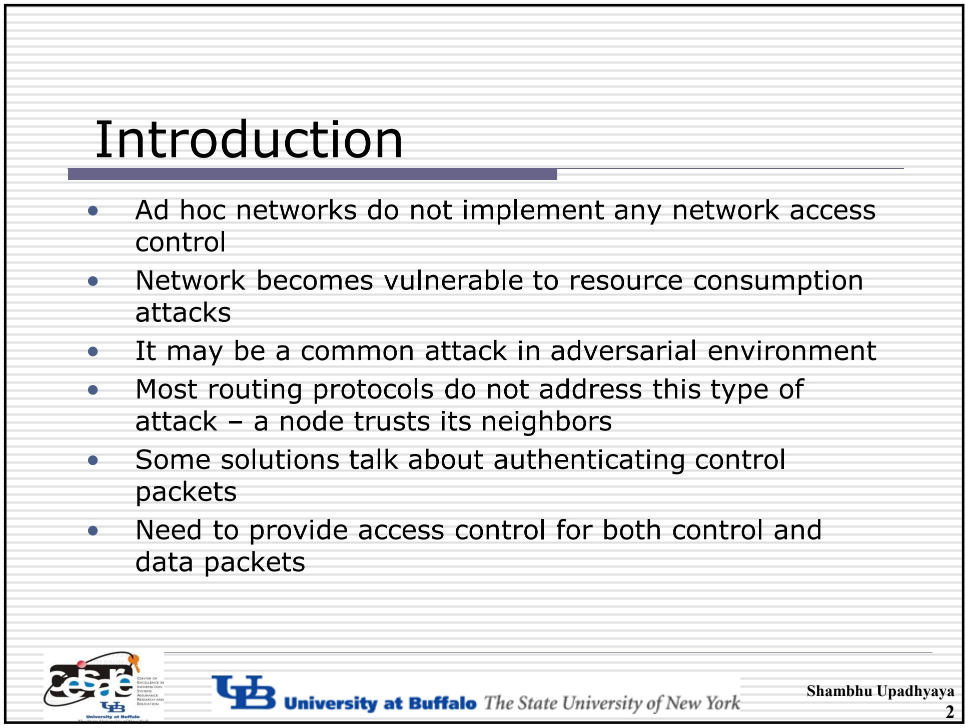


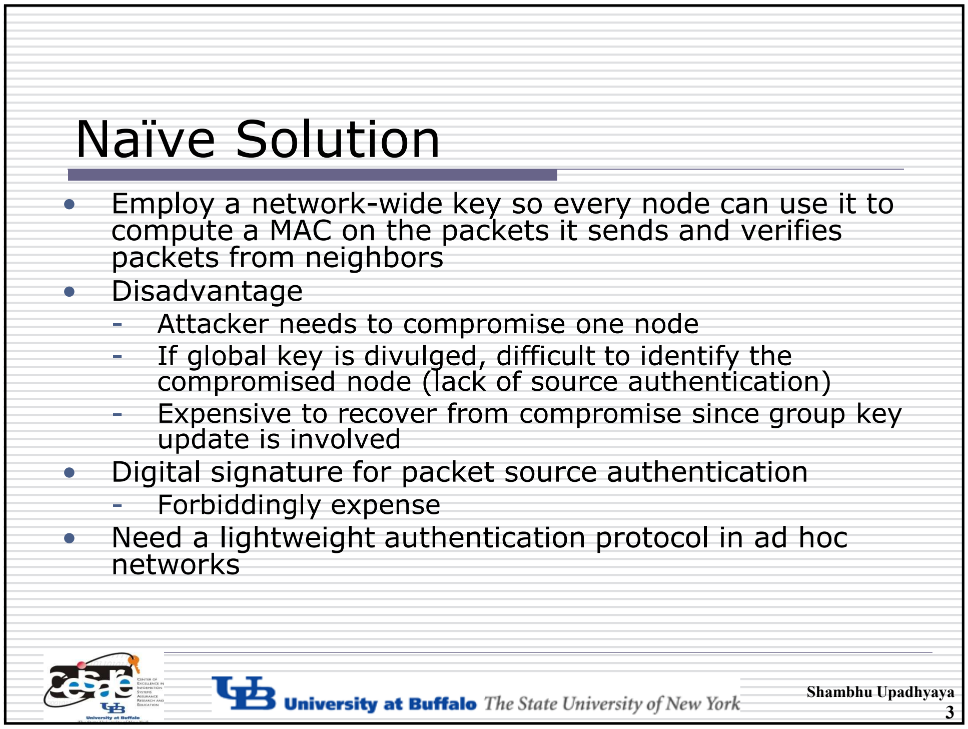
Ad Hoc Networks – Network Access Control

Shambhu Upadhyaya
Wireless Network Security
CSE 566 (Lecture 22)



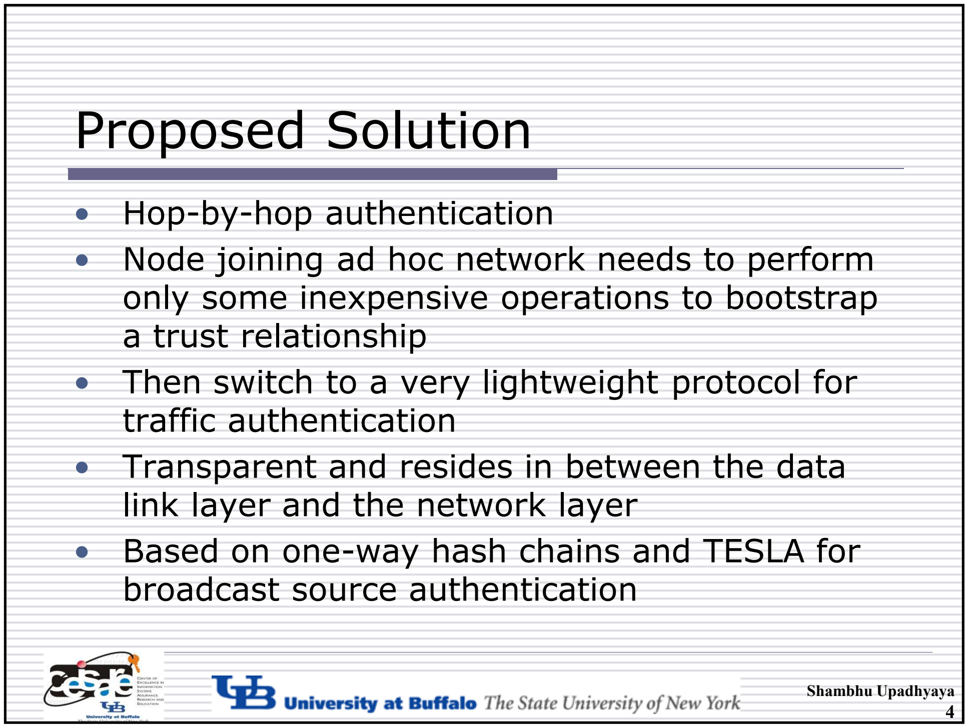
Introduction

- Ad hoc networks do not implement any network access control
- Network becomes vulnerable to resource consumption attacks
- It may be a common attack in adversarial environment
- Most routing protocols do not address this type of attack – a node trusts its neighbors
- Some solutions talk about authenticating control packets
- Need to provide access control for both control and data packets



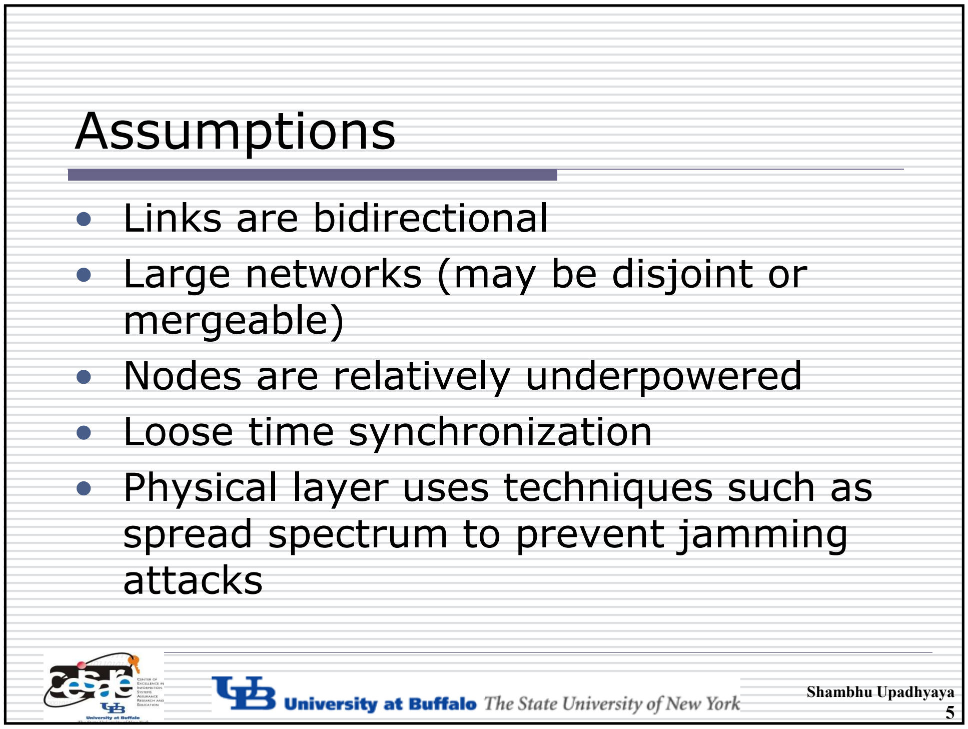
Naïve Solution

- Employ a network-wide key so every node can use it to compute a MAC on the packets it sends and verifies packets from neighbors
- Disadvantage
  - Attacker needs to compromise one node
  - If global key is divulged, difficult to identify the compromised node (lack of source authentication)
  - Expensive to recover from compromise since group key update is involved
- Digital signature for packet source authentication
  - Forbiddingly expense
- Need a lightweight authentication protocol in ad hoc networks



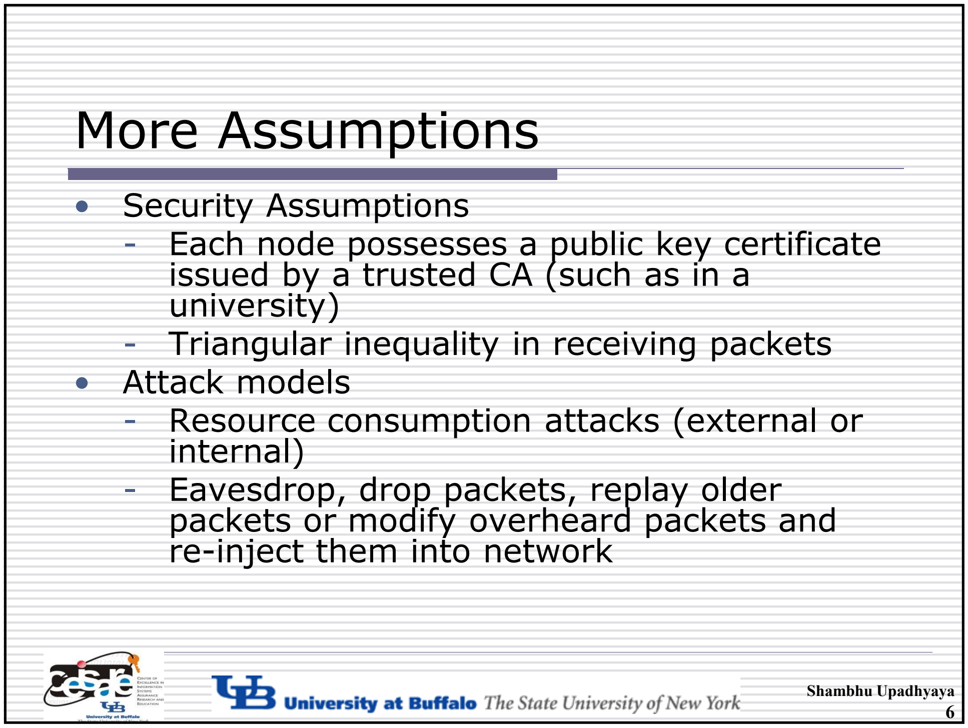
Proposed Solution

- Hop-by-hop authentication
- Node joining ad hoc network needs to perform only some inexpensive operations to bootstrap a trust relationship
- Then switch to a very lightweight protocol for traffic authentication
- Transparent and resides in between the data link layer and the network layer
- Based on one-way hash chains and TESLA for broadcast source authentication



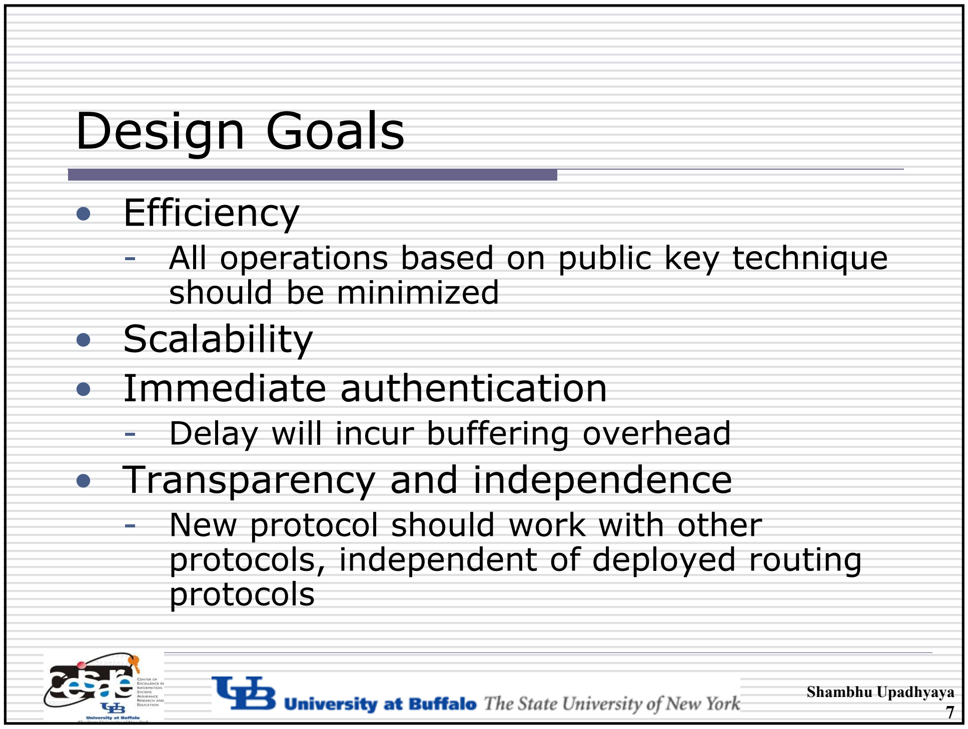
Assumptions

- Links are bidirectional
- Large networks (may be disjoint or mergeable)
- Nodes are relatively underpowered
- Loose time synchronization
- Physical layer uses techniques such as spread spectrum to prevent jamming attacks



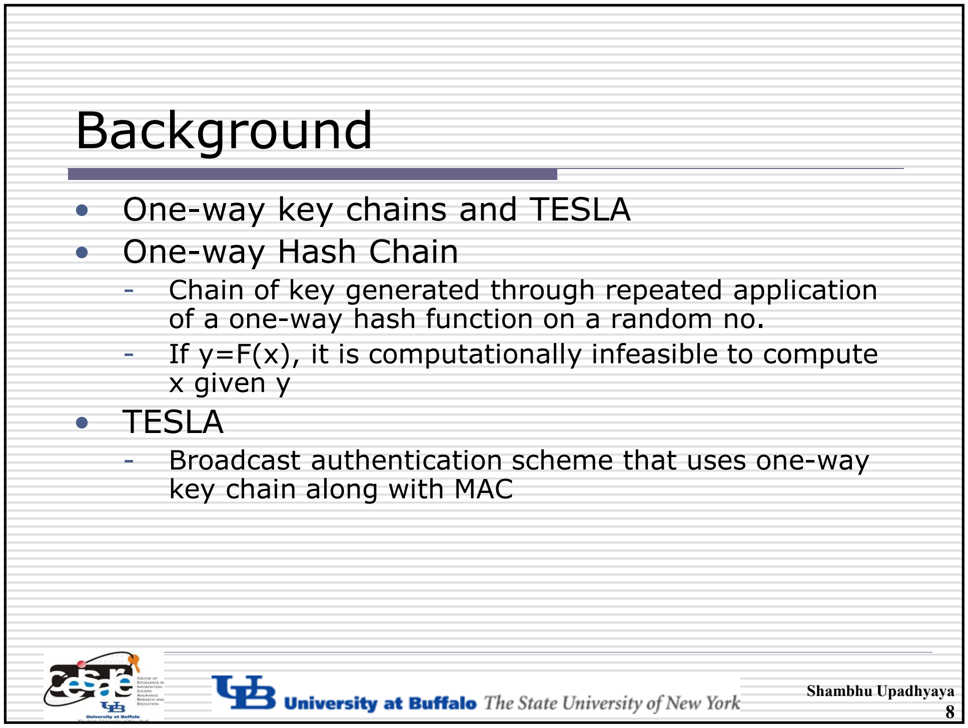
More Assumptions

- Security Assumptions
  - Each node possesses a public key certificate issued by a trusted CA (such as in a university)
  - Triangular inequality in receiving packets
- Attack models
  - Resource consumption attacks (external or internal)
  - Eavesdrop, drop packets, replay older packets or modify overheard packets and re-inject them into network



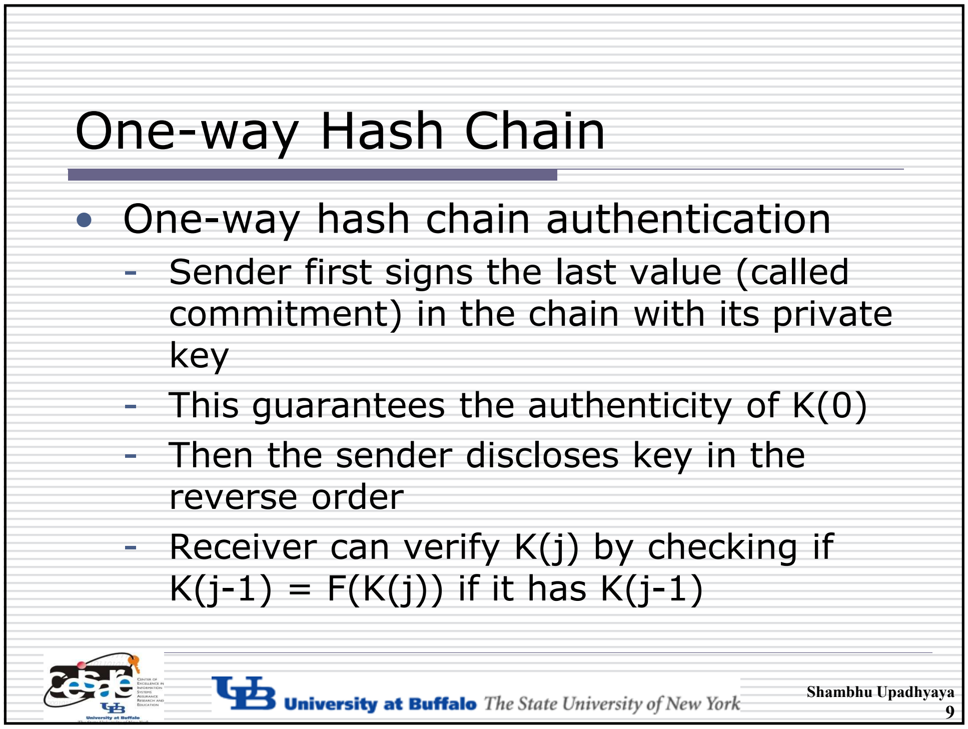
Design Goals

- Efficiency
  - All operations based on public key technique should be minimized
- Scalability
- Immediate authentication
  - Delay will incur buffering overhead
- Transparency and independence
  - New protocol should work with other protocols, independent of deployed routing protocols



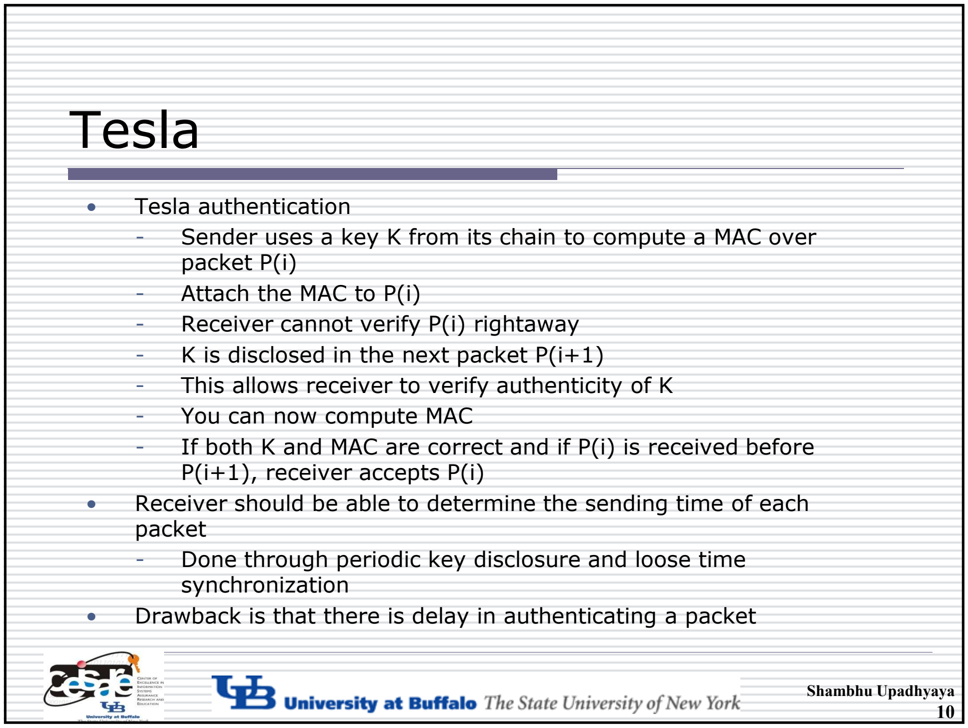
Background

- One-way key chains and TESLA
- One-way Hash Chain
  - Chain of key generated through repeated application of a one-way hash function on a random no.
  - If y=F(x), it is computationally infeasible to compute x given y
- TESLA
  - Broadcast authentication scheme that uses one-way key chain along with MAC



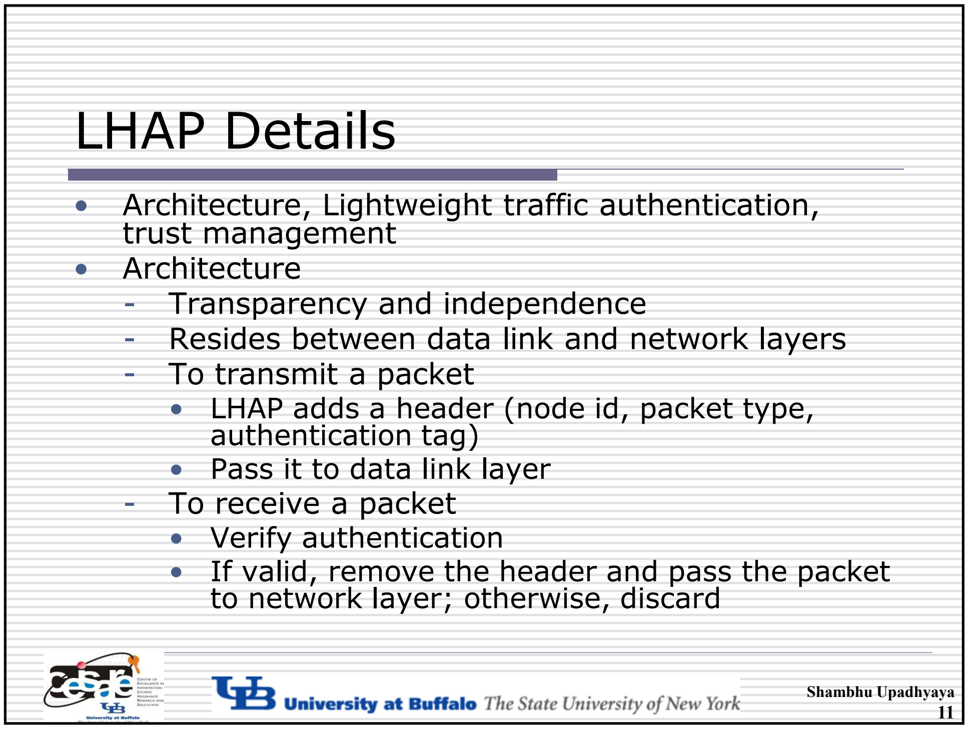
One-way Hash Chain

- One-way hash chain authentication
  - Sender first signs the last value (called commitment) in the chain with its private key
  - This guarantees the authenticity of K(0)
  - Then the sender discloses key in the reverse order
  - Receiver can verify K(j) by checking if K(j-1) = F(K(j)) if it has K(j-1)



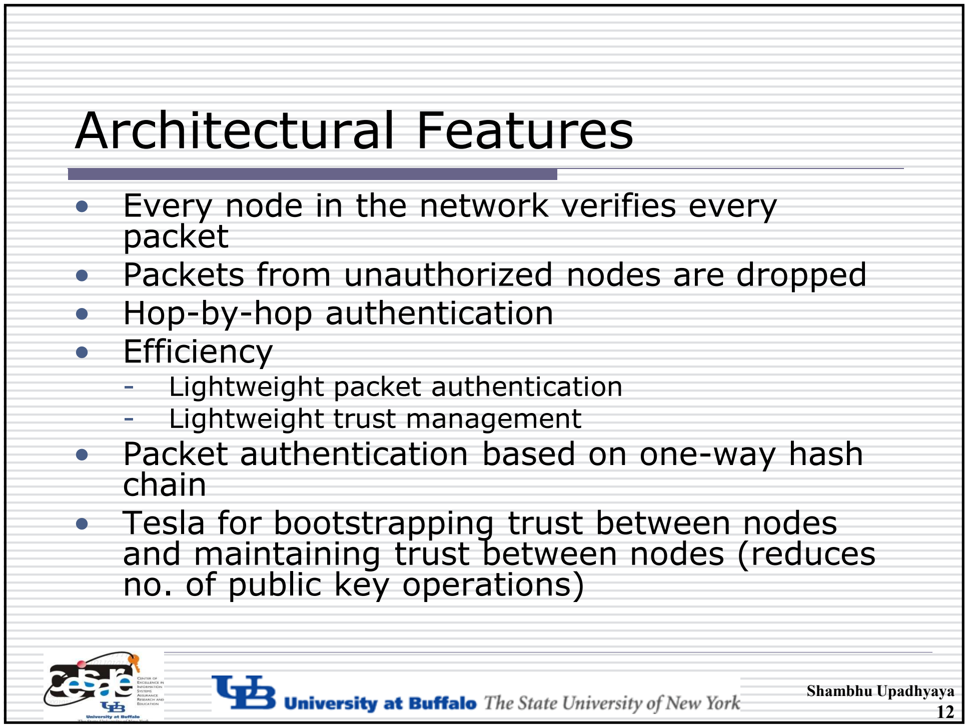
Tesla

- Tesla authentication
  - Sender uses a key K from its chain to compute a MAC over packet P(i)
  - Attach the MAC to P(i)
  - Receiver cannot verify P(i) rightaway
  - K is disclosed in the next packet P(i+1)
  - This allows receiver to verify authenticity of K
  - You can now compute MAC
  - If both K and MAC are correct and if P(i) is received before P(i+1), receiver accepts P(i)
- Receiver should be able to determine the sending time of each packet
  - Done through periodic key disclosure and loose time synchronization
- Drawback is that there is delay in authenticating a packet



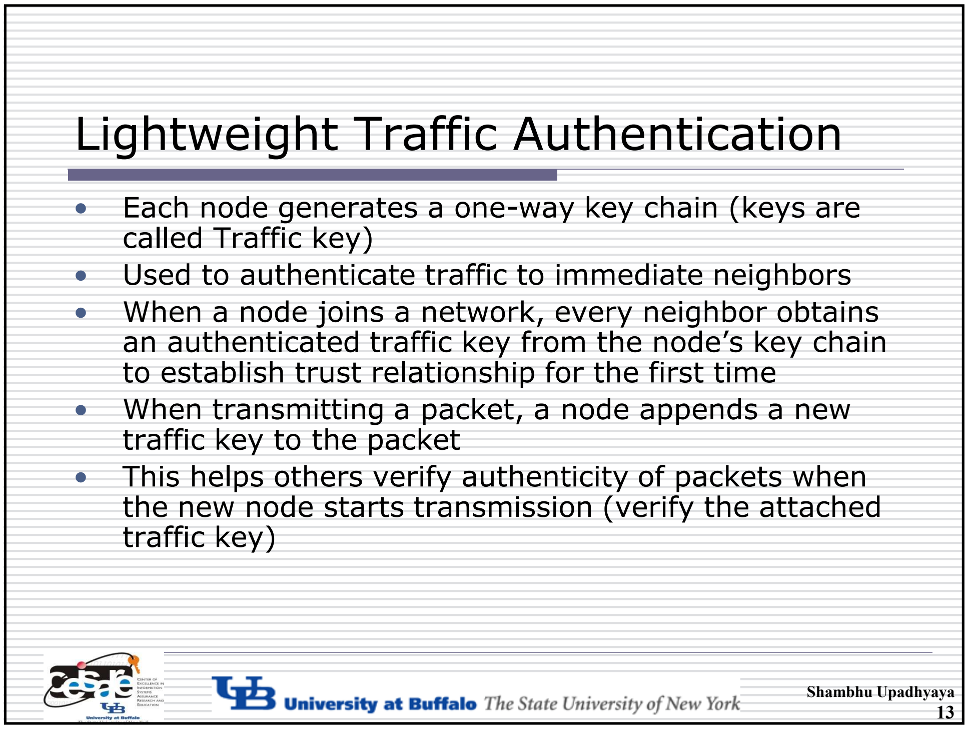
LHAP Details

- Architecture, Lightweight traffic authentication, trust management
- Architecture
  - Transparency and independence
  - Resides between data link and network layers
  - To transmit a packet
    - LHAP adds a header (node id, packet type, authentication tag)
    - Pass it to data link layer
  - To receive a packet
    - Verify authentication
    - If valid, remove the header and pass the packet to network layer; otherwise, discard



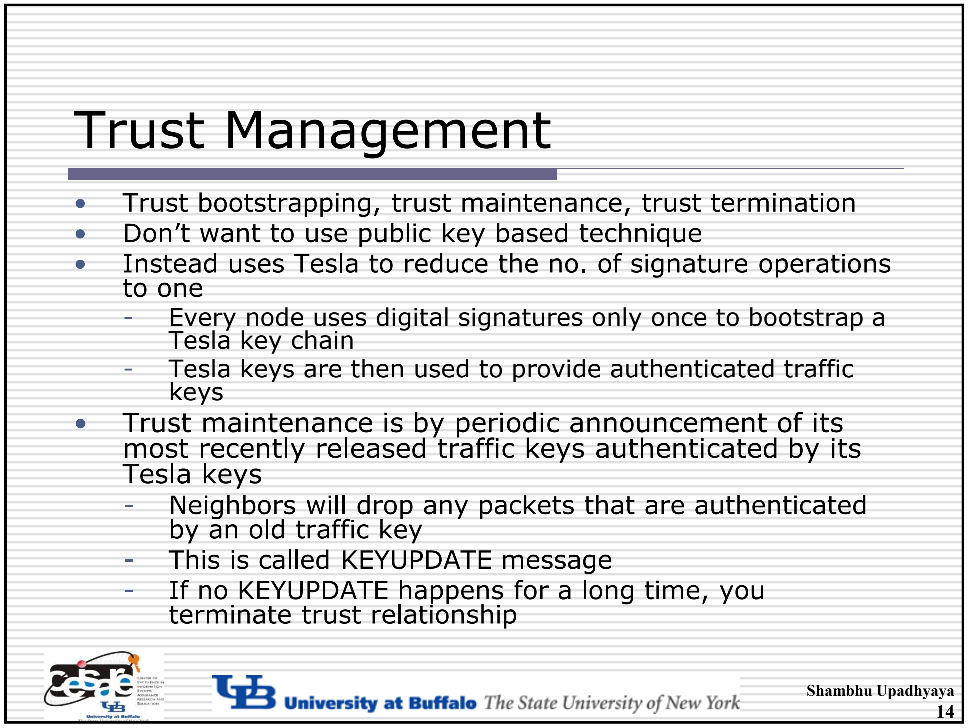
Architectural Features

- Every node in the network verifies every packet
- Packets from unauthorized nodes are dropped
- Hop-by-hop authentication
- Efficiency
  - Lightweight packet authentication
  - Lightweight trust management
- Packet authentication based on one-way hash chain
- Tesla for bootstrapping trust between nodes and maintaining trust between nodes (reduces no. of public key operations)



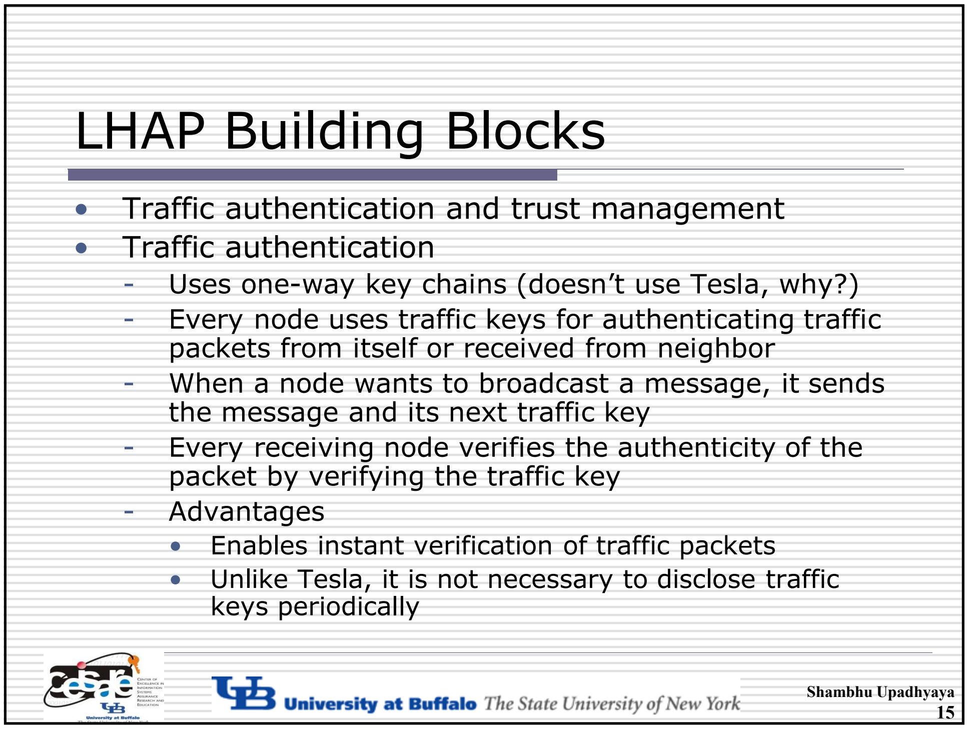
Lightweight Traffic Authentication

- Each node generates a one-way key chain (keys are called Traffic key)
- Used to authenticate traffic to immediate neighbors
- When a node joins a network, every neighbor obtains an authenticated traffic key from the node’s key chain to establish trust relationship for the first time
- When transmitting a packet, a node appends a new traffic key to the packet
- This helps others verify authenticity of packets when the new node starts transmission (verify the attached traffic key)



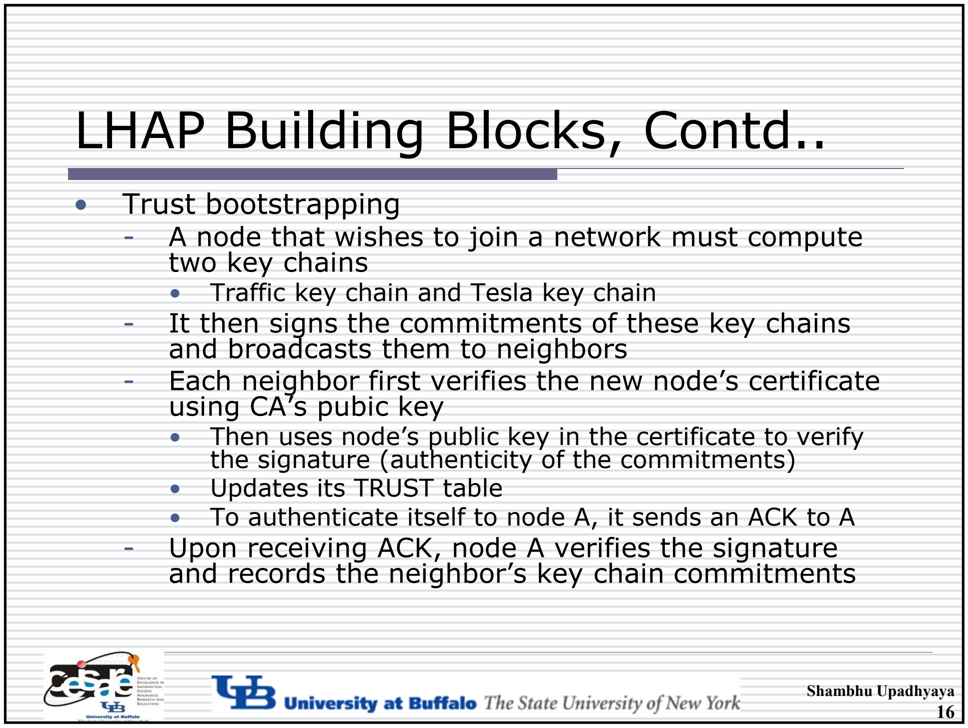
Trust Management

- Trust bootstrapping, trust maintenance, trust termination
- Don’t want to use public key based technique
- Instead uses Tesla to reduce the no. of signature operations to one
  - Every node uses digital signatures only once to bootstrap a Tesla key chain
  - Tesla keys are then used to provide authenticated traffic keys
- Trust maintenance is by periodic announcement of its most recently released traffic keys authenticated by its Tesla keys
  - Neighbors will drop any packets that are authenticated by an old traffic key
  - This is called KEYUPDATE message
  - If no KEYUPDATE happens for a long time, you terminate trust relationship



LHAP Building Blocks

- Traffic authentication and trust management
- Traffic authentication
  - Uses one-way key chains (doesn’t use Tesla, why?)
  - Every node uses traffic keys for authenticating traffic packets from itself or received from neighbor
  - When a node wants to broadcast a message, it sends the message and its next traffic key
  - Every receiving node verifies the authenticity of the packet by verifying the traffic key
  - Advantages
    - Enables instant verification of traffic packets
    - Unlike Tesla, it is not necessary to disclose traffic keys periodically



LHAP Building Blocks, Contd..

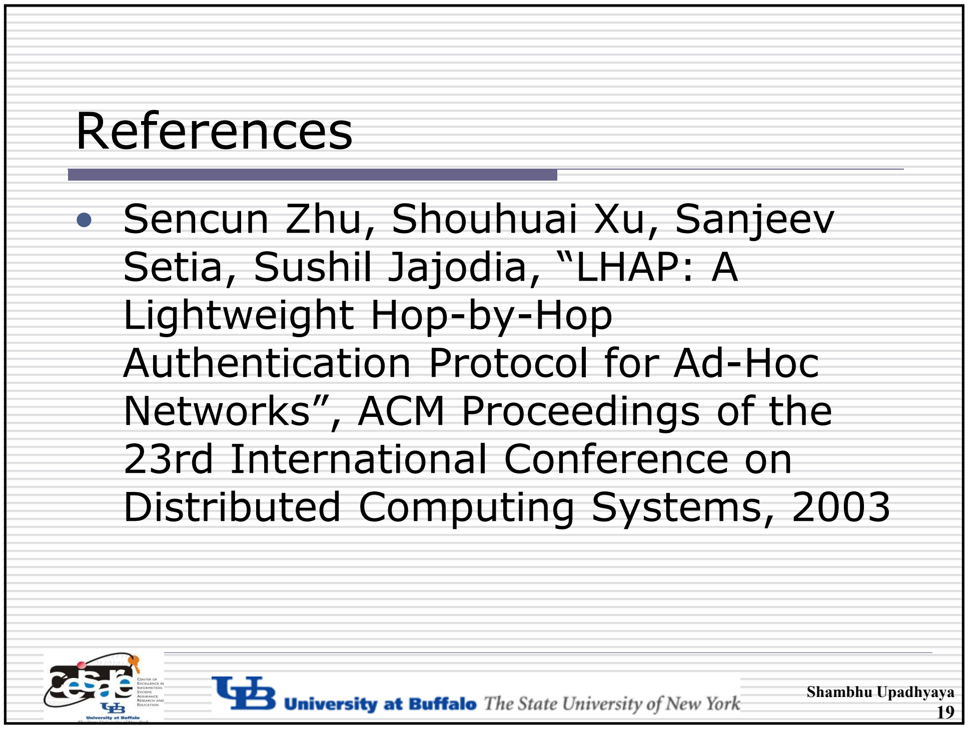
- Trust bootstrapping
  - A node that wishes to join a network must compute two key chains
    - Traffic key chain and Tesla key chain
  - It then signs the commitments of these key chains and broadcasts them to neighbors
  - Each neighbor first verifies the new node’s certificate using CA’s pubic key
    - Then uses node’s public key in the certificate to verify the signature (authenticity of the commitments)
    - Updates its TRUST table
    - To authenticate itself to node A, it sends an ACK to A
  - Upon receiving ACK, node A verifies the signature and records the neighbor’s key chain commitments

LHAP Building Blocks, Contd..

- Maintenance
  - Periodically each node broadcasts a KEYUPDATE message to neighbors
  - Update the TRUST tables accordingly
- Termination
  - When a compromised node is detected and announced (permanent)
  - If a node doesn't receive a valid KEYUPDAATE message from a neighbor for longer than one Tesla interval (temporary)

Summary

- Provides protection against all kinds of attacks – outside attacks, wormhole and rushing attacks and insider attacks
- Simulation indicates that LHAP is efficient and allows a tradeoff between security and performance
  - Bandwidth overhead, and amount of normal packet drop etc. are studied



References

- Sencun Zhu, Shouhuai Xu, Sanjeev Setia, Sushil Jajodia, “LHAP: A Lightweight Hop-by-Hop Authentication Protocol for Ad-Hoc Networks”, ACM Proceedings of the 23rd International Conference on Distributed Computing Systems, 2003