Special Issue of Engineering and Scientific International Journal (ESIJ)
Technical Seminar & Report Writing - Master of Computer Applications - S. A. Engineering College (TSRW-MCA-SAEC) - May 2016
ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

Wireless Anomaly Detection based on IEEE 802.11 Behavior Analysis

Sakthi Bharathi [#1],V.Sujatha [#2]

[1]*Department of Computer Applications, S.A. Engineering college, Chennai-77.*
Sakthibharathi100@gmail.com
[2]*Asst Prof., Department of Computer Applications, S.A. Engineering College, Chennai-77.*

Abstract— In this article, we portray an variance according to the intrusion finding system for the IEEE 802.11 wireless networks based on behavioral study to sense deviations from usual behaviors that are triggered by wireless network attacks. Our anomaly behavior study of the 802.11 protocols is based on monitoring the n-consecutive evolutions of the etiquette state machine.

Keywords— wireless ,anomaly detection, malware

1. Introduction

With the exponential growth in the deployment of Wireless Local Area Networks (WLAN), the security issue of these networks has become a major concern for both users and providers. The first wireless LAN standard, IEEE 802.11, has been ratified in 1997 [1]. Since then, different revisions have been conducted to improve the base standard [2]. Although most of the revisions have focused on the performance, the IEEE 802.11i [3] standard was dedicated to security amendments. The failure of current wireless protocols to address these vulnerabilities makes intrusion detection for wireless networks extremely important. The Intrusion Detection Systems (IDSs) can provide more secure networks by monitoring the behavior of the protocol to detect any anomalous events triggered by wireless attacks. Although different intrusion detection systems are available for wired networks, they cannot be applied directly to wireless networks. While the intrusion detection systems in wired networks are working on different layers of the network, in wireless networks, we cannot easily access the content of the top layers which are often encrypted. Therefore, unlike the wired networks, most of the wireless intrusion detection systems operate at the two lower layers (Physical and Data Link).

2. Existing System Classification

In the anomaly detection technique, the system defines a model for the normal behaviour of the network and detects any deviation from this normal model as an anomalous behaviour. Unlike the Misuse detection, an anomaly detection system with a well-defined normal model can detect new attacks, and there is no need to manually update attack signature library. With better detection performance and no need for manual updates, the anomaly detection is a promising technique, and it is actively pursued by researchers.

Disadvantages of existing system:

- Security Issues
- Slow Processing.
- Inaccurate

3. Methodology

Our anomaly behavior analysis approach is defined over a universe U, which is a finite set of events. U is partitioned into two subsets N and A, which represent the Normal and Abnormal events respectively, such that N ∪ A = U and N ∩ A =∅. To model the U, we use the representation map R.

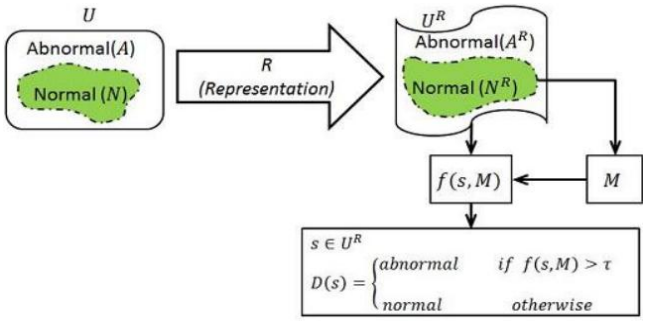

Fig.1: Diagramatic representation of methodology

Which is a function, mapping the events in U to the patterns in UR as U R ⇒ UR. Likewise, the NR and AR respectively represent the Normal event set N , and Abnormal event set A,such that N R ⇒ NR, A R ⇒ AR and NR ∪ AR = UR. A detector is defined as a system D = (f, M) with two components f and M, where f is an anomaly characterization function defined as f : UR × M →[0, 1] and M is the memory of the system that keeps the extracted normal model from represented normal events NR. With an output between 0 and 1, function f specifies the degree of abnormality for a sample s ∈ UR through comparing it with the stored normal model M. The greater the value of f (s, M), the more abnormality degree for the sample s. The detector D is a binary classifier, which classifies a sample s

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

∈ UR as normal or abnormal by comparing it with M. We can consider D as:

$$D(s) = \begin{cases} abnormal & if\ f(s, M) > \tau \\ normal & otherwise \end{cases}$$

Where τ specifies the detection threshold. Detection occurs when the detector classifies a sample as abnormal, regardless of whether it is really an anomaly or a normal sample which is mistakenly classified as anomaly. The detection errors are defined over a test set UR t which is a subset of UR, UR t ⊆ UR. Two types of errors are considered for a detector: false positive and false negative.

The false positive happens when a normal sample s ∈ NR is detected as an abnormal event and is defined as ε+ = {s ∈ NR | D (s) = abnormal};the false negative occurs when the detector classifies an abnormal sample s ∈ A R as a normal event(undetected anomalies), that is ε− = {s ∈ AR | D (s) = normal}To design a detector D we need to define the following components as it is shown in the figure 1.

U:The Event set
R: The representation map
f: The anomaly characterization function
M: The Normal model
τ : The detection threshold

The objective is to design an efficient Anomaly detector for IEEE 802.11 based on protocol behavior analysis which can be achieved by decreasing the detection errors, + and -.

4. Detector Design

In our approach, we partially model the protocol behavior by statistically modeling the ***n*** consecutive protocol transitions during a time interval *T* . By partially modeling the protocol behavior in each time interval *Ti*, we only analyze the active sessions during that time interval instead of keeping the state of all communication sessions during their lifetime. The intuition behind this technique is that most of the active attacks either show abnormal transition sequences in the protocol or excessively repeat the normal or abnormal protocol transitions.By statistically modeling the sequence of protocol transitions, we can detect the attacks through observing one or both of these footprints. Based on the formulated problem.

In what follows, we will describe our IEEE 802.11 anomaly behavior detector by defining the aforementioned required components. The representation map *R* and anomaly characterization function *f* are defined based on multiset concept. A multiset is a set of objects with a special property that allows the set to have repeated members. The formal definition of a multiset and its operations is as follows:

Definition 1: A *multiset*, or *bag*, is a set of objects in which the member repetition is allowed [24]. Formally, given a set *S*, a multiset is defined as S*(S, c)*, where the function *c*:S→ *Z*+ counts how often each member *s* ∈ *S* occurs in S. We use S*(s)* as shorthand for *c(s)*. We say that *s* is a *member* of S. denoted as *s* ∈ S, if S*(s)* ≥ 1. A multiset is shown by double curly-brackets, for example, S = {{*s*1, *s*1} is a multiset over S where S*(s*1*)* = 2, and S*(s)* = 0 for all *s* ∈ *S*\{*s*1}. For a finite multiset S, S denotes its *cardinality* and is defined as *s*∈*S* S*(s)*. If S1 and S2 are two multisets on S, their intersection is defined as S = S1 ∩ S2 where for all *s* ∈ *S*, S*(s)* =min*(*S1 *(s)* S2*(s))*. Similarly, their *union*, is S = S1 ∪ S2, where for all *s* ∈ *S*, S*(s)* = max*(*S1 *(s)*, S2 *(s))* and their *sum*, is S = S1 S2 where for all *s* ∈ *S*, S*(s)* = S1 *(s)*+S2*(s)*. The *empty multiset* ∅ of *S* is the multiset that ∅*(s)* = 0 for all s∈ *S*.

In what follows we will discuss the five steps of how to design the components of an IEEE 802.11 anomaly behaviordetector*Step 1 (Generating the Event Set **U**):* The event set *U* for IEEE 802.11 is defined as the set of all possible exchanged frames through the IEEE 802.11 protocol. By investigating the frame format of the protocol [1], we extract two kinds of features: a *session-key* and a *frame-type*. The ***session-key*** feature is used to categorize the frames under different flows of frames called ***sessions*** and denoted as *Sl*. The *session-key* for IEEE 802.11 is considered as a pair of addresses which specifies the endpoints of the communication. The *frame-type* feature is used to differentiate between different types.

5. Technical Feasibility

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. This will lead to high demands being placed on the client. The developed scheme must have a diffident obligation, as only minimal or null changes are required for implementing this system.

6. Social Feasibility

This includes the process of preparation the client to employ the system proficiently. The client must not feel threatened by the system, instead must accept it as inevitability. The stage of getting by the clients solely depends on the methods that are employed to educate the user about the confidence must be raised so that he is also able to make some user of the system.

7. Conclusion

In this project, we have reviewed the IEEE 802.11 security issues and briefly reviewed anomaly detection techniques. The main contribution of this article is that it initiates an incongruity behavioral analysis methodology and intrusion detection system which can detect different

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

types of IEEE 802.11 attacks with high detection rate (more than 99%) and low false alarms (less than 0.1%). In addition it has been verified that the proposed approach has a good tolerance against frame loss which is a general concern in wireless networks which can occur owing to mobility of the nodes or traffic congestion. Our approach is based on supervised learning and anomaly based behavioural analysis technique that builds statistical metrics of fixed size sequential patterns, known as n-gram, to characterize the normal protocol transitions over a period of time during training phase. We have shown that by using n-grams of size 4 we can accurately detect wireless attacks with less than 0.1% false positive alarms (+ < 0.1%). We have also shown that our approach can accurately detect the known WIFI attacks as: Disassociation Flood, Deauthentication attack, Injection Test, Association Flood, Fake Authentication and Authentication Flood with good false positive rates. We are currently developing other statistical measures that can be used to detect other types of wireless attacks. Since our methodology is based on partially modeling of the protocol state machine, it can be easily applied to other protocols such as Zigbee, Bluetooth, etc.

References

[1] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen", Computer, Vol. 31, no. 2, 1998, pp. 26–34.
[2] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography", IEEE Security Privacy, Vol. 1, no. 3, May/Jun. 2003, pp. 32–44.
[3] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding- a survey", Proc. of IEEE, Vol. 87, Jul. 1999, pp. 1062–1078.
[4] Y.-M. Cheng and C.-M. Wang, "A high-capacity steganographic approach for 3D polygonal meshes", Vis. Comput., Vol. 22, nos. 9–11, 2006, pp. 845–855.
[5] S.-C. Liu and W.-H. Tsai, "Line-based cubism-like image—A new type of art image and its application to lossless data hiding", IEEE Trans. International Conference in Forensics Security, Vol. 7, no. 5, Oct. 2012, pp. 1448–1458.
[6] I.-C. Dragoi and D. Coltuc, "Local-prediction-based difference expansion reversible watermarking", IEEE Trans. Image Process., Vol. 23, no. 4, Apr. 2014, pp. 1779–1790.
[7] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color, and gray-scale images", IEEE MultiMedia, Vol. 8, no. 4, Oct./Dec. 2001, pp. 22–28.