Containing DoS Attacks in Broadcast Authentication in Sensor Networks

(Ronghua Wang, Wenliang Du, Peng Ning)

Advanced Computer Networks
CS577 – Fall 2013
WPI, Worcester.

Presented by Pankaj Didwania
Dec.10th, 2013

Introduction

- Sensor networks using Public Key Cryptography (PKC) are susceptible to Denial of Service (DoS) attacks.
- Attackers keep broadcasting bogus messages incurring extra costs, in an attempt to exhaust the energy of the honest nodes.
- The long time to verify each message using PKC increases the response time of the nodes.
- Impractical for the nodes to validate each incoming message before forwarding it.

Intro…

This paper

- Discusses the DoS attacks attempting to drain node energy.
- Increase response time to broadcast message degrade overall performance.
- Presents a dynamic window scheme, where sensor nodes determine whether first to verify a message or first to forward the message.
- Accomplishes this by analyzing the distance of the malicious attacker node.
- And how many hops the message has travelled.

Intro…

- Forwarding First Method : Upon receiving these faked messages, sensor nodes forward them to their neighbors before they authenticate.

  -Sensors eventually drop the faked messages after the verification fails, but the damage has already been made.

- Authentication-first method : Verify each message before forwarding it.

  -Faked messages get dropped at the first-hop neighbors of the malicious nodes, so nodes beyond them will not be affected. Although this is preferable when dealing with faked messages, it has significant penalty on legitimate broadcast messages, because it takes time for sensor nodes to conduct message authentication.

Proposed Scheme

- Dynamic Window Scheme: Combination of the authentication-first and the forwarding-first scheme, which can achieve a good trade-off between the broadcast delay for authentic messages and energy savings for faked messages.
- Sensor nodes gradually shift to auth-first scheme if they start receiving many faked messages, but will remain in forwarding-first mode if the majority of the messages they receive are authentic. The decision is based on the validity of the incoming broadcast messages they receive.

Design & Analysis

- AIMD - An old concept, now being applied to Network Sensors.[Additive Increase Multiplicative Decrease]
- Sensor Nodes have no idea on who is malicious and who is not.
- Sensor nodes are extremely resource-constrained.
- They should not be carried away by the overwhelming attacks from the adversaries.
- This DoS resistant scheme is the key contribution of this paper.
- Analyze the various patterns of DoS attacks the adversaries may implement; evaluate performance under these attacks.

System Model

- Attacking Model:

  - The goal of the attackers is to exhaust the energy of the sensor nodes.

  - And to increase the response time of the sensor nodes to the authentic broadcast messages.

- Primary attacking method of the adversaries is to broadcast large number of faked messages.
- Attackers may forward authentic messages from time to time to fool honest nodes.
- Adversaries deploy malicious sensors or compromise honest nodes.

System Model - Assumptions

- Attacks are static.
- Adversaries, Sensor Nodes and Base Stations stay in fixed locations throughout the attack.
- Topology of the network is fixed.
- Attackers can choose their locations or take multiple identities, but they cannot move during the attack.

Design Goals

- Defend sensor networks against DoS attacks.
- Especially ones that aim at exhausting the energy of sensor nodes.
- Main goal is to reduce the damage of the attacks on the entire network.
- Contain the damage of DoS attacks to a small portion of the sensor nodes.
- Effectiveness; Efficiency; Responsiveness; Flexibility;

A DYNAMIC WINDOW SCHEME…

- Sensor nodes need to drop faked messages as early as possible.
- Need a mechanism to single out the malicious node(s).
- Drop faked packets from those malicious nodes.
- Authentication-first not the best choice as it causes delays.
- Messages from these nodes be verified before being forwarded.
- Messages from other sources be forwarded before being verified.

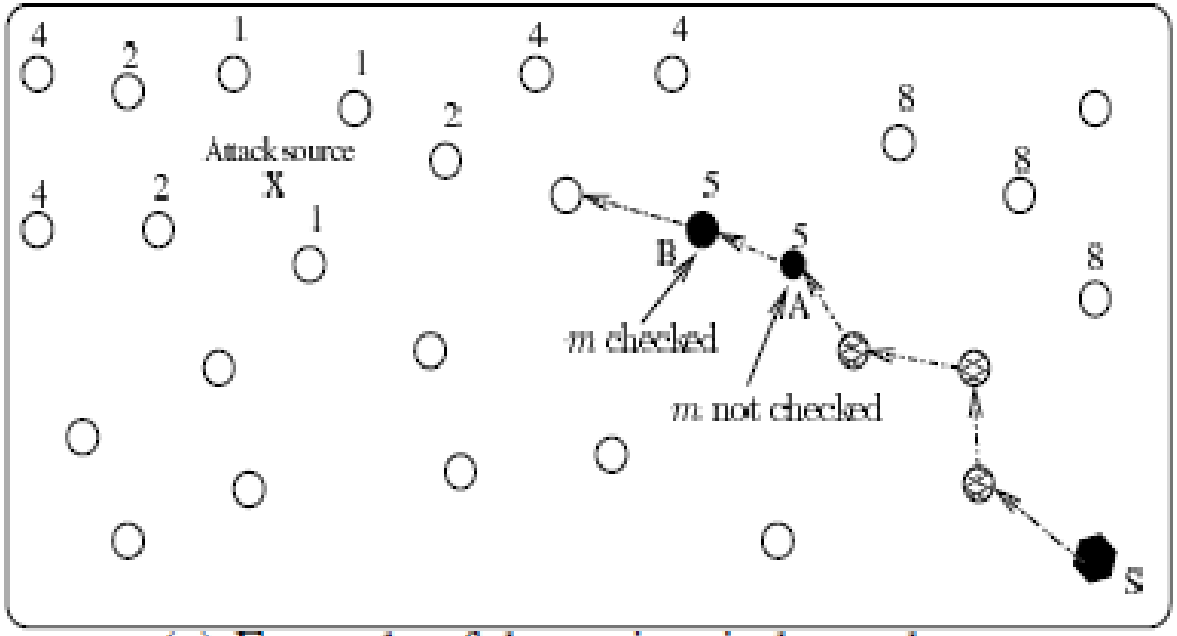
A DYNAMIC WINDOW SCHEME…

- Malicious nodes always pretend to be forwarding messages instead of initiating new ones.
- Honest nodes can't determine they are the first-hop victims of malicious nodes.
- Question: Is it possible that sensors gradually shift toward authentication-first mode in a way such that eventually, only the first-hop victims of the attackers stay in authentication-first mode?

A DYNAMIC WINDOW SCHEME…

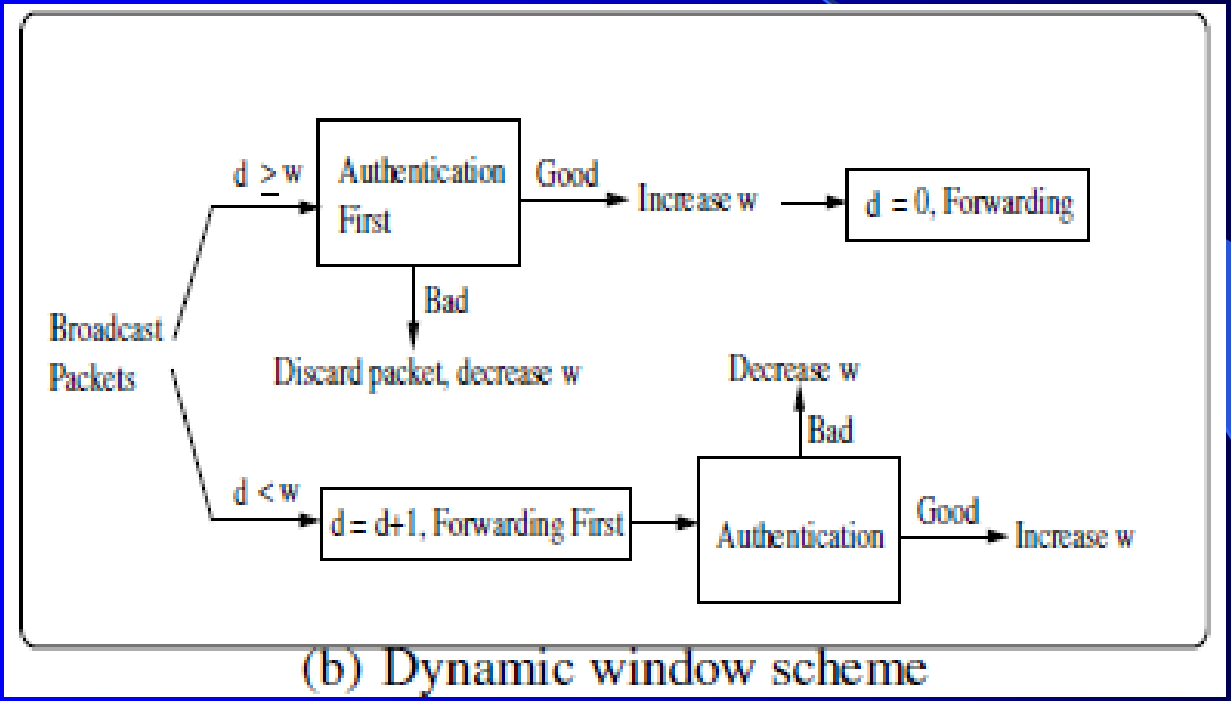
- In DWS, each sensor node s maintains a new parameter 'authentication window size' (w). This parameter specifies the largest number of hops an incoming message can be forwarded without being verified. i.e. a cutoff number.
- Each broadcast message m keeps record of distance (da) which is used to record the number of hops the message has passed since its last authentication.
- If $d < w$, s is in the forwarding-first mode, it increases d and forwards m without verification.
- If $d \geq w$, s is in the authentication-first mode which authenticates m first.
- if the authentication fails, s drops m; otherwise, s resets d to 0, and forwards m to its next hop neighbors.

A DYNAMIC WINDOW SCHEME…



(a) Example of dynamic window scheme

A DYNAMIC WINDOW SCHEME…



(b) Dynamic window scheme

DWS - Scheme overview

- System Initialization
- Message Broadcast
- Message forwarding and updating
- Authentication window size updates

DWS - Properties of the basic scheme

- Non-consecutive Authentic message Attack (NAA):

Property #1: If there are no consecutive authentic messages during DoS attacks, faked messages will eventually be dropped by the first two hops of the sensor nodes.

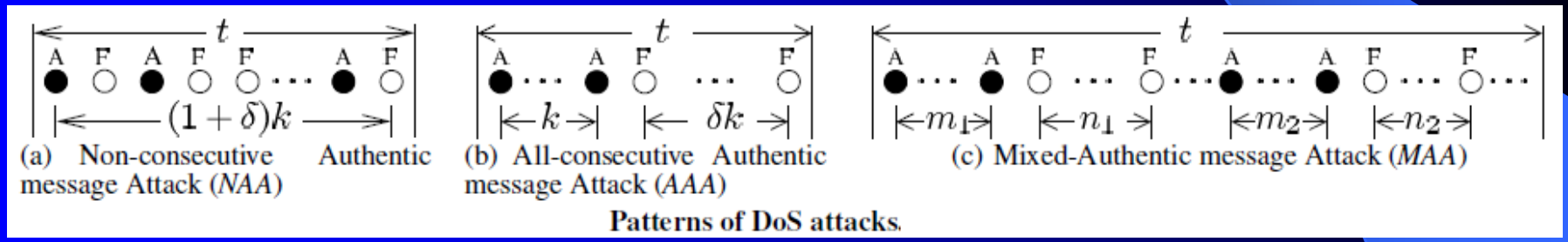
DWS - Properties of the basic scheme

- All-consecutive Authentic message Attack (AAA):

  Property #2: Given k authentic messages and k faked ones, if the k authentic messages are consecutive, faked ones will reach the most sensor nodes. In this case, at least $k - \lceil \log(k + 1) \rceil$ faked messages are dropped by the one-hop nodes..

DWS - Properties of the basic scheme

- Mixed-Authentic Message attack (MAA):



(a) Non-consecutive Authentic message Attack (*NAA*)

(b) All-consecutive Authentic message Attack (*AAA*)

(c) Mixed-Authentic message Attack (*MAA*)

Patterns of DoS attacks.

Energy saving in the presence of DoS attacks

THEOREM :

- In NAA, sensor nodes two hops away from the attacker are immune from the attack;
- In AAA, sensor nodes more than two hops away from the malicious attacker will receive at most ⌈log(k + 1)⌉ faked messages.

Broadcast delay for authentic messages

- Observation If v1, v2, · · · , vi are sorted (in increasing or decreasing order), then the number of nodes that are in authentication - first mode is at most :

$$\sum_{j=1}^{j=\omega_{max}} \lceil \frac{v_j}{j} \rceil$$

Extension of the Basic Scheme

- Window size updating functions: For the scheme to be effective in containing DoS attacks, window size updating functions should have the following properties.

  (1)Gradient distribution

  (2) Fast decrease

  (3) Slow increase

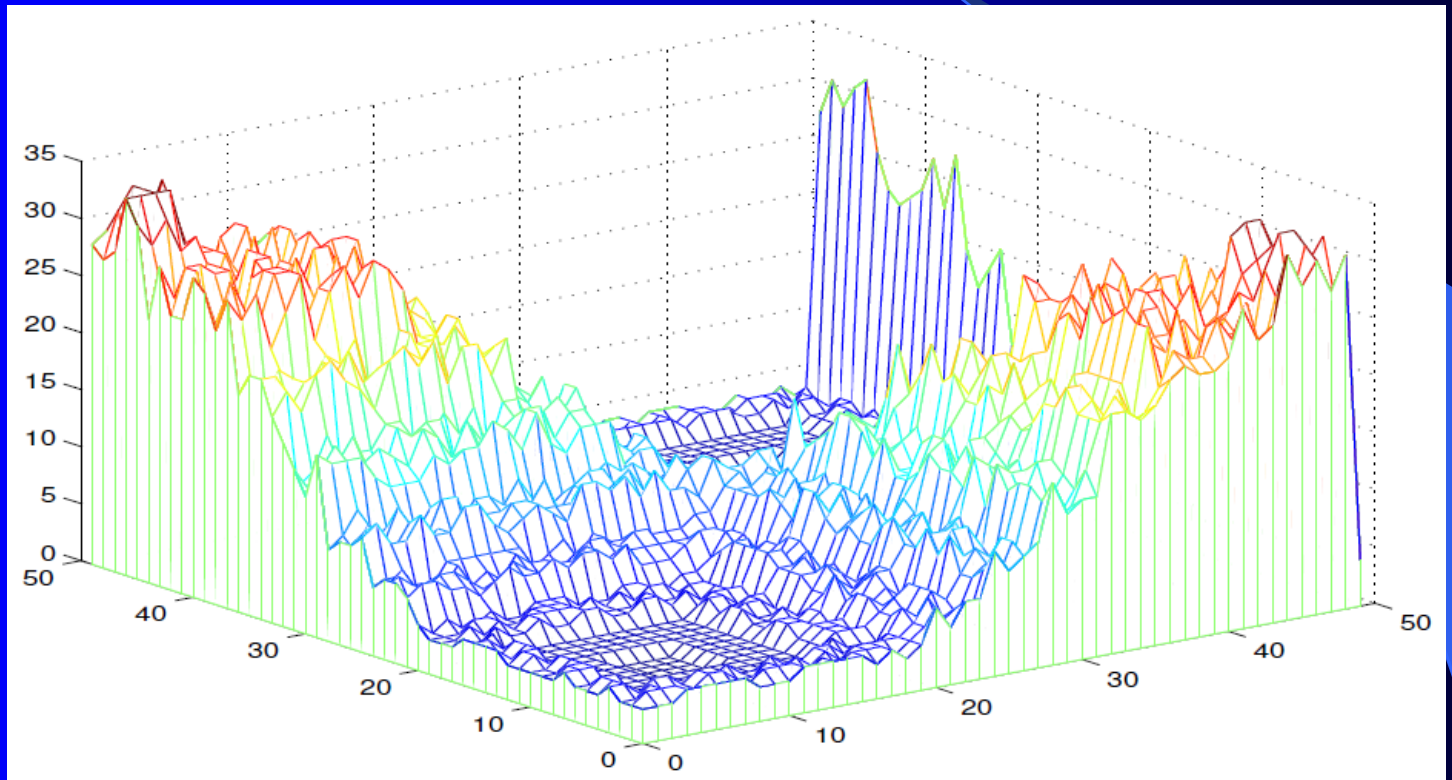
Extension of the Basic Scheme

- General window size updating functions

Property 2.1 *(Extension of Property 2) Given k authentic messages and δk faked messages, and given $\psi_f(\omega) = \omega + \alpha$, $\psi_s(\omega) = \omega/\beta$, if the adversary tries to affect most nodes, at least $\{\delta k - \lceil \log_\beta(\alpha k + 1) \rceil\}$ faked messages are dropped by the first hop of the malicious nodes.*

Multi-source attacks

- Two malicious nodes located at (10, 10) and (35, 35) keep broadcasting faked messages.



Window size on sensors under multi- attacks

Multi-source attacks

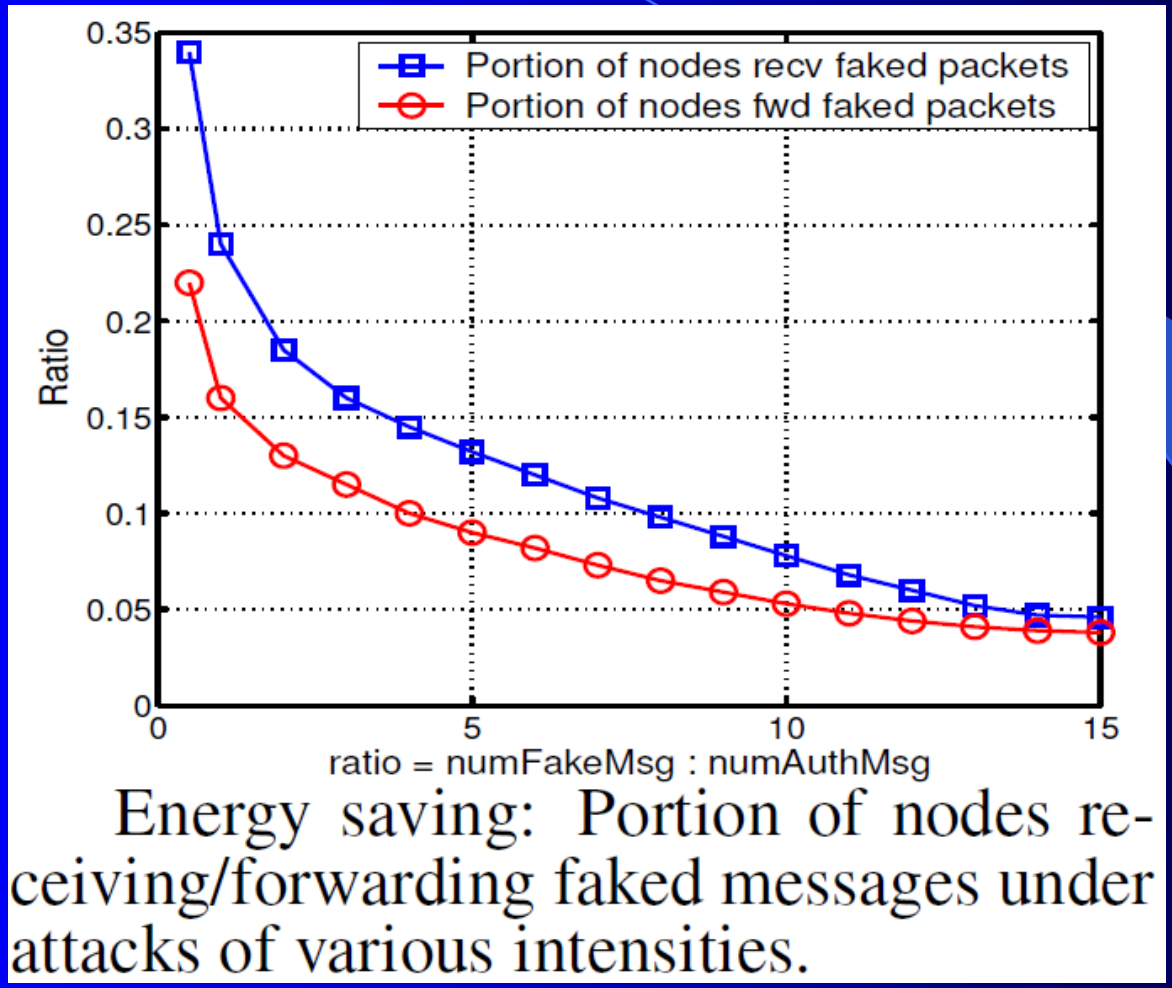
- Sensor nodes close to them will be affected, but for nodes far away from both of them, the impact is quite limited.
- Faked messages broadcast from the malicious nodes are dropped by the intermediate nodes.
- The multiple malicious nodes will divide the entire network into several smaller sub-areas.
- Sensor nodes close to the attackers will have smaller authentication window than nodes far away.
- When a message arrives at these nodes, it is more likely that this message will be verified before being forwarded.

EVALUATION AND ANALYSIS

- Env. setup : 5000 sensor nodes randomly deployed
- Area = 200m×200m.
- Transmission range of sensor nodes = 6m.
- Assumption : Msg Authentication Duration = 2 sec.
- Base stations & attackers are at fixed locations.
- Simulate the Mixed-Authentic Message Attacks (more realistic)
- Malicious nodes keep sending faked messages.
- They may also forward authentic messages intermittently.
- Initially, the auth. window size on each sensor node = 64 (Wmax).

Simulations and results

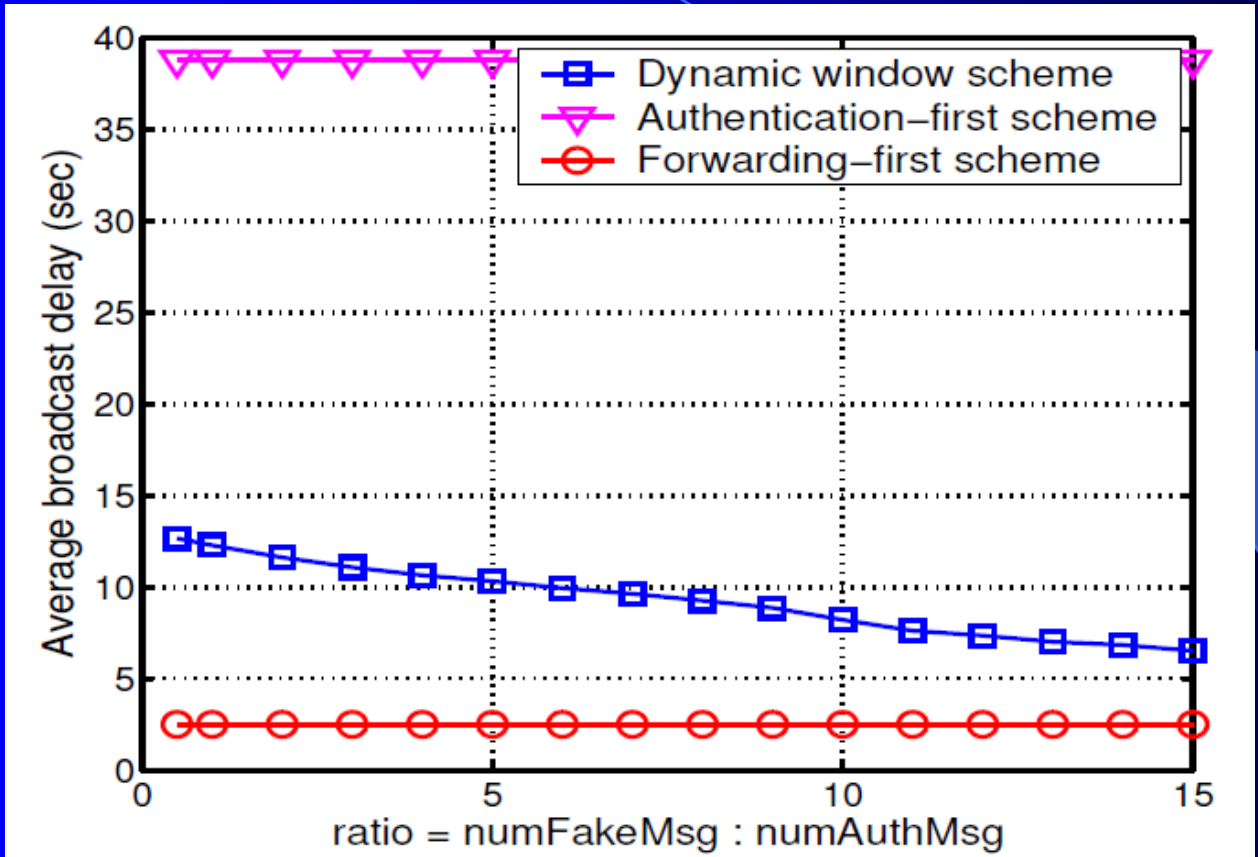
- Intensity of DoS attacks



Energy saving: Portion of nodes receiving/forwarding faked messages under attacks of various intensities.

Simulations and results

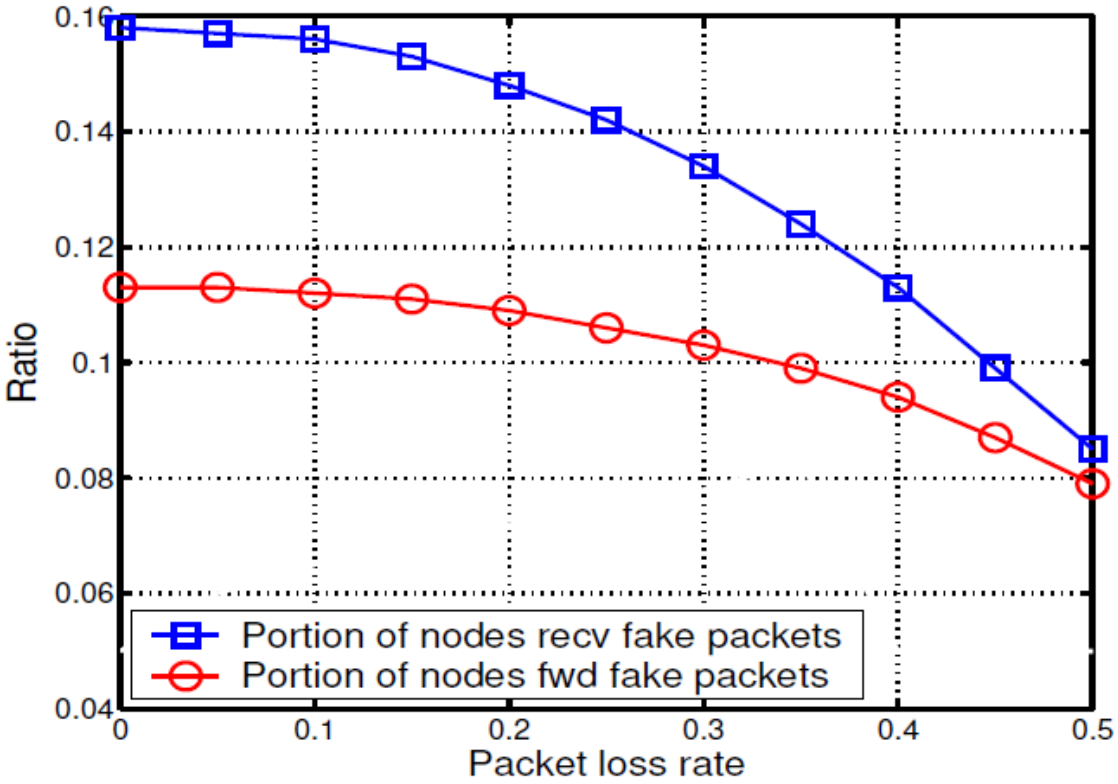
- Intensity of DoS attacks



Broadcast delay for authentic messages under various attack intensities

Simulations and results

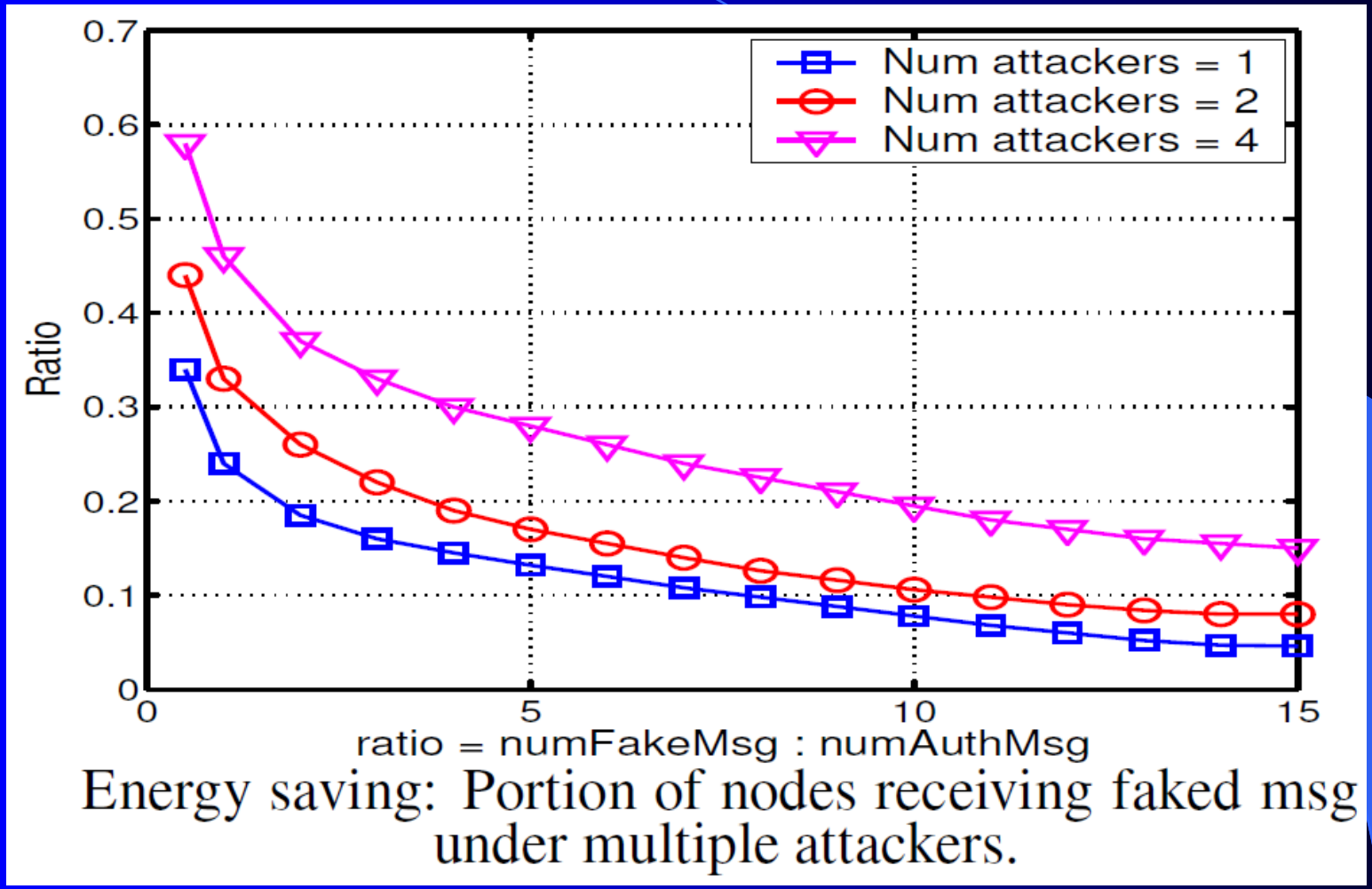
- Packet loss rate



Energy saving: Portion of nodes receiving/forwarding faked messages under various packet loss rates

Simulations and results

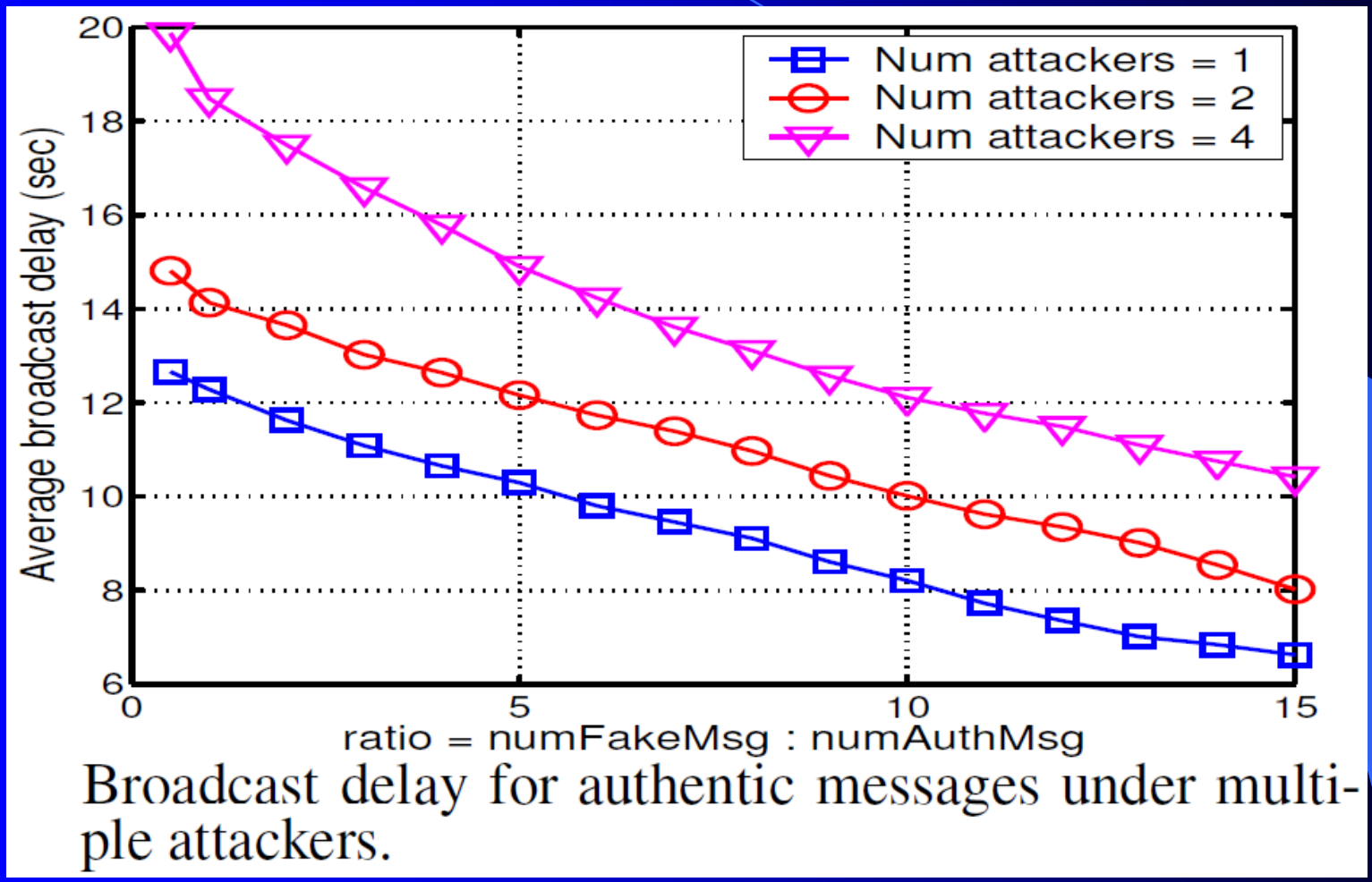
- Multiple malicious attackers



Energy saving: Portion of nodes receiving faked msg under multiple attackers.

Simulations and results

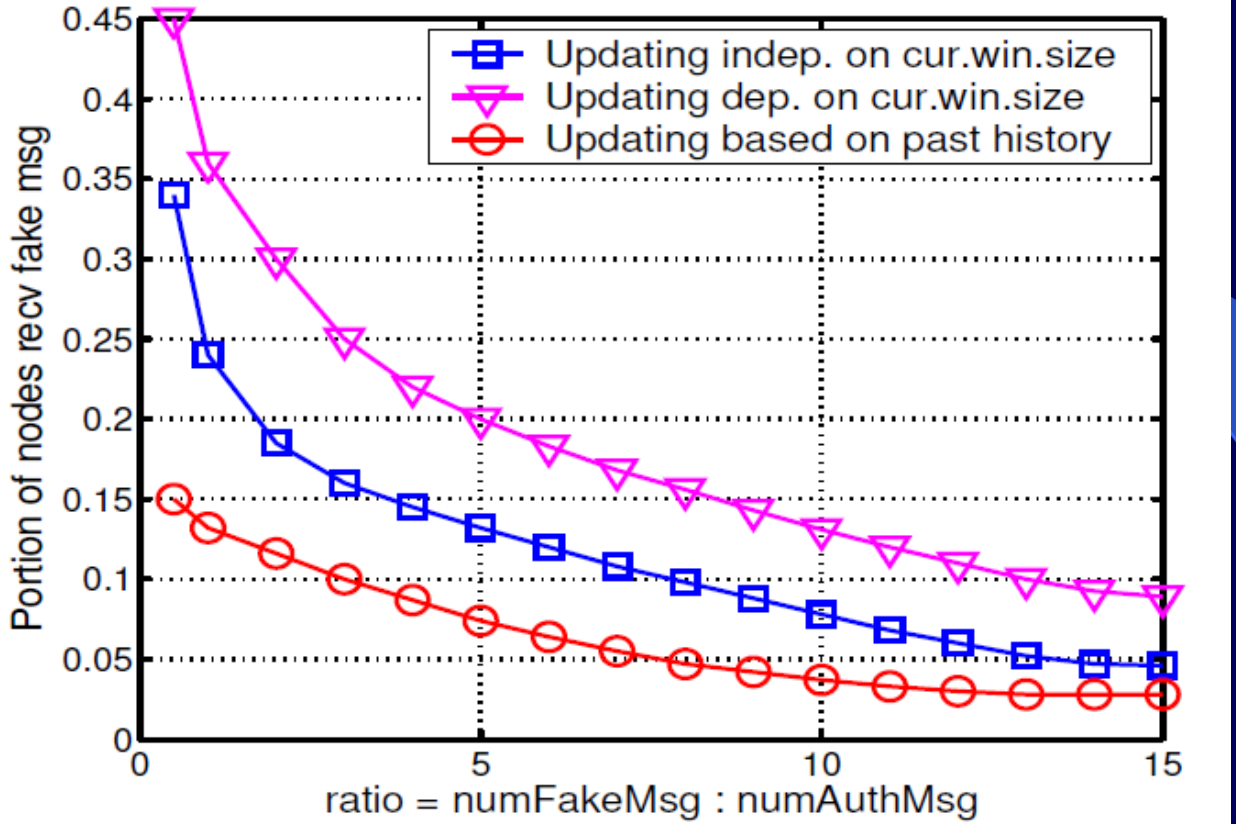
- Multiple malicious attackers



Broadcast delay for authentic messages under multiple attackers.

Simulations and results

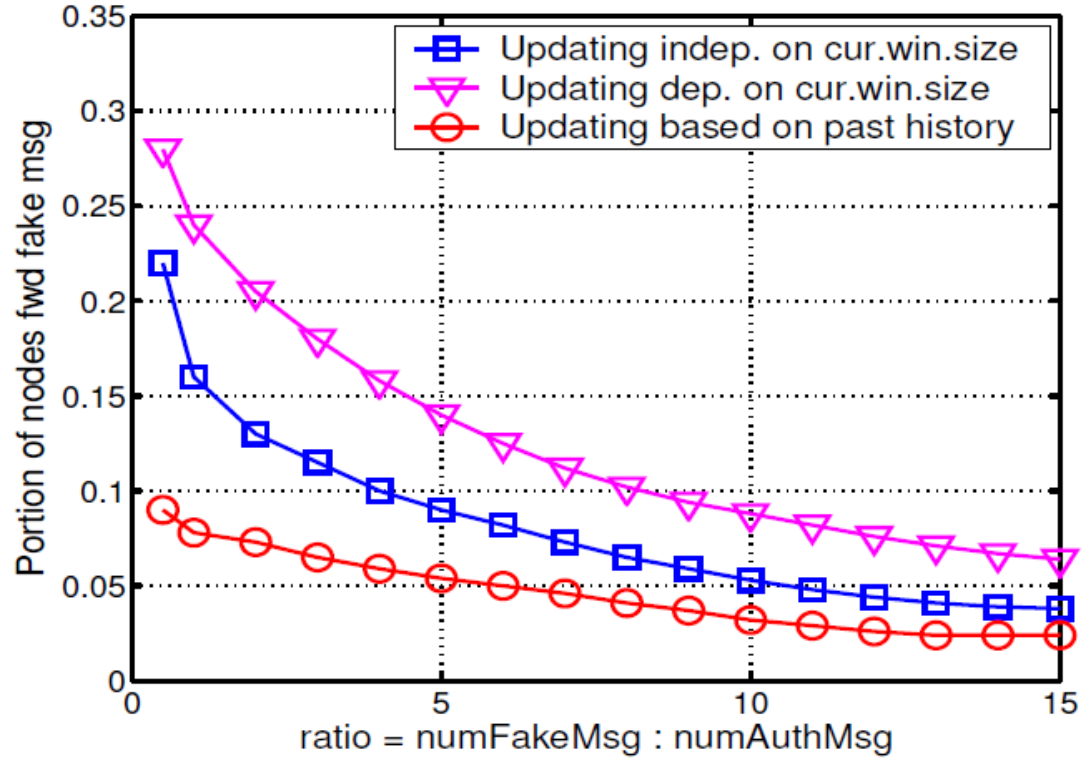
- Effects of various ways to update window size



Energy saving: Portion of nodes receiving fake messages

Simulations and results

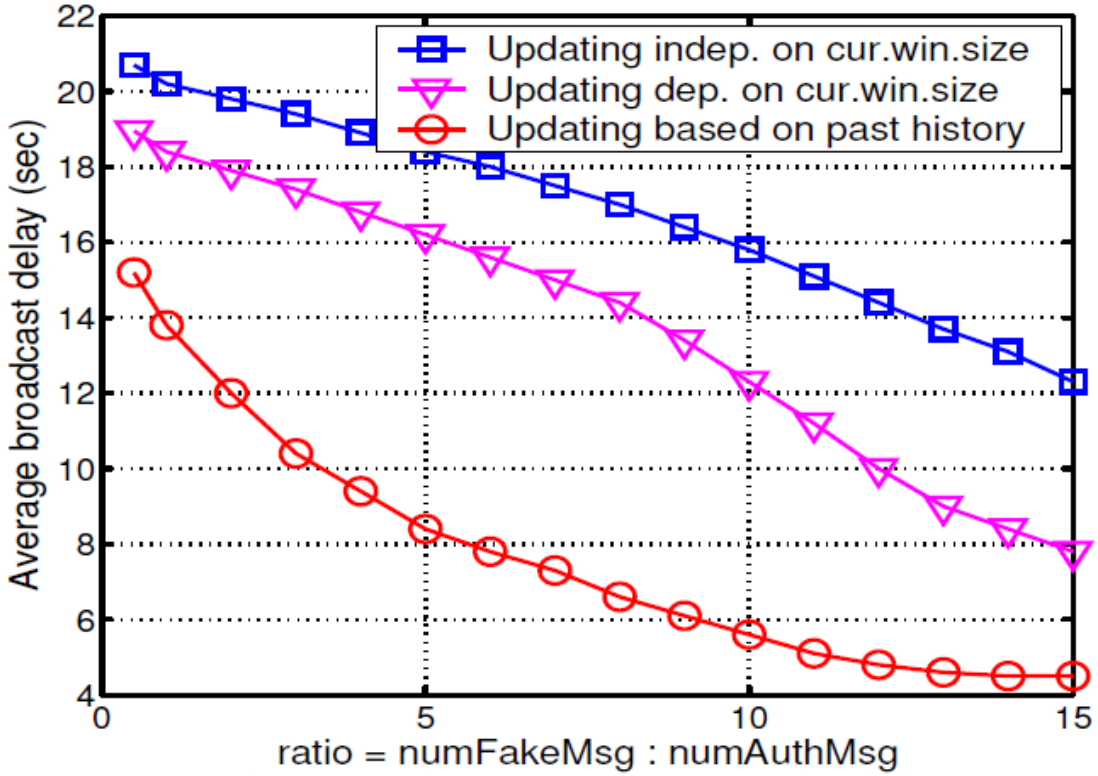
- Effects of various ways to update window size



Energy saving: Portion of nodes forwarding fake messages.

Simulations and results

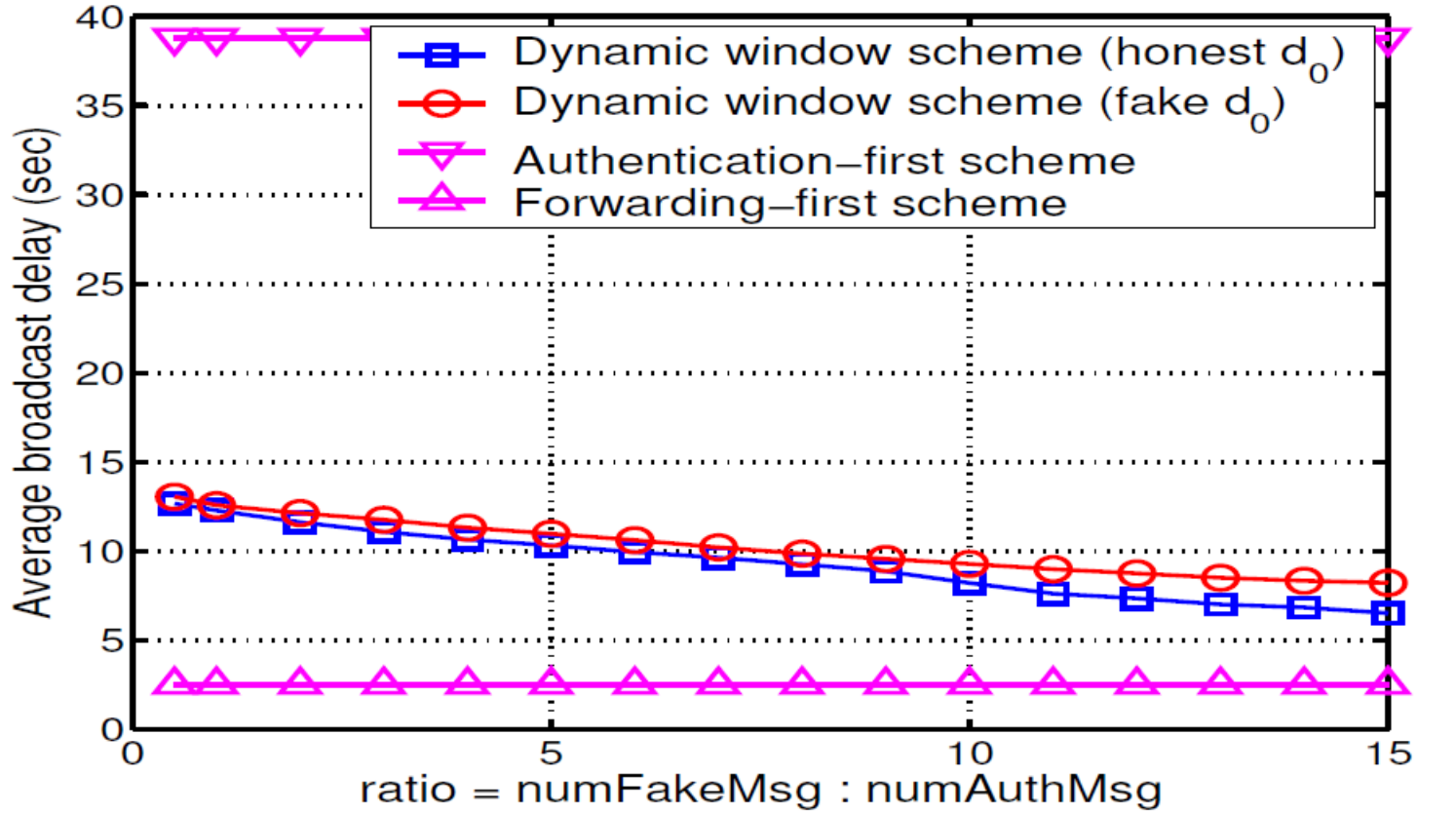
- Effects of various ways to update window size



Broadcast delay for authentic messages of various ways to update window size.

Simulations and results

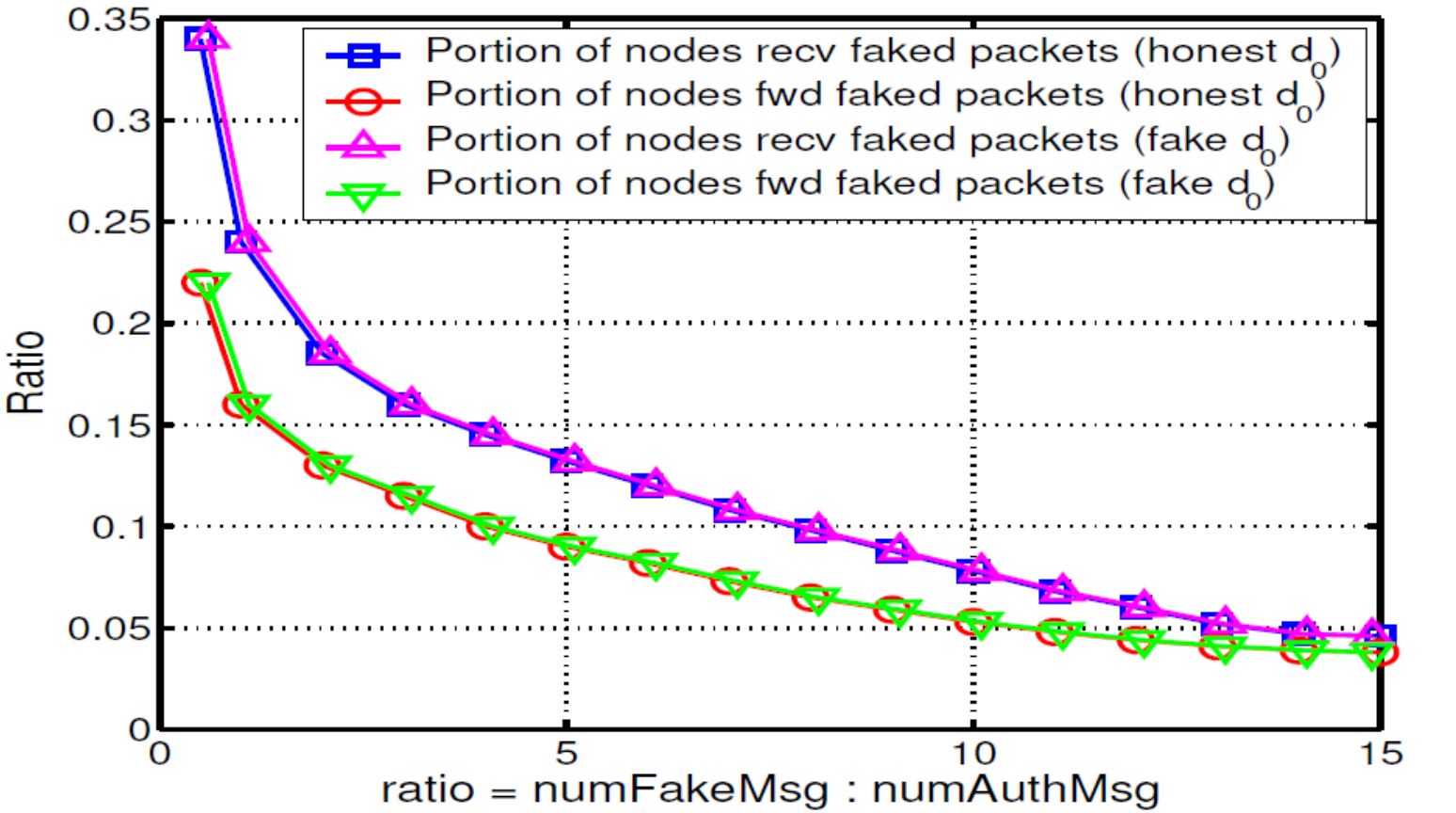
- Handling attacks that change da value



Broadcast delay for authentic messages if attackers change d_a.

Simulations and results

- Handling attacks that change da value



Energy saving: Portion of nodes receiving fake messages if attackers change d_a.

Conclusion

- Denial of Service attacks are very difficult to prevent in sensor networks.
- Classify DoS attacks and their different attacking patterns
- Presented a dynamic window scheme that can effectively contain the damage of DoS attacks to a small portion of the nodes.
- The scheme allows each individual node to make its own decision on whether to forward a message first or verify it first.

Conclusion…

- Even though sensors have no idea where the malicious attackers are, they can effectively locate the attackers and contain the damage caused by them.
- The scheme is efficient, and does not introduce too much broadcast delay.
- It is flexible: the parameters of the scheme can be configured such that the different needs of the various applications are met.

References

- Paper: Containing denial-of-service attacks in broadcast authentication in sensor networks. by: Ronghua Wang and team.
- Prof. Kinicki's presentation from previous year at WPI.

Questions