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

Abstract:

With the widespread use of Internet of Things (IoT) devices provides an opportunity for service providers to develop new streams of revenue. For end users, IoT has the potential to provide solutions that can dramatically enhance productivity and quality in security, health, education, and many other areas. However, this large number of diverse devices will also increase severe security threat to the end users.

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.

We proposed a novel Intelligent Roaming Intrusion detection system for the 6LowPAN based IoT. In our proposed solution, we primarily target internal attacks such as spoofed or altered information, sinkhole, and selective-forwarding. Conventional IDS are centralized in nature and suffers from scalability limitation and bottleneck failure. Our approach faces neither of these problems. It can efficiently be extended to detect other attacks within reasonable response time. Our solution overhead is small enough to deploy it on constrained nodes with limited processing power, battery power and communication and storage capability.

Introductions:

We divide our idea in four phases, which are -

Network Setup:

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

Intelligent IDS:

Our IDS is present in every node and is trained in lab environment with the type of data that will flow through that node 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. 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.

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

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

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

Roaming Heuristic:

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. 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.

Time Extension Algorithm:

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.

Applications:

Our solution can be used in various scenarios to find anomalies and stop attacks like spoofed or altered information, sinkhole, and selective-forwarding. Examples are:

- Battlefield Surveillance
- Industrial process monitoring and Data Centre Monitoring
- geo-fencing of gas and oil pipelines

Future Work:

We can do more research to get much better response time and detect much larger spectrum of attacks. We can give better algorithm to divide network into k clusters and analyse the performance of clusters by simulating the network on varying value of k to get its optimal value for total number of nodes N.

By multiple simulations of our network system, we can find better values of upper and lower thresholds to avoid sending false alarm or miss any intrusion in the system.

Also, In our Time Extension Algorithm, we are increasing time exponentially to be on the safer side and not miss any intrusion, but by multiple simulations, we can try linear or polynomial growth in active time period of an IDS and get the best possible strategy to increase time of an IDS.

We can work on finding first node of a region more effectively using game theory techniques.