Global Cyber Challenge - Peace-a-thon

# Intelligent Roaming Intrusion detection system for the 6LowPAN based IoT

Bhale Pradeepkumar , Sahil sharma

Department of Computer Science and Engineering

Indian Institute of Technology Guwahati, Assam-781039

# Project Summary:

- Internet of Things (IoT) devices provides an opportunity for service providers to develop new streams of revenue.
- IoT has the potential to provide solutions that can dramatically enhance productivity and quality in security, health, education, and many other areas.
- Any compromise in security and privacy at IoT network may lead to worse consequences.
- Therefore research on security aspects of IoT is very important.

## Project Objective:

- A lot of research has been done to secure a 6LowPAN based IoT network from different types of external attacks.
- But there is a chance that a compromised node of the network can successfully launch an internal attack.
- This type of attack detection very difficult. 6LoWPAN nodes are resource constrained in terms of processing power, battery power and communication and storage capability.

- Proposed Intelligent roaming IDS for IOT n/w using Roaming Heuristic and Time Extension Algorithm.

# Project Objective:

- Intelligent Roaming IDS Work within reasonable response time and overhead is small enough to deploy it on constrained nodes

- Execution of various attacks and their detection mechanism on a real test bed.

## Internet of Things (IoT):

- Resource-constrained devices connected Internet via IPv6 and 6LoWPAN networks [6].

- Securities provided to IoT nodes at different layers include [1][2]:
  - TLS and DTLS at Transport
  - IPSec at Network
  - Link Layer Security by IEEE 802.15.4

- Still IoT are exposed to various attacks such as
  - Sybil, clone ID, routing (wormhole, sinkhole, selective-forwarding) attacks [3][4].

- Intelligent Roaming IDS is necessary to detect all malicious activities and attacks

# Intelligent Roaming IDS :

We divide our idea in three phases, which are -

## I. Network Setup:

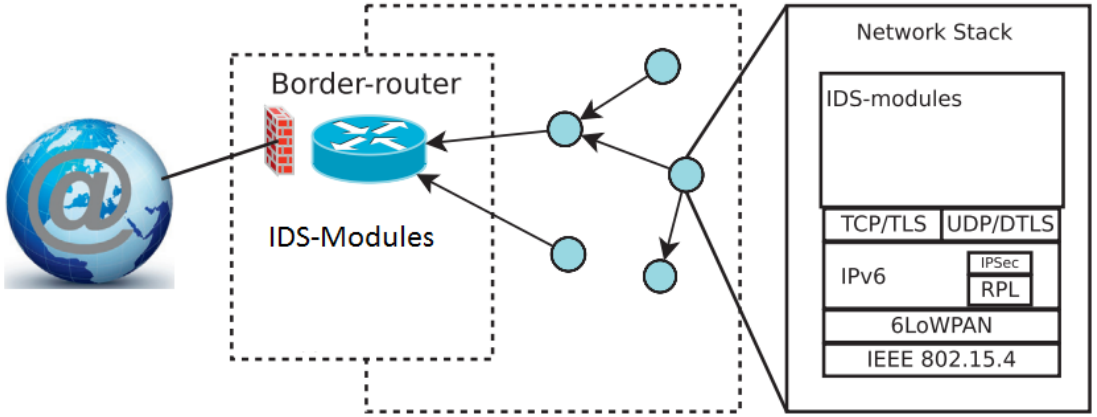


Fig.1 6LowPAN devices are connected to a Border Gateway Router(6BR) [5]

- For a network topology with N interconnected nodes, we divide the network into multiple K sub networks each having p nodes.

## I. Network Setup: (cont…)

- We use K-Clustering algorithm to divide the network such that delay distance between any two subnetworks is maximum.
- Each node contains a module which will work as our intelligent IDS.
- These N nodes are connected to a Border Gateway Router(6BR) on which we are running a generic IDS preventing external attacks.
- Internal attacks are prevented using our Intelligent IDS.

## II. Intelligent IDS:

- IDS is present in every node and is trained in lab environment in actual network.
- Every node keeps a log file of data that has been transmitted by it since last time IDS was active in this node.
- When IDS gets active in a node, it reads the log file and compare it with its trained dataset to find anomalies.
- We define two thresholds, lower and upper threshold, such that if variations are below lower threshold than node is in Safe state.

## II. Intelligent IDS: (cont...)

- If variations are in between lower and upper threshold, then node is in warning state.
- If variations are above upper threshold, then node is in alarm state.
- Once the scanning in a node is done, IDS is made inactive and it clears the log file of that node to start logging its new data flow.

## II. Intelligent IDS: (cont...)

➢ **Intelligent IDS contains 3 States:**

1. **Safe State:** IDS is made inactive and next node's IDS is made active.

2. **Warning State:** IDS active time period is extended using our Time Extension Algorithm and next node's IDS is made active.

3. **Alarm State:** IDS is made inactive sending an alarm and next node's IDS is made active.

## II. Intelligent IDS: (cont…)

- Initially all IDS's are inactive in a region. We select starting node using Dijkstra's algorithm on the region.
- We calculate delay of each node with every other node and get the minimum of maximum of all delays of a node with other nodes of that region.
- This will give us a starting node for our roaming heuristic. For the most time, only one IDS is active in a region.

## II. Intelligent IDS: (cont…)

- The active time period of an IDS in a node is T
- If anomalies are between lower and upper threshold, we increase the active time of that particular IDS module according to our time extension algorithm.
- After time T, another node in the region starts it IDS. We use DFS to reach to the next node in that region.

## III.Time Extension Algorithm:

- The active time period of an IDS in a node is T
- Initially an IDS is supposed to run for time period T to detect anomalies in data.
- In warning state of a node, we extend active time of its IDS exponentially to 2T then 4T and so on till variations goes down below threshold reaching Safe State or go above upper threshold reaching Alarm State.
- If active time of that IDS reach a hard time limit value assigned by us than IDS will stop generating an alarm.

# References:


[1] N. Kushalnagar, G. Montenegro, C. Schumacher, IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals, RFC 4919, August 2007.

[2]Y. Hu, A. Perrig, D. Johnson Wormhole attacks in wireless networks IEEE Journal on Selected Areas in Communications, 24 (2) (2006), pp. 370-380

[3]K. Hwang, M. Cai, Y. Chen, M. Qin Hybrid intrusion detection with weighted signature generation over anomalous internet episodes IEEE Transactions on Dependable and Secure Computing, 4 (1) (2007), pp. 41-55

[4] S. M. Banik and L. Pena, "Deploying agents in the network to detect intrusions," *2015 IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS)*, Las Vegas, NV, 2015, pp. 83-87.

[5] Shahid Raza, Linus Wallgren, Thiemo Voigt, SVELTE: Real-time intrusion detection in the Internet of Things, In Ad Hoc Networks, Volume 11, Issue 8, 2013, Pages 2661-2674.

[6] E. M. Chakir, M. Moughit and Y. I. Khamlichi, "A real-time risk assessment model for intrusion detection systems," *2017 International Symposium on Networks, Computers and Communications (ISNCC)*, Marrakech, 2017, pp. 1-6.