IP 기반 유비쿼터스 센서 네트워크에서의 침입 탐지

시드 아민 오베이드 O, 홍충선

경희대학교 컴퓨터공학과

obaid@networking.khu.ac.kr, cshong@khu.ac.kr

Detecting Intrusion in IP-Based Ubiquitous Sensor Networks

Syed Obaid Amin O and Choong Seon Hong

Department of Computer Engineering, Kyung Hee University,

Abstract

A novel Intrusion Detection and Response System (IDRS) for IP based Ubiquitous Sensor Networks (IP-USN) is proposed. According to the best of our knowledge this is the first security framework for any kind of IP based sensor devices. The proposed scheme is fast, lightweight in terms of computation and memory, which make it appropriate for resource constrained sensor devices.

1. Introduction

The term IDRS (Intrusion Detection and Response System) is used to indicate a system which has both intrusion detection and intrusion response capabilities. Intrusion detection means that the system is capable of detecting cyber attacks such as (D)DoS or any other sort of intrusion. On the other hand, intrusion response refers to the actions taken to avoid the intrusion, for instance changing rule in Firewall or tracing an attack path that is commonly known as Traceback.

This paper proposes a IDRS for IP-USN and presents initial results achieved so far. According to the best of our knowledge this is the first effort in this regard. The main focus of our research is to come up with a fast and lightweight IDRS so that we can apply it on resource constrained sensor networks. Our contribution can be outlined as follows:

- We accentuate the need of an IDRS specifically tailored for IP-USN environment,
- Identify possible attack models in IP-USN environment,
- Design a generalized architecture for IP-USN IDRS and
- Implement an IDRS based upon the generalized architecture.

2. IP Based Sensor Networks (IP-USN) and possible attack models

With the help of IP stack a sensor node can utilize most of the services which are offered by traditional IP networks. Moreover, intellectual property conditions for IP networking technology are either more favorable or at least better understood than proprietary and newer solutions. Therefore workgroups such as IETF's 6LoWPAN [7], are working on the integration of IP with sensor networks. However, along with advantages such as high accessibility, scalability and possible convergence to Next Generation Networks (NGN) this integration also brings disadvantages of both worlds. Cyber attacks which were only possible on IP networks are now possible on sensor networks as well. We identified three possible attack models on IP-USN environment and propose an IDRS framework keeping these models in view.

a. Attack Model 1(Attacks from the Internet Hosts)

By having IP addresses, sensor nodes are now directly reachable to the Internet users. However, this feature, along with accessibility, also increases the chances for sensor nodes to be attacked by the Internet users. Possible attack types are flooding to drain the power source quickly, intercepting or stealing the critical data, unauthorized access and so on. The heterogeneity in IP and USN networks makes difficult to detect this form of attacks because a normal IP traffic could be dangerous for resource constrained

* "This research was supported by the MKE under the ITRC support program supervised by the IITA"(IITA-2008-(C1090-0801-0016))

sensor nodes. These attacks can be minimized by using pre-installation measures such as authentication and firewalls however; none of the solution is lightweight. Moreover, traditional IDRS are not applicable due to dissimilarity of traffic pattern in IP-USN design. Therefore, a need off IDRS specifically tailored for IP-USN is solicited and inevitable.

b. Attack Model 2 (Attacks within Sensor Networks)

Varieties of attacks are possible on sensor networks as discussed in [1]. Due to inherited characteristics of sensor networks, IP-USN devices can also be circumvented by these attacks. Along with it, in specialized IP-USN, like 6LoWPAN, IPv6 Neighbor Discovery (ND) RFC 2461 [2] and Address Autoconfiguration RFC 2462 [3] mechanisms are used to learn the local topology of the network. Neighbor Discovery in 6LowPAN links is also susceptible to threats as detailed in [4]. All these facts demand a specialized IDRS which is capable to cope with new class of attacks possible in IP-USN devices.

c. Attack Model 3 (Attacks on the Internet Clients)

This scenario cannot be considered as a DDoS attack; even then it could be a serious threat. This scenario mainly deals with false data injection in which an adversary feeds wrong data to the sink and consequently to the Internet clients. Detection points could be a sink, intermediate nodes and/or the cluster head, depending upon the computational power of the relevant nodes. This threat can be minimized by using cryptography, filtering or statistical schemes for false data identification. We found that all of these solutions are directly applicable to IP-USN environment. Therefore our research didn't target this class of attack model.

III. Intrusion Detection and Response System for IP-USN.

The main module of IDRS resides on IP-USN gateway, which has a support of dual stack. Considering the heterogeneity of IP-USN environment, we defined two separate components, namely IPA (Internet Packet Analyzer) and UPA (USN Packet Analyzer) which analyze the traffic according to the packet type for detecting attacks. The interaction between them is shown in Figure 1.

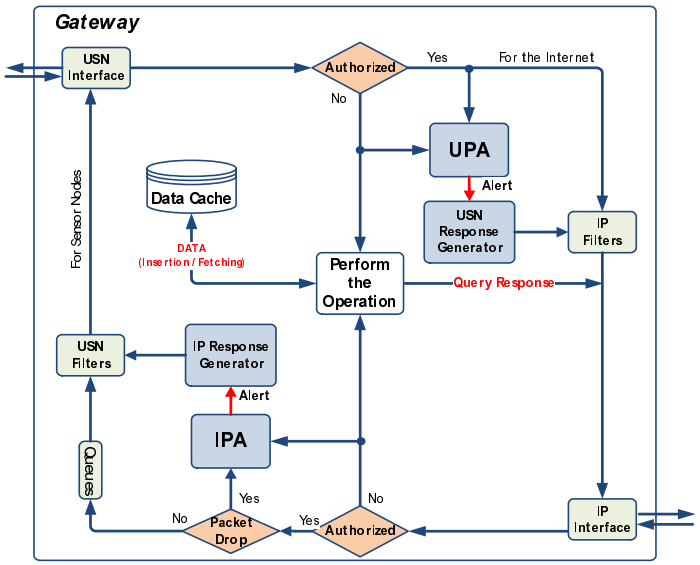

Figure 1. IP-USN Gateway internal architecture

IPA consists of two main cascaded components named as Anomaly Detector and Pattern Classifier. Anomaly detector is responsible to detect the abnormal traffic surging towards the sensor nodes. On the other hand, pattern classifier classifies the attack types such as TCP SYN attack or ICMP Flood or so on. The reason for choosing hybrid architecture is multifold. As discussed above the definition of abnormality or anomaly is different for both network paradigms. As a consequence, there are chances that an activity which is malicious for USN networks can go unobserved by IPA. Therefore, we need a mechanism which can detect even a minute intrusion and as early as possible. However, this requirement comes with a price of increased false alarms hence we supported our architecture with pattern classifier to reduce the false alarm rates. The internal architecture of IPA is shown in Figure 2.

IPA only starts to investigate incoming traffic when queues of congestion avoidance algorithms overflow and do not accept more packets, as shown in Figure 2. Usually congestion avoidance algorithms discard incoming packets when their queues are full. In our scheme we store the discarded packets for further investigation of the intrusion, and pass it to anomaly detector. The anomaly detector then applied three tests as shown in Figure 2 to check the abnormal behavior. If any malicious activity or abnormality is detected then the control is passed to the packet classifier. The packet classifier runs the simple pattern matching algorithm for checking the predefined attack types on the stored buffer. If the number of packets of

a specific protocol is found to be greater than user defined threshold an alert is generated.

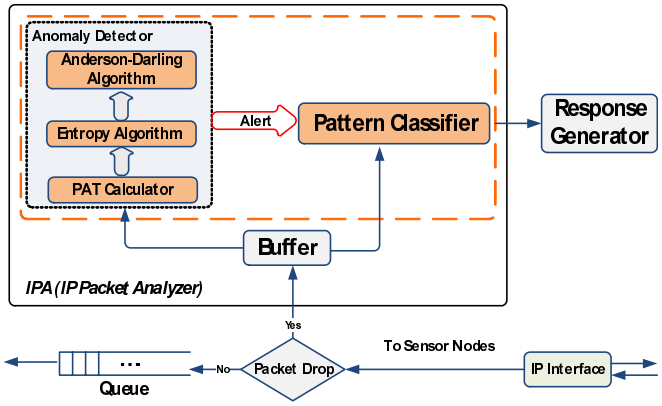

Figure 2. Internal architecture of IPA (Internet Packet Analyzer)

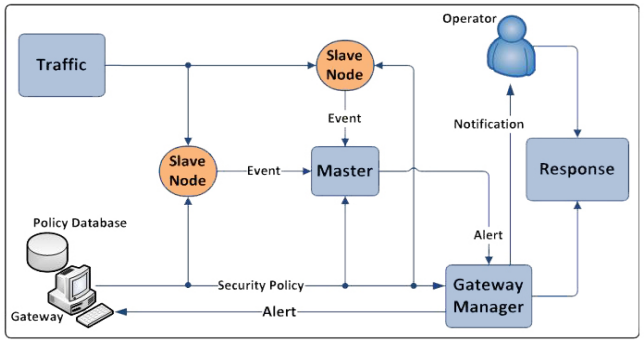

Figure 3. Working of Distributed USN-IDRS

On the other hand, for UPA we use distributed approach. We define two types of devices in the USN side of IP-USN networks. One type of devices acts as surveillant nodes and generate the alert messages; we named it as a slave node. The generated messages are then sent to the master node which in turn takes the decision and enforce policy within its domain. There could be multiple master and slave nodes in a network. Master node can also detect an intrusion. Considering the example of 6LowPAN, FFDs would be working as master nodes while RFDs would be acting as slave nodes. A conceptual workflow of whole scheme is shown in Figure 3. To illustrate the working of given architecture we implemented a UPA and distributed USN-IDS in a simulated environment. This system was made to detect jamming and selective forwarding attack on USN [6]. Figure 4 shows the block diagram of the IDS resides on the slave nodes.

Along with IDRS we also propose a concept of data caches, which stores the recent readings taken from the sensor nodes and upon the request from the users; these caches deliver them the stored value rather than probing sensors again for taking the readings. Data cache can be deployed at the base stations or/and at the cluster head. With the help of data caches we can greatly reduce the number transmission of sensor nodes which consequently increases their lifetime. Our concept of data caches can minimize the DDoS attacks up to great extent; however data caches are not able to deliver real time data. This deficiency can be overcome by tuning the cache's refresh rates and/or allowing authorized users to access the sensor networks directly.

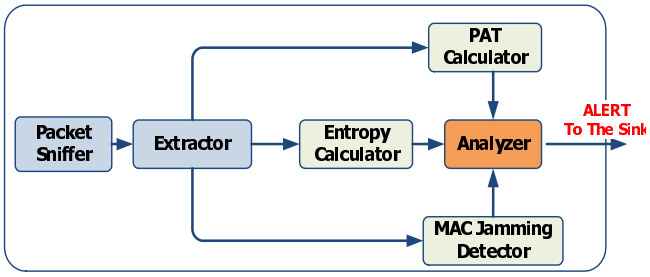

Figure 4. Block Diagram of UPA Slave Nodes

UPA slaves comprises of two major components namely TAD (Traffic Anomaly Detector) and MAC Jamming Detector responsible for detecting deceptive and constant jamming [6], respectively as shown in Figure 4.

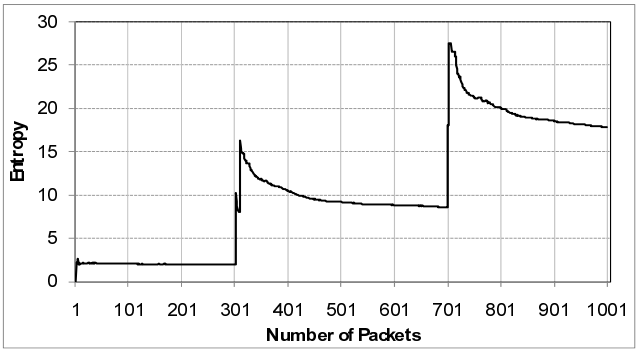

Figure 5. Entropy values for a short-lived DDoS attack

IV. Evaluation Results

In initial stage we implemented UPA in a simulated environment using SENSE simulator [5]. Figure 5 shows the entropy calculation for a short term DDoS attack. Before the attack begins, source address entropy calculation revolves around value of 2. As the attacker starts to spoof the source addresses, the entropy abruptly changes to 17, and then gradually starts to become stable. Second spike, near the packet count of 700, also shows this behavior when an attacker starts to come with even more source

addresses. This abrupt change notification is then send to the analyzer as shown in Figure 4, which after inspecting the data rate can generate an attack signal.

To evaluate the performance of an IDS, attack detection time, number of false positives (false alarms) and number of false negatives (misses) are few of the key metrics. According to our simulation results, the number of false positives and number of false negatives (misses) are minimum at α= 0.9, Th_{min}= *0.03 secs.* and Th_{max}= *4 secs.* Two more parameters in which we were interested are intrusion detection speed and the number of alerts generated. Higher number of alerts indicates higher degree of attack. Figure 6 depicts the minimum time required by a node to detect an attack as the number of attackers increases. It is clear from the figure that as the number of attackers crosses a certain threshold, indicated by β, the detection delay drops drastically. β can be considered as a threshold for a number of attackers after which attackers start to affect the network severely. Similar results were observed in the alert generation, as shown in Figure 7, when the number of attackers crosses the threshold value *β* the number of alert generating nodes increases greatly. This behavior complements our proposal, as with the help of reduced detection delay and higher number of alerts a sink can more rapidly conclude about an attack.

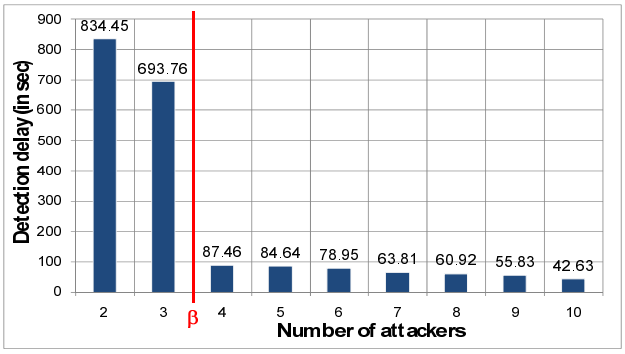

Figure 6. Detection time vs. number of attackers.

V. Conclusions:

In this paper we discussed the attack types possible in IP-USN environment. We also discussed merits and demerits of traditional response schemes on sensor networks. For this research, we took a bottom up approach, means; starting from attacks on traditional sensor networks we will move ourselves towards IP-USN specific attack scenarios. So far we have implemented an IDS for USN. Optimal values for threshold have been defined as well. Our next target is to define a complete traceback protocol which may include details of packet structure, message transitions and so on. Energy consumption and traceback efficiency will also be evaluated.

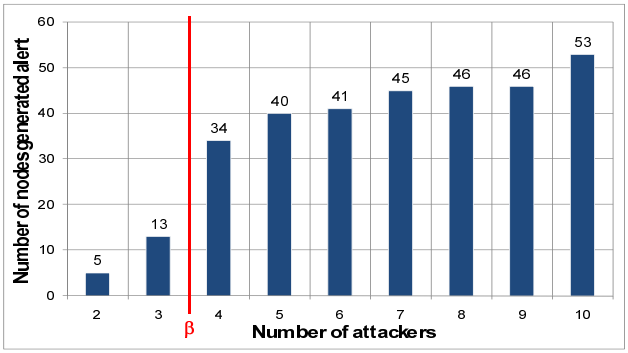

Figure 7. Number of observing nodes vs. number of attackers.

References:

[1] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures”, in Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003, Page(s): 113-127.

[2] T. Narten, E. Nordmark and W. Simpson, “Neighbor Discovery for IP Version 6 (IPv6)”, RFC2461, IETF , December 1998.

[3] S. Thomson and T. Narten, “IPv6 Stateless Address Autoconfiguration”, RFC 2462, December 1998.

[4] P. Nikander, Ed., J. Kempf and E. Nordmark, “IPv6 Neighbor Discovery (ND) Trust Models and Threats”, RFC 3756, IETF, May 2004.

[5] SENSE (Sensor Network Simulator and Emulator) Version 3.0.3, http://www.ita.cs.rpi.edu/sense/index.html

[6] Wenyuan Xu, Ke Ma, Wade Trappe, and Yanyong Zhang, "Jamming Sensor Networks: Attack and Defense Strategies", IEEE Network, Volume 20, Issue 3, May-June 2006, Page(s): 41- 47.

[7] IPv6 over Low power WPAN (6lowpan), http://www.ietf.org/html.charters/6lowpan-charter.html