A Signature Key and Positioning Based Approach to Secure Heterogenous Network

Mrs. S. Saranya

Assistant Professor
Department of Computer Science and Engineering
SRM University
Tamil Nadu, India- 603203

Sudhir Kumar. P

Department of Computer Science and Engineering
SRM University
Tamil Nadu, India- 603203.Email-

Abstract

Now a days the heterogeneous networks are one of the advanced networks in the real world and this network is better in service providing. Normally, the heterogeneous network is a mixed network that is used to share the information from one network to another network. But, still the security of this network is not effective, because the heterogeneous network is unstructured and mixed network. In this paper there are two rules proposed. One is Negative Selection and another is Danger Theory. NS theory is the traditional Understanding of anomaly detection in the Human Immune System. DT is a radical new concept that challenges the main fundamentals of the NS theory. Also this paper enhances secure verification process. Verification process is enhanced by using combination of RSA algorithm and Digital signature technique along with updating the position of the node. Even more security enhancement is given by giving a message pattern to every node and creating a detector set for anomaly detection. Threshold levels are given to every network in order prevent DDOS attack.

Keywords-Heterogeneous network, Threshold level, Anomaly detection, Danger theory.

1. Introduction

The demand for anytime, anywhere, anyhow communication is one of the major challenges for future generation networks. One key approach to address this issue is by accommodating an interworked architecture among the existing and future access networks via a common platform, preferably Internet Protocol (IP) based platform. As each access network is interworked together, any malicious security threat will no more be confined to a single access network. In such a hostile environment, the impact of an attack on the network may be easily spread beyond a typical epidemic attack (i.e., where the impact is locally bounded within a single access network) to a more severe pandemic proportion, due to the migration of security Aspirations for a boundless communication paradigm for future generation networks have changed the conventional way of looking at network security. With such a vision, security techniques should not only be securing local end- users but also be protecting entire net- works from malicious adversaries.

1.1 Negative Selection

In the NS theory, the exact nature (i.e., either good or bad) of an antigen can be identified by discriminating "self" and "non self" markers presented at the cell's surface. Generally, these two markers distinguishes between a human cell (self) and a foreign antigen (non self). This discrimination process begins with the evolution of T cells in a lymphoid organ, called the thymus. T cell is a white blood cell that tailors the HIS to respond to specific antigens. According to the NS theory, during the evolution process any immature T cells that match self protein

markers are destroyed, whereas those with non self markers are kept in the thymus to reach the maturity stage. The mature T cells are then released from the thymus for searching out the specific targeted foreign antigens. Once an infectious antigen (i.e., with non self marker) is detected, the T cells bind themselves to the antigen, and starts the elimination process with the help of B cells (i.e., a white blood cell that creates antibodies).

The elimination of self T cells at the early stage is mainly to ensure these T cells from not attacking the human body self cells, which may lead to an autoimmune syndrome such as diabetes mellitus type 1 and rheumatoid arthritis. The decision of retaining cells with the non self rather than the self in the initial stage justifies the name of the theory.The motivations for adopting NS theory for detecting anomalies blossomed since the pioneering work by Forrest et al. in. In particular, they proposed an NS inspired architecture to identify anomalies (e.g., viruses) in computer systems.

Since then, there has been a significant amount of effort from the research community to develop computational models inspired by the NS theory, for example. Most of the existing studies have employed the "learning" mechanisms of the NS model to create a pattern-matching rule that can identify self-non self features in the targeted system. For example, in NS inspired detection the normal behavior is regarded as self and the intrusive behavior as non self. The detectors (e.g., patterns of the network traffic, host activities) are then randomly generated to emulate the generation of T cells in HIS. In the training stage these detectors are exposed to the normal events and any matching detectors are removed from the detector sets (i.e., the NS process). The remaining detectors are then used to detect the abnormal behavior. The detectors, which correctly match the anomalous behavior, are kept for future use [10]. However, recently Tangential. Has proposed a new breed of NS called avidity based model for constructing detector set in IDS. This model adopts the principles of HIS and gene expression programming (GPE), and exploits the advantages of both NS and positive selection (i.e., retain self elements). By integrating these twodetectionPrinciples, their model is capable of addressing two common issues in NS, i.e., scalability and coverage.

1.2. DANGER THEORY

The DT emphasizes the notion that a foreign antigen can be detected by reacting to danger signals , which are triggered whenever a cell is invaded by a malicious antigen. According to Matzinger, The danger situation arises from cell distress. Therefore, identifying the cause of cell distress, either apoptosis or necrosis, is the key for detecting foreign antigens in the human body. In principle, apoptosis corresponds to a natural cell death whereas the necrosis refers to an unintended cell death that can be caused by a foreign antigen, wound, etc. This identification process is governed by a three-signal rule frame- work called as lymphotic laws. According to this law, the first signal, referred to as the initiation signal (IS), is triggered by a distressed cell to initiate the detection process. The second signal is the recognition signal (RS), which is used for antigen detection, and the last signal is the co-stimulation signal (CS), which is utilized for ensuring that the distress is really caused by the antigen. The correlation of these signals ensures that the T cells correctly discriminate between the apoptotic and the necrotic natures of distress. Once the foreign antigen is detected, the distressed cell establishes a spatial area, called a Danger Zone (DZ), around itself to mitigate and localize the impact of the attack. This process enables the distressed cell to stimulate cells within the DZ coverage to aid the mitigation process.

In regards to DT inspired detection principles, Mark Burgess was among the earliest researchers to apply the DT algorithm for detecting anomalies in computer systems. Several other notable works are a DT inspired host intrusion detection systems (HIDS) ,the detection of Bots [18], computer worm detection using T cell immunity and tolerance , and a double layer detection model for denial-of-ser- vice (DOS) attacks using the interaction principle of cells in human body [20].

The aforementioned literatures justify the possibility of adopting the NS and the DT into IDS. While the proposed solutions have been proven to be viable in small-scale computer and mobile networks, it is important to examine the practicality of these two detection theories in a heterogeneous networking environment**.**

1.3. DIGITAL SIGNATURE

A DS algorithm is used by a signatory to generate a digital signature on data and by a verifier to verify the authenticity of the signature. Each signatory has a public and private key. The private key is used in the signature generation process and the public key is used in the signature verification process. For signature generation and verification, the data which is referred to as a message, M, is reduced by means of the Secure Hash Algorithm (SHA-1). An adversary, who does not know the private key of the signatory, cannot generate the correct signature of the signatory. In other words, signatures cannot be forged. However, by using the signatory's public key, anyone can verify a correctly signed message. A means of associating public and private key pairs to the corresponding users is required. That is, there must be a binding of a user's identity and the user's public key. This binding may be certified by a mutually trusted party. For example, a certifying authority could sign credentials containing a user's public key and identity to form a certificate. Systems for certifying credentials and distributing certificates are beyond the scope of this standard. NIST intends to publish separate document(s) on certifying credentials and distributing certificates.

2. Related Works

Hofmeyr S. A. and Forrest.s" Architec --ture for an Artificial Immune System" it introduces Artificial immune system (ARTIS) ,negative selection algorithm, Memory-based detection method but main disadvantage is The Lack of robustness, adaptivity and autonomy.

Jungwon Kim, William O. Wilson, Uwe Aickelin and Julie McLeod" Cooperative Automated worm Response and Detection Immune Algorithm(CARDINAL) inspired by T-cell Immunity and Tolerance",it deals with Cooperative Automated worm Response and Detection Immune Algorithm. In constantly hostile environment, the traditional manual patching approach to protecting systems is clearly not effective.

Kephart J.O "A Biologically Inspired Immune System for Computers", it discusses about the computer immune system ,here The rate of the new virus is high. Due to the interconnectivity and interoperability between computers, the viruses will be spread to all other computers and worms to spread much more.

Stephanie Forrest and Catherine Beauchemin "Computer Immunology" it uses Agent Based Model techniques, cellular automata (CA) techniques.Here The problem is Not possible to analyze the functional behavior of a provided mechanism more rigorously.

Wang,.H , Zhang D, and Shin K. G [5] "Change-Point Monitoring for the Detection of DoS Attacks", it follows the algorithms Change-Point Monitoring (CPM),Cumulative Sum (CUSUM). The problem is Not possible to analyze the functional behavior of a provided mechanism more rigorously.

3. Proposed Method

In this paper there are two concepts proposed for detecting the malicious node and to secure the heterogeneous network. Those two concepts are Negative selection (NS) and Danger Theory (DT).In the NS, a foreign antigen (i.e., malicious external particle) in the network can be identified according to a self-nonself principle. DT is used for detecting malicious anomalies in a heterogeneous network. Considering DT as the best method after analyzing results from both theories. RSA algorithm is used for encryption along with Digital signature technique. Threshold levels are used to prevent network from DDOS attacks. Positioning technique is also used in improving security. Even a detector set is also used making the security powerful.

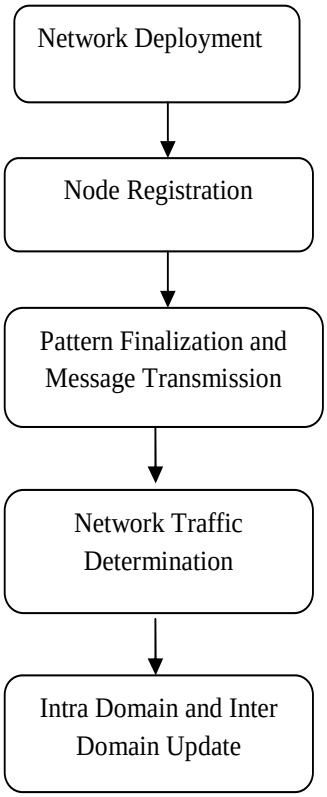

Figure 1. Proposed Architecture Model Flow

3.1. Network Deployment

This module contains details about the heterogeneous network deployment. This heterogeneous network contains two networks. One is wired network and another is wireless network. The two networks are connected by backbone. First, the wireless network contains PDSN (Packet data serving node), SGSN (Serving GPRS support node), BSC and nodes. In the wired network PDSN is connected to SGSN and SGSN is connected to Base station controller, and all access point (AP) is in control of base station and all nodes are in control of AP. Second, the UMTS network contains GGSN (Gateway GPRS support node), SGSN, RNC (Radio network controller), and mobile modes. The GGSN is connected to SGSN, and SGSN is connected to RNC, then RNC is connected to AP.

3.2. Node Registration

This module contains details about registration of every node in the network. In wireless network the node will make registration by entering required details and sent to AP. AP generate secret key, public key and signature, and sent signature and secret key to user and update pubic key, private key and signature to Base station controller, finally updated to backbone. In wired network, all nodes make registration by entering required details and submit to AP. The AP generates public key and corresponding private key and signature, and sent secret key, signature to corresponding user and also update with public key to RNC. Finally, public key, secret key and signature are updated to Backbone. Position of a node will be its access point. If it is a wireless node access point address will be updated whenever changed.

3.3. Pattern Finalization and Message Transmission

Initially assigns message patterns for all system. Then generate n number of pattern using pseudo random generator. After that back bone will match all patterns with generated pattern, remove matched pattern from the list and create detector set to find the unknown user data. Then in wireless network, one node sent message with its signature keyword to another node via Access Point. The Access Point Receives message and check whether the message is from authorized node or not by sending check request to PDSN. Also check the message pattern is not in Detector set or not. Then remove signature, encrypt the message using corresponding receiver public key and add their signature and sent to corresponding receiver node. Then receiver node will receive the message and verify the signature and view.

3.4. Network Traffic Determination

This module contains details about network traffic determination. Initially if one node in the network detects abnormal condition then the node initiates detection process. Then it creates the Initiation Signal and submits to APC. The APC examines the traffic. If the traffic exceeds the threshold value then the DT detection process ensures that the network only reacts to a “confirmed” malicious traffic. Then

compute the Danger Zone based on the attack strength and likelihood ratio. If the traffic value is huge differ from threshold value then the larger coverage will be imposed. when the danger signal reports a weak DoS attack on the SGSN, an update can be sent to other SGSNs in the same network domain.If the attack is relatively stronger, the SGSN may also want to update not only its peer SGSNs but also other lower tier nodes in the domain.For extreme cases such as distributed DoS (DDoS) and worms, the network may consider an update to other network domains as well.

3.5. Intra Domain and Inter Domain Update

In intra-domain, APC sends RS to SGSN. So, SGSN recognizes occurrence of a suspicious attack. Then SGSN sent RS to RNC. Then RNC will forward the RS to all lower nodes. Then DZ is established only when the node receives CS from its upper layer. If node has not received CS in particular interval then the node is deactivated, so all its lower node is deactivated. In inter domain update the APC handles CE procedure. This procedure facilitates notification process for other APCs of other network. Then the receiver APC decides to alert all the nodes and initiates DZ mechanism. Then provide new private key and signature to identified DZ.

4. Experimental Method

In the experimental procedure, some of the nodes will be registered. Nodes will contain both wired and wireless devices. In registration time itself public, private, signature will be issued and updated to upper layers. After that many experiments will be done on those networks by sending a message from unauthorized device in the network and verifying the results.

After getting the results the percentage of anomaly detection will be calculated and response from the networks will be observed. Huge amounts of data will be which cuts off the limit of threshold value in each network individually and attack detection levels will be observed.

5. Conclusion

This paper is intended to improve the security in heterogeneous network. So by using combination some old and new techniques, I have proposed a new technique in order to enhance security in Heterogeneous networks. Also by using the threshold level technique DDOS attacks can be prevented. Hacking into the network also becomes very hard.

6. References

[1] Hofmeyr S. A.and Forrest.s " Architecture for an Artificial Immune System", Conference, Capetown , Australia. , August 2010,pp 329-346.

[2] Jungwon Kim, William O. Wilson, Uwe Aickelin and Julie McLeod " Cooperative Automated worm Response and Detection Immune Algorithm(CARDINAL) inspired by T-cell Immunity and Tolerance, Conference, Ottwa,Canada , July 2008,pp 223-235.

[3] Kephart J.O "A Biologically Inspired Immune System for Computers". Conference, Jamica, West Indies , April 2009,pp 294-308.

[4] Stephanie Forrest and Catherine Beauchemin "Computer Immunology" it uses Agent Based Model techniques, cellular automata (CA) techniques. Conference, Durban, South Africa , October 2010,pp 143-149.

[5] Wang,.H , Zhang D, and Shin K. G "Change-Point Monitoring for the Detection of DoS Attacks. Conference, Ankara , Turkey , March 2008,pp 256-268.