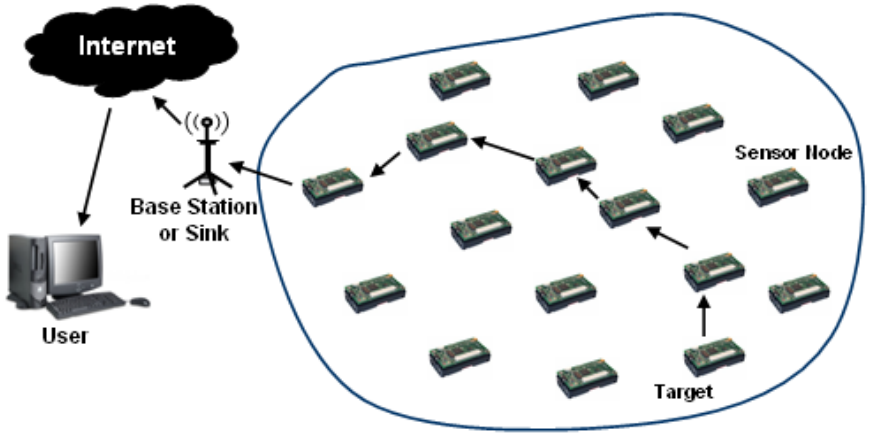
Energy-Efficient Secure Routing in Heavily Deployed Wireless Sensor Networks

Presenter

Al-Sakib Khan Pathan
DCS, IIUM, Malaysia

Wireless Sensor Network

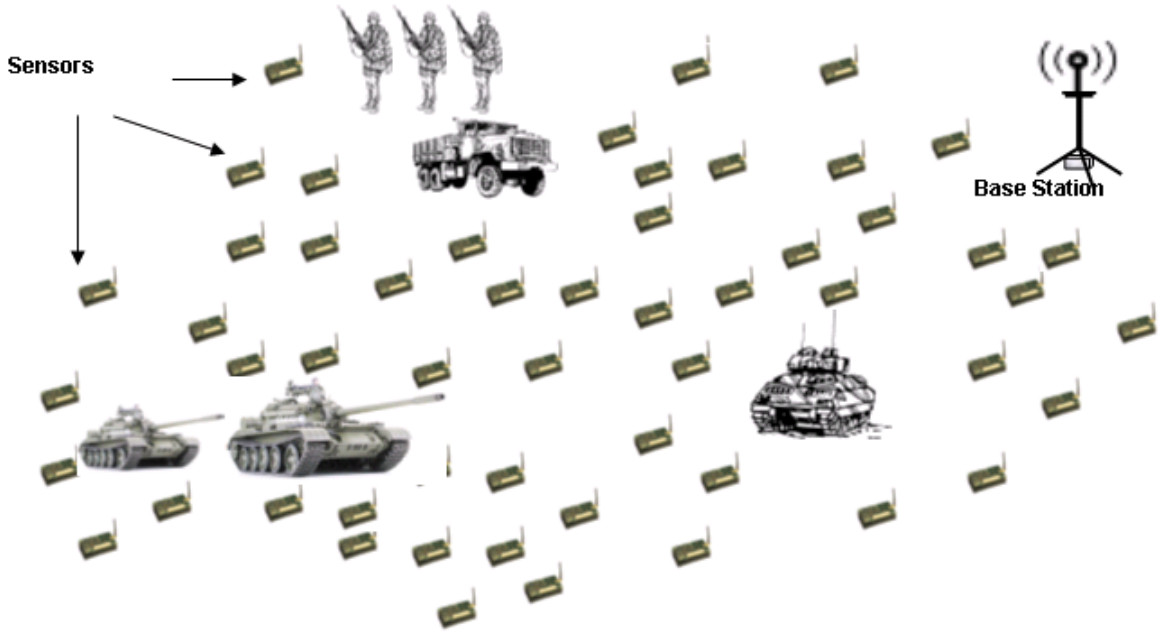
- Wireless networks consisting of a large number of motes
  - Self-organizing
  - Highly integrated with changing environment and network
  - Highly constrained resources
    - processing, storage, bandwidth, power
- Facilitate large scale deployment
  - Health care monitoring
  - Surveillance
  - Traffic monitoring
  - Military applications
  - Habitat monitoring
  - Disaster Warning



MICA2 Mote: An Example

- ATmega128L 8-bit processor at 8 MHz
- 128KB program memory (flash)
- 512KB additional data flash memory
- 433, 868/916, or 310 MHz multi-channel radio transceiver
- 38.4 kbps radio, 500-1000 feet outdoor range (depending on versions) with a size of only 58 x 32 x 7 (mm)
- Usually it is run by TinyOS operating system and powered by 2 AA sized batteries

An Application Scenario



WSN Security Angles

- Viewing Angle 1
  - (a) Key Management
  - (b) Secure Routing
  - (c) Secure Services
  - (d) Intrusion Detection Systems (IDS) [outsider, insider]
- Viewing Angle 2
  - (a) Physical security
  - (b) Deployment security (sparse or dense, etc.)
  - (c) Topological security (cluster, hierarchy, tree, etc.)
  - (d) Wireless communication security
  - (e) Data security

WSN Security Angles

- Viewing Angle 3: Holistic Security
  - (a) Application layer security
  - (b) Transport layer security
  - (c) Network layer security
  - (d) Data link layer security
  - (e) Physical layer security

- **Holistic Security!**

Assumptions & Preliminaries

- Densely deployed sensors in the network
- Initially all the nodes and the base station (BS) have same transmission ranges
- All nodes and the BS are time-synchronized
- Once deployed, sensors remain relatively static
- BS cannot be compromised in any way
- All transmissions from a node are isotropic (in all directions or local broadcast)
- Links between two nodes are bidirectional
- Each node has a pre-loaded shared secret key with BS

Preliminaries

- Three states of nodes
  - **Non-forwarding**
    - Radio transceiver is OFF but sensing circuitry is ON
  - **Forwarding**
    - Both transceiver and the sensing circuits remain ON
  - **Active**
    - This is same as forwarding state but this term is used to differentiate two phases of the protocol's operation
    - Initially all nodes are in active state for some time

Assumptions & Preliminaries

- Active State Time:
  - Let, *v* be a node and $N_1(v)$ be the number of one hop neighbors of *v* for a particular transmission range *r*. Let, T_{rtt} be the round trip time for data propagation between the longest distant pair within one hop neighbors. Then, the active state time for *v* is given by the equation, $T_{active} = T_{rtt} \times N_1(v)$
- In our protocol, within the time T_{active}, a node could be able to determine whether it should participate in the tree as a forwarding node or not
- One-way Hash Chain (OHC) [Lamport, 1979]:
  - A sequence of numbers K_n, K_{n-1}, …. K_0 such that, $\forall_i: 0 \leq i < n$, $K_i = F(K_{i+1})$
  - ***F*** $\rightarrow$ One-way function that is repeatedly applied on a seed K_r

Tree Construction & OHC init.

- **Tree Construction and OHC Initialization**
  - Base station *B* initiates the network formation process and generates a control packet

    bcm: $B|sid|ren|dist|fid|HS_0|MAC_{K_i}(B|sid|ren|dist|fid|HS_0)$

    Here,
    - *sid* → sender's id
    - *ren* → remaining energy of the sender
    - *dist* → cumulative distance from *B*, calculated using signal strength
    - *fid* → id of the selected immediate upstream forwarder
    - HS_0 → initial hash number
    - MAC_{K_i} → Message Authentication Code generated by using key K_i, which is the number in the key chain corresponding to time slot t_i

Tree Construction & OHC init.

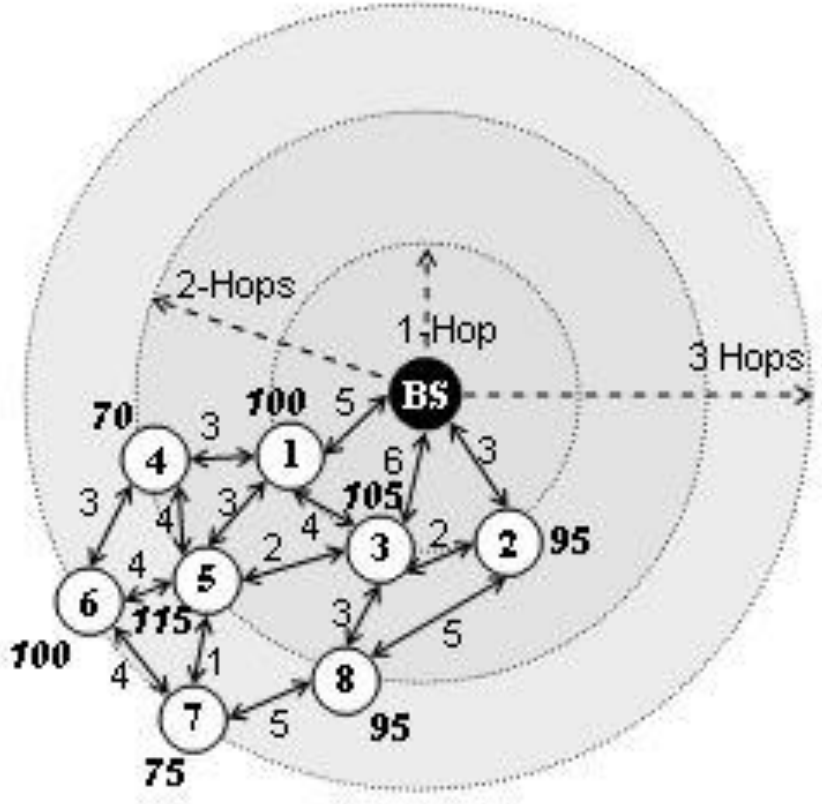
- One hop neighbors of BS first get the message
- Each node receiving the control message stores HS_0 from the first received message
- Each node calculates the distance up to base station via different upstream nodes and chooses the node as a forwarder of which D_s/E_r is the lowest
- Each node also stores the ids of the sending nodes
- Each node waits for time, $T_{wait} = \{D_s/E_r\} \times R$. R is the ratio of a node's initial energy and transmission range
- After T_{wait} node senses the channel and re-transmits

Tree Construction & OHC init.

- The re-transmitted message includes the node's information and *fid* is set as the chosen forwarder node's id
- As the link is bidirectional, the re-transmission of the message by the downstream node is heard by the upstream nodes and the forwarder knows that, the downstream node chose itself as a forwarder
- This process continues and eventually the whole network is structured as a sink rooted tree
- To authenticate HS_0, BS releases K_i in time slot t_{i+d}
- Non-forwarding nodes are set within T_{active}

Before Execution of the Phase 1

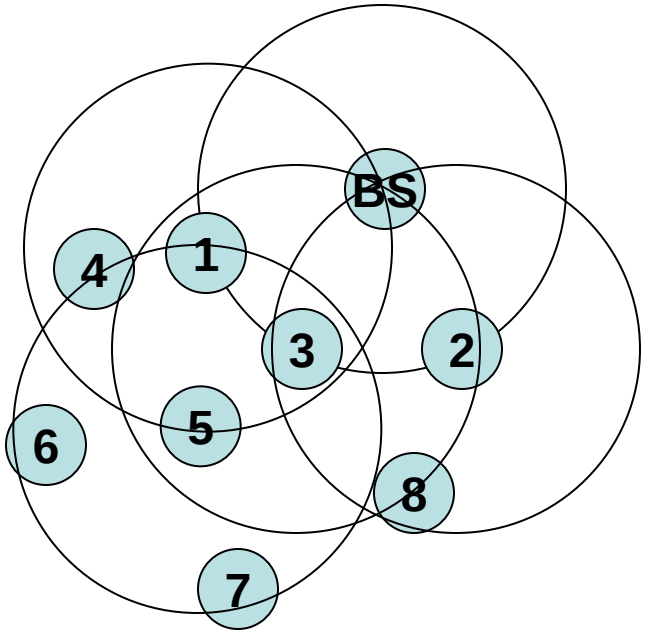
- **Before execution of first phase**
- All the white nodes are in active status.
- We have shown the N-hop (N = 1, 2, 3 …) neighbors of the sink on the circumference of the same circle regardless of their actual calculated distances from the sink.



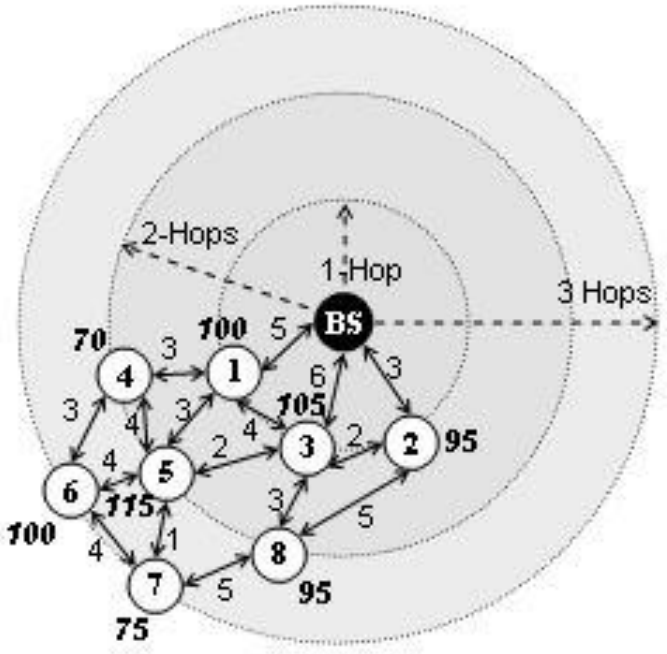
Network Structuring

bcm:

$B|sid|ren|dist|fid|HS_0|MACK_i(B|sid|ren|dist|fid|HS_0)$



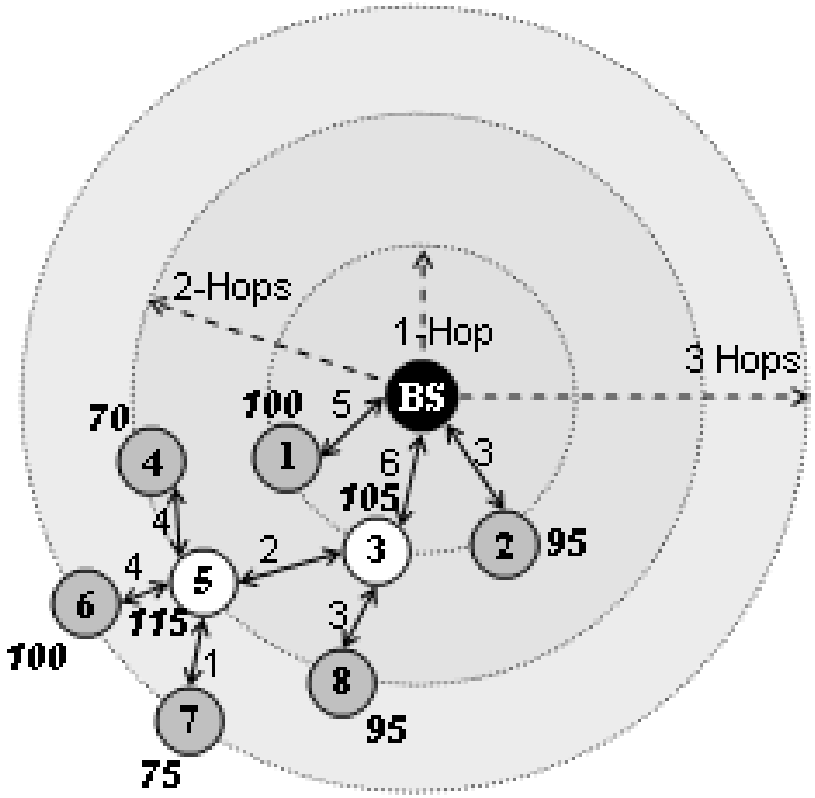
Reference Model



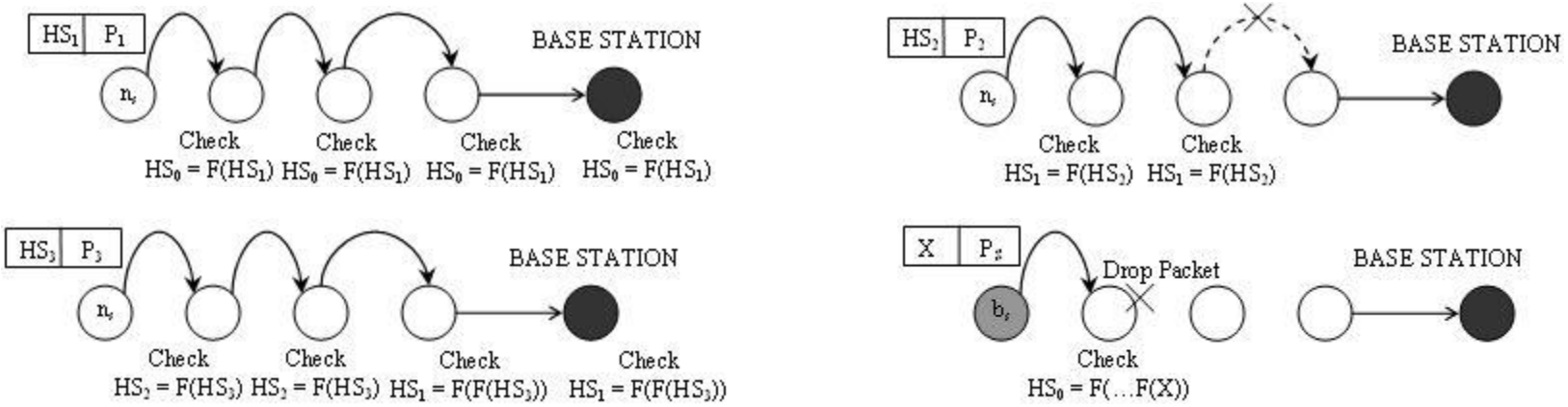
After Execution of Phase 1

- **After execution of first phase**

- The gray nodes are in non-forwarding status while the other two nodes are in forwarding status. In these figures, we have shown the N-hop (N = 1, 2, 3 …) neighbors of the BS on the circumference of the same circle regardless of their actual calculated distances from the base station



Secure Data Transmission



Network Operation and Secure Data Transmission from sensor to BS

→To validate OHC number, each intermediate node n_1, n_2, ... , n_m maintains a verifier I_{n_s} for each n_s. n_s is the source node.

→ Bogus packet is detected in the very next hop and cannot travel far, which saves the network from consuming unnecessary energy

→ Repeated checking of OHC number to handle packet loss for particular source

Optional Key Refreshment

- Optional Key Refreshment
  - Depending upon the requirement or application at hand. It provides data freshness and better security
  - BS periodically broadcasts a message,

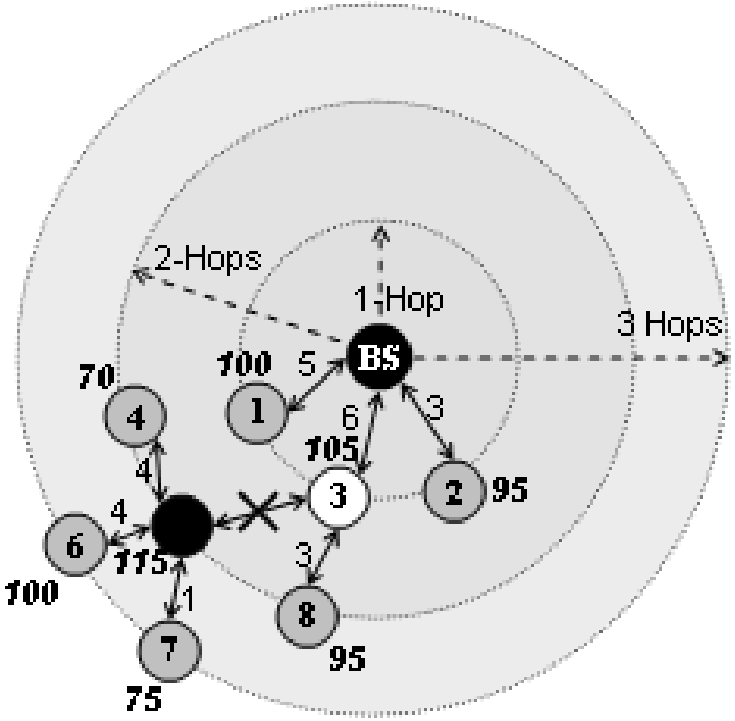
    $B|K_s|\ MAC_{K_j}(B|K_s)$ with a new session key K_s
  - Authentication of K_s is done as previous
  - Each node or the targeted set of nodes perform X-OR operation with their current shared key to get the new key
  - This key is used for encryption of data while sending

Broken Path Recovery

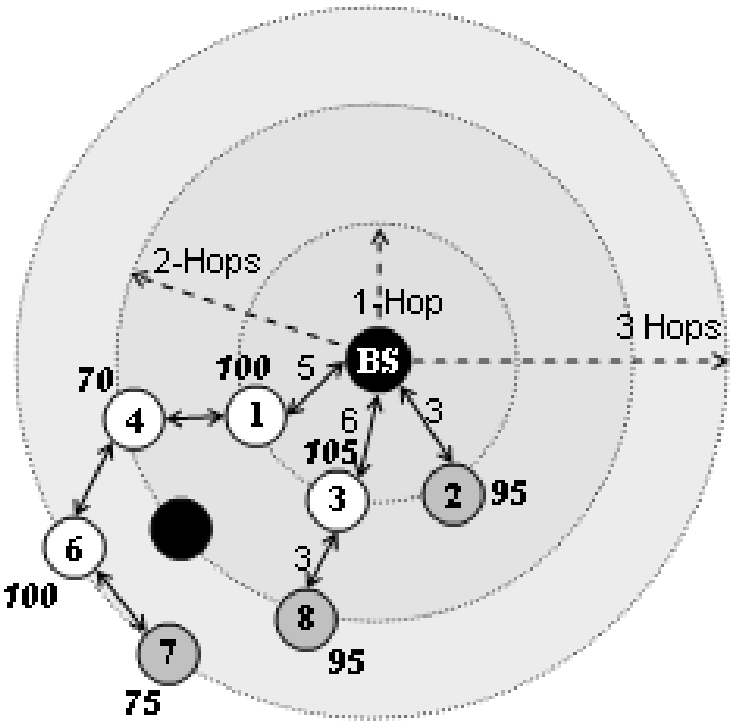
- Broken Path Recovery
  - Stored knowledge of upstream nodes is used for this
  - Sometimes, OHC re-initialization is necessary, periodic re-construction → finding out an optimal value of re-initialization of the network is left as our future work

Figures to Explain

Broken Path



Repaired Path

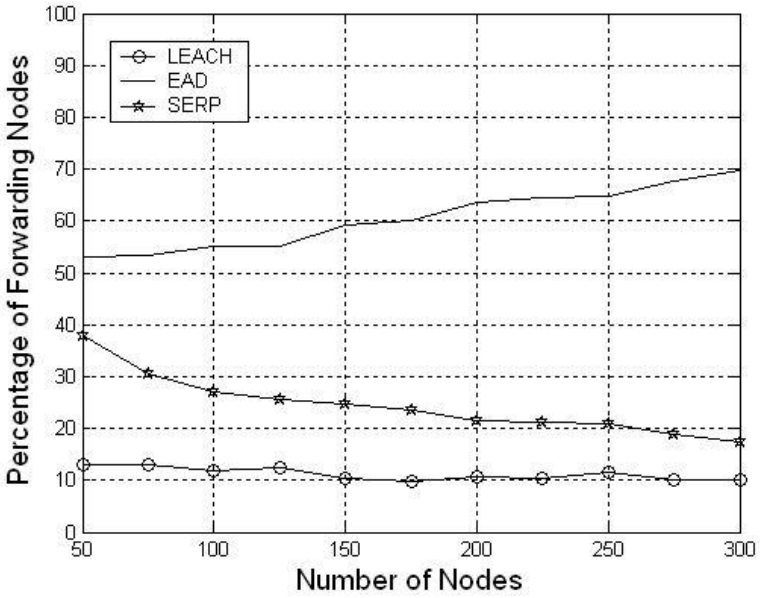


Simulation Parameters

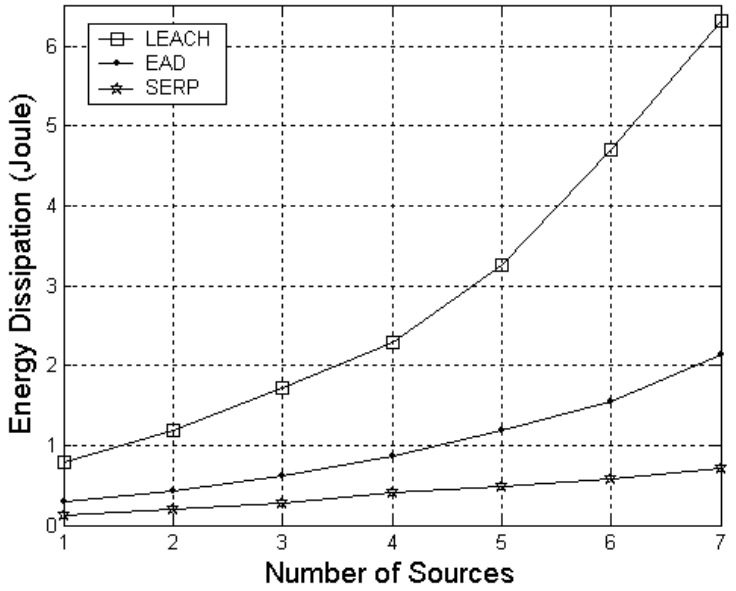
Parameters	Values
Simulation time	1,300 s
Simulation area	100×100 m^2
Total number of nodes	50–300
Initial energy	2 J
Transmit/receive electronics (L_E)	50 nJ bit^{-1} m^{-2}
Transmission power	5.85e−5 W
Receive signal threshold	3.152e−20 W
Sleep mode energy	0
Number of sources	1–7
Offered load	4–6 pps
Transmission range	25 m
Packet size	2,048 bytes

Results

LEACH: [Heinzelman et al., 2000]

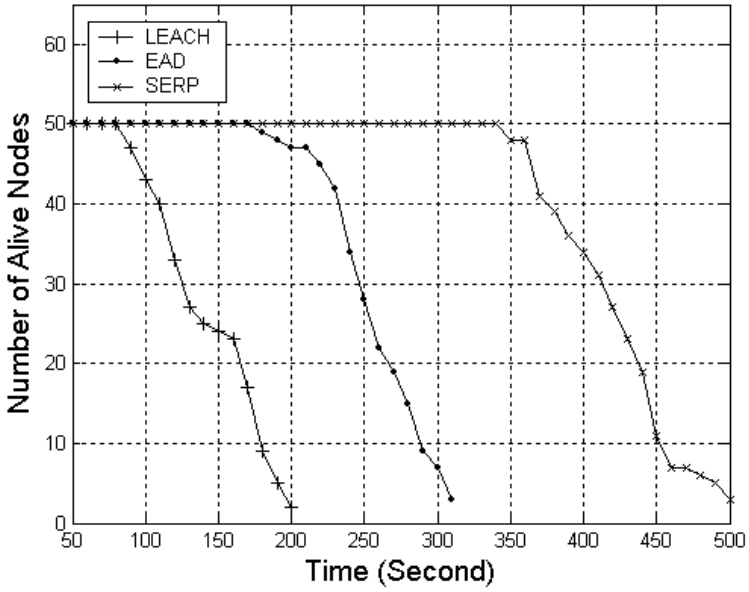


EAD: [Azzedine et al., 2003]

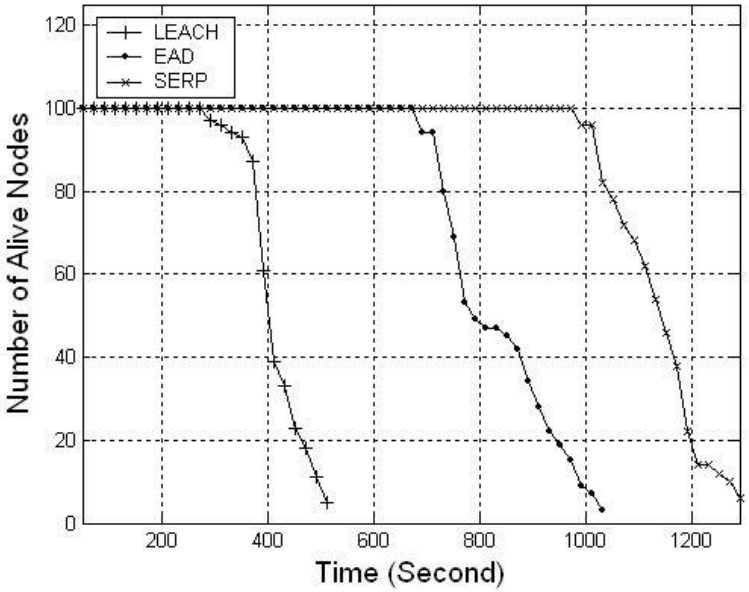


Results

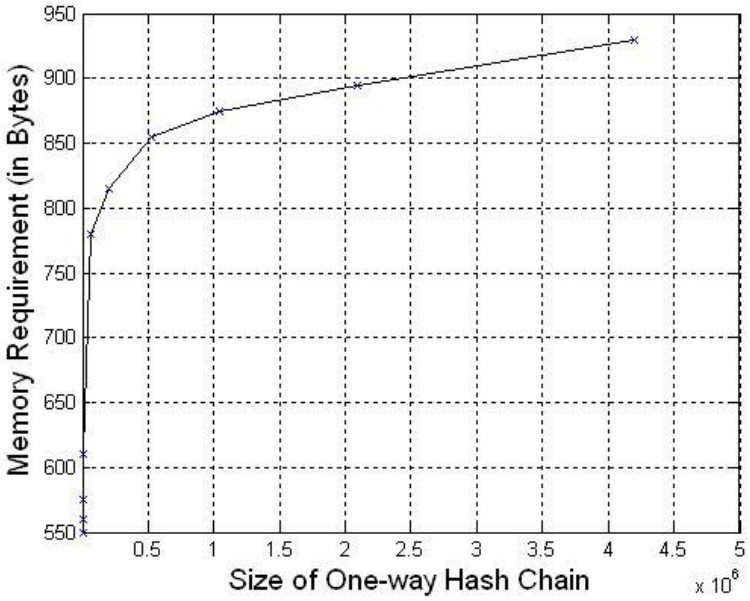
LEACH: [Heinzelman et al., 2000]

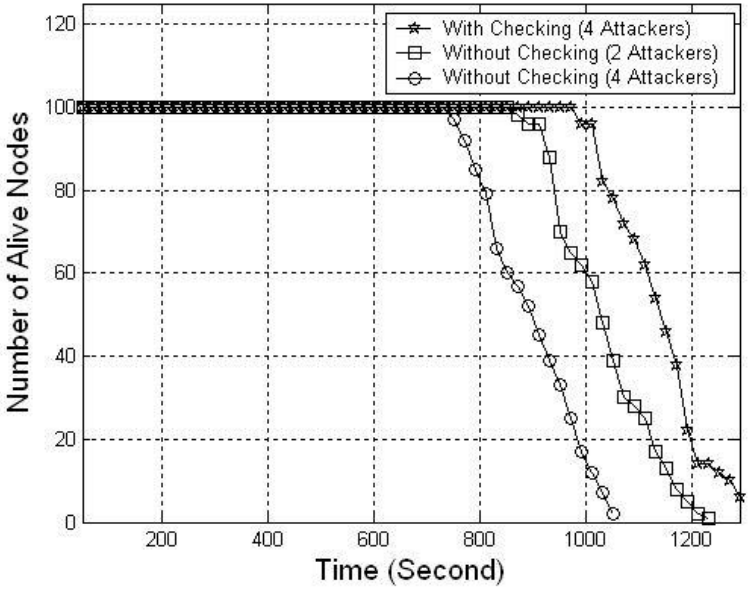


EAD: [Azzedine et al., 2003]



Results


Memory Requirement (in Bytes)
Size of One-way Hash Chain
x 10^6
950
900
850
800
750
700
650
600
550
0.5
1
1.5
2
2.5
3
3.5
4
4.5
5


With Checking (4 Attackers)
Without Checking (2 Attackers)
Without Checking (4 Attackers)
Number of Alive Nodes
Time (Second)
120
100
80
60
40
20
0
200
400
600
800
1000
1200

Energy Gains

- Energy-efficient structuring of the network
- Bogus packets cannot travel more than one hop which saves consumption of energy
- Periodic re-structuring keeps the balance of energy drain of the nodes
- The entire network can show some sort of graceful degradation

About Security

- Hop by hop authentication checking for each packet from each source node
- Base station also can detect false packet and stops any further transmission from the rogue node
- Refreshed Key, if needed in the application
- Outsider Attack
  - No chance. Will be detected
- Insider Attack
  - Compromised nodes
  - BS accepts data if at least δ nodes send the same report
  - Periodic re-initialization of OHC is helpful

Future Research Directions

- Scopes of future research
  - Finding an optimal value for network restructuring
  - Developing an IDS and merging it with these two mechanisms to provide a complete security management solution

Major References

[Das and Bharghavan, 1997] Connected Dominating Sets, CDS I, CDS II

Das, B. and Bharghavan, V., "Routing in Ad-Hoc Networks Using Minimum Connected Dominating Sets," Proceedings of the IEEE International Conference on Communications (ICC'97), pp. 376-380

[Erdös and Rényi, 1959]

Erdös, P. and Rényi, A. 'On Random Graphs', Publicationes Mathematicae, Vol. 6: 290–297, 1959

[Lamport, 1979] One-way Hash Chain

Lamport L., Constructing digital signatures from one-way function. Technical report SRI-CSL-98, SRI International, October 1979

[Heinzelman et al., 2000] LEACH

Heinzelman W.R., Chandrakasan A., Balakrishnan H., "Energy-efficient communication protocol for wireless microsensor networks," Proceedings of the 33rd Annual Hawaii Inter-national Conference on System Sciences (HICSS), 2000, pp 3005–3014

[Azzedine et al., 2003] EAD

Azzedine B., Xiuzhen C., Joseph L., "Energy-aware datacentric routing in microsensor networks," Proceedings of the 8th MSWiM 2003, San Diego, pp. 42–49

THANK YOU

Questions and Answers

spathan@ieee.org, sakib@iium.edu.my

???