CSE 707: Wireless Networks Security – Principles and Practices

Shambhu Upadhyaya

Computer Science and Engineering

University at Buffalo

Lecture 2

September 4, 2024

University at Buffalo
The State University of New York

CENTER OF EXCELLENCE IN INFORMATION SYSTEMS ASSURANCE RESEARCH AND EDUCATION

Outline

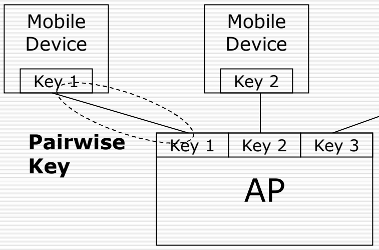
- □ TKIP and AES-CCMP (1 hour)
- □ Break
- □ Ad hoc networks security and sensor networks security (1 hour)
- □ Student presentation topics discussion

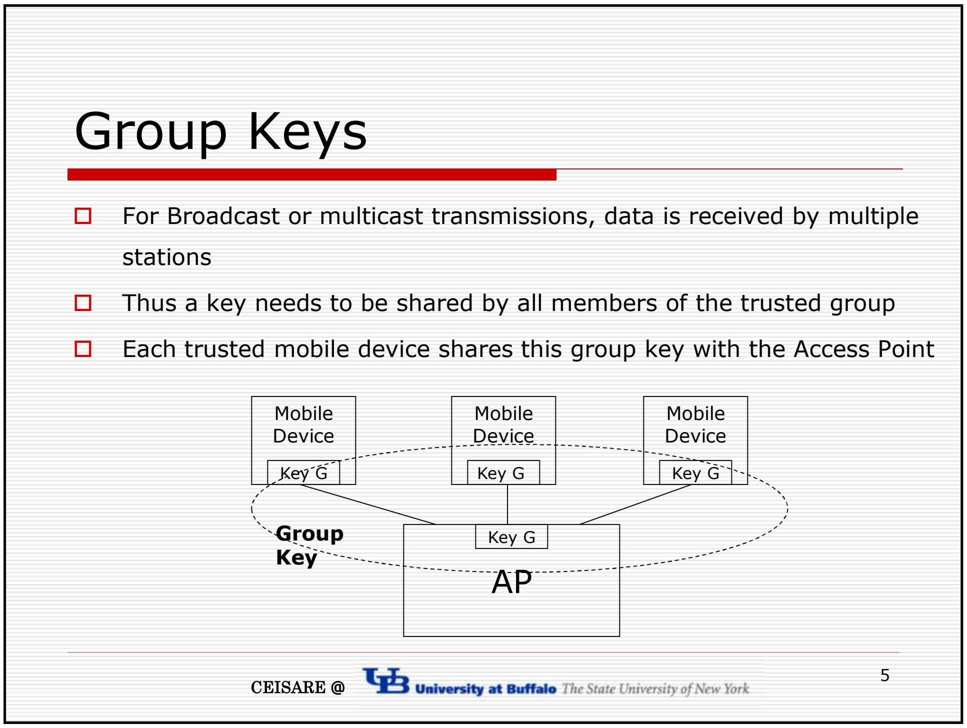
WPA and RSN Key Hierarchy

- In WEP, there is a single key
- In 802.1X model, data can start flowing once access point has the key, but WPA/RSN has more steps
- In WPA/RSN, you start with a Pairwise Master Key (PMK) at the top of the hierarchy
- Temporal keys are derived from PMK for use during each session
- PMK can be delivered from upper layer authentication protocol or can use a preshared secret (Radius can be used for this purpose)
- There exists a unique PMK for each mobile host

Pairwise Keys

- Unicast data sent between two stations has to be private
- For this purpose a pairwise key is used, know to the two parties
- Each mobile device has a unique pairwise key with the AP

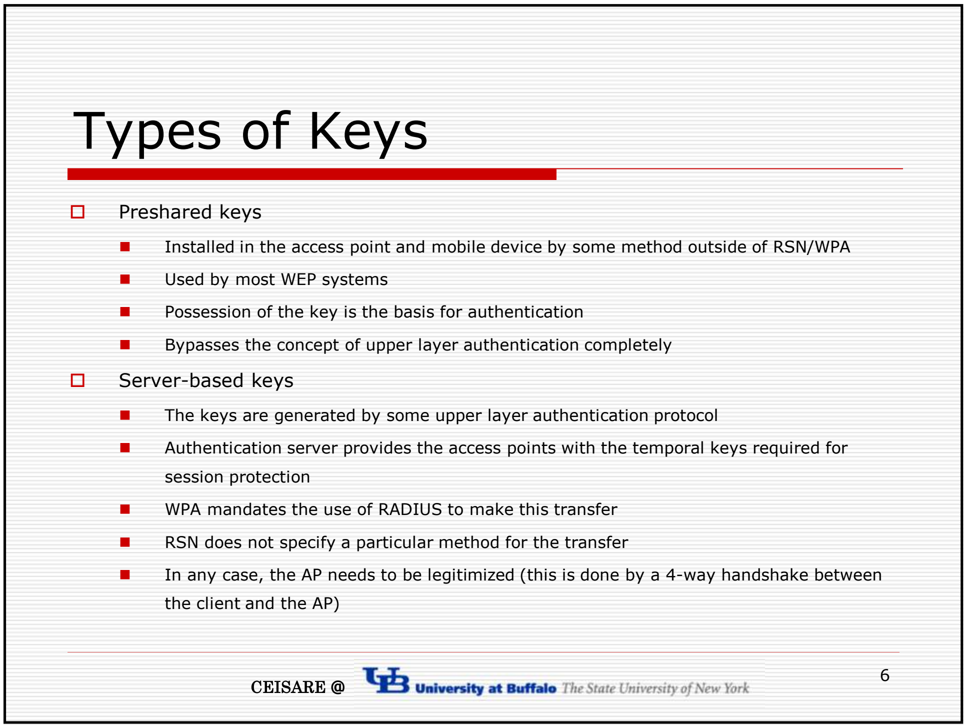




Group Keys

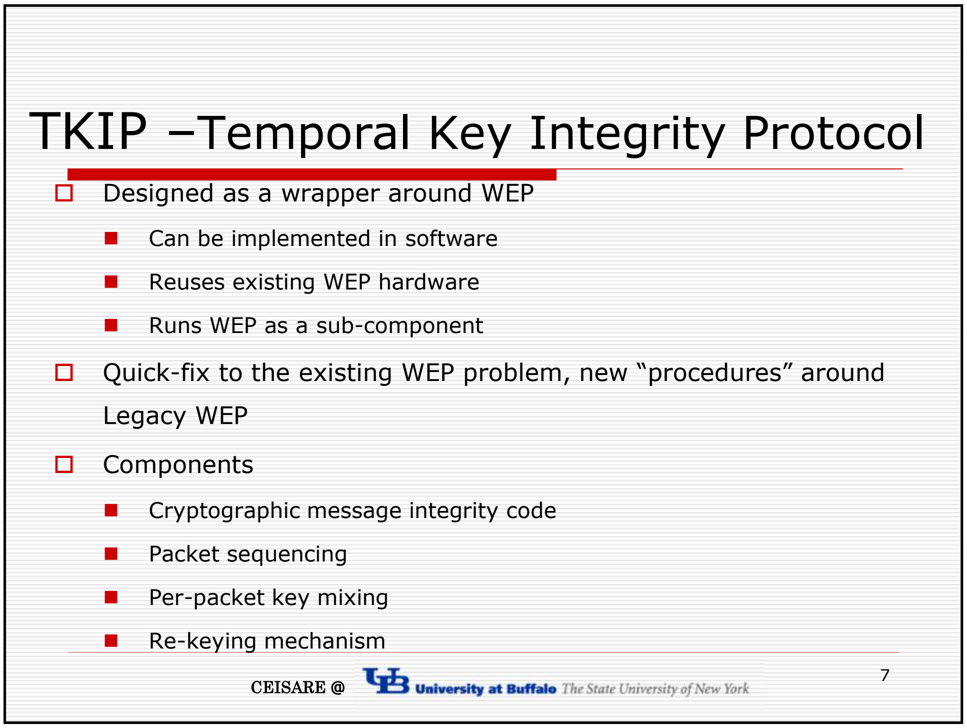
- For Broadcast or multicast transmissions, data is received by multiple stations
- Thus a key needs to be shared by all members of the trusted group
- Each trusted mobile device shares this group key with the Access Point

Mobile Device
Key G
Mobile Device
Key G
Mobile Device
Key G
Group Key
Key G
AP



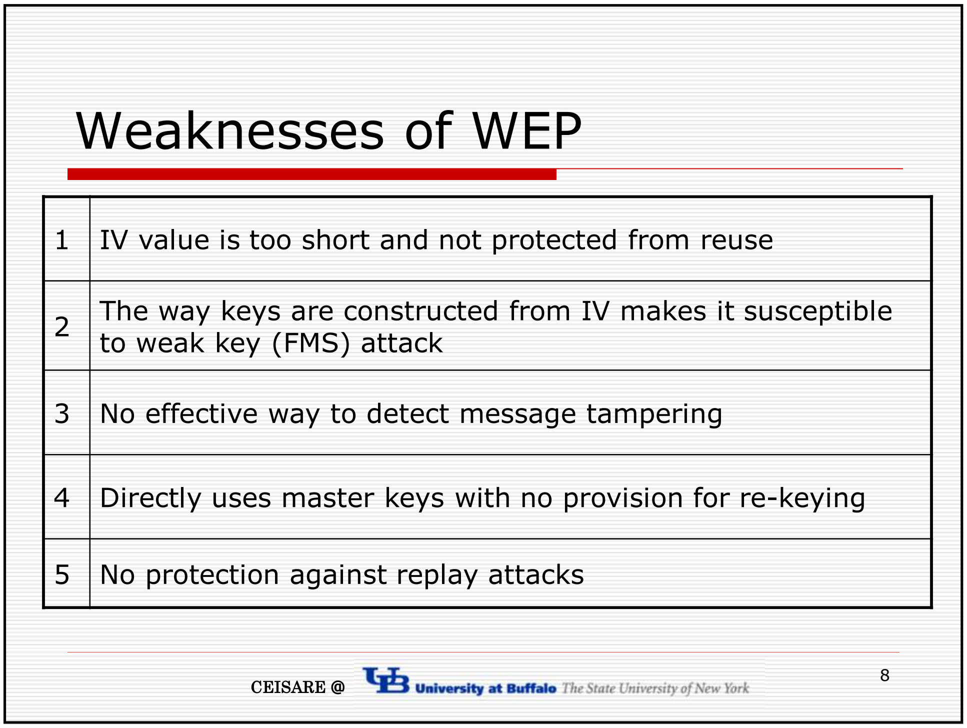
Types of Keys

- Preshared keys
  - Installed in the access point and mobile device by some method outside of RSN/WPA
  - Used by most WEP systems
  - Possession of the key is the basis for authentication
  - Bypasses the concept of upper layer authentication completely
- Server-based keys
  - The keys are generated by some upper layer authentication protocol
  - Authentication server provides the access points with the temporal keys required for session protection
  - WPA mandates the use of RADIUS to make this transfer
  - RSN does not specify a particular method for the transfer
  - In any case, the AP needs to be legitimized (this is done by a 4-way handshake between the client and the AP)



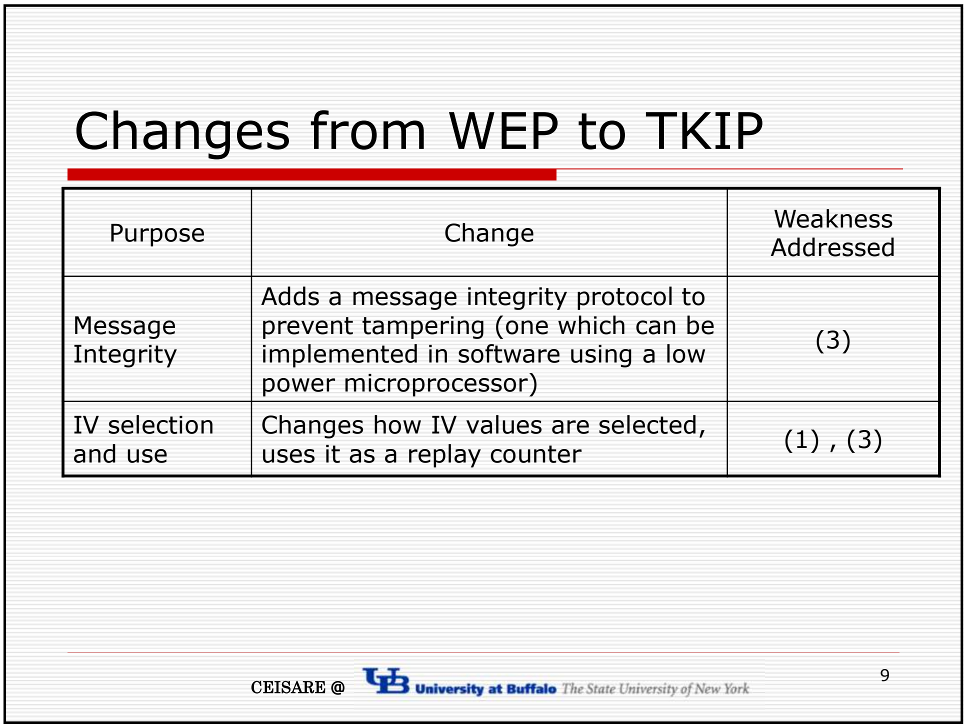
TKIP –Temporal Key Integrity Protocol

- Designed as a wrapper around WEP
  - Can be implemented in software
  - Reuses existing WEP hardware
  - Runs WEP as a sub-component
- Quick-fix to the existing WEP problem, new “procedures” around Legacy WEP
- Components
  - Cryptographic message integrity code
  - Packet sequencing
  - Per-packet key mixing
  - Re-keying mechanism



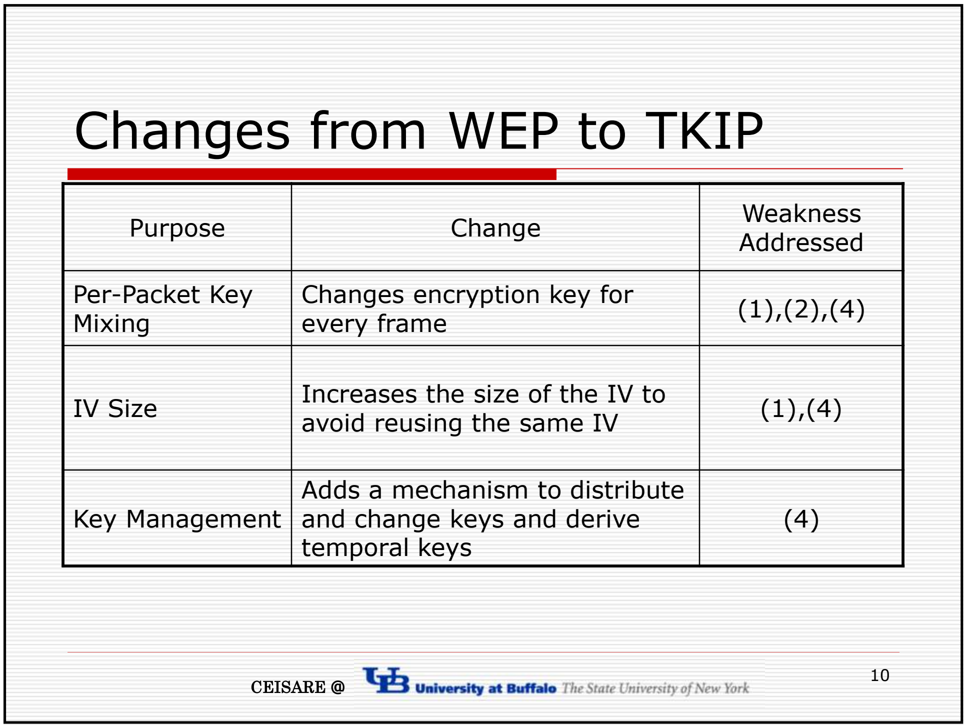
Weaknesses of WEP

1	IV value is too short and not protected from reuse
2	The way keys are constructed from IV makes it susceptible to weak key (FMS) attack
3	No effective way to detect message tampering
4	Directly uses master keys with no provision for re-keying
5	No protection against replay attacks



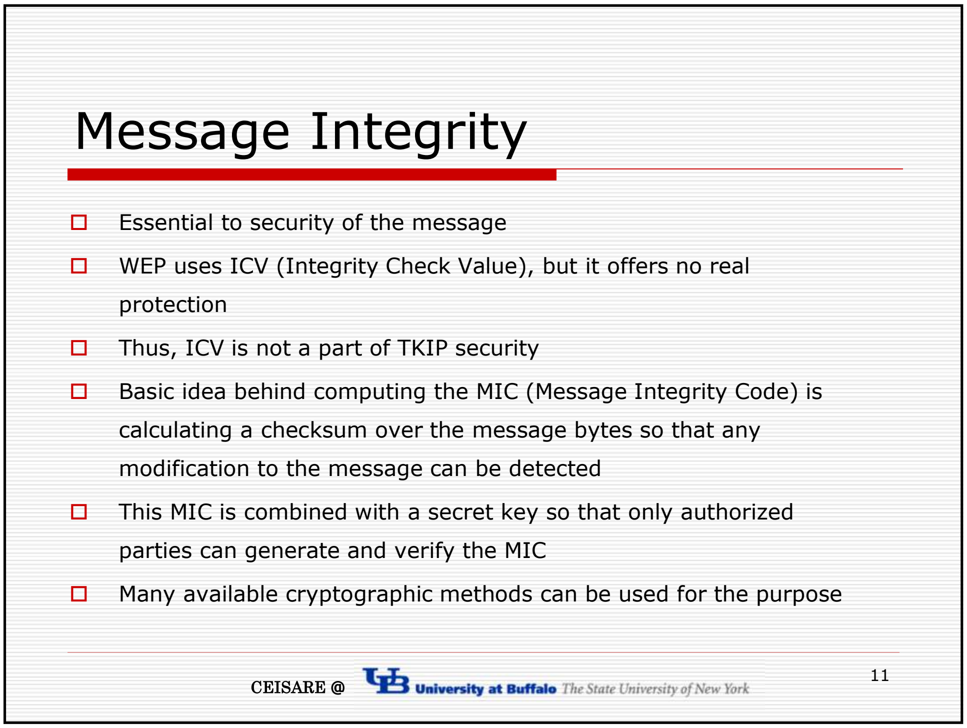
Changes from WEP to TKIP

Purpose	Change	Weakness Addressed
Message Integrity	Adds a message integrity protocol to prevent tampering (one which can be implemented in software using a low power microprocessor)	(3)
IV selection and use	Changes how IV values are selected, uses it as a replay counter	(1) , (3)



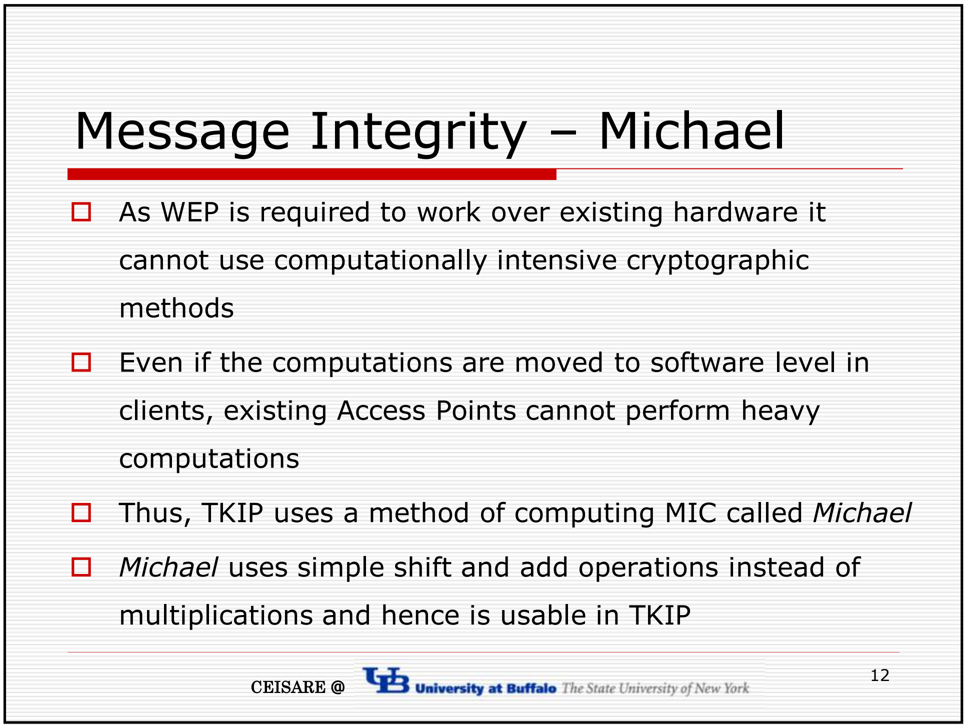
Changes from WEP to TKIP

Purpose	Change	Weakness Addressed
Per-Packet Key Mixing	Changes encryption key for every frame	(1),(2),(4)
IV Size	Increases the size of the IV to avoid reusing the same IV	(1),(4)
Key Management	Adds a mechanism to distribute and change keys and derive temporal keys	(4)



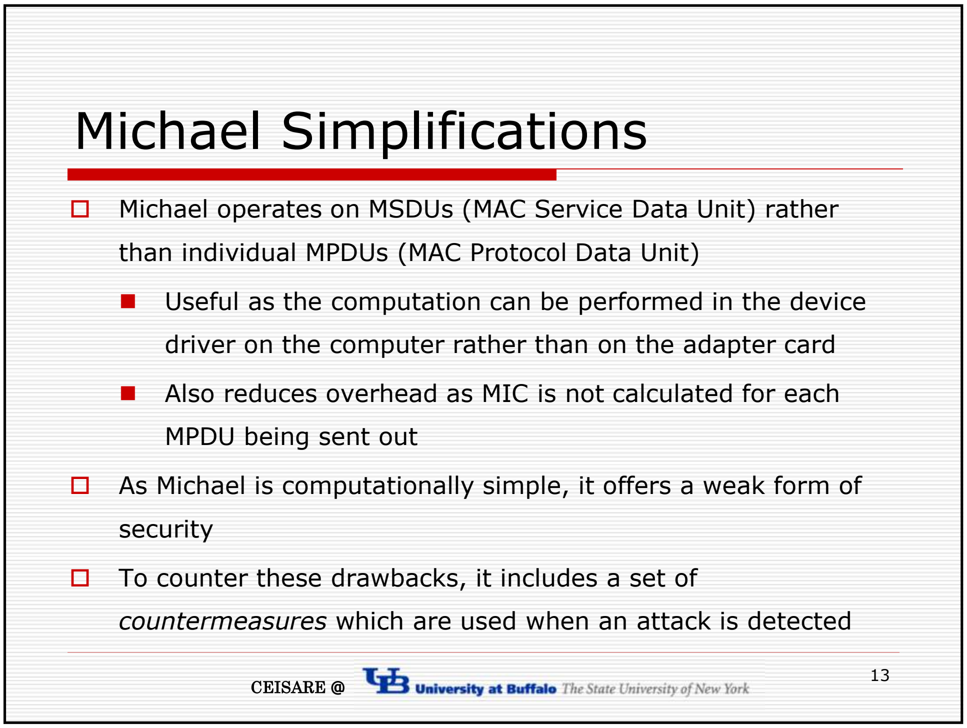
Message Integrity

- Essential to security of the message
- WEP uses ICV (Integrity Check Value), but it offers no real protection
- Thus, ICV is not a part of TKIP security
- Basic idea behind computing the MIC (Message Integrity Code) is calculating a checksum over the message bytes so that any modification to the message can be detected
- This MIC is combined with a secret key so that only authorized parties can generate and verify the MIC
- Many available cryptographic methods can be used for the purpose



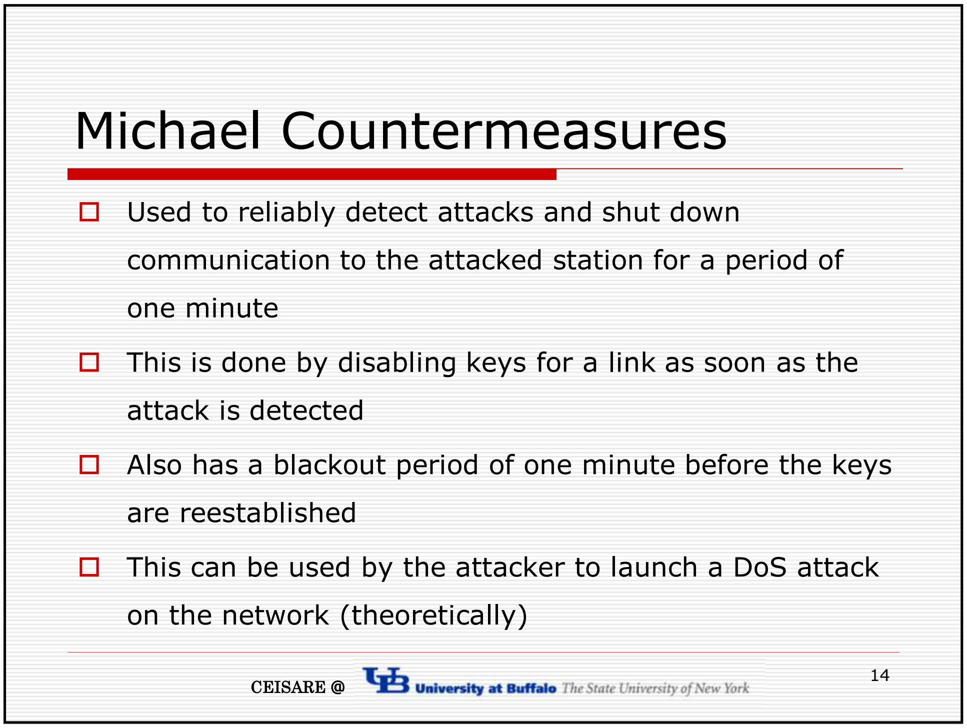
Message Integrity – Michael

- As WEP is required to work over existing hardware it cannot use computationally intensive cryptographic methods
- Even if the computations are moved to software level in clients, existing Access Points cannot perform heavy computations
- Thus, TKIP uses a method of computing MIC called *Michael*
- *Michael* uses simple shift and add operations instead of multiplications and hence is usable in TKIP



Michael Simplifications

- □ Michael operates on MSDUs (MAC Service Data Unit) rather than individual MPDUs (MAC Protocol Data Unit)
  - ■ Useful as the computation can be performed in the device driver on the computer rather than on the adapter card
  - ■ Also reduces overhead as MIC is not calculated for each MPDU being sent out
- □ As Michael is computationally simple, it offers a weak form of security
- □ To counter these drawbacks, it includes a set of *countermeasures* which are used when an attack is detected



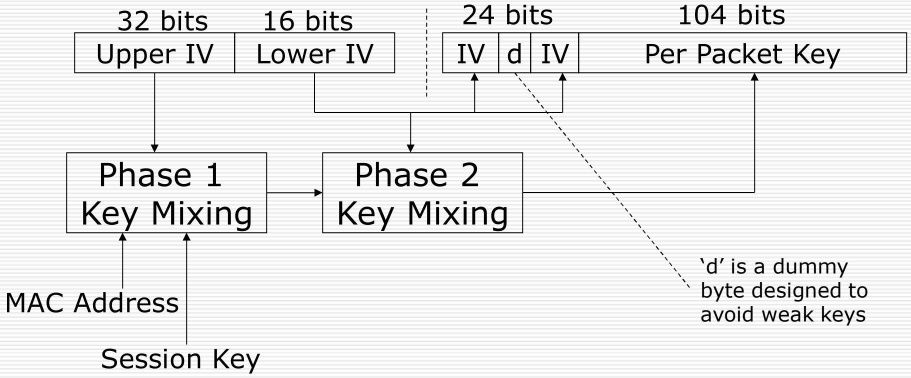
Michael Countermeasures

- □ Used to reliably detect attacks and shut down communication to the attacked station for a period of one minute
- □ This is done by disabling keys for a link as soon as the attack is detected
- □ Also has a blackout period of one minute before the keys are reestablished
- □ This can be used by the attacker to launch a DoS attack on the network (theoretically)

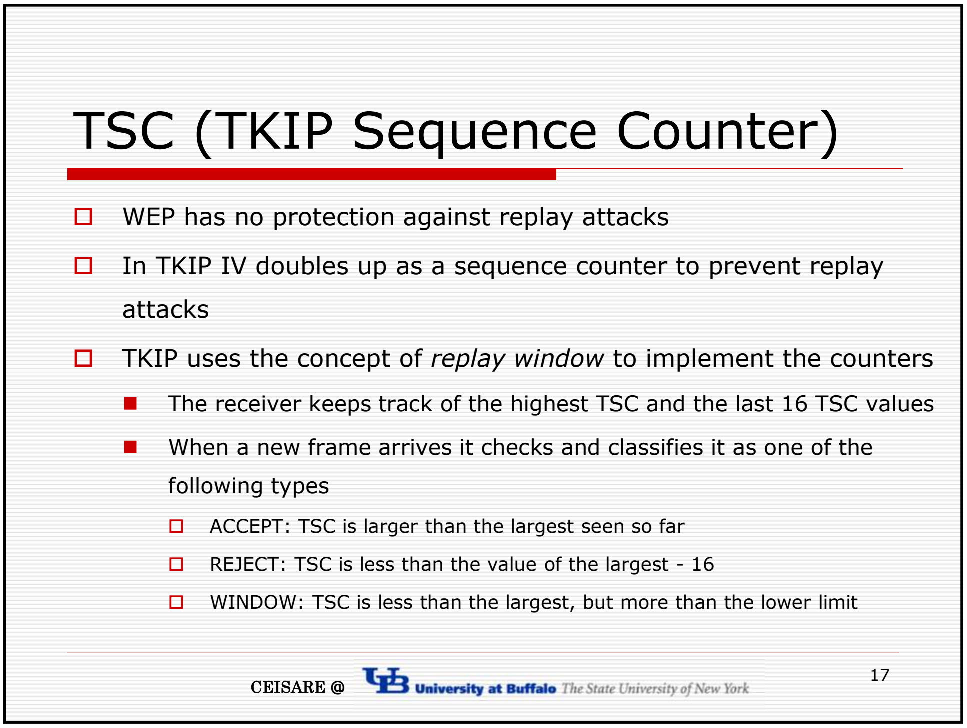
IV Selection and Use

- TKIP has the following major changes in the way IVs are used as compared to WEP
  - IV Size is increased from 24 to 48 bits
  - IV has a secondary role as a sequence counter to avoid replay attacks
  - IVs are constructed so as to avoid certain ‘weak keys’
  - Instead of directly appending it with the secret key, IVs are used to generate mixed keys

IV Use in TKIP

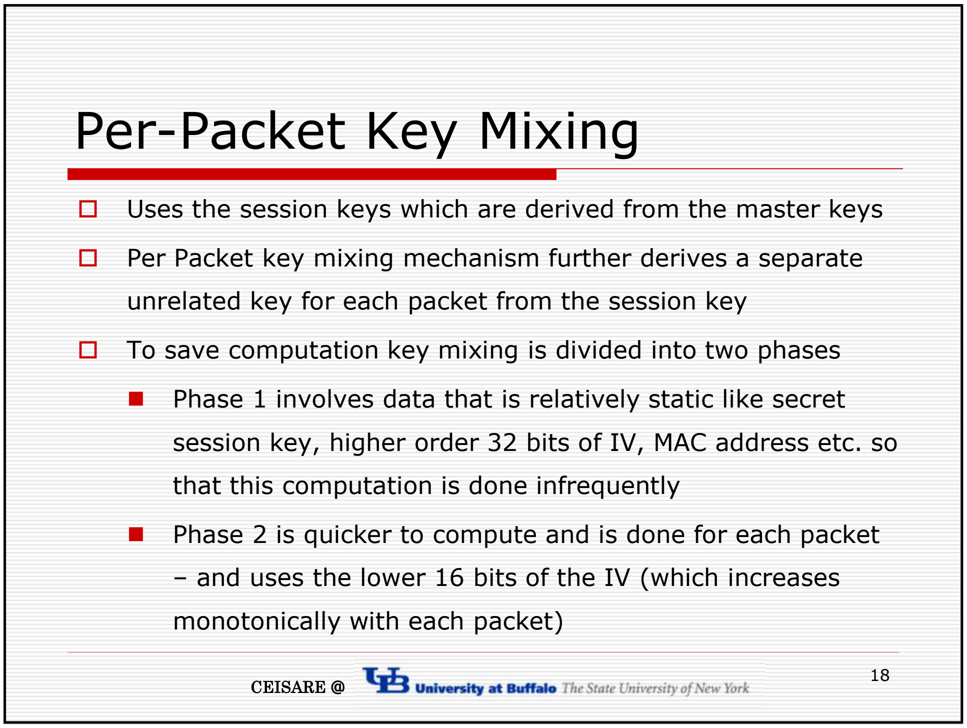


Creating the RC4 Encryption Key



TSC (TKIP Sequence Counter)

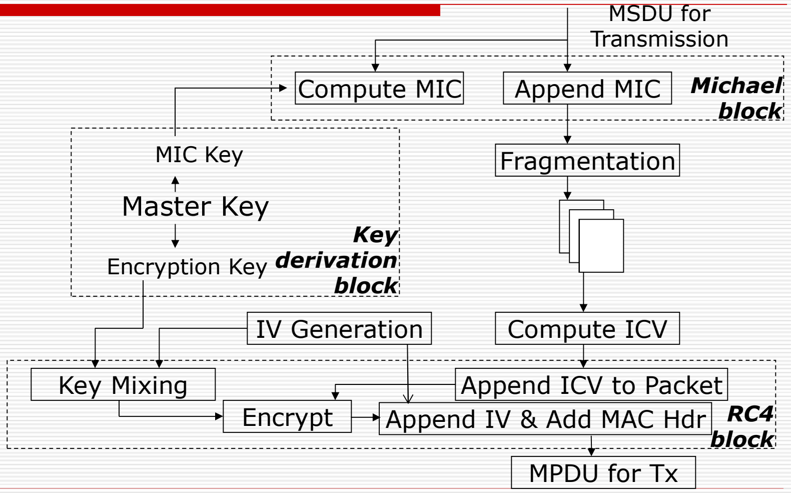
- □ WEP has no protection against replay attacks
- □ In TKIP IV doubles up as a sequence counter to prevent replay attacks
- □ TKIP uses the concept of *replay window* to implement the counters
  - ■ The receiver keeps track of the highest TSC and the last 16 TSC values
  - ■ When a new frame arrives it checks and classifies it as one of the following types
    - □ ACCEPT: TSC is larger than the largest seen so far
    - □ REJECT: TSC is less than the value of the largest - 16
    - □ WINDOW: TSC is less than the largest, but more than the lower limit



Per-Packet Key Mixing

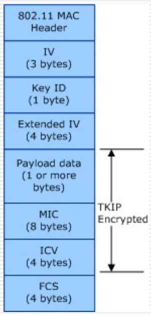
- □ Uses the session keys which are derived from the master keys
- □ Per Packet key mixing mechanism further derives a separate unrelated key for each packet from the session key
- □ To save computation key mixing is divided into two phases
  - ■ Phase 1 involves data that is relatively static like secret session key, higher order 32 bits of IV, MAC address etc. so that this computation is done infrequently
  - ■ Phase 2 is quicker to compute and is done for each packet – and uses the lower 16 bits of the IV (which increases monotonically with each packet)

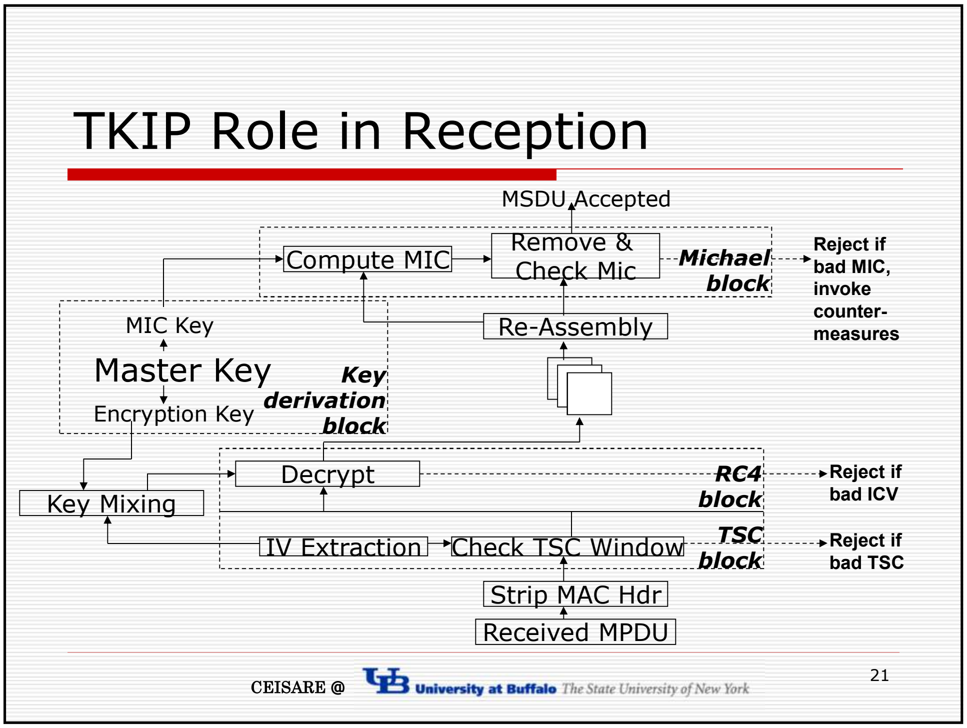
TKIP Role in Transmission



TKIP MPDU Frame

- Initialization Vector (IV)
- Key Identifier (ID)
- Extended IV
- Payload Data
  - MPDU data
- MIC
  - The MIC value is computed using the Michael algorithm over the entire payload data of the MSDU
- Integrity Check Value (ICV)
  - The checksum value computed over the unencrypted payload data
- Frame Check Sequence (FCS)
  - (CRC) computed over all fields of the MPDU


802.11 MAC Header
IV (3 bytes)
Key ID (1 byte)
Extended IV (4 bytes)
Payload data (1 or more bytes)
MIC (8 bytes)
ICV (4 bytes)
FCS (4 bytes)



TKIP Role in Reception

MSDU Accepted

Compute MIC

Remove & Check Mic

Michael block

Reject if bad MIC, invoke counter-measures

MIC Key

Master Key

Encryption Key

Key derivation block

Re-Assembly

Decrypt

RC4 block

Reject if bad ICV

Key Mixing

IV Extraction

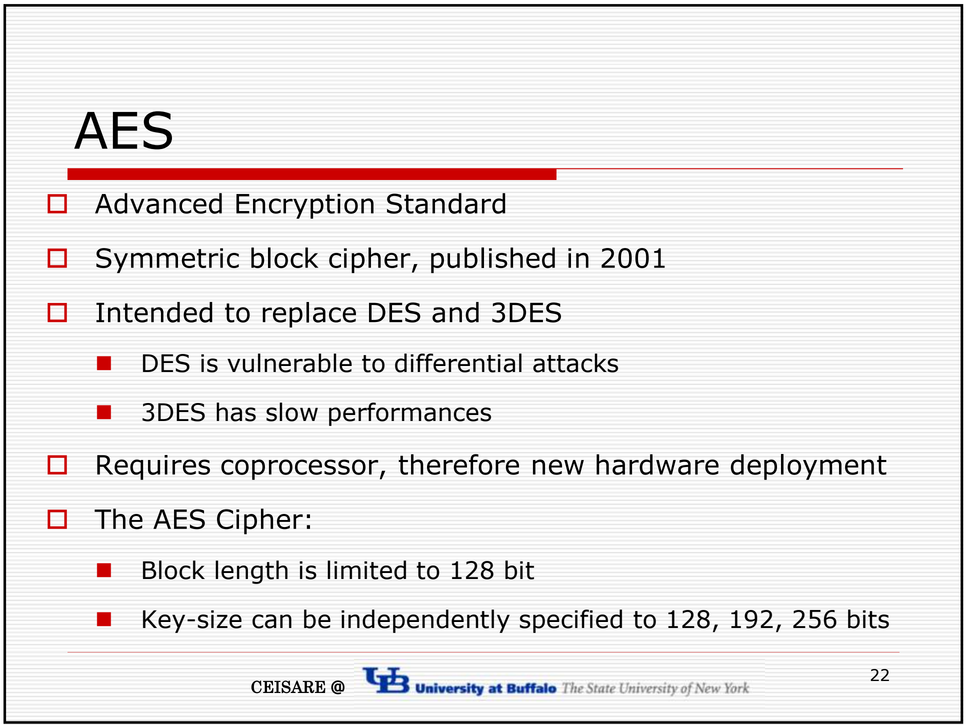
Check TSC Window

TSC block

Reject if bad TSC

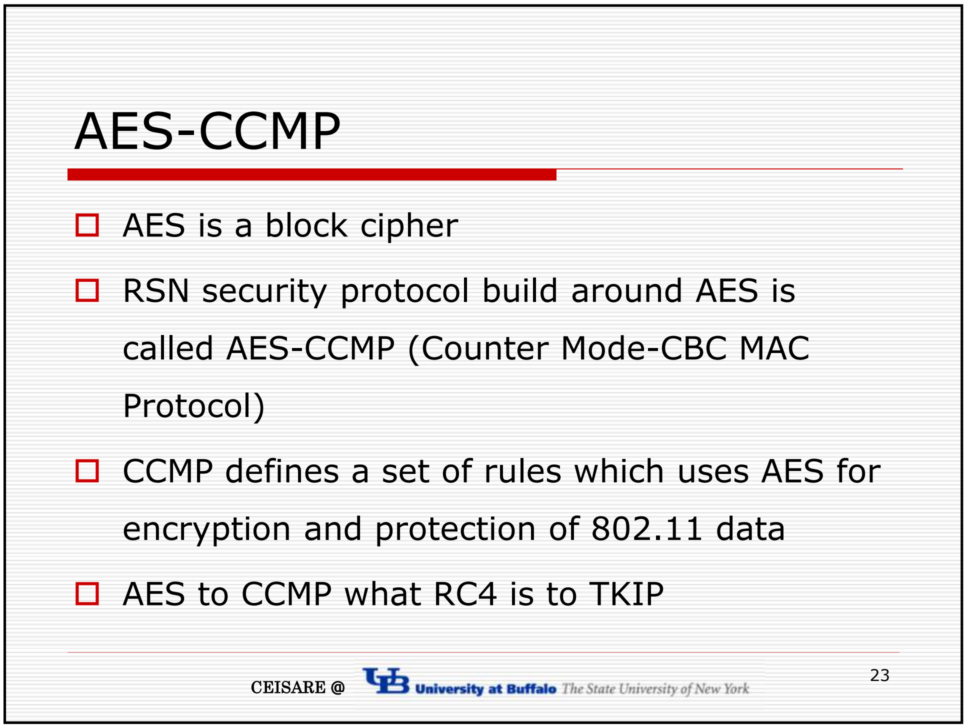
Strip MAC Hdr

Received MPDU



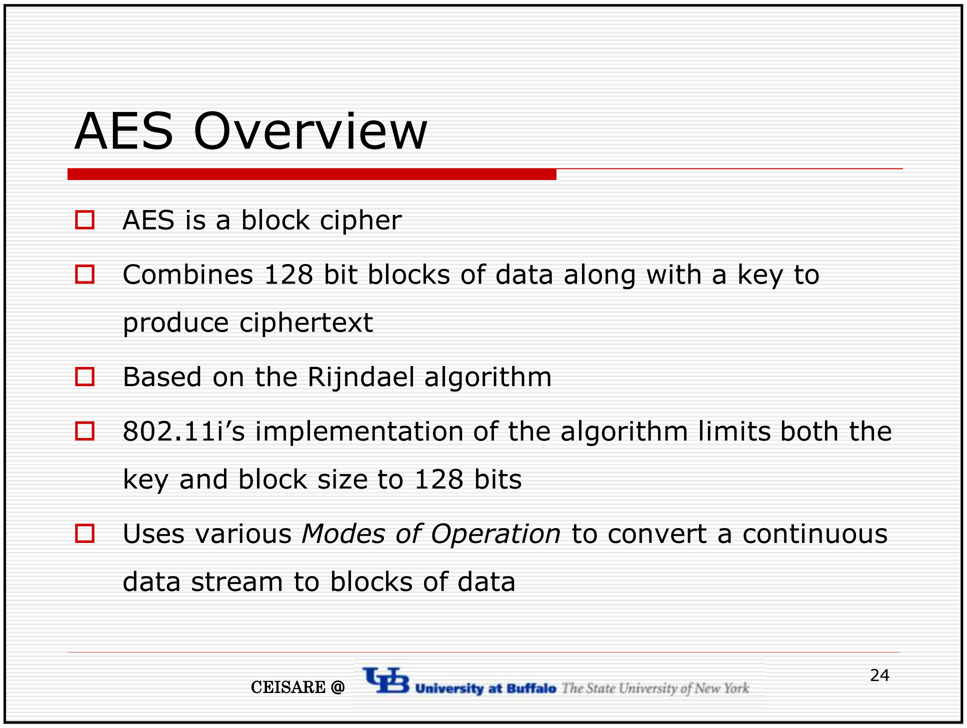
AES

- Advanced Encryption Standard
- Symmetric block cipher, published in 2001
- Intended to replace DES and 3DES
  - DES is vulnerable to differential attacks
  - 3DES has slow performances
- Requires coprocessor, therefore new hardware deployment
- The AES Cipher:
  - Block length is limited to 128 bit
  - Key-size can be independently specified to 128, 192, 256 bits



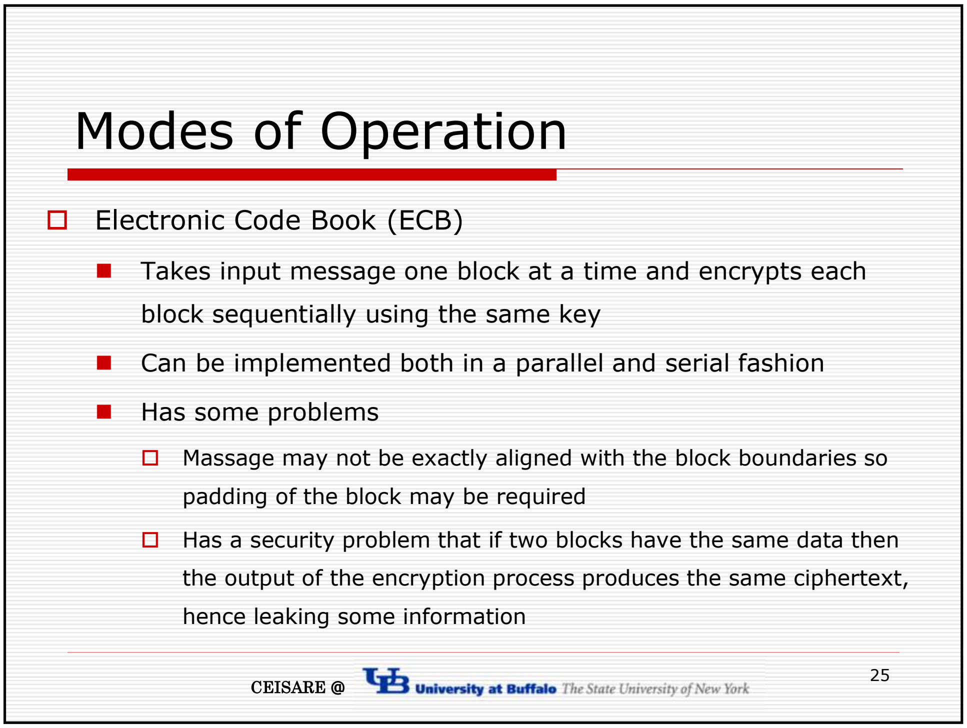
AES-CCMP

- AES is a block cipher
- RSN security protocol build around AES is called AES-CCMP (Counter Mode-CBC MAC Protocol)
- CCMP defines a set of rules which uses AES for encryption and protection of 802.11 data
- AES to CCMP what RC4 is to TKIP



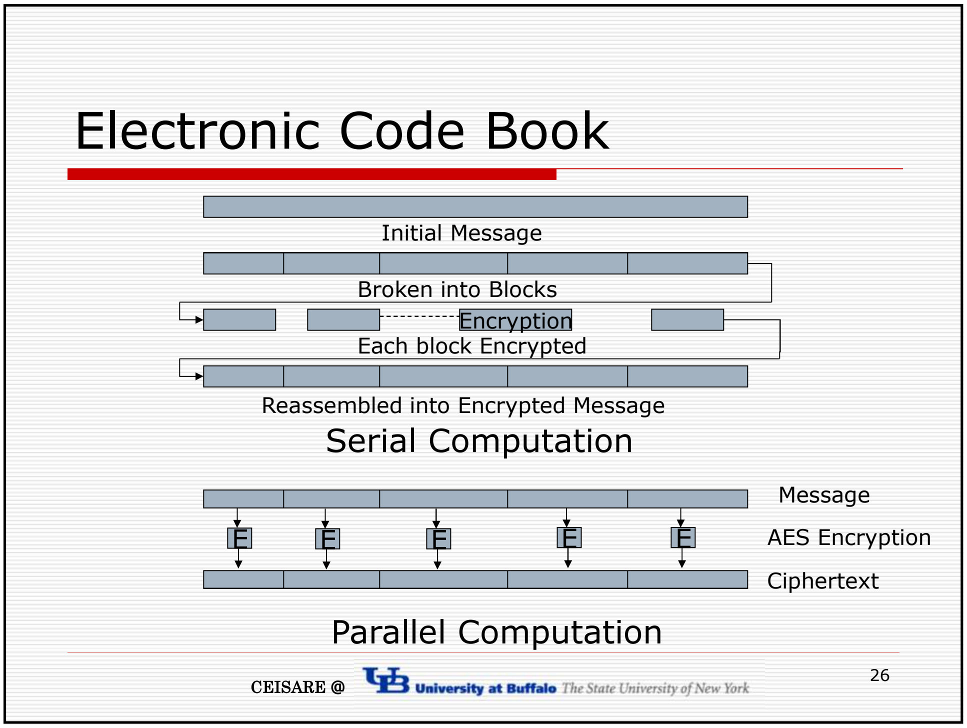
AES Overview

- AES is a block cipher
- Combines 128 bit blocks of data along with a key to produce ciphertext
- Based on the Rijndael algorithm
- 802.11i’s implementation of the algorithm limits both the key and block size to 128 bits
- Uses various *Modes of Operation* to convert a continuous data stream to blocks of data



Modes of Operation

- □ Electronic Code Book (ECB)
  - ■ Takes input message one block at a time and encrypts each block sequentially using the same key
  - ■ Can be implemented both in a parallel and serial fashion
  - ■ Has some problems
    - □ Massage may not be exactly aligned with the block boundaries so padding of the block may be required
    - □ Has a security problem that if two blocks have the same data then the output of the encryption process produces the same ciphertext, hence leaking some information



Electronic Code Book

Initial Message

Broken into Blocks

Encryption

Each block Encrypted

Reassembled into Encrypted Message

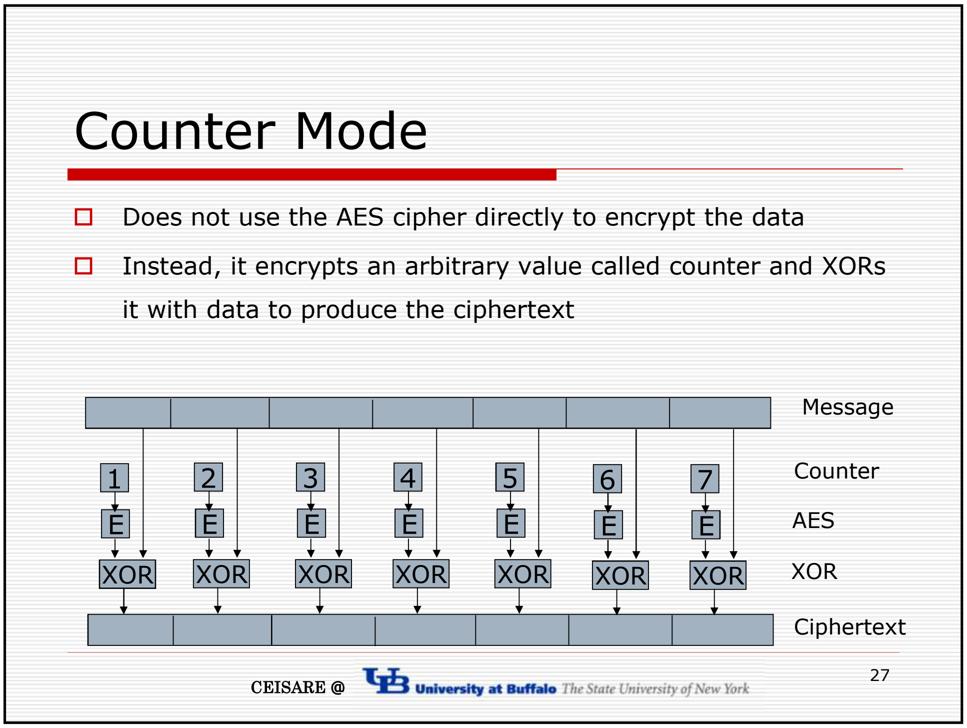
Serial Computation

Message

AES Encryption

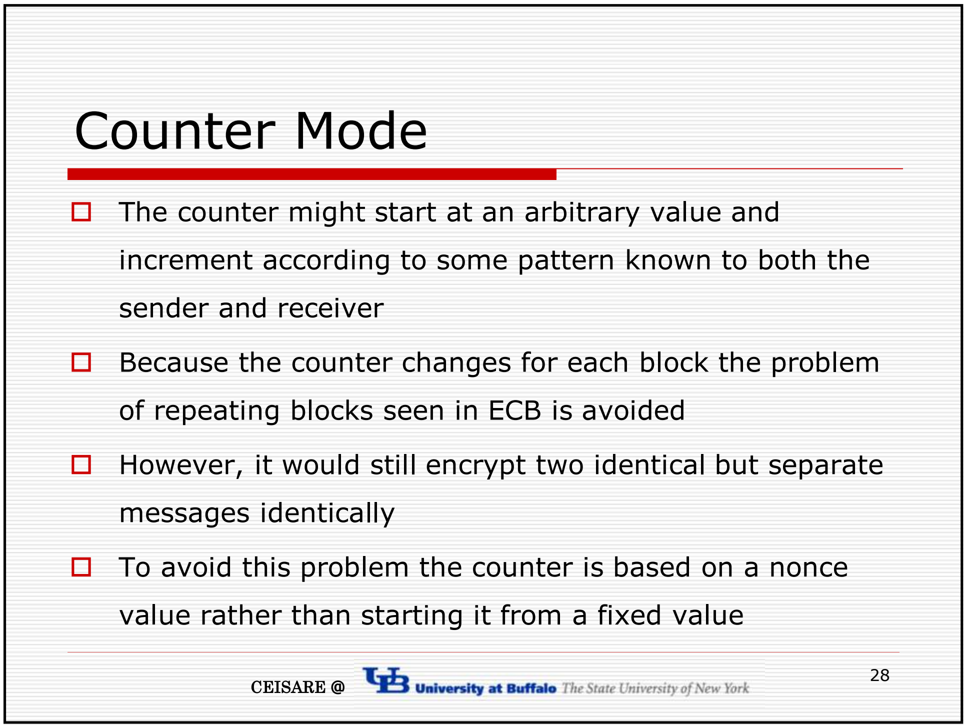
Ciphertext

Parallel Computation



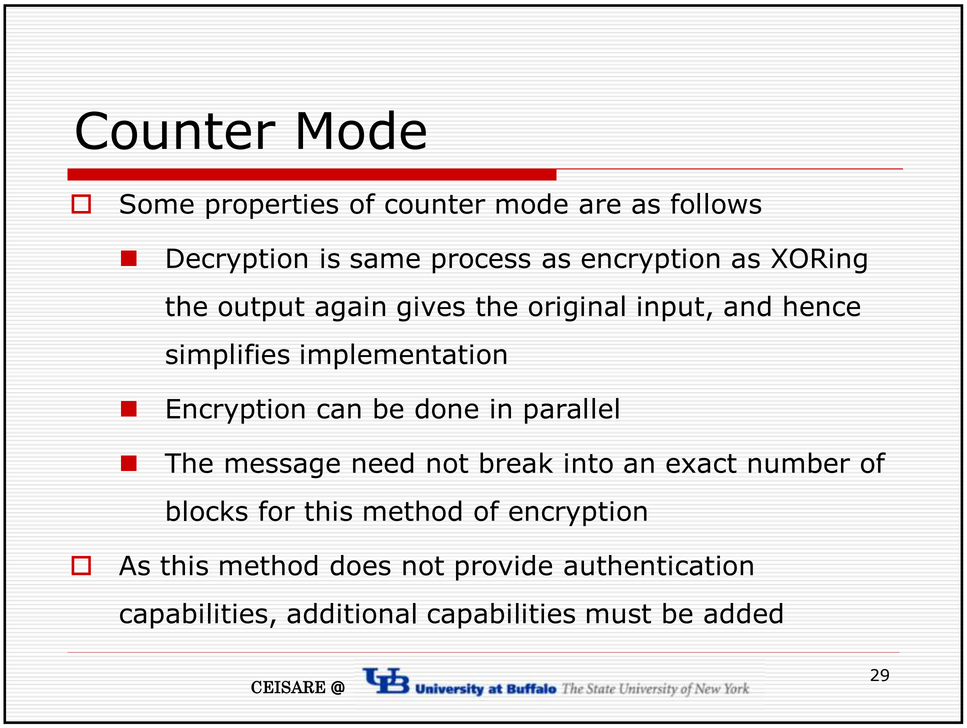
Counter Mode

- □ Does not use the AES cipher directly to encrypt the data
- □ Instead, it encrypts an arbitrary value called counter and XORs it with data to produce the ciphertext



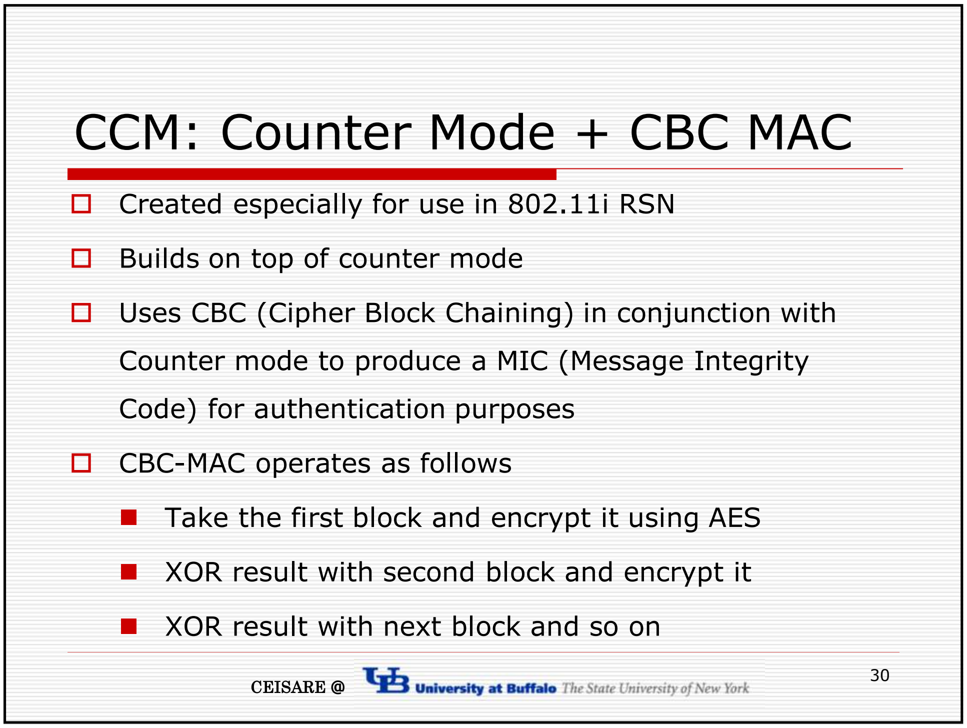
Counter Mode

- □ The counter might start at an arbitrary value and increment according to some pattern known to both the sender and receiver
- □ Because the counter changes for each block the problem of repeating blocks seen in ECB is avoided
- □ However, it would still encrypt two identical but separate messages identically
- □ To avoid this problem the counter is based on a nonce value rather than starting it from a fixed value



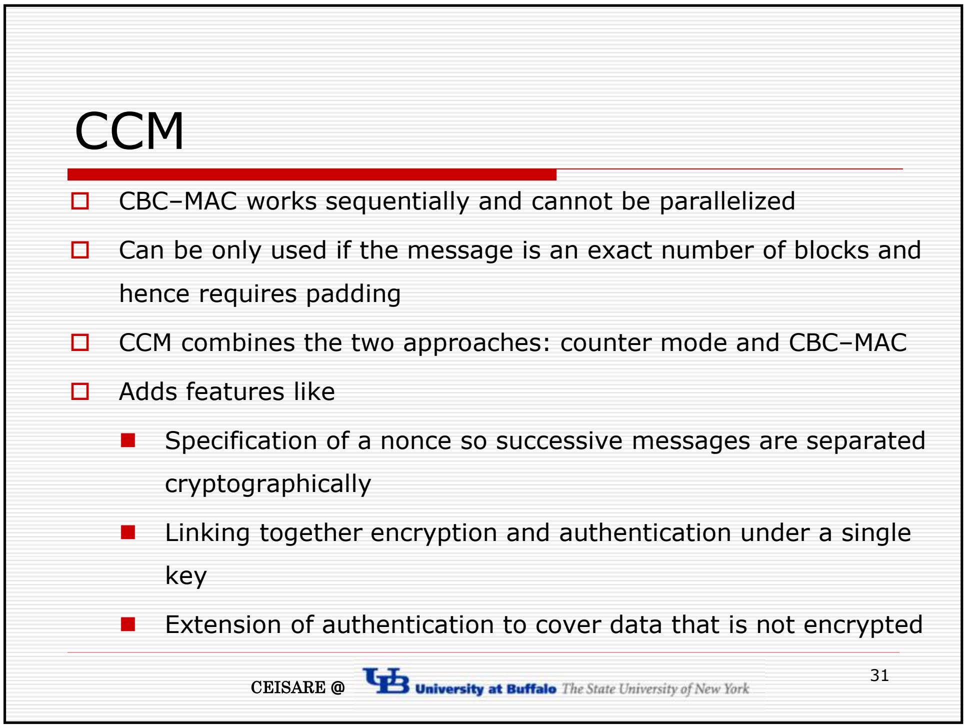
Counter Mode

- Some properties of counter mode are as follows
  - Decryption is same process as encryption as XORing the output again gives the original input, and hence simplifies implementation
  - Encryption can be done in parallel
  - The message need not break into an exact number of blocks for this method of encryption
- As this method does not provide authentication capabilities, additional capabilities must be added



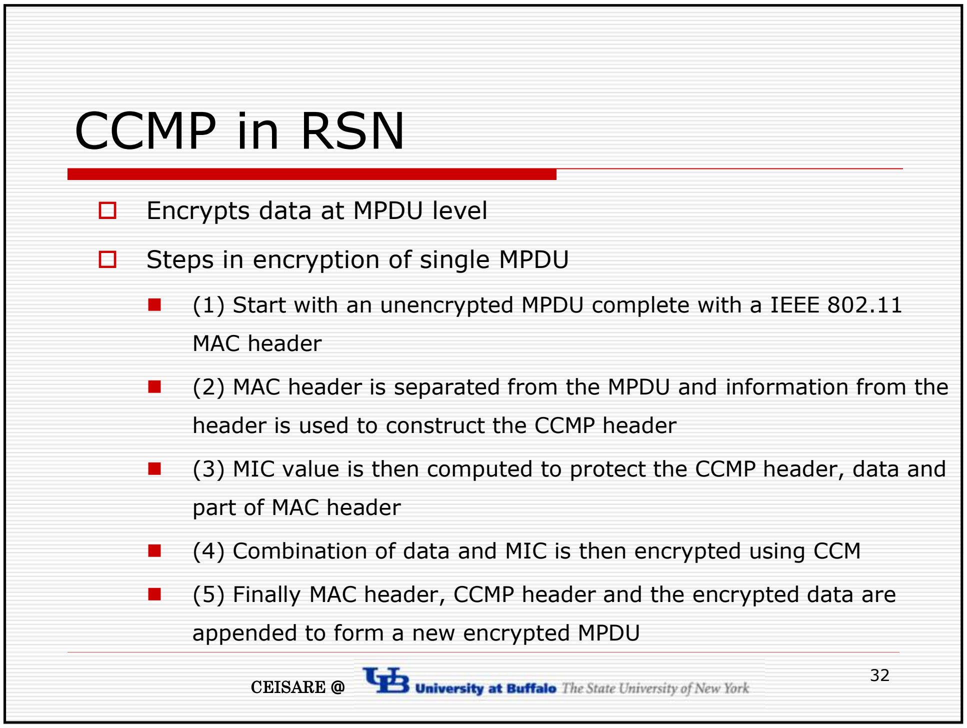
CCM: Counter Mode + CBC MAC

- Created especially for use in 802.11i RSN
- Builds on top of counter mode
- Uses CBC (Cipher Block Chaining) in conjunction with Counter mode to produce a MIC (Message Integrity Code) for authentication purposes
- CBC-MAC operates as follows
  - Take the first block and encrypt it using AES
  - XOR result with second block and encrypt it
  - XOR result with next block and so on



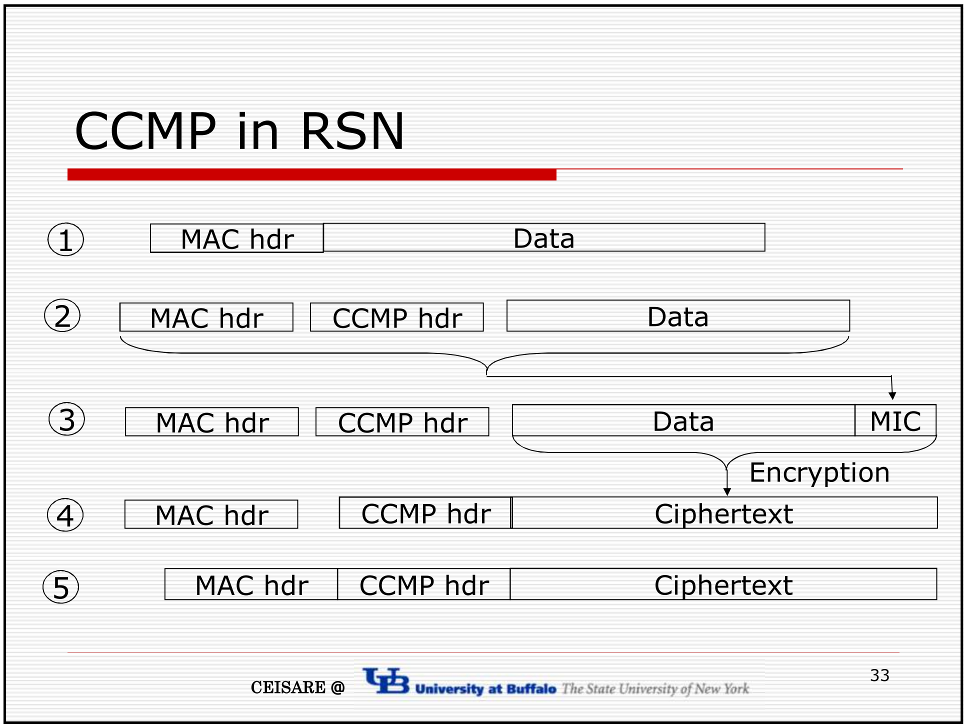
CCM

- □ CBC–MAC works sequentially and cannot be parallelized
- □ Can be only used if the message is an exact number of blocks and hence requires padding
- □ CCM combines the two approaches: counter mode and CBC–MAC
- □ Adds features like
  - ■ Specification of a nonce so successive messages are separated cryptographically
  - ■ Linking together encryption and authentication under a single key
  - ■ Extension of authentication to cover data that is not encrypted



CCMP in RSN

- □ Encrypts data at MPDU level
- □ Steps in encryption of single MPDU
  - ■ (1) Start with an unencrypted MPDU complete with a IEEE 802.11 MAC header
  - ■ (2) MAC header is separated from the MPDU and information from the header is used to construct the CCMP header
  - ■ (3) MIC value is then computed to protect the CCMP header, data and part of MAC header
  - ■ (4) Combination of data and MIC is then encrypted using CCM
  - ■ (5) Finally MAC header, CCMP header and the encrypted data are appended to form a new encrypted MPDU



CCMP in RSN

① MAC hdr | Data

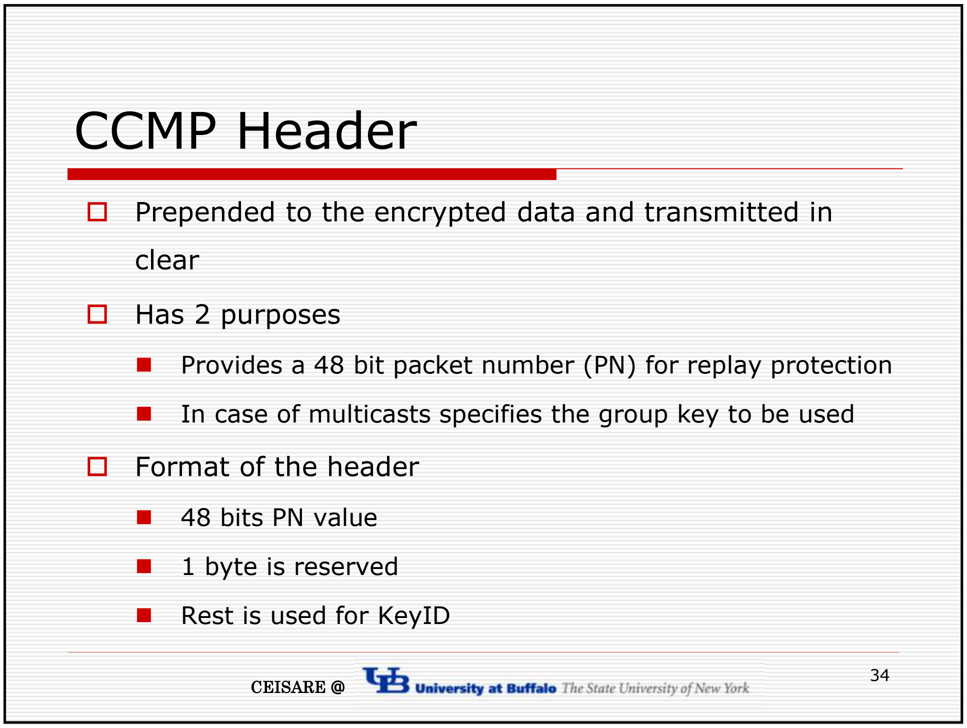
② MAC hdr | CCMP hdr | Data

③ MAC hdr | CCMP hdr | Data | MIC

Encryption

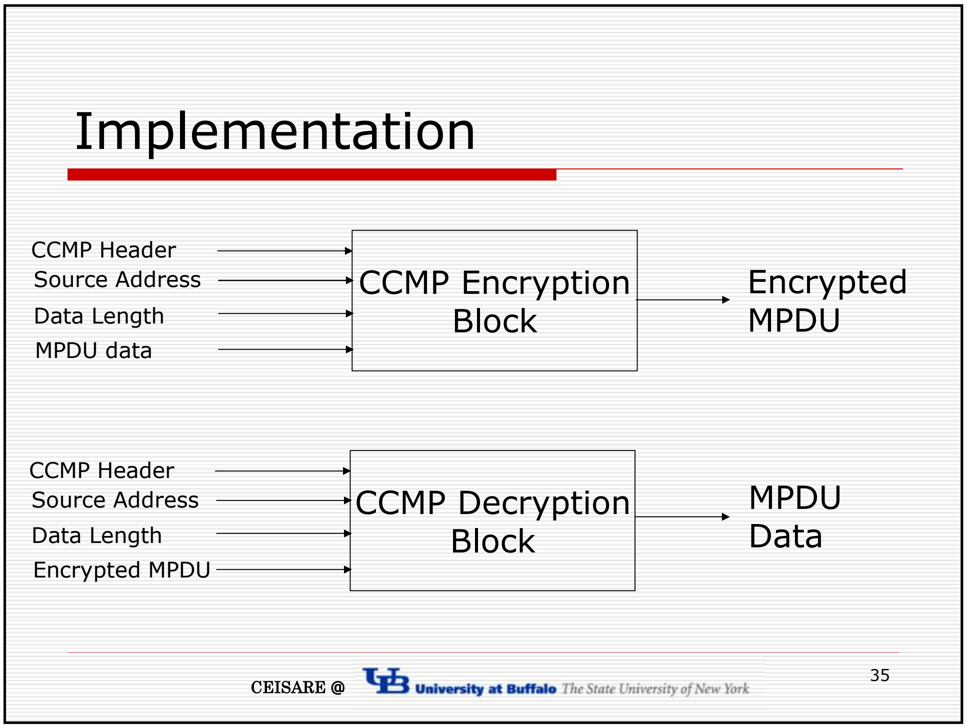
④ MAC hdr | CCMP hdr | Ciphertext

⑤ MAC hdr | CCMP hdr | Ciphertext



CCMP Header

- Prepended to the encrypted data and transmitted in clear
- Has 2 purposes
  - Provides a 48 bit packet number (PN) for replay protection
  - In case of multicasts specifies the group key to be used
- Format of the header
  - 48 bits PN value
  - 1 byte is reserved
  - Rest is used for KeyID



Implementation

CCMP Header
Source Address
Data Length
MPDU data

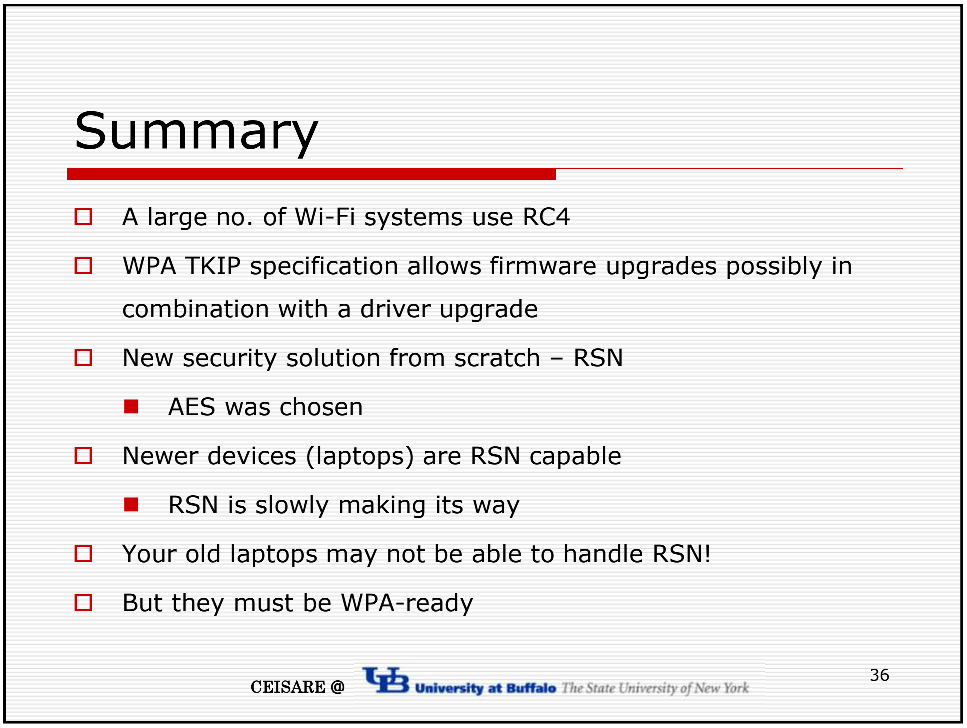
CCMP Encryption Block

Encrypted MPDU

CCMP Header
Source Address
Data Length
Encrypted MPDU

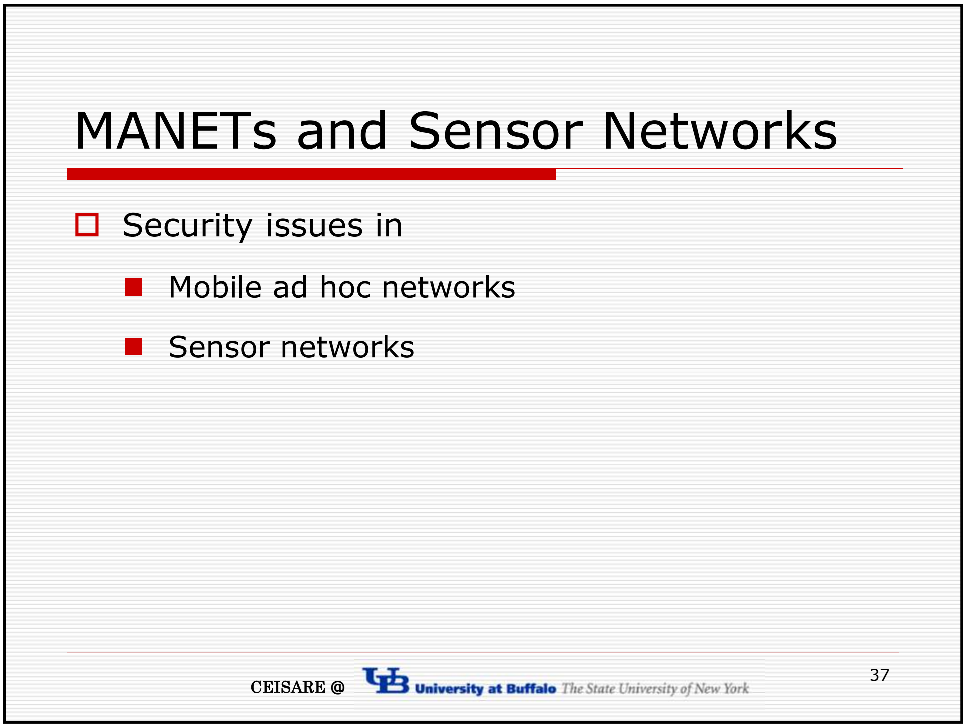
CCMP Decryption Block

MPDU Data



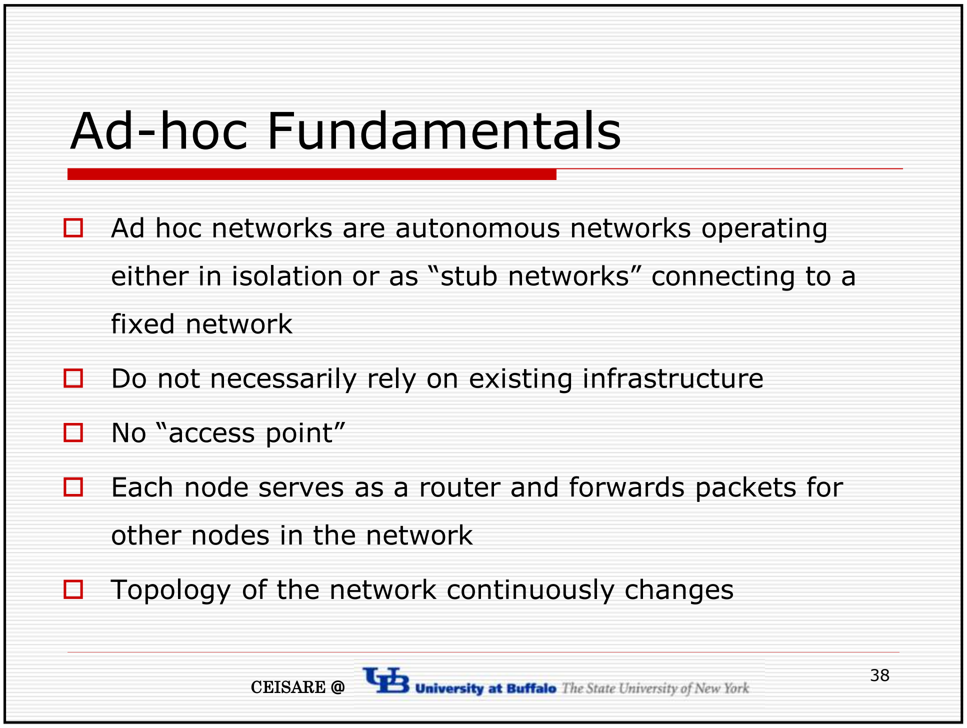
Summary

- □ A large no. of Wi-Fi systems use RC4
- □ WPA TKIP specification allows firmware upgrades possibly in combination with a driver upgrade
- □ New security solution from scratch – RSN
  - ■ AES was chosen
- □ Newer devices (laptops) are RSN capable
  - ■ RSN is slowly making its way
- □ Your old laptops may not be able to handle RSN!
- □ But they must be WPA-ready



MANETs and Sensor Networks

- Security issues in
  - Mobile ad hoc networks
  - Sensor networks



Ad-hoc Fundamentals

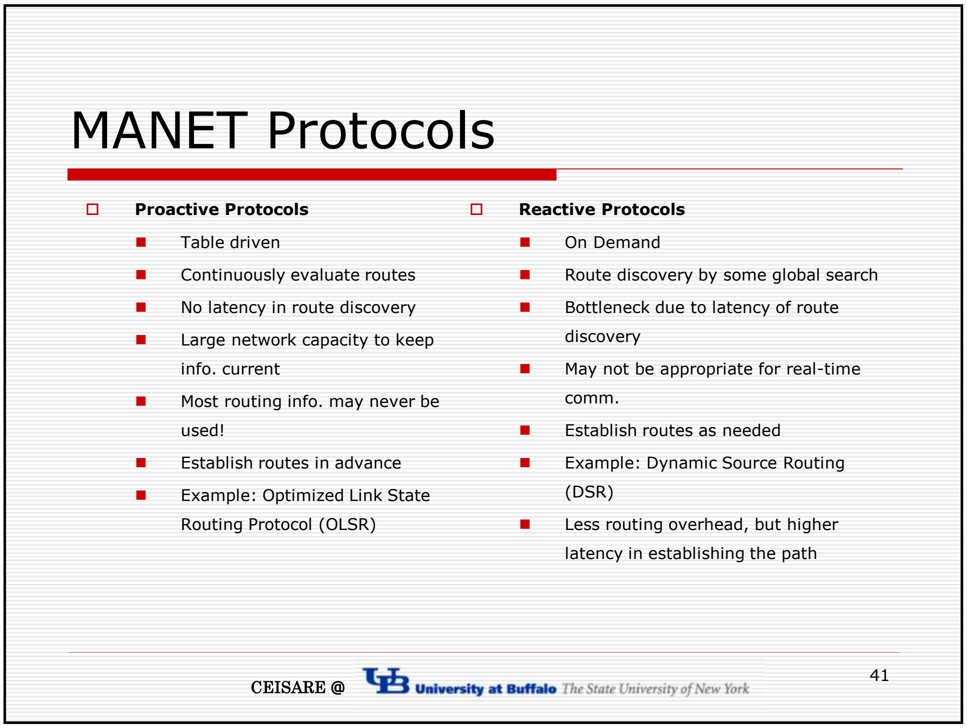
- Ad hoc networks are autonomous networks operating either in isolation or as “stub networks” connecting to a fixed network
- Do not necessarily rely on existing infrastructure
- No “access point”
- Each node serves as a router and forwards packets for other nodes in the network
- Topology of the network continuously changes

Challenges

- Limitations of the Wireless Network
  - Packet loss due to transmission errors
  - Variable capacity links
  - Frequent disconnections/partitions
  - Limited communication bandwidth
  - Broadcast nature of the communications
- Limitations Imposed by Mobility
  - Dynamically changing topologies/routes
  - Lack of mobility awareness by system/applications
- Limitations of the Mobile Computer
  - Short battery lifetime
  - Limited capacities

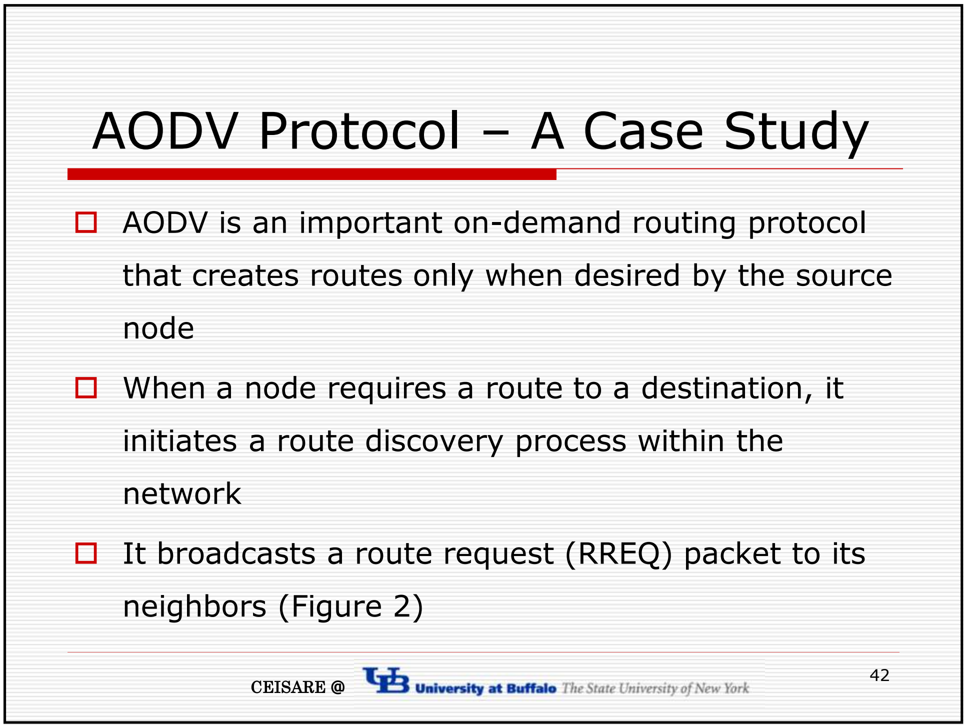
Applications

- Military
  - Rapidly deployable battle-site networks
  - Sensor fields
  - Unmanned aerial vehicles
- Disaster management
  - Disaster relief teams that cannot rely on existing infrastructure
- Neighborhood area networks (NANs)
  - Shareable Internet access in high density urban settings
- Impromptu communications among groups of people
  - Meetings/conferences
  - Wearable computing
- Automobile communications



MANET Protocols

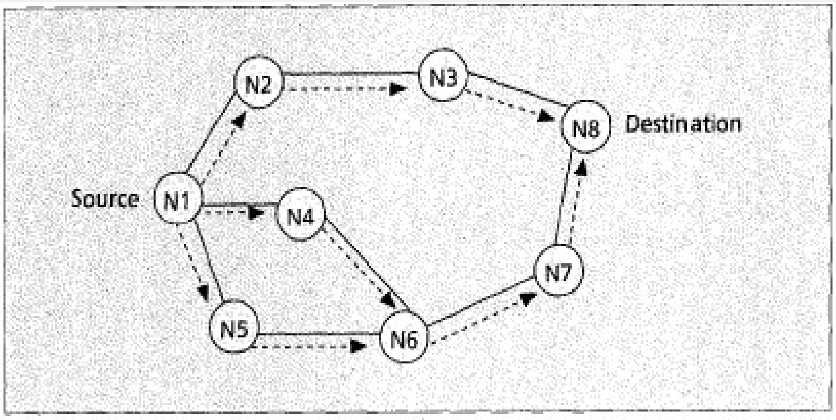
- **Proactive Protocols**
  - Table driven
  - Continuously evaluate routes
  - No latency in route discovery
  - Large network capacity to keep info. current
  - Most routing info. may never be used!
  - Establish routes in advance
  - Example: Optimized Link State Routing Protocol (OLSR)
- **Reactive Protocols**
  - On Demand
  - Route discovery by some global search
  - Bottleneck due to latency of route discovery
  - May not be appropriate for real-time comm.
  - Establish routes as needed
  - Example: Dynamic Source Routing (DSR)
  - Less routing overhead, but higher latency in establishing the path



AODV Protocol – A Case Study

- 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)

AODV Protocol (Contd.)

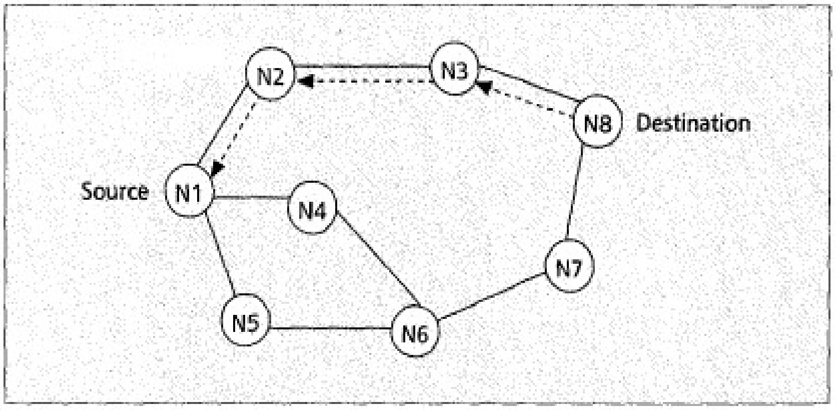


■ **Figure 2.** *Propagation of RREQ.*

AODV Protocol (Contd.)

□ 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

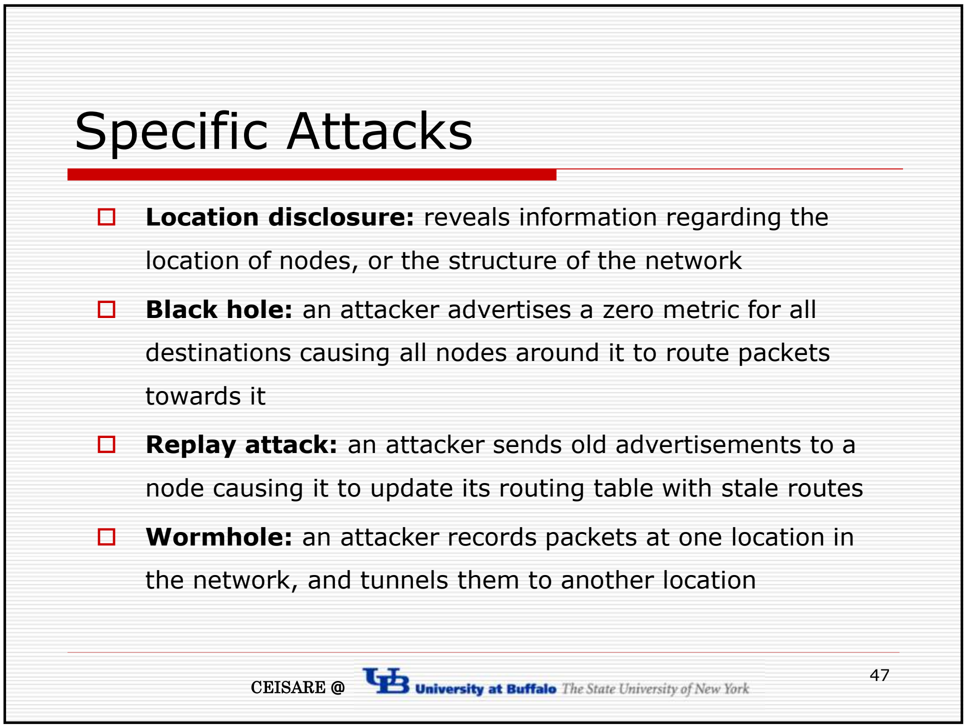
AODV Protocol (Contd.)



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

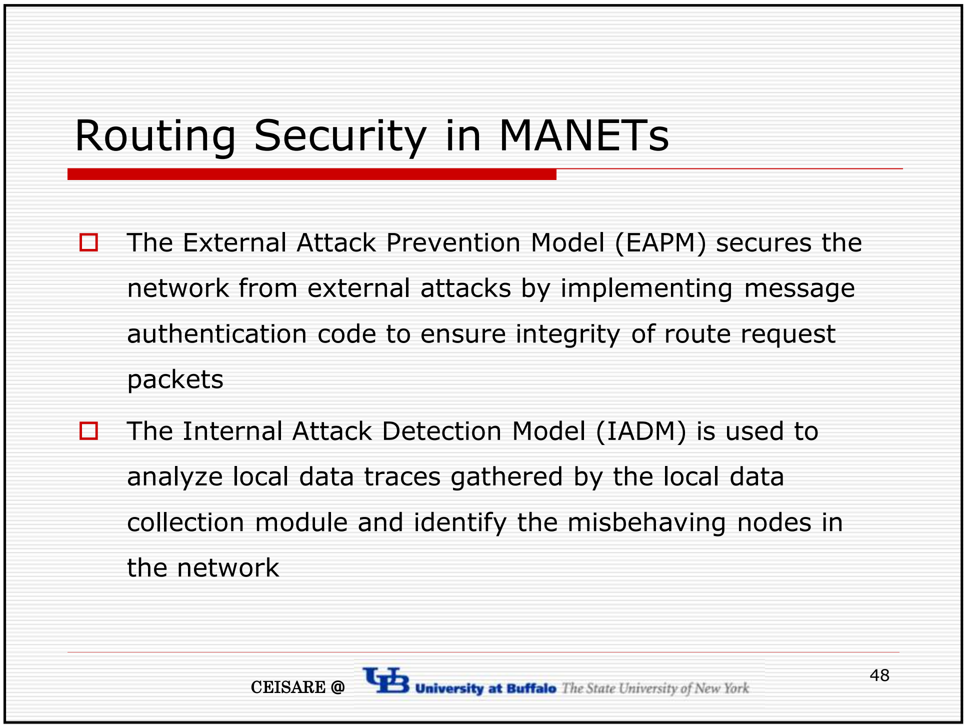
Security Goals and Challenges

- Availability
  - Survive despite DoS attack
  - Primary concern: Key management service
- Confidentiality
- Integrity
- Authentication
- Non-repudiation
- Challenges
  - Use of wireless links leads ad hoc networks susceptible to link attacks
  - Relatively poor protection, as in battlefields
  - So for high survivability, distributed architecture needed
  - Dynamic network topology: ROUTING
  - Scalable security mechanisms



Specific Attacks

- **Location disclosure:** reveals information regarding the location of nodes, or the structure of the network
- **Black hole:** an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it
- **Replay attack:** an attacker sends old advertisements to a node causing it to update its routing table with stale routes
- **Wormhole:** an attacker records packets at one location in the network, and tunnels them to another location



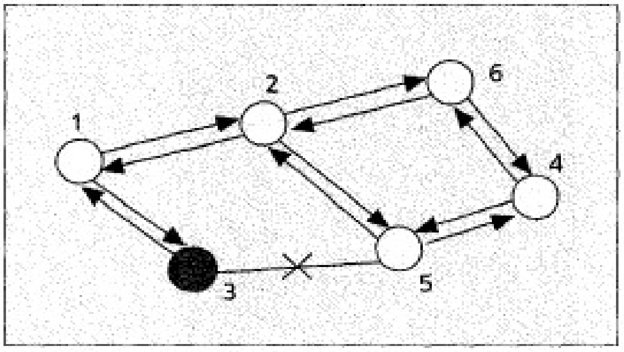
Routing Security in MANETs

- The External Attack Prevention Model (EAPM) secures the network from external attacks by implementing message authentication code to ensure integrity of route request packets
- The Internal Attack Detection Model (IADM) is used to analyze local data traces gathered by the local data collection module and identify the misbehaving nodes in the network

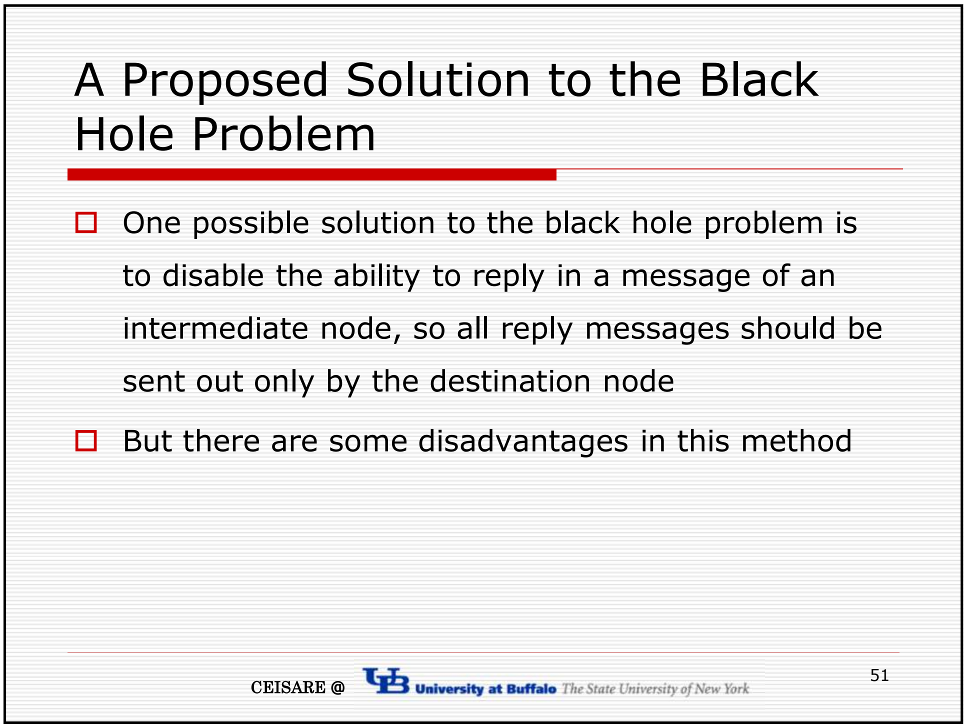
The Black Hole Problem in AODV Protocol – Case Study (Contd.)

- 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 (Contd.)

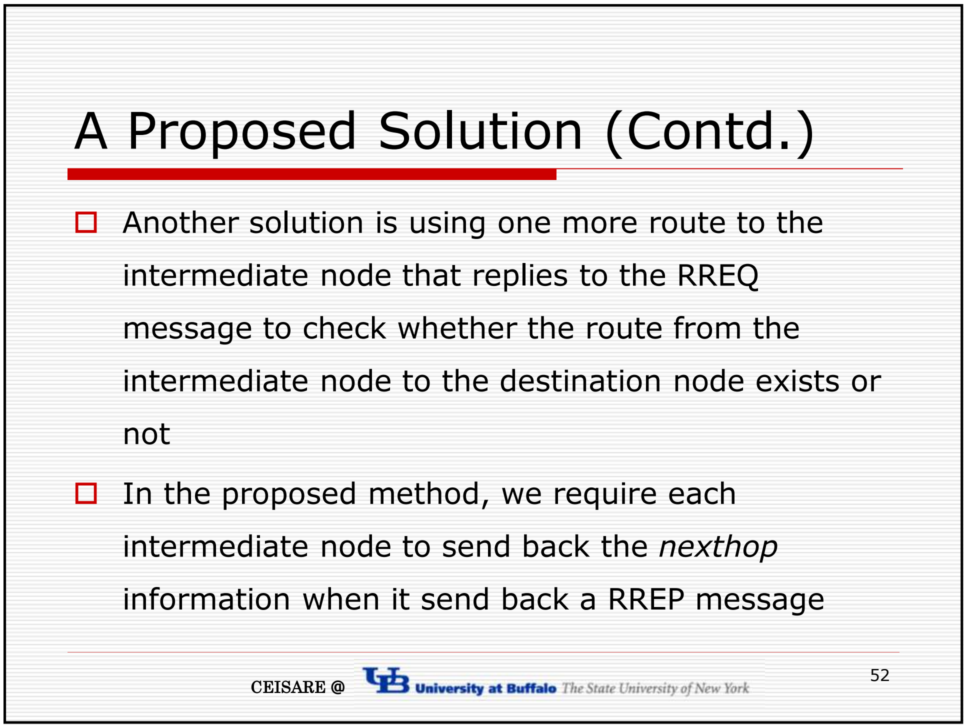


■ **Figure 4.** *The black hole problem.*



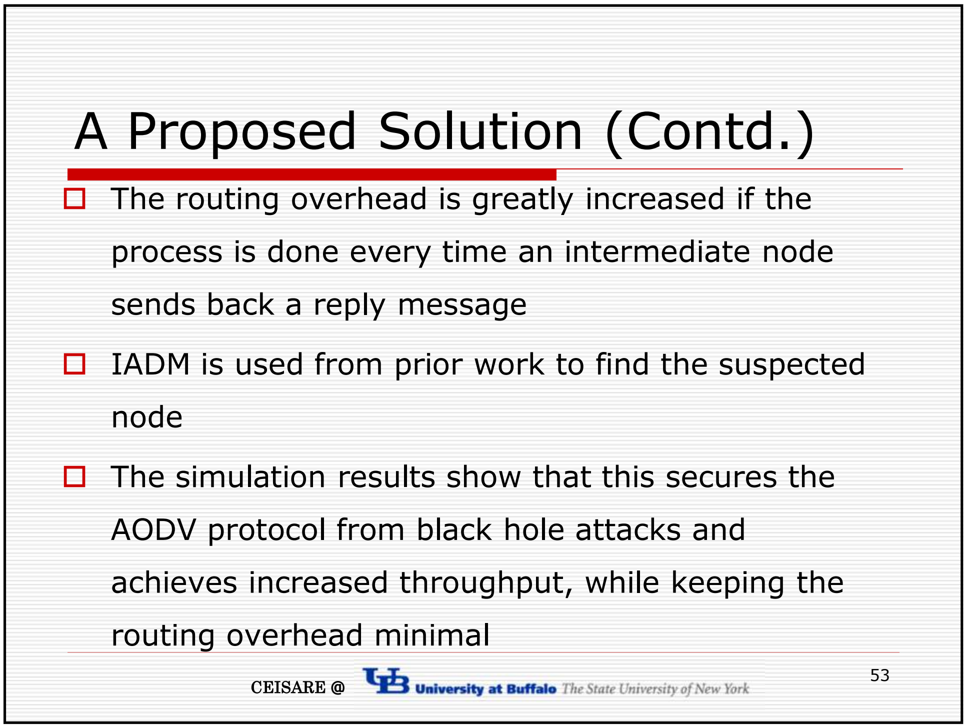
A Proposed Solution to the Black Hole Problem

- 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



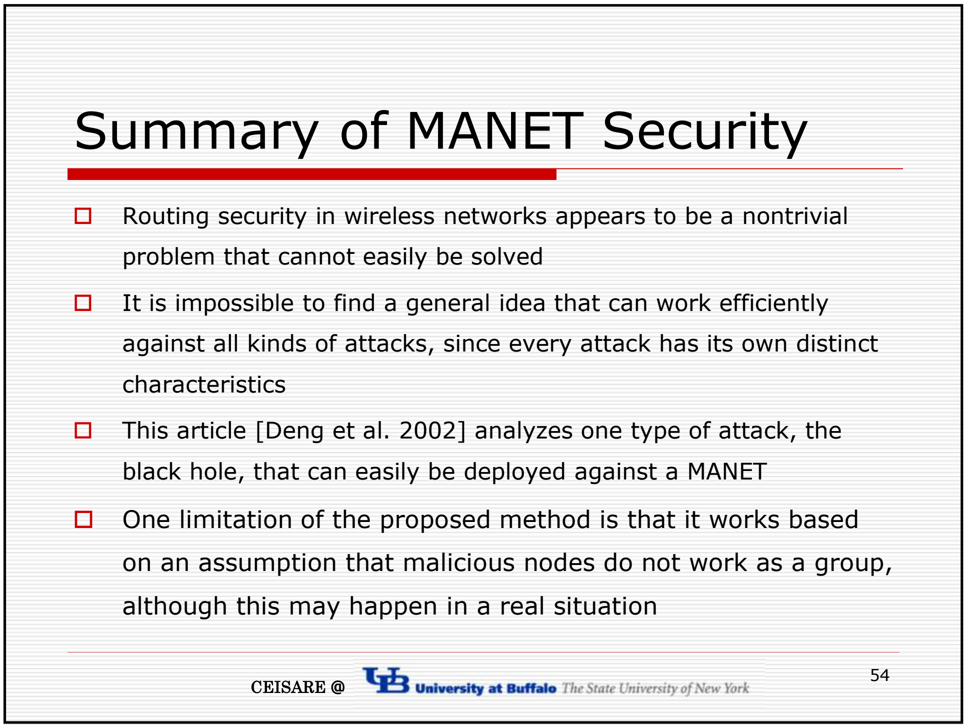
A Proposed Solution (Contd.)

- 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



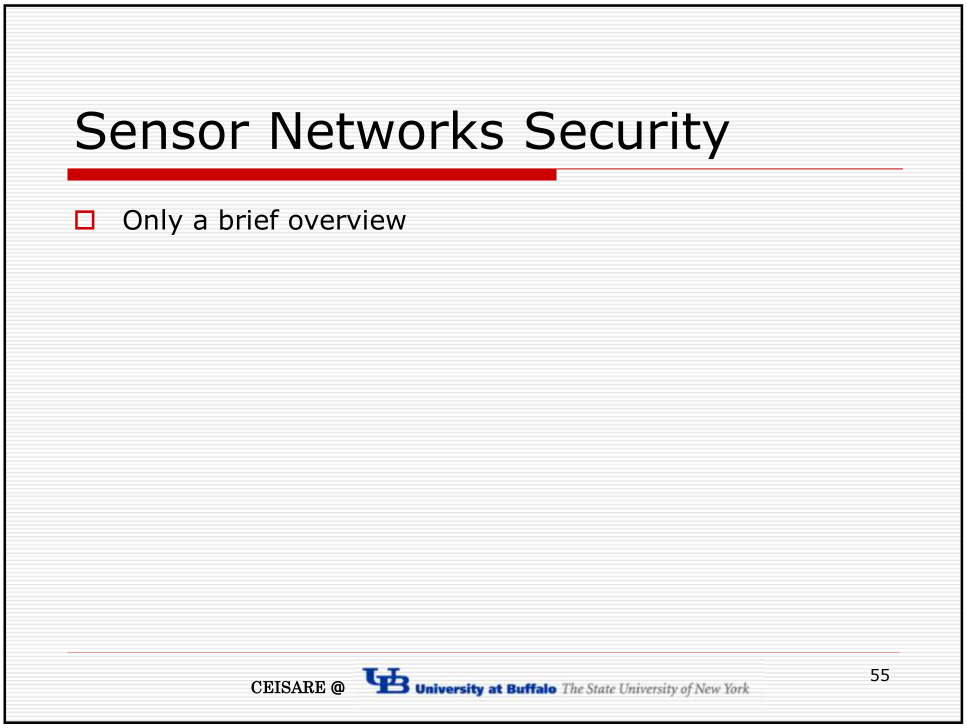
A Proposed Solution (Contd.)

- 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



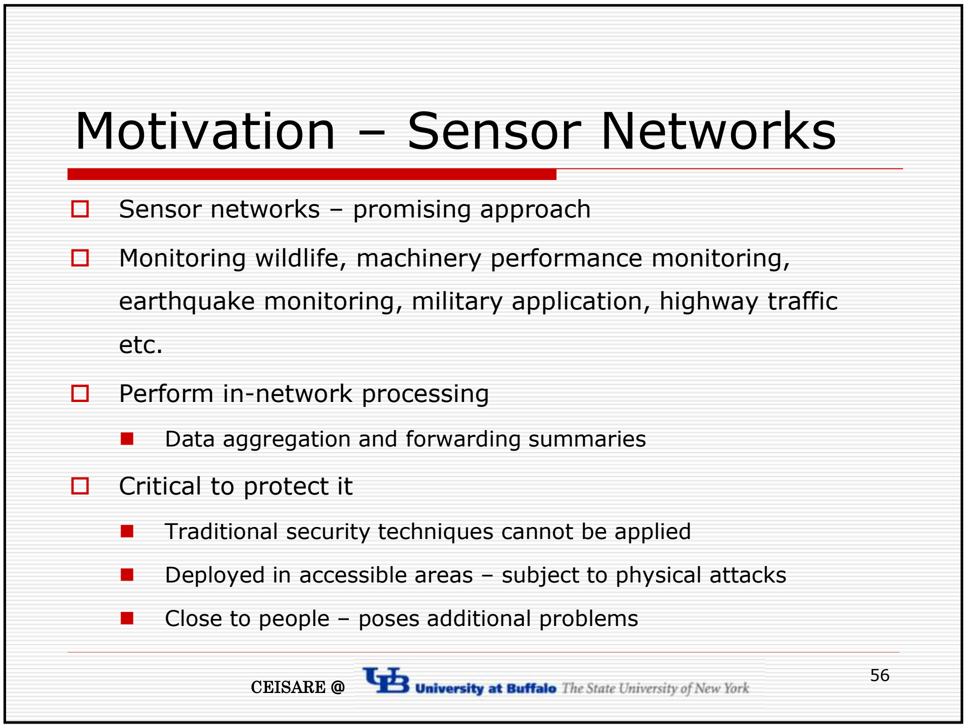
Summary of MANET Security

- 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 [Deng et al. 2002] 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



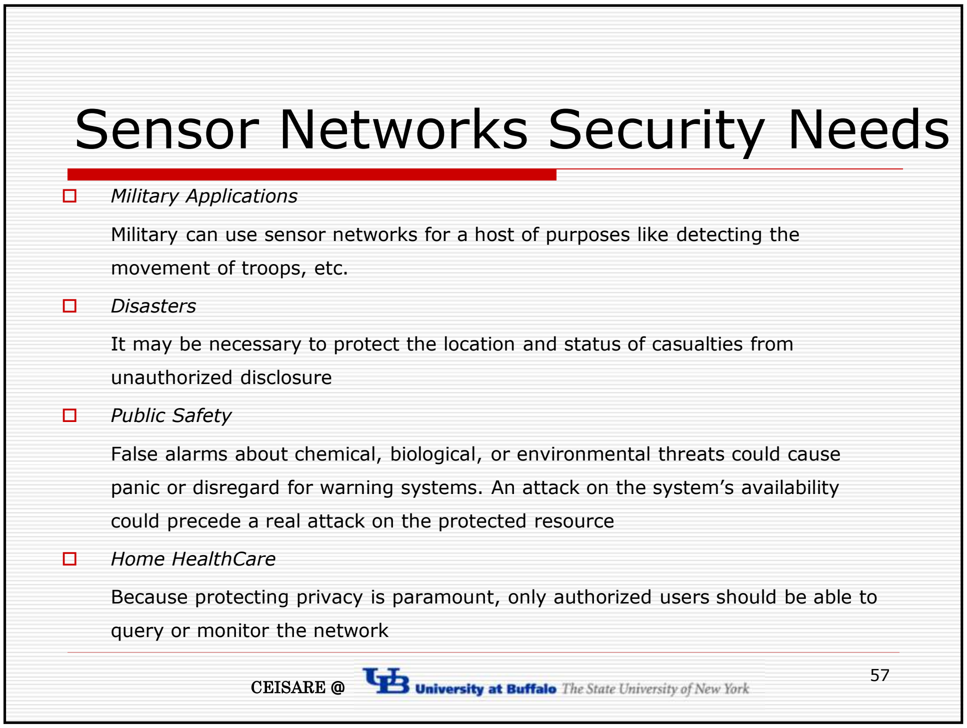
Sensor Networks Security

- □ Only a brief overview



Motivation – Sensor Networks

- □ Sensor networks – promising approach
- □ Monitoring wildlife, machinery performance monitoring, earthquake monitoring, military application, highway traffic etc.
- □ Perform in-network processing
  - Data aggregation and forwarding summaries
- □ Critical to protect it
  - Traditional security techniques cannot be applied
  - Deployed in accessible areas – subject to physical attacks
  - Close to people – poses additional problems



Sensor Networks Security Needs

- □ *Military Applications*

  Military can use sensor networks for a host of purposes like detecting the movement of troops, etc.

- □ *Disasters*

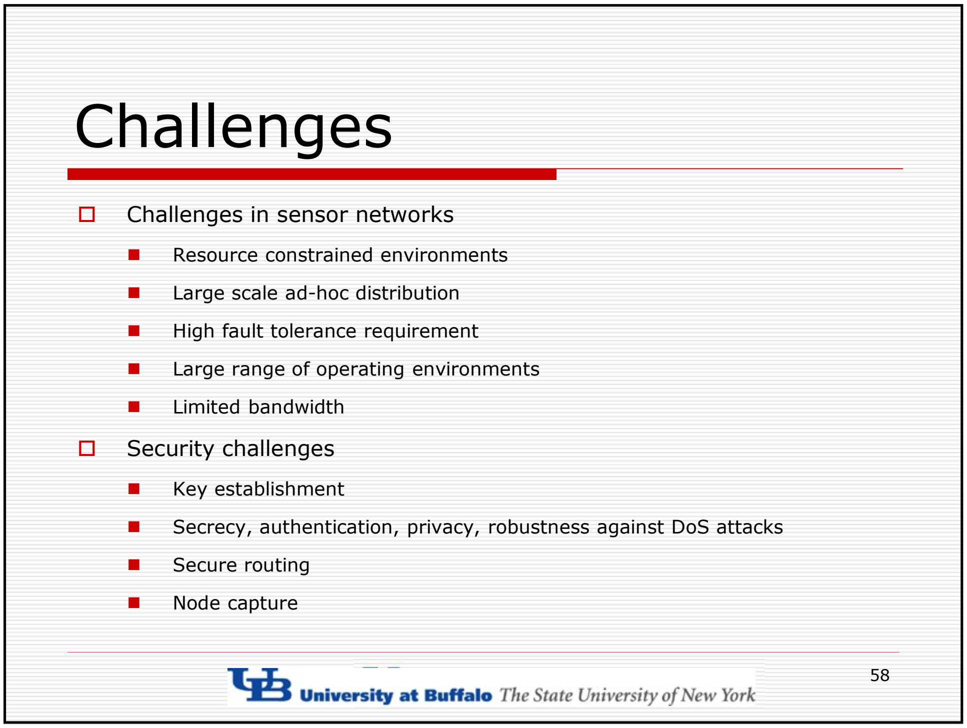
  It may be necessary to protect the location and status of casualties from unauthorized disclosure

- □ *Public Safety*

  False alarms about chemical, biological, or environmental threats could cause panic or disregard for warning systems. An attack on the system's availability could precede a real attack on the protected resource

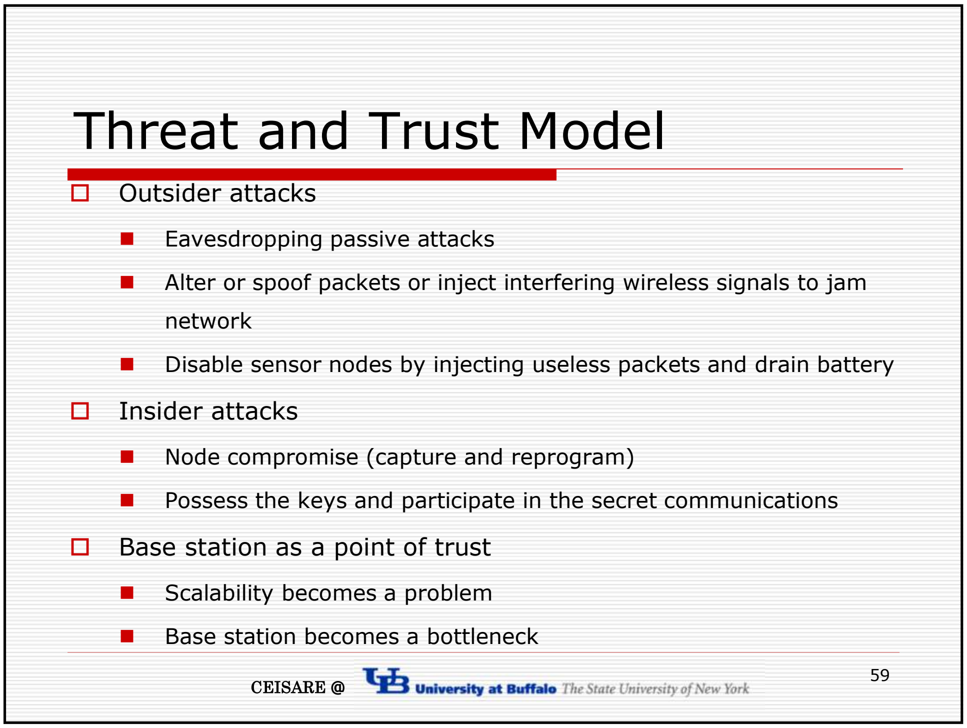
- □ *Home HealthCare*

  Because protecting privacy is paramount, only authorized users should be able to query or monitor the network



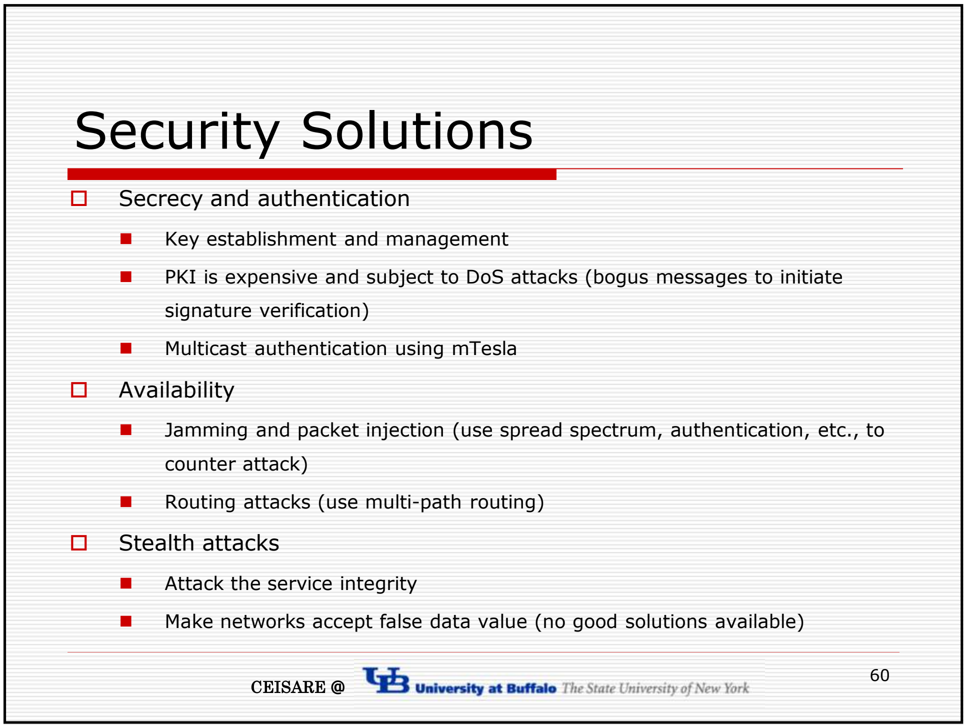
Challenges

- □ Challenges in sensor networks
  - Resource constrained environments
  - Large scale ad-hoc distribution
  - High fault tolerance requirement
  - Large range of operating environments
  - Limited bandwidth
- □ Security challenges
  - Key establishment
  - Secrecy, authentication, privacy, robustness against DoS attacks
  - Secure routing
  - Node capture



Threat and Trust Model

- Outsider attacks
  - Eavesdropping passive attacks
  - Alter or spoof packets or inject interfering wireless signals to jam network
  - Disable sensor nodes by injecting useless packets and drain battery
- Insider attacks
  - Node compromise (capture and reprogram)
  - Possess the keys and participate in the secret communications
- Base station as a point of trust
  - Scalability becomes a problem
  - Base station becomes a bottleneck



Security Solutions

- Secrecy and authentication
  - Key establishment and management
  - PKI is expensive and subject to DoS attacks (bogus messages to initiate signature verification)
  - Multicast authentication using mTesla
- Availability
  - Jamming and packet injection (use spread spectrum, authentication, etc., to counter attack)
  - Routing attacks (use multi-path routing)
- Stealth attacks
  - Attack the service integrity
  - Make networks accept false data value (no good solutions available)

Attacks and Defenses

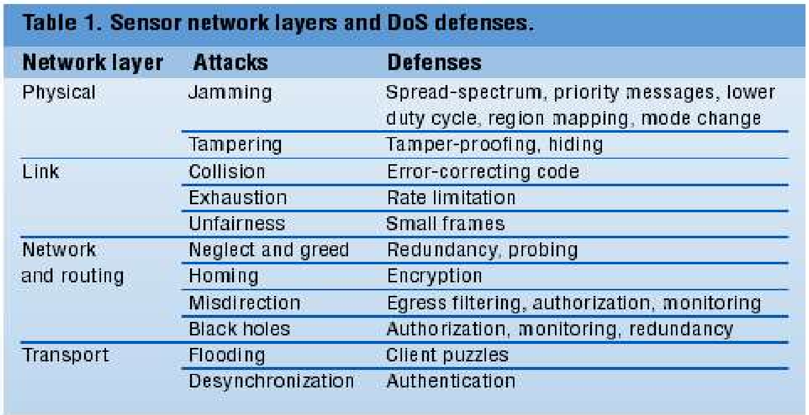
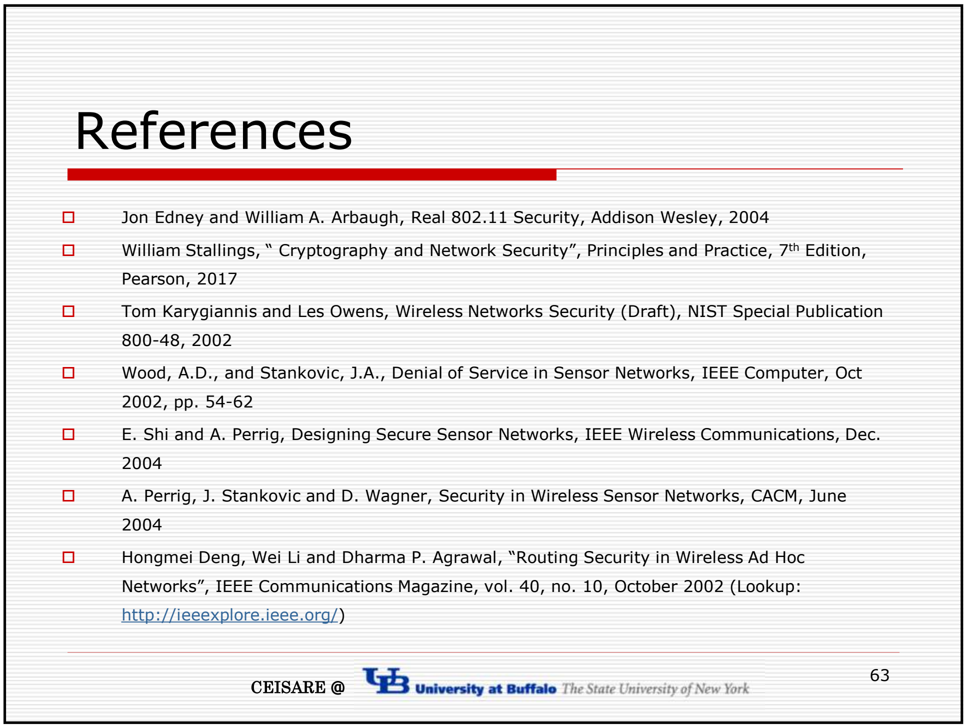


Table 1. Sensor network layers and DoS defenses.

Network layer	Attacks	Defenses
Physical	Jamming	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change
	Tampering	Tamper-proofing, hiding
Link	Collision	Error-correcting code
	Exhaustion	Rate limitation
	Unfairness	Small frames
Network and routing	Neglect and greed	Redundancy, probing
	Homing	Encryption
	Misdirection	Egress filtering, authorization, monitoring
	Black holes	Authorization, monitoring, redundancy
Transport	Flooding	Client puzzles
	Desynchronization	Authentication

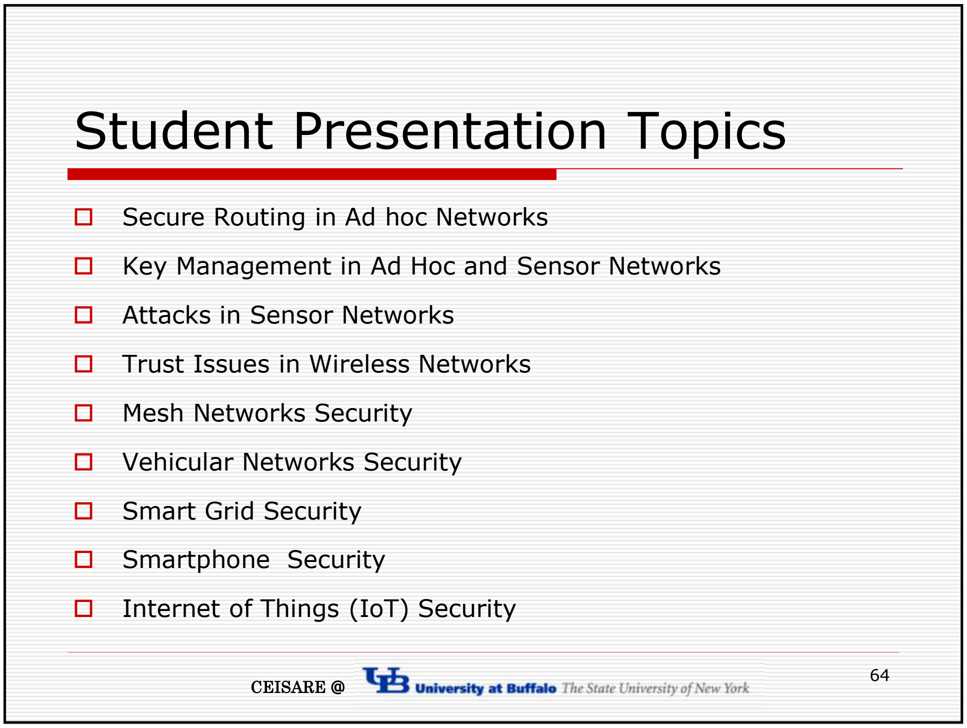
Summary

- Secure routing is vital to acceptance and use of sensor networks
- The current protocols lack the support and are inherently insecure
- Authentication and cryptography presents the first line of defense but is not enough
- Security in sensor networks is an open problem and requires much more work



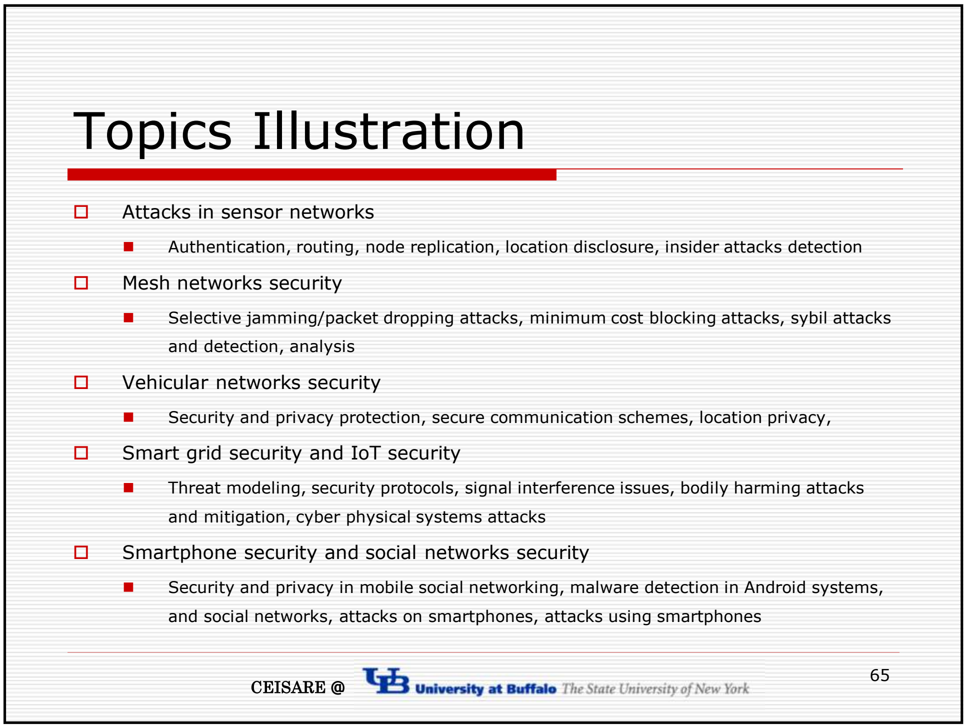
References

- Jon Edney and William A. Arbaugh, Real 802.11 Security, Addison Wesley, 2004
- William Stallings, " Cryptography and Network Security", Principles and Practice, 7th Edition, Pearson, 2017
- Tom Karygiannis and Les Owens, Wireless Networks Security (Draft), NIST Special Publication 800-48, 2002
- Wood, A.D., and Stankovic, J.A., Denial of Service in Sensor Networks, IEEE Computer, Oct 2002, pp. 54-62
- E. Shi and A. Perrig, Designing Secure Sensor Networks, IEEE Wireless Communications, Dec. 2004
- A. Perrig, J. Stankovic and D. Wagner, Security in Wireless Sensor Networks, CACM, June 2004
- Hongmei Deng, Wei Li and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine, vol. 40, no. 10, October 2002 (Lookup: http://ieeexplore.ieee.org/)



Student Presentation Topics

- Secure Routing in Ad hoc Networks
- Key Management in Ad Hoc and Sensor Networks
- Attacks in Sensor Networks
- Trust Issues in Wireless Networks
- Mesh Networks Security
- Vehicular Networks Security
- Smart Grid Security
- Smartphone Security
- Internet of Things (IoT) Security



Topics Illustration

- Attacks in sensor networks
  - Authentication, routing, node replication, location disclosure, insider attacks detection
- Mesh networks security
  - Selective jamming/packet dropping attacks, minimum cost blocking attacks, sybil attacks and detection, analysis
- Vehicular networks security
  - Security and privacy protection, secure communication schemes, location privacy,
- Smart grid security and IoT security
  - Threat modeling, security protocols, signal interference issues, bodily harming attacks and mitigation, cyber physical systems attacks
- Smartphone security and social networks security
  - Security and privacy in mobile social networking, malware detection in Android systems, and social networks, attacks on smartphones, attacks using smartphones