

# Trust Based Intrusion Detection System to Detect Insider Attacks in IoT systems

Ambili K N, Jimmy Jose

Department of Computer Science and Engineering  
National Institute of Technology Calicut, India

December 18, 2019

Seoul, South Korea

# Overview

- 1 Introduction
  - Layers in IoT
  - Intrusion Detection System
- 2 Attacks in IoT
- 3 Attacks Considered
- 4 Routing Protocols Considered
  - RPL
  - CoRPL
  - CARP
- 5 Trust Based IDS Solution
  - Our Solution
  - Pseudocode
    - in RPL and CoRPL
    - in CARP
- 6 Conclusion
- 7 References

- special significance due to application in everyday life
- devices directly connected to the Internet or through gateway forming a LAN
- made of wired or wireless sensors and its applications
- communication model can be
  - client/server
  - publish/subscribe
  - push/pull

# Layers in IoT [1]

- Business Layer
- Application Layer
- Service Management Layer
- Object Abstraction Layer
- Object Layer

# Intrusion Detection System

- rule based [4]
- anomaly based [4]
- specification based [8]
- distributed trust based [6, 7]

# Attacks in IoT [2, 3]

- inherits all attacks from the Internet
- application layer attacks like web-based attack, social engineering attack, buffer overflow and denial of service
- network layer attacks like blackhole, sinkhole and wormhole

# Attacks Considered

- sinkhole - group of malicious nodes send packets only to a particular sink node
- blackhole (packet dropping) - variation of sinkhole wherein only one sink is present [10]. Mitigation is considered in [5].
- wormhole - two nodes which are at strategically important positions in the network decide to pair and analyze the network data

# Routing Protocols Considered

- RPL [11, 12], CoRPL [14] and CARP [13]
- source IP spoofing in malicious shorter path advertisement facilitates attacks



- builds up a DODAG - destination oriented directed acyclic graph
- messages include
  - DIO - DODAG information object
  - DIS - DODAG information solicitation
  - DAO - DODAG advertisement object
  - DAO-ACK - DAO acknowledgement
- DIO inform neighbours of a node's presence
- nodes respond with DIO-ACK and connects to a parent node
- DIS enquires about neighbouring nodes

- variant of RPL for cognitive systems
- uses the same set of messages as in RPL
- each node keeps information of forwarding set

- underwater routing protocol
- structures the nodes as a complete network
- messages include
  - HELLO - flooded from sink through the network
  - PING - begin communication by broadcasting PING control message to neighbours
  - PONG - reply messages

# Our Solution - Trust Based IDS

- trust score is calculated based on node behaviour detected from responses to request queries
- trust score is stored in blockchain
- blockchain is managed by consortium of network managers
- leader election in complete network is used to arrive at trust to be stored in blockchain

# Our solution - Trust Based IDS

- initial trust score evaluated based on configuration details loaded into the device at the time of shipment
- every node maintains neighborhood table
- trust score is calculated based on the observed behavior
- indices include honesty, lack of cooperation and reception of packets only from neighboring nodes

# Our solution - Distributed Leader Election

- Each participating node is a monitor node and prepares transaction record.
- Transaction records are sent to all neighbor nodes at specific intervals of time.
- The node with highest trust score, as per latest information in blockchain is chosen as the leader.

# Our solution - Transaction Records

- PIPO or packets in packets out attribute is a two-dimensional vector with the ID of neighbor node as the first field and difference between packets in and packets out as the second field in each row.
- Route attribute is a list of unique routes in the packets the node receives.
- Unknown sender is the third attribute which indicates the count of packets received from unknown senders (those not present in its neighborhood table).

PIPO	Route	Unknown Sender
------	-------	----------------

Figure: Transaction record in trust based IDS

# Pseudocode

- input: transaction record of all participating nodes
- output: alert message and new trust scores
- pseudocode: repeat until a new trust score for any other node higher than the self score of the leader is obtained
  - 1 Gather the transaction details of all member nodes.
  - 2 PIPO values of communicating nodes is compared. If equal, increment trust score of both the nodes, else do nothing.
  - 3 Compare the list of unique routes and check if any route other than the one permitted by routing protocol appears. If yes, decrement the trust score of all nodes from the point at which discrepancy occurs, else do nothing.
  - 4 If unknown sender count is greater than zero, check the routes to see if nodes not permitted as per the routing table appears. If yes, decrement the trust score of the just preceding node.
  - 5 If the evaluated trust score of a node is less than that in the latest block of blockchain, raise an alert message to participating nodes except the currently evaluated node of an intrusion detection.
  - 6 Include new trust scores record to blockchain.
  - 7 Initialize trust score of each node to last trust score from the ledger.



The neighborhood table is loaded and kept updated with IPv6 addresses from DIO and DAO messages. The transaction record can be loaded with the information from DIO and DAO messages in the following way:

- Each row of PIPO field will have IPv6 address of neighborhood node as first entry fetched from DIO messages received and the aggregate count of messages passed between them as the second entry.
- The route field has to be generated by the node for this specific application by appending IP address at the application level at each node. This can be picked from route field in DAO message.
- Unknown sender field is loaded based on the count of IPv6 addresses in DIO messages not known, as per the neighborhood table maintained.

## using pseudocode in CARP

The neighborhood table is loaded and kept updated with IPv6 addresses from PING and PONG messages. The transaction record is loaded with information from PING and PONG messages in the following way:





- Each row of PIPO field will have IPv6 address of neighborhood node as first entry fetched from PING or PONG messages received and the aggregate count of messages passed between them as the second entry.
- The route field has to be generated by the node for this specific application by appending application level route field with IP address at each node.
- Unknown sender field is loaded based on the count of IPv6 addresses in PING messages not known, as per the neighborhood table maintained.

# Conclusion




- trust based IDS has been proposed with trust scores stored in distributed immutable ledger
- detection of blackhole, wormhole and sinkhole attacks in network layer is done using trust scores
- out-of-band wormhole has not been considered
- maintaining large neighborhood table may be difficult





-  *Internet of things: a survey on enabling technologies, protocols and applications*, Recent trends in combinatorics, A.Al-Fuqaha, M. Guizani, M Mohammadi, M. Aledhari, M. Ayyash, IEEE Communications Surveys Tutorials 17(4), 2347-2376, 2015
-  *Securing the Internet of Things: Challenges, threats and solutions*, Panagiotis I. Radoglou Grammatikis, Panagiotis G. Sarigiannidis, Ioannis D. Moscholios, 2019, Elsevier Internet of Things, Volume 5, pp.41-70
-  *Enforcing security in Internet of Things frameworks: A systematic literature review*, Mohab Aly, Foutse Khomh, Mohamed Haoues, Alejandro Quintero, Soumaya Yacout, 2019, Internet of things, Elsevier Volume 6

# References II

-  *A survey of intrusion detection in Internet of Things* Bruno Bogas Zarpelao, Rodrigo Sanches Miani, Claudio Toshio Kawakani, Sean arlisto de Alvarenga, 2017, Journal of Network and Computer Applications, Volume 84
-  *Mitigation of black hole nodes in MANET* Ming-Yang Su, Kun-Lin Chiang, Wei-Cheng Liao, International, 2010, Symposium on Parallel and distributed processing with applications,ISPA 2010, Taipei
-  *Trust-Based Intrusion Detection in Wireless Sensor Networks*, Fenye Bao, Ing-Ray Chen, MoonJeong Chang, Jin-Hee Cho, 2011, IEEE International Conference on Communications, IEEE, Kyoto
-  *Distributed Trust based Intrusion Detection Approach in Wireless Sensor Network*, R. Dhakne, Dr. P.N. Chatur, 2015, Communication, Control and Intelligent Systems IEEE, Mathura, India

# References III

-  *Specification- based IDS for securing RPL from topology attacks*, Anhtuan Le, Jonathan Loo, Yuan Luo, Aboubaker Lasebae, 2011, IFIP Wireless Days (WD), IEEE, Niagara Falls, Ontario, Canada
-  *A trust based intrusion detection system for mobile RPL based networks*, Faiza Medjek, Djamel Tandjaoui, Imed Romdhani, Nabil Djedjig, 2017, IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data, IEEE, Exeter
-  *Malicious packet dropping: how it might impact the TCP performance and how we can detect it* Xiaobing Zhang, S.F. Wu, Zhi Fu, Tsung-Li Wu, 2000, IEEE Proceedings 2000 International Conference on Network Protocols, IEEE, Osaka, Japan

-  *RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks*  
<https://tools.ietf.org/html/rfc6550> Accessed 16 Sept 2019
-  *The routing protocol for Low-Power and Lossy Networks (RPL) Option for carrying RPL information in Data-Plane Datagrams,*  
<https://tools.ietf.org/html/rfc6553> Accessed 16 Sept 2019
-  *Channel-aware routing for underwater wireless networks* Stefano Basagni, Chiara Petrioli, Roberto Petrocchia, Daniele Spaccini, 2012, IEEE 2012 Oceans Yeosu, IEEE, Yeosu, South Korea
-  *CORPL: A routing protocol for cognitive radio enabled AMI networks, IEEE Transactions on smart grid,* Adnan Aijaz, Hongjia Su, Abdol-Hamid Aghvami, , doi: 10.1109/TSG.2014.2324022

# Thank You!!