



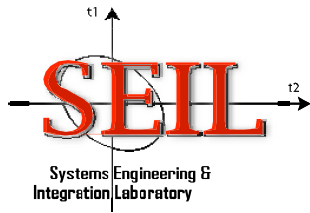
Attacks and Defenses Utilizing Cross-Layer Interactions in MANET

John S. Baras and Svetlana Radosavac

**Department of Electrical and Computer Engineering
Institute for Systems Research
University of Maryland College Park**

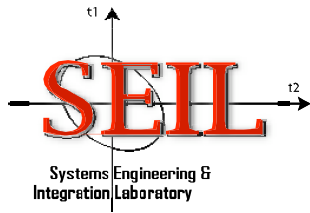
**NATO Cross-Layer Workshop
NRL, June 2-3, 2004**

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 01 DEC 2007		2. REPORT TYPE N/A		3. DATES COVERED	
4. TITLE AND SUBTITLE Attacks and Defenses Utilizing Cross-Layer Interactions in MANET				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Department of Electrical and Computer Engineering Institute for Systems Research University of Maryland College Park				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited.					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 22	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



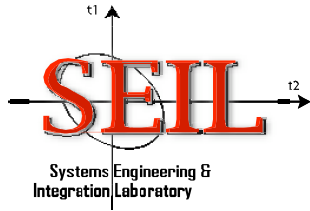
Motivation

- Possibility of Denial of Service (DoS) attacks in the MAC layer
- **MAC and routing layers interact**
- **Current protocols offer insufficient cross-layer interaction**
- Possible to cause an attack by **manipulating traffic in the MAC layer** and propagate attack to the routing layer
- **Need for additional interaction between MAC and routing:**
 - MAC needs to pass information to routing in case of congestion
 - Routing decides on new routes that are not affected by congestion;
 - IDS makes sure the new routes don't contain malicious nodes
- **Goal: Detect the intrusion, minimizing detection time t_D and the number of false alarms, while maximizing the probability of detection P_D**



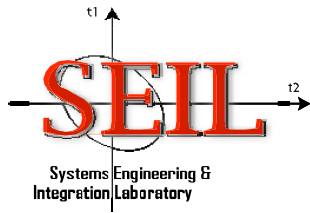
MAC Layer Issues

- Issues:
 - How to **differentiate** between an **attack** and **congestion** in wireless networks?
 - **Randomness** of Contention Window (CW) brings additional uncertainty in detection process
 - How long a node can stay malicious without being detected? What does it do in case of collision?
 - Is it realistic to assume the existence of **stealthy attacks**?
 - What is the number of nodes needed for attack detection, in particular **partition detection**?
 - Which parameters MAC and routing need to **measure and exchange** for efficient cross-layer Intrusion Detection Scheme?



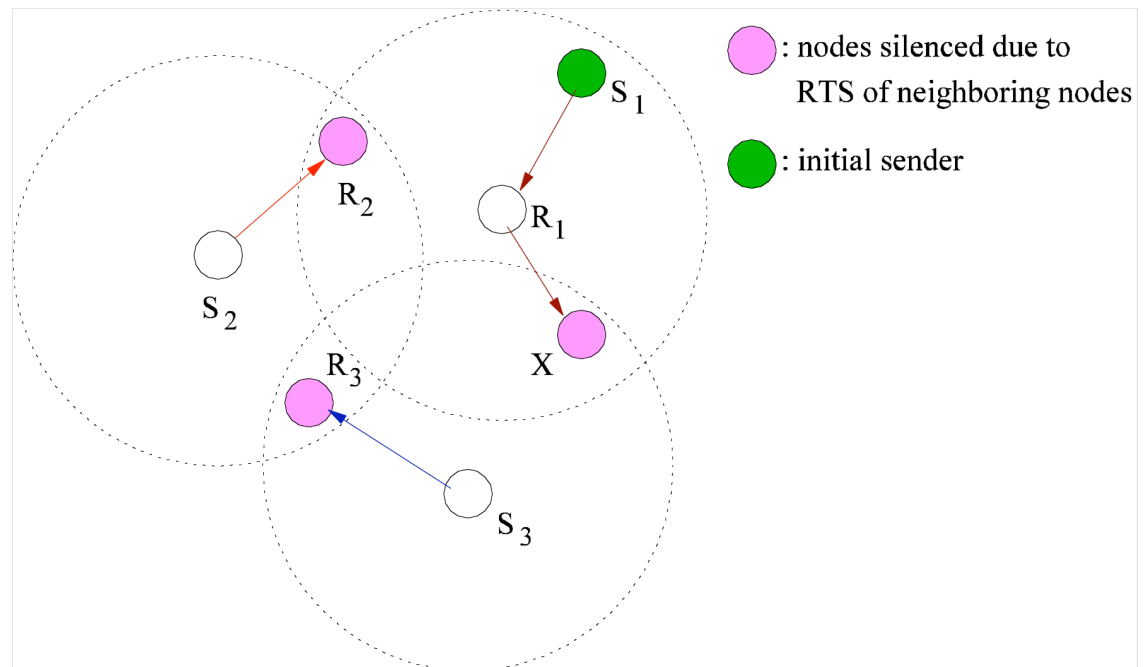
Routing issues

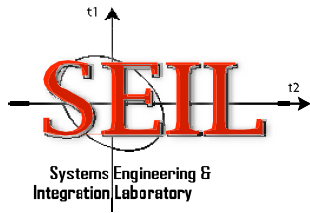
- Routing **does** influence the performance of MAC
- Routing chooses routes independently of MAC
- MAC only forwards the packet to the given node → **may lead to failures**
- Due to congestion and interference, MAC may not be able to deliver the packet
- Routing uses alternate route which is in vicinity of existing one → most likely unsuccessfully!
- **Solution:** let MAC and routing interact with each other and with the IDS
- **IDS:** has past behavior patterns and information from both MAC and routing;
 - Delivers final decision
 - Communicates with routing and MAC



MAC issues

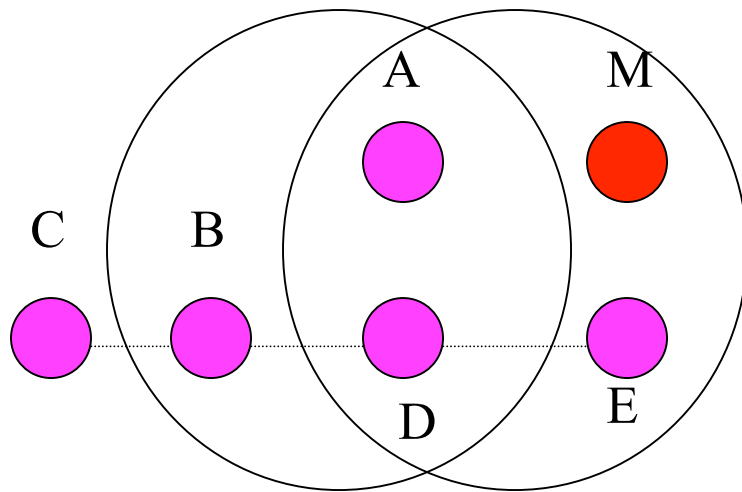
- Even without attacks MAC suffers from several problems:
 - RTS/CTS propagation
 - Unfairness due to exponential backoff
 - Path interference – can lead to chain reaction *_if attacked this way, not likely to find the attacker!*
- Solution:
 - Avoid *interfering paths*
- How?
 - Conflict graphs





Possible Attacks

Attack 1



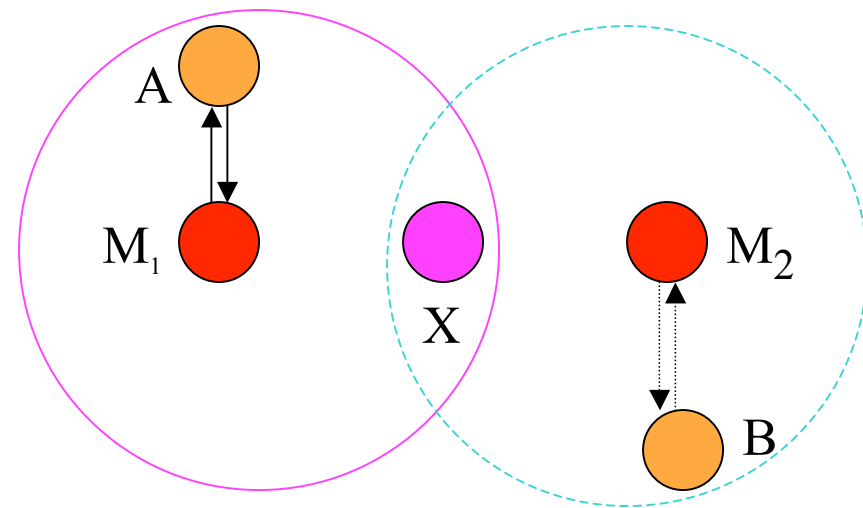
**M “blocks” D
from communicating**

Attack 2

Two colluding attackers M_1 and M_2

First transmission $M_1 \Rightarrow A$

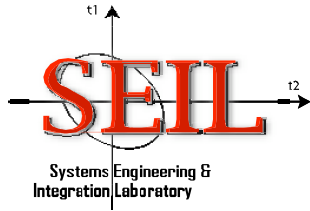
X has to defer



Second transmission $M_2 \Rightarrow B$

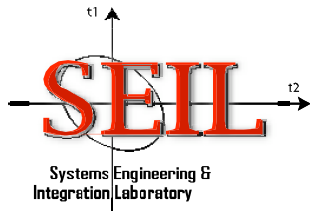
X has to defer

**M_1, M_2 synchronize
D is “blocked” from communicating**

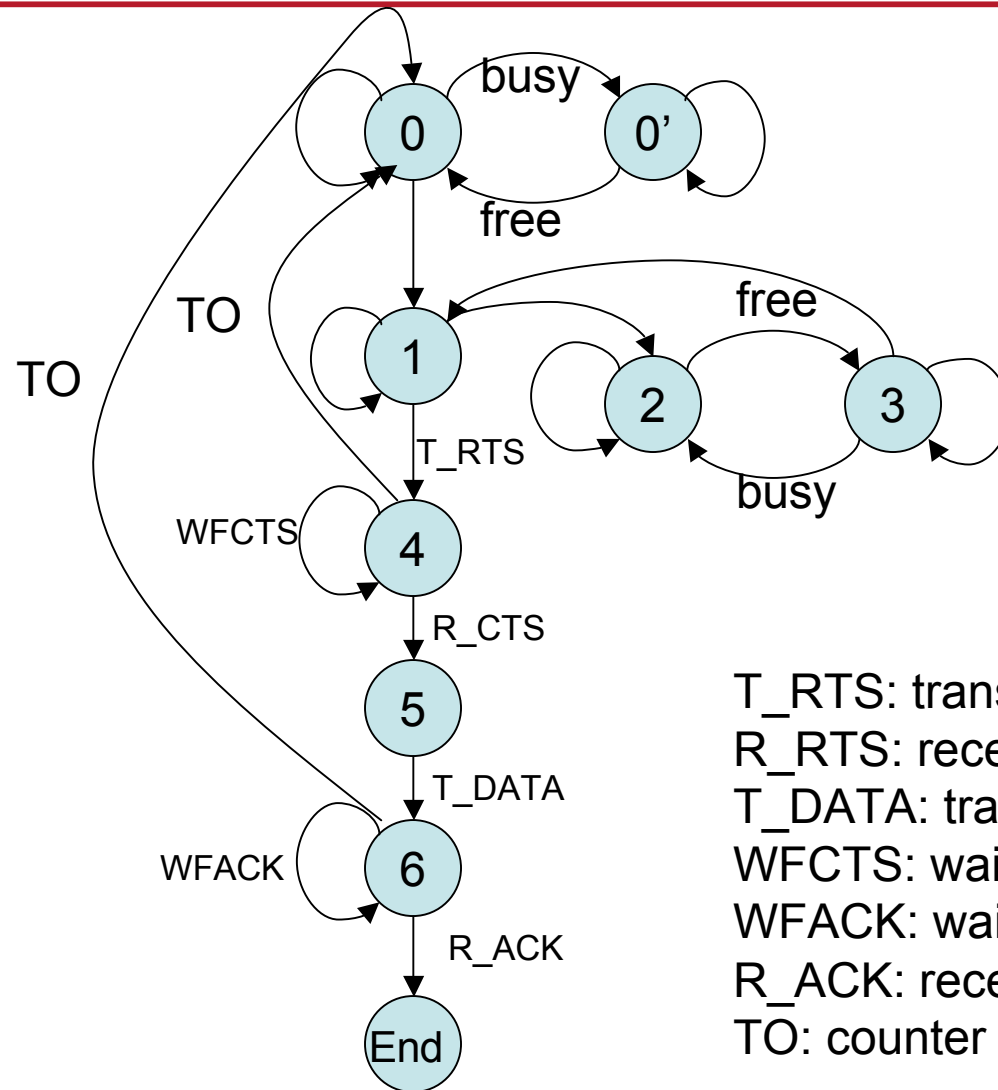


Node classification

- **Normal**
 - Obeys the rules of MAC layer protocols when both sending and receiving packets.
 - Will not behave selfishly and will reply to RTS requests from other nodes
 - Will update their CW, NAV etc. according to the rules of the protocol
- **Misbehaving**
 - **Goal:** gain priority in the network or disrupt already existing routes.
 - Usually change the value of **CW, NAV value, Duration/ID** field in the packet, etc.
- **Malicious**
 - All communication done following the MAC layer protocol
 - Will employ legitimate communications which result in DoS in one or multiple nodes and attack propagation through the network.
- **Issues:**
 - best strategy for detection of misbehaving nodes
 - How long a malicious node can stay malicious? Will it eventually collide with normal node?
 - What is the best strategy to stay undetected?
 - What about colluding nodes?

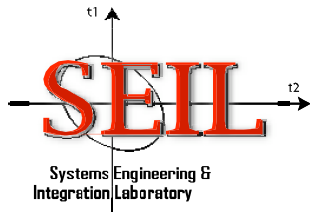


Formal Model

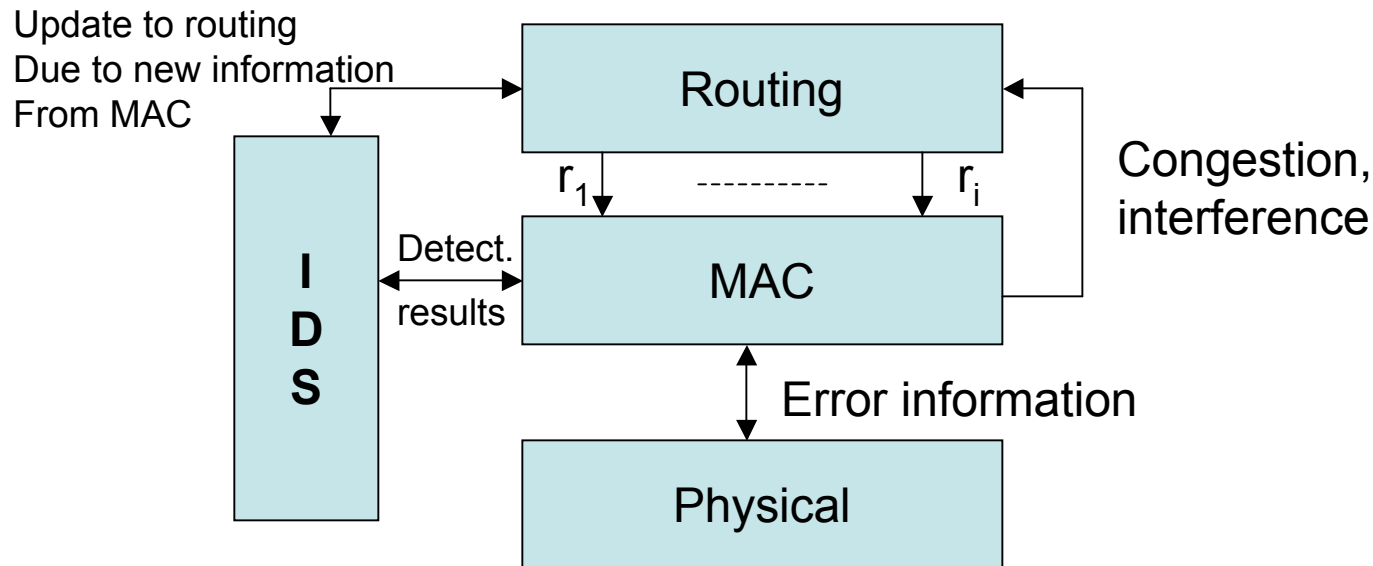


- MAC protocols easier to model than routing
- Represent MAC protocols in the form of EFSMs
- Need to impose **time constraints**
- In combination with logic useful as addition to IDS

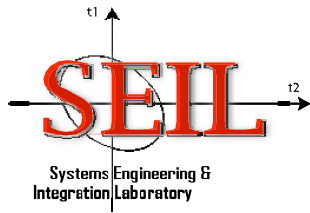
T_RTS: transmit RTS
 R_RTS: receive RTS
 T_DATA: transmit data
 WFCTS: wait for CTS
 WFACK: wait for acknowledgement
 R_ACK: receive ACK
 TO: counter timed out



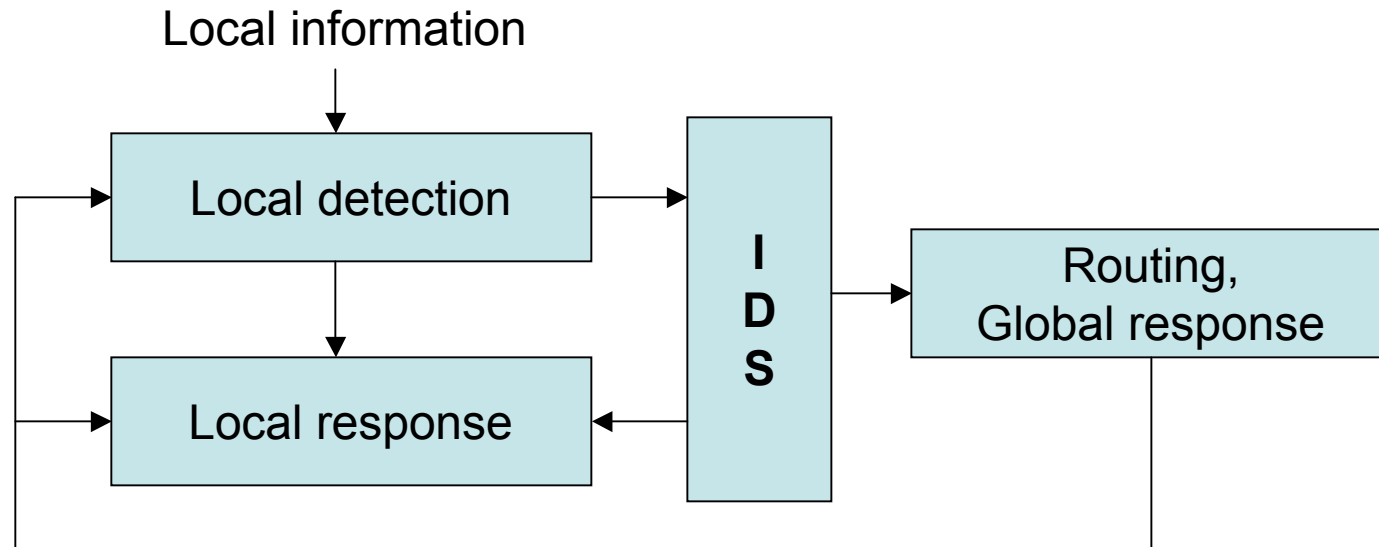
Cross-layer scheme



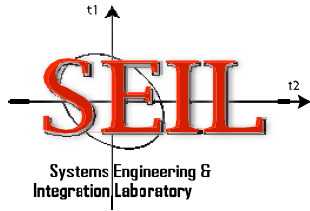
- Routing sends several choices to MAC
- MAC uses: **local detection, interference information, information from the physical layer,...**
- MAC delivers the result back to routing _ subset of original routes
- Consults IDS if necessary->**global detection**



Detection scheme in MAC



- Input: local information
- Local detection: use Neyman-Pearson rule to detect the attack
- If not able to decide forward to IDS and let it decide
- Issue local (global) response and exchange the information with routing



Local Detection

$$P(\text{Receiver} = \text{busy} | \text{Sender} = \text{busy}) = 1$$

$$P(\text{Receiver} = \text{busy} | \text{Sender} = \text{idle}) = p$$

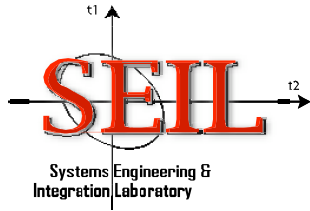
Hypothesis testing:

H_0 = Sender is normal

H_1 = Sender is malicious

Log-likelihood defined as:

$$L = \frac{P_{H_1}}{P_{H_0}} = \begin{matrix} H_1 \\ > \\ < \\ H_0 \end{matrix} \eta$$



Local Detection

- Due to channel conditions the receiver may not count the backoff correctly

B_s : the actual backoff of sender

B_r : backoff observed at the receiver side

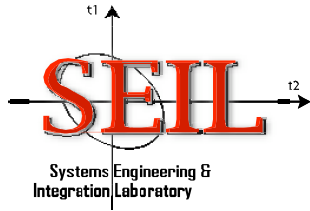
B_t : threshold for backoff

Two cases:

$$B_r \geq B_t : P_{H_0} = 1 \wedge P_{H_1} = 0$$

$$B_r < B_t : P_{H_0} = P(B_s > B_t \mid B_r < B_t) = P(\text{making more than } B_t - B_r \text{ errors})$$

$$P_{H_1} = P(B_s < B_t \mid B_r < B_t) = P(\text{making } [0, B_t - B_r) \text{ errors})$$



Local Detection

- For $B_r < B_t$ log-likelihood ratio becomes:

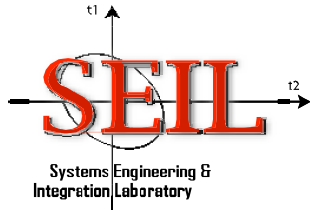
$$p^{B_r} \underset{H_0}{\overset{H_1}{>}} \eta', \eta' = f(\eta, B_t, \text{assigned backoff})$$

- Decision rule:

$$H_1 : B_r < \eta'$$

$$H_0 : B_r > \eta'$$

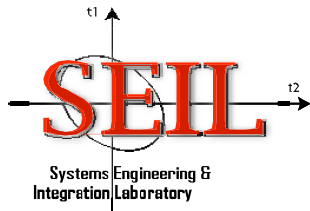
$$H_1 \text{ with probability } \gamma : B_r = \eta'$$



Tradeoffs



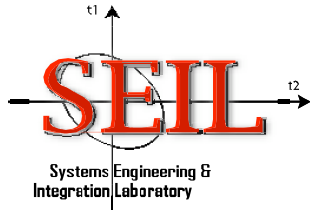
- If B_r is increased, the number of errors is decreased (probability of correct, fastest detection increases).
- Log-likelihood ratio decreases with B_r increasing.
- When B_r increases the probability of classifying the node as normal increases.
- **But** the probability of false alarm increases
- Concerned about the probability of false alarm
- When backoff not fixed even normal nodes can transmit after a small number of idle slots.
- When backoff fixed, concerned about colluding nodes and malicious nodes listening to my transmission



Distributed detection



- Helps in decreasing number of false alarms and missing attacks
- *NP rule for distributed detection:*
 - For a predetermined probability of false alarm, $P_F = _$, find optimum local and global decision rules $\Gamma = (\gamma_0, \gamma_1, \dots, \gamma_N)$ that minimize the global probability of miss
- Vector of local observations: $B_o = \{b_{o_1}, \dots, b_{o_N}\}$
- Each node makes decisions based on local observations and sends its log-likelihood ratio to IDS
- **Local decision** vector: $u = \{u_1, \dots, u_N\}$
- **Global decision** vector: $u_0 = \gamma_0(u), u_0 = \{0, 1\}$



Distributed Detection



- Optimal test given by:

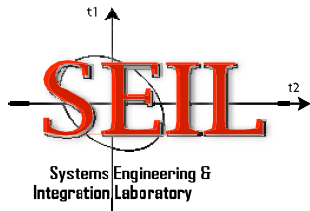
$$\Lambda(u) = \frac{P(u | H_1)}{P(u | H_0)} = \begin{cases} > \lambda_0, \text{ decide } H_1 \\ < \lambda_0, \text{ decide } H_0 \end{cases} = \text{decide } H_1 \text{ with prob. } \gamma$$

- Special case: P_D of all nodes are identical and P_F of all nodes are identical

- The optimal decision rule becomes: $k \underset{H_0}{\overset{H_1}{>}} \eta'$

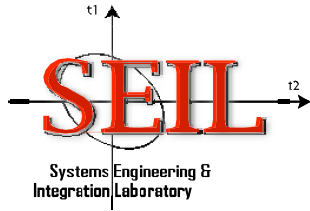
k : number of nodes choosing H_1

$$\eta' = f(P_D, P_F, N, \eta)$$



Attack Detection

- For detection of more sophisticated attacks we formulate **theorems** (series of rules a fault-free MAC protocol cannot violate)
 - e.g. cannot violate exponentially growing contention window w.r. to next successful transmission time
- For **attack detection** Automatic Model Checking is executed with input of the relevant rule (theorem) parameters from the nodes under examination
- Non-allowed behaviors of system denoted as σ_i
- **Safety behavior**: σ
- σ is satisfied when $\neg\sigma_1 \wedge \neg\sigma_2 \wedge \dots \wedge \neg\sigma_n$ are satisfied
- If there is σ_i s.t. the safe behavior is violated, the **model checker goes backwards and saves the time history** together with values of related variables
- **This scheme can be used for automatic attack/fault generation**



Attack Detection

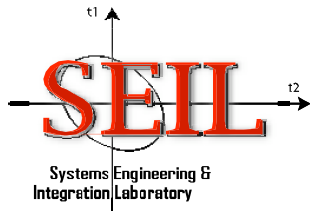
- The *vulnerable period* of IEEE 802.11 MAC is in RTS/CTS exchange
- We formulate the following theorem:
 - *Two processes cannot be in their critical section at the same time:*

$$AG(\neg(P_i.s = c \wedge P_j.s = c))$$

- *A process that wants to enter its critical section is eventually able to do so:*

$$AG(P_i.s = A \Rightarrow AF(P_i.s = c))$$

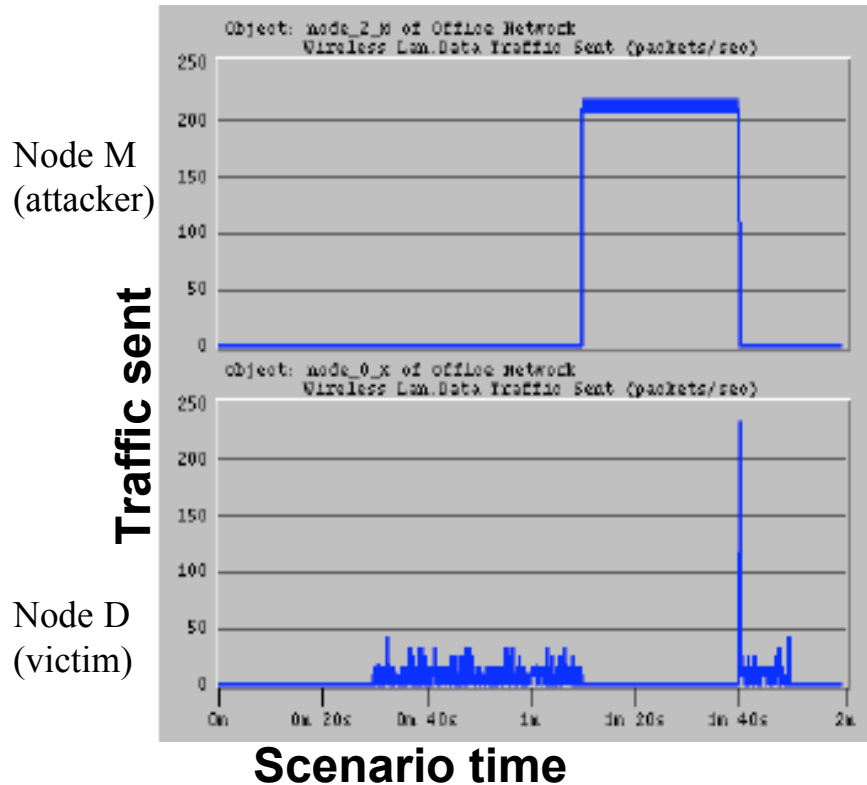
- First rule helpful in case when other nodes assign backoff to sender!



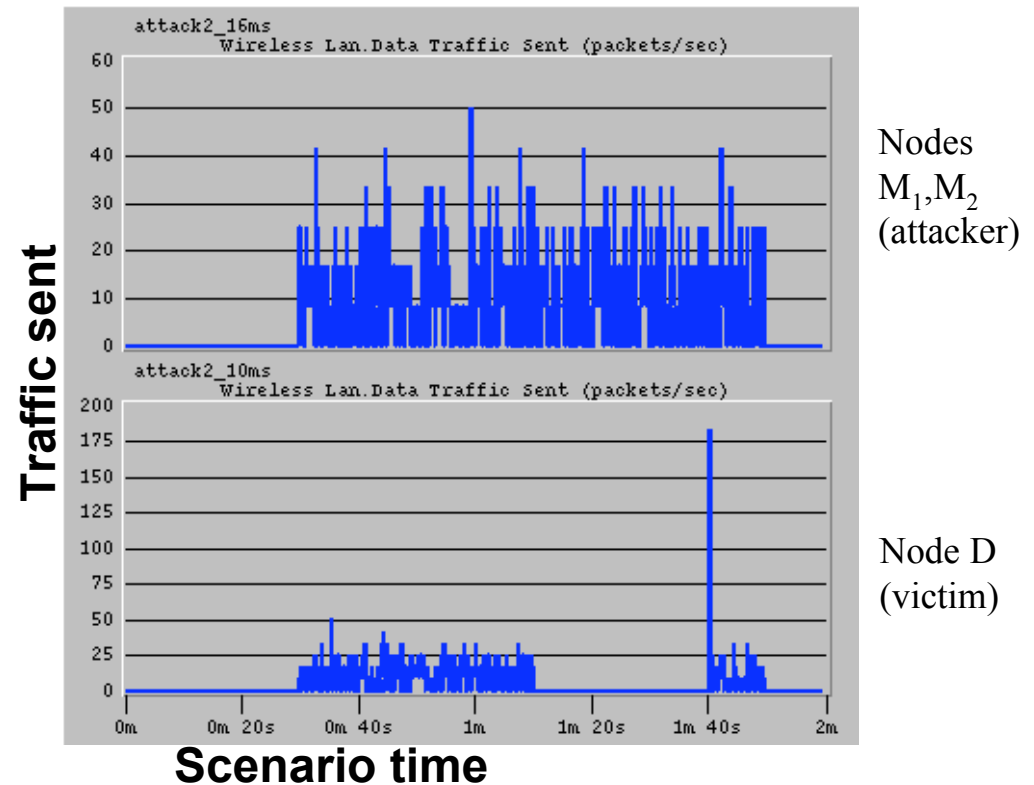
Results

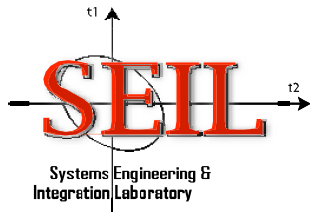
Attacks propagate from MAC to routing disabling key nodes:

Attack 1 results:



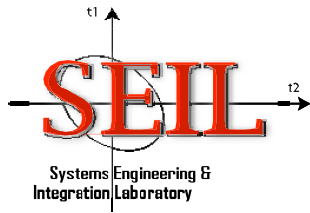
Attack 2 results:





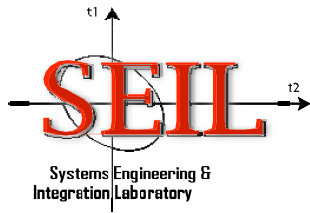
Conclusions

- **Need to implement cooperation between MAC and routing** to be able to detect attacks more efficiently
- Other attacks apart from CW misuse exist: NAV, other kinds of backoff counter abuse, ...
- **MAC can be modeled using Formal Models**
- Duration of malicious behavior depends on the traffic
- Stealthy attacks exist in short term, long-term existence depends on traffic and interference
- Conflict graphs good approach for solving problems of interference
- Need to simplify the problem since it's NP-complete!



Future Work

- Construct an Intrusion Detection System with ability to detect and classify known attacks using techniques presented and detect unknown attacks **using a database of attack features**
- How to detect anomalies in wireless networks?
- **Model other MAC protocols using EFSMs**
- Use the system for online attack generation that are passed to IDS and added to existing database of attacks
- Event ordering and correct timing have crucial roles in MAC protocols: necessary to **use ordered models of execution** with explicit timings
- Define the ordered model of execution with **multiple goals**
- Describe changes in state variables that lead to certain states



Future Work (cont.)

- Enable **automatic attack generation** using **EFSM models of MAC layer**
- **Challenges:**
 - Range of attacks is much wider in wireless than in wired networks;
 - How to distinguish between an attack and high volume of traffic?
 - **Which parameters to exchange between layers** to achieve efficient intrusion detection?
 - How to detect unknown attacks **without high false positive rate**?
 - Lack of data for testing; collaboration with industry and DoD Labs
- Potential approach - combination of **model checking** and **theorem proving** techniques.
- Plan to use a combination of analytical techniques from graph theory, dynamic games, distributed detection, temporal logic, hybrid automata