Sinkhole Attack Detection and Avoidance Mechanism For RPL In Wireless Sensor Networks

By

Ansar Jamil, Mohammed Qassim Ali and Muhammed E. Abd Alkhalec

ansar@uthm.edu.my

Content Title

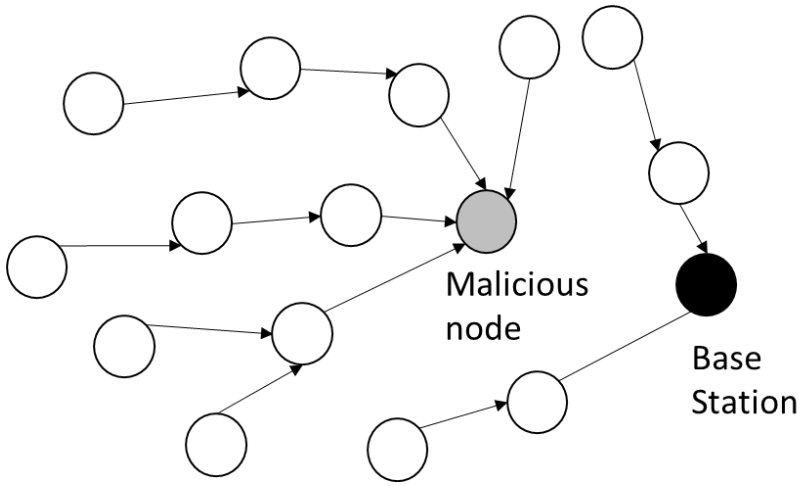
- Introduction
- Overview of CLS-RPL
- CLS-RPL Design
- Simulation experiment
- Results
- Conclusion

Introduction

Security Issue in WSN

- Security issue is one of the main problem in Wireless Sensor Network (WSN) and Internet of Things (IoTs).
- RPL(Routing protocol for low power and lossy networks) is a standard routing protocol for WSN, is not to be missed from being attacks.
- Performance of RPL is reduced significantly after being attacked. Sinkhole attack is one of the most common attacks to WSN and RPL, threatening the network capability by discarding packets and disrupting routing paths.

Sinkhole Attack on RPL



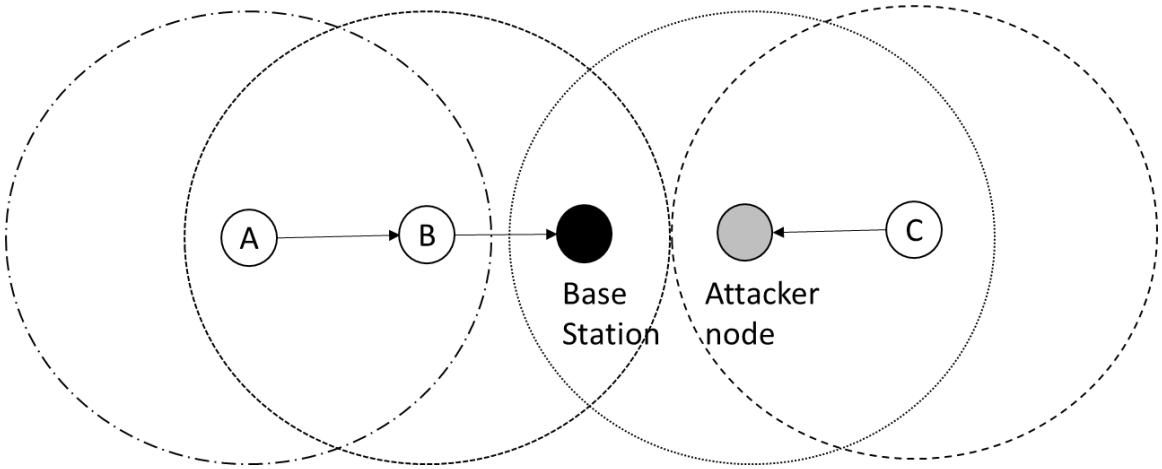
- In sinkhole attack, the objective of an attacker is to attract almost all traffic in the network through a malicious node, which act as a metaphorical sinkhole or a node with the lowest rank.
- In order to achieve it, the malicious node is purposely located near the base station.
- The malicious node just simple drop all received packets or corrupt it before sending it to the next node.
- Effect of sinkhole attacks becomes more severe when the malicious node attacking a main route to the base station.

Overview of CLS-RPL

Cross Layers Secured-RPL (CLS-RPL)

- This paper proposes a new Secured-RPL routing protocol to detect and avoid sinkhole attack in the network, which is called Cross Layers Secured RPL (CLS-RPL). This routing protocol is enhanced of the existing RPL routing protocol.
- CLS-RPL is a cross-layers security mechanism that involves network layer and data link layer.
- Data link layer responsible to overhear its parent transmission after sending certain number of packets and record number of overhearing of its parent node.
- Number of overhearing information is used to determines status of a parent node either attacker node or legitimate node.
- Network layer uses updated status of each parent node is provided to RPL in the network layer. If attacker node is detected, RPL changes its route avoiding the attacker node.

Overhearing concept



- Node B is located within the transmission of node A.
- Node B becomes the intermediate node for node A to deliver packets to the base station.
- Since node B is a legitimate node and the parent node of Node A, any transmitted packets by node A, node B forwards the packets to the base station. At the time node B is forwarding the packets to the base station, node A can overhear the transmissions of node B and receive it.
- Otherwise, all packets from node C will be dropped by the attacker node that caused node C does not overhear any transmission from the attacker node.

CLS-RPL Design

Design of CLS-RPL

The design implementation of CLS-RPL can be divided into three main parts:

1. calculation of number of overhearing transmission of parent node
2. sinkhole attack detection
3. sinkhole attack avoidance.

CLS-RPL security algorithm

CLS-RPL security algorithm	
a) Calculation number of overhearing	
1.	Node start sending packets to its parent node.
2.	Node start overhearing for any packet transmission of its parent node.
3.	When the node received a packet transmission, check the source of the packet, If the source address of the packet belong to its parent node, add one to the number of overhearing
4.	After 10 packet transmissions, determine number of overhearing, N.
b) Detection of sinkhole Attacker	
5.	Based on the number of overhearing, N, the node determine status of its parent node, p_{status}either legitimate node or attacker node.
6.	Decision making:
	If N > 0; Legitimate node If N=0; Attacker node
7.	Update p_{status} to CLS-RPL routing protocol (network layer)
c) Avoiding Sinkhole Attack	
8.	If p_{status}s equal to legitimate node, Remain the cost of its parent node. CLS-RPL keeps the parent node.
9.	If p_{status} is equal to attacker node, Cost of its parent node is set to the maximum value, which removes the attacker nodes as the parent candidates. Then, CLS-RPL will select another node as a new parent that provides the least cost to the sink.

Calculation of Overhearing

- Contikimac determines the number of overhearing of its parent's transmission after every 10 packets transmission to its parent node.
- After the first packet is just transmitted, Contikimac starts recording number of overhearing of its parent transmission, N
- Each time Contikimac has detected a packet transmission of its parent node, number of overhearing will be increased by one, $N = N + 1$
- This cumulative value, N will be taken as the final number of overhearing after completed sending 10 packets and determine status of the parent node (legitimate or attacker node)

Sinkhole Attack Detection

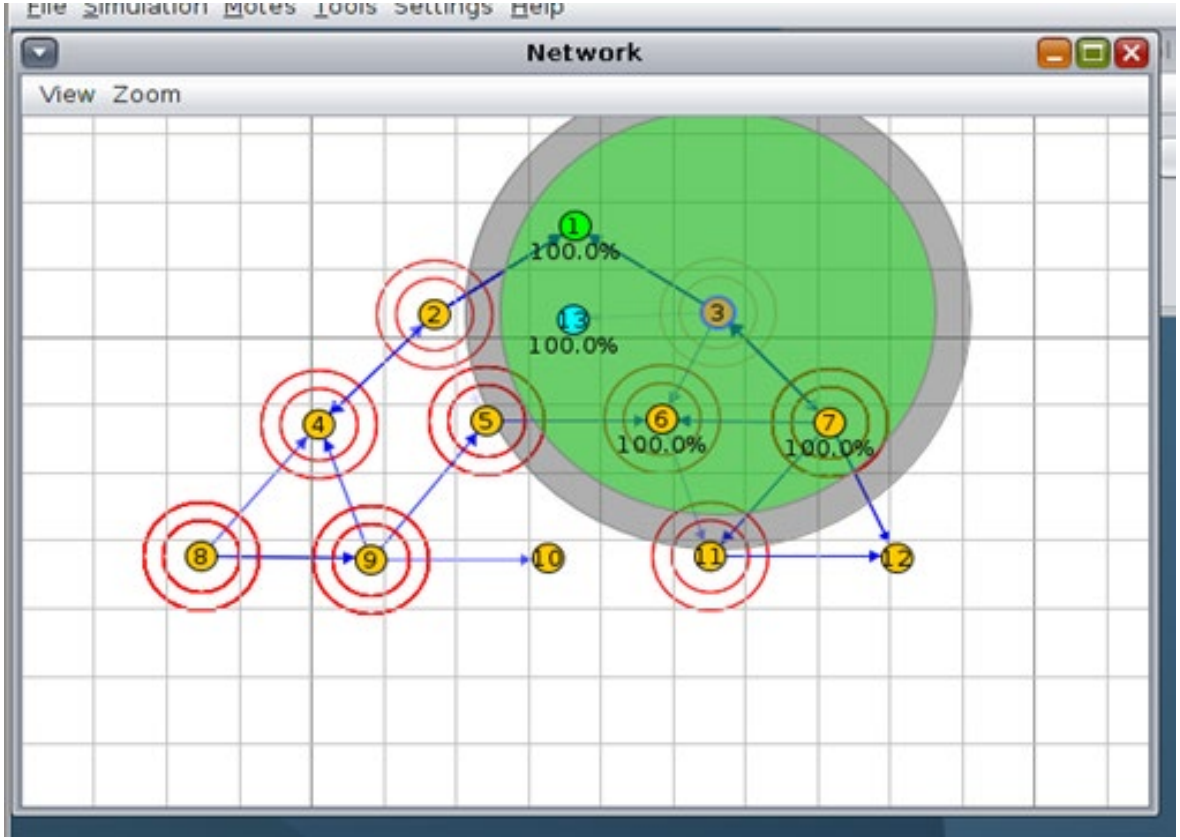
- Based on the finalized N values, CLS-RPL determines status of its parent node, p_{status} either legitimate node or attacker node.
- If number of overhearing,N is more than 0, the p_{status} is legitimate node. However, If number of overhearing,N is equal to 0, this mean p_{status} is attacker node.
- Then, the parent status, p_{status} is updated to CLS-RPL routing protocol (which is network layer).

Sinkhole Attack Avoidance

- CLS-RPL routing protocol checks the parent status, p_{status}.
- If the p_{status} is legitimate node, CLS-RPL does not change the path cost of the parent node and keeps the parent node as the best candidate to forward data to the base station.
- However, if the p_{status} is attacker node,
  - CLS-RPL will set path cost of the parent node to the maximum value, which removes the attacker nodes as the parent candidates. This means, CLS-RPL will not select the attacker as the parent node anymore and isolate it from the network.
  - CLS-RPL avoids any node from sending packets through the attacker node.
  - Then, CLS-RPL select another node as a new parent that provides the least cost to deliver data to the sink from the best parent candidates.

Simulation Experiment

Simulation Topology



- The network consist of 12 sensor nodes (node ID: 1 to 12) arranged in a tree topology
- 1 attacker node (node ID: 13) located near the base station

Simulation Configuration

Table 1. Simulation Configuration

Simulation Parameters	
Simulation tool	Contiki 3.0 Cooja simulator
Mote type	Sky mote
Number of nodes	11
Number of sink node	1
Number of attacker node	1
Radio medium	UDGM: Distance Loss
Transmission range	30 m
Interference range	35 m

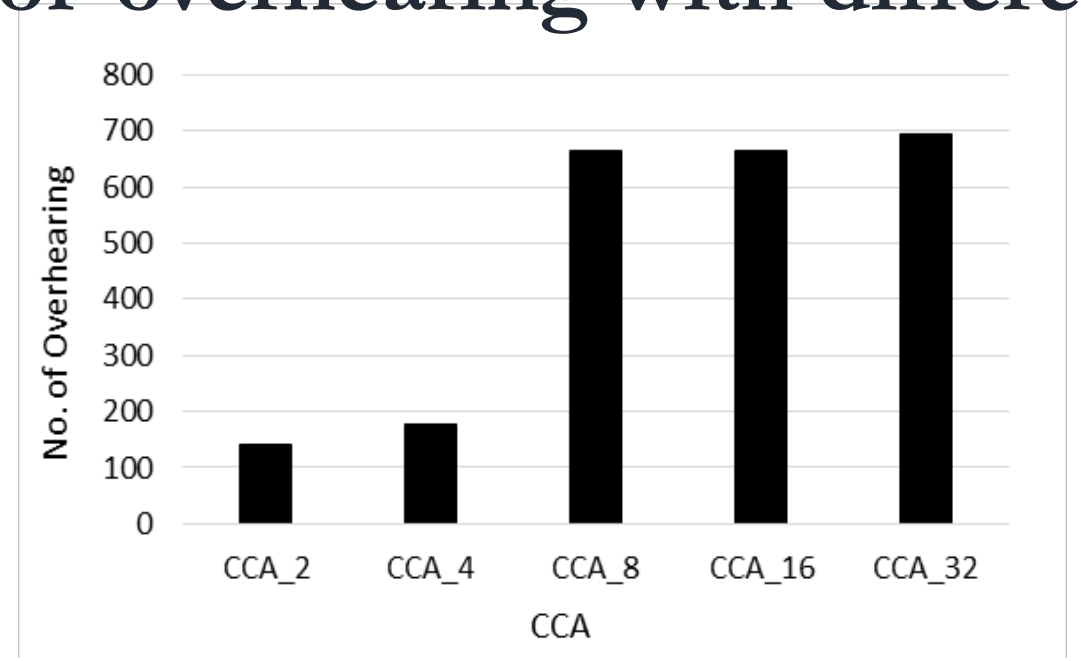
Simulation Scenarios

The simulation experiment was conducted in four different simulation scenarios as follows:

- RPL without attacker node.
- RPL with attacker node.
- CLS-RPL without attacker node
- CLS-RPL with attacker node

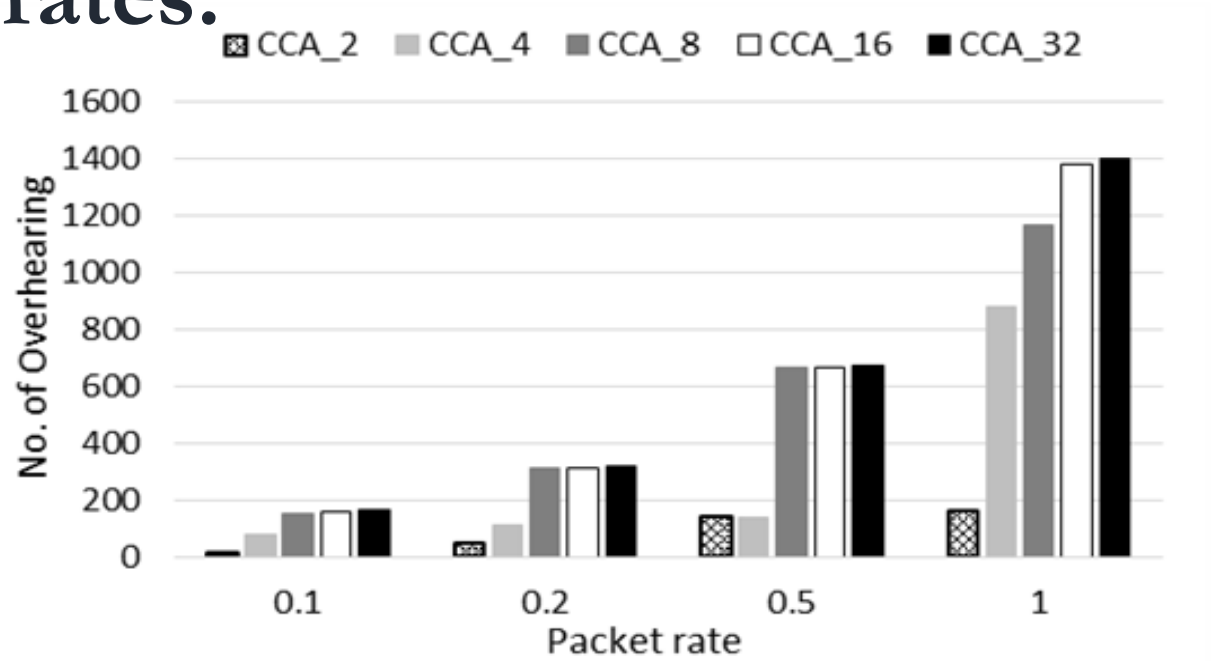
Results

Number of overhearing with different CCA



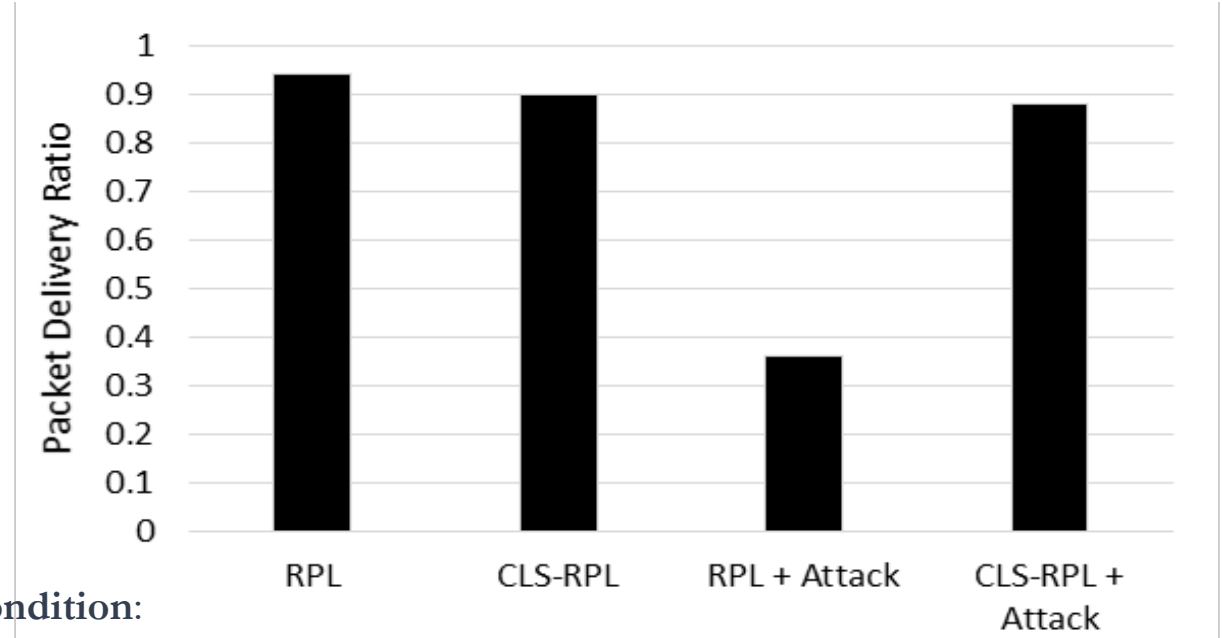
- number of overhearing is increased when the rate of CCA is increased.
- It is expected because as CCA rate is increased, Contikimac wake-ups to check the channel more frequent that will increase probability to overhear transmission from other nodes.
- Furthermore, if a packet transmission is detected during wake-ups the receiver is kept on to be able to receive the packet and the subsequent packets.
- The CCA_2 recorded the lowest number of overhearing, which equal to 140. Otherwise, CCA_32 recorded the highest number of overhearing equal to 695.

Number of overhearing for different packet rates.



- Number of overhearing is increased as the number of packets rates is increased in the network.
- The more packet transmitted in the network, a node detects more number of packet transmission that will increase number of overhearing.
- The lowest number of overhearing is recorded by packet rate 0.1 packet/s. The highest number of overhearing is recorded by packet rate 1 packet/s.

Average packet delivery ratio for different simulation scenarios.



Normal condition:

- CLS-RPL performance comparable performance when compared to RPL equal to 0.9 approximately.

Sinkhole attack:

- CLS-RPL outperforms RPL by far.
- RPL suffers during the sinkhole attack just recorded 0.36 packet delivery ratio.
- CLS-RPL able to deal with the attack by detecting and avoiding it provides 0.88 packet delivery ratio.
- This means CLS-RPL gives a significant improvement of packet delivery ratio about 52% when compared to RPL.

Conclusion

- CLS-RPL routing protocol is a cross-layer routing protocol that uses information from the data link layer.
- CLS-RPL uses overhearing (eave-listening) to detect and avoid sinkhole attack.
- If a node does not hear any transmitted packets from its parent node after sending a number of packets, this means its parent node is a sinkhole attacker. The node stop sending packets and remove the attacker node as it parent and find alternative parent node.
- Otherwise, if the node hears transmitted packets from its parent node, this means its parent node is a legitimate node and continues to send more packets. In order to determine performance of
- The finding shows that CLS-RPL provides 52% improvement in term of packet delivery ratio when compared to RPL protocol.

Thank You