A Novel Intrusion Detection Framework for IP-Based Sensor Networks

Syed Obaid Amin[1], Young jig Yoon[2], Muhammad Shoaib Siddiqui[3] and Choong Seon Hong[4]

Department of Computer Engineering,

School of Electronics and Information, Kyung Hee University, Korea.

obaid@networking.khu.ac.kr[1]

yjyoon@networking.khu.ac.kr[2]

shoaib@networking.khu.ac.kr[3]

cshong@khu.ac.kr[4]

***Abstract*— Utilization of IP in sensor networks converges them to a unified and simple naming and addressing hierarchy. Thereby, allowing us to be benefited from the existing well established tools and technologies of IP networks. Along with many other unveiled issues, securing IP-USN (IP based Ubiquitous Sensor Network) is of great concern for researchers so that future market satisfaction and demands can be met. Without a proper security framework, it is hard to envisaged IP-USN realm. In this paper we propose a novel Intrusion Detection Framework for IP-USN. 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[*].**

I. INTRODUCTION

IP based Ubiquitous Sensor Network (IP-USN) is an effort to build the "Internet of things". Korea is appearing as a prominent participant in this area. 6 out of 11 standardization proposals submitted by Korea to the IETF 6LowPAN Working Group [7] prove this fact and able to draw the world's attention on the IP-USN facilitation. Along with many other unveiled issues, securing IP-USN is of great concern for researchers so that future market satisfaction and demands can be met. Without a proper security framework, it is hard to envisaged IP-USN realm. For instance, IP-USN environments such as ubiquitous patient care systems which are connected to patients to monitor levels of medications and procedural outcome can be affected by the internal or external network attacks. Denial of service attacks against such networks may permit fatal damage to the health and safety of the people. Therefore a proper security framework is required and unavoidable.

This paper proposes an IDS (Intrusion Detection System) 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 IDS so that we can apply it on resource constrained sensor networks. Our contribution can be outlined as follows:

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

II. 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 IDS 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 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 IDS are not applicable due to dissimilarity of traffic pattern in IP-USN design. Therefore, a need off IDS specifically tailored for IP-USN is solicited and inevitable.

[*] This work was partially supported by NIA, KOREA under the KOREN program and the MKE under the ITRC support program supervised by the IITA"(IITA-2008-(C1090-0801-0016)). Dr. CS Hong is corresponding author.

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 IDS 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 IDS 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.

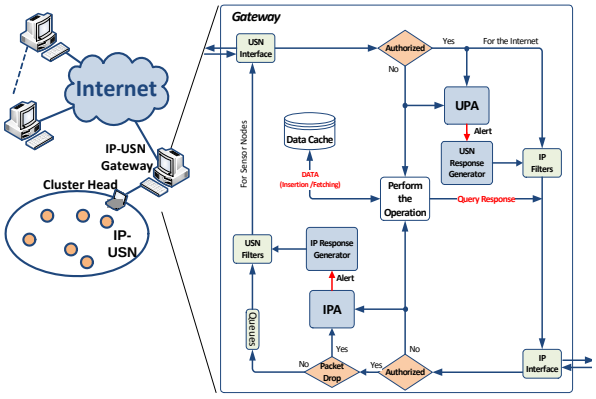

Figure 1. IP-USN Gateway internal architecture

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.

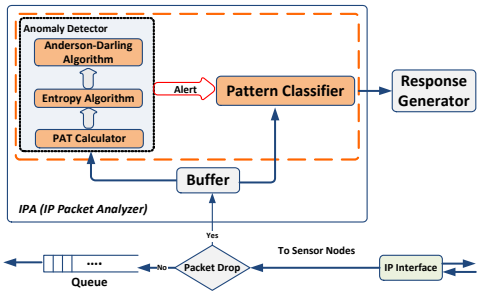

Figure 2. Internal architecture of IPA

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.

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. To illustrate the working of given architecture we implemented a UPA and distributed USN-IDS in a simulated environment. Figure 3 also shows the block diagram of the IDS resides on the slave nodes.

Along with IDS we also propose a concept of data caches. Data cache 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.

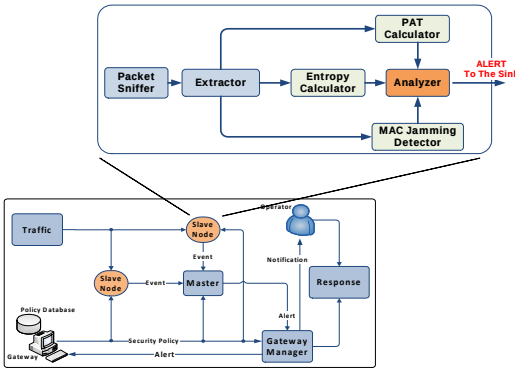

Figure 3. Working of UPA slave nodes

IV. Evaluation Results

In initial stage we implemented UPA in a simulated environment using SENSE simulator [5]. Figure 4 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. These abrupt change notifications are then send to the analyzer as shown in Figure 3, which after inspecting the data rate can generate an attack signal.

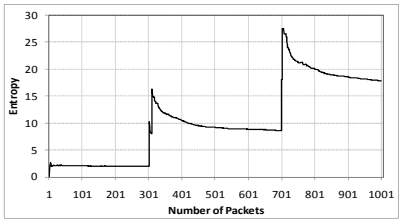

Figure 4. Entropy values for a short-lived DDoS attack

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 $\alpha = 0.9$, $Th_{min} = 0.03$ *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 5(a) 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 5(b), 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.

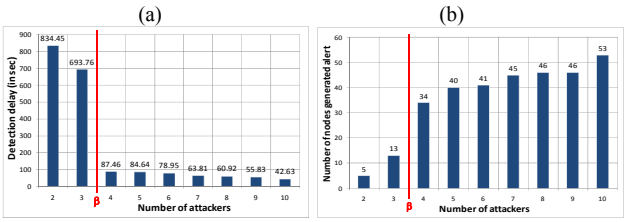

Figure 5. Detection time and number of alert generating nodes vs. number of attackers.

V. Conclusions:

In this paper we propose an intrusion detection framework for IP-USN environment. We started our discussion by describing possible attack types in IP-USN. We also discussed merits and demerits of traditional intrusion detection 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. Along with the complete implementation of IP-USN IDS, our next target is to define a complete traceback protocol which may include details of packet structure, message transitions, energy consumption and traceback efficiency.

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] 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