JPR INFO
Journal of Pharma Research

Journal of Pharma Research
Available online through
www.jprinfo.com

Research Article
ISSN: 2319-5622

Security Protocol in Network Traffic by Intrusion Detection

Vintha Rajya Lakshmi[1]*, M. Krishna Kanth[2]
[1]*MTech Student, Vikas Group of Institutions, Vijayawada.*
[2]*Assistant Professor, Vikas Group of Institutions, Vijayawada.*

Received on: 31-12-2014; Revised and Accepted on: 23-01-2015

ABSTRACT

The Internet has emerged as a medium for wide-scale electronic communication involving financial transactions and other sensitive information. Encrypted exchanges between principals are widely used to ensure data security. Security protocols are rules that govern such encrypted exchanges. This paper describes a system for detecting intrusions on encrypted exchanges over public networks by recognizing the characteristics of security protocols and attacks on them.

Key words: *Wireless sensor networks, security, internal and external intrusion detection.*

INTRODUCTION

Network Security is an important field of Computer Science. With the emergence of the Internet as a medium for wide-scale exchanges of sensitive information and financial transactions, maintaining the security and integrity of messages sent over public networks is very important. Our research combines two common security technologies to provide protection for electronic information exchange over public networks.

1. Intrusion Detection:

The aim of intrusion detection systems is to detect attacks against computer systems and networks. Intrusion detection systems detect attempts by legitimate users of the information systems to abuse their privileges or to exploit security vulnerabilities and attempts by external parties to infiltrate systems to compromise private information, manipulate communications, or to deny service.

There are two main designs available to IDSs for detecting attacks: 1) the misuse detection design and 2) the anomaly detection design. These two methods share many characteristics, yet are complementary in that they each have strengths where the other has weaknesses.

2. Security Protocols:

Data encryption has long been used as a means of ensuring the security and integrity of data when transmitted over public networks. Algorithms such as DES, the International Data Encryption Algorithm and the Advanced Encryption Standard make use of keys to encrypt plain text messages before they are transmitted. However, even perfect encryption is not sufficient to prevent communication from being compromised. Encryption is implemented by rules (security protocols) that define and govern the interactions between the parties to encrypted sessions.

Security protocols allow key exchange, authentication, and privacy through strong encryption. These protocols define the content and order of exchanges between the communicating principals. Early security protocols were short, usually with less than five messages. They were also simple, often developed for execution in a single, non-current session, with no branching or decision mechanisms. The classic Needham and Schroeder Conventional Key Protocol is representative of early protocols and is shown in **Fig. 1**.

***Corresponding author:**
Vintha Rajya Lakshmi
MTech Student, Vikas Group of Institutions,
Vijayawada, INDIA.
**E-Mail:* vsurendra.cse@gmail.com

A→S: A, B, Na
S→A : E(Kas:Na,B,Kab,E(Kbs : Kab,A))
A→B : E(Kbs : Kab, A)
B→A: E(Kab : Nb)
A→B: E(Kab : Nb – 1)

Fig. 1: classic Needham and Schroeder Conventional Key Protocol

3. The Secure Enclave Attack Detection System:

The Secure Enclave Attack Detection System (SEADS) is a system that can detect attacks on security protocols within an enclave of valid and recognized parties that communicate using a public network. In this environment, security protocol activity based on the message exchanges within the enclave is gathered by an Activity Monitor and compared against a knowledge base of attack signatures on protocols. This allows the Intrusion Detection Engine (IDE) to detect attempts to subvert the security protocols and to identify suspicious activities. The SEADS architecture is shown in **Fig. 2.**

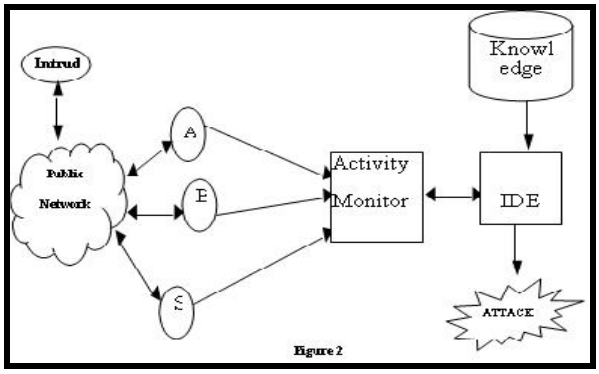

Fig. 2: SEADS architecture

The detection mechanism of the Intrusion Detection Engine (IDE) is constructed based on the knowledge-based paradigm. The IDE detects anomalous, malicious, or suspicious protocol activity occurring within the secure enclave based upon previously gathered attack signatures.

Detecting Intrusions Using Security Protocol Characteristics:

The goal of our research is to show that formal definitions of attacks on security protocols can be represented as signatures that can be stored in a knowledge base and compared against

ongoing activity to detect attacks. This is done using specific characteristics of protocols. When our system recognizes a specific signature of activity that corresponds to a known attack, we signal that an attack has occurred.

1. Constructing Signatures of Attacks:

An important feature of the technique is that the detection mechanism does not rely upon knowledge of the payload of the messages exchanged between the principals during protocol sessions. This is because the IDE detects attacks based upon the characteristics of the security protocols themselves. The signatures constructed from protocols and their known attacks are represented by:

(1) The protocols that are in use
(2) The principals (originator and recipient) involved
(3) The messages that are sent
(4) The messages that are received
(5) The concurrent sessions that occurs,

Table No. 1: Constructing Signatures of Attacks

	Session	Message #	Action	Sender	Receiver
NSCKP	X	1	send	A	S
NSCKP	X	1	receive	A	**S**
NSCKP	x	2	send	S	**A**
NSCKP	x	2	receive	S	**A**
NSCKP	x	3	send	A	**B**
NSCKP	x	3	receive	A	**B**
NSCKP	x	4	send	B	**A**
NSCKP	x	4	receive	B	**A**
NSCKP	x	5	send	A	**B**
NSCKP	**x**	**5**	**receive**	**A**	**B**

The given description of the protocol includes information about the payload data exchanged by the principals. However, as previously mentioned, the IDE does not rely on payload information for its detection mechanism. Rather, it relies on the proper sequencing of messages in the session. The NSCKP can be represented by the signature given in Table No. 3.

Protocol

Intrusion detection is analyzed in two scenarios: single sensing detection and multiple sensing detection. In single sensing detection the intruder is detected by a single sensor. But at least three sensors should detect the intruder in a collaborative manner to find out the exact location of the Intruder. Therefore we have analyzed the multiple sensing detection too.

We derive the expected intrusion distance and evaluate the detection probability in different application scenarios. Given a maximal allowable intrusion distance Dmax = η, we theoretically capture the impact on the detection probability in terms of different network parameters, including node density, sensing range, and transmission range. For example, given an expected detection distance E(D), we can derive the node density with respect to sensor's sensing range. In this paper, we derive the expected intrusion distance and evaluate the detection probability in different application scenarios.

Sensor Network Deployment:

A heterogeneous WSN in a three dimensional (3D) plane with N sensors, denoted by a set N = (n1, n2, n3…nn) is considered, where n_i is the i^{th} sensor. These sensors are uniformly and independently deployed in a cube area A = L*L*L. Such a random deployment results in a 3D Poisson point distribution of sensors. All sensors are static once the WSN has been deployed. In a heterogeneous WSN, here we consider two types of sensors, that is, Type 1 and Type 2.Type 1 sensors have the sensing radius of rs1, and the transmission range of rx1 and Type 2 sensors have the sensing radius of rs2, and the transmission range of rx2.

A Type 1 sensor can only sense the intruder within its sensing coverage area that is a disk with radius rs1 centered at the sensor. Similarly Type 2 sensor can only sense the intruder within its sensing coverage area that is a disk with radius rs2 centered at the sensor. Denote the node density of the Type 1 Sensor in a heterogeneous WSN as λ1. Denote the node density of the Type 2 Sensor in a heterogeneous WSN as λ2 In a WSN, a point is said to be covered by a sensor if it is located in the sensing range of any sensor(s). The WSN is thus divided into two regions, the covered region, which is the union of all sensor coverage disks, and the uncovered region, which is the complement of the covered region within the area of interest A. In our network model, the intruder does not know the sensing coverage map of the WSN.

Network Coverage and Broadcast Reachability:

The data collected by any of the sensors in WSN has to be transmitted in to the base station. If this transmission fails, it is meaningless even the sensor which may be in any location of the network senses critical information such as the presence of a sensor. Therefore it is essential that the network connectivity is always maintained in a WSN. Network connectivity can be defined as the probability that a packet broadcasted from any sensor can reach all the other sensors in the network. There is an another term in WSN called Broadcast reachability .Broadcast reach ability can be defined as the probability that a packet broadcasted from sensor in the WSN can reach all the other sensors in the network. Given node densities and the transmission ranges of different sensors deployed in a WSN, we can calculate the network connectivity or the broadcast reachability. On the other hand, if the required network connectivity (or broadcast reachability) is specified, we can compute the required transmission ranges in terms of node density. Thus, the minimal transmission power can be obtained for the purpose of power efficiency.

Simulation and Verification

The simulation is done using MatLab. The analytical results are compared with simulation results. We can see that both are matching.

1. Performance Evaluation:

The sensors are uniformly distributed in a cubicle three dimensional space of 100*100*100 meters . The sensing range is varied from 0 to 40 meters and maximal allowable intrusion distance is 5 meters. The graph shows the detection probability. It is found that the detection probability remains same as in the case of analytical results, thus proving the correctness of the analytical model. The **fig. 3** shows Single-Sensing detection probability and Multi sensing- detection probability. It is evident that the single sensing detection probability is higher than that of multi sensing-detection probability .This is because the multi sensing detection imposes a stricter requirement on detecting the intruder (e.g., at least 3 sensors are required). Fig. 4 also demonstrates that the detection probability in single sensing detection approaches the value 1 when the sensing range of type 1 increases to a certain threshold. For example, in the single-sensing detection, the intruder can be detected with probability 1 if the sensing range exceeds 25. In order to get the result we fixed the type 2 sensors as 300 and its sensing range is set as 10. Total 200 type 1 sensors are deployed uniformly and its sensing range is varied from 0 to 40. Fig. 4 shows that the sensing range significantly impacts the detection probability of a heterogeneous WSN. To investigate the influence of a sensor's sensing range on an average intrusion distance of a WSN, we fix the number of sensors as N = 500 and vary the sensing range. **Fig. 4** demonstrates multi sensing detection probability in the same environment as that used for single sensing.

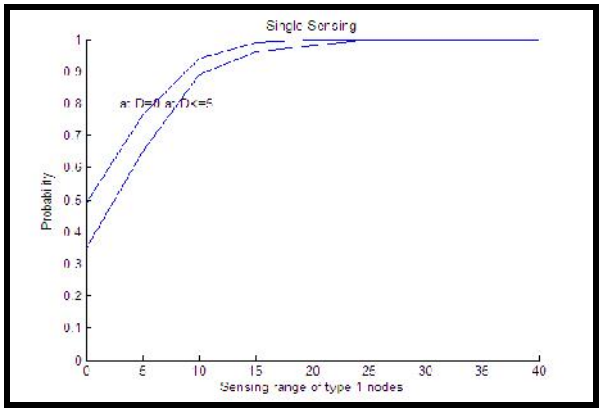

Fig. 3: Single sensing probability analysis

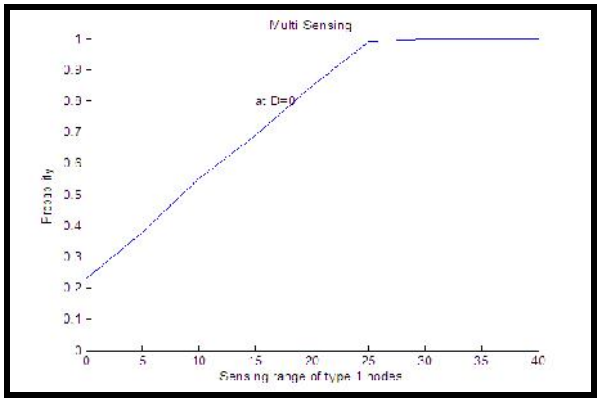

Fig. 4: Multisensing probability analysis

CONCLUSION

This paper discuss the probability of intrusion detection in a WSN deployed in a three dimensional space. This probability gives an insight in to the required number of sensors in a given deployment, their sensing and transmission range to efficiently detect an intruder in a given WSN. We have developed an analytical model for intrusion detection and applied the same into single-sensing detection and multiple-sensing detection scenarios for heterogeneous WSNs. The correctness of the analytical model is proved by simulation .It defines and examines network connectivity in heterogeneous WSN which helps to select critical network parameters according to the application.

REFERENCES:

1. John Clark & Jeremy Jacob. AttackingAuthenticationProtocols, High Integrity Systems1, **1996**; 5: 465-474.
2. H. Debar, M. Dacier, A. Wespi. Towards a Taxonomy of Intrusion Detection Systems, Elsevier Science B.V31, **1999**; 805-822.
3. Dorothy E. Denning, An Intrusion-Detection Model, IEEE computer Society Symposium on Research in Security and Privacy, **1986**.
4. Dorothy Denning and G.Sacco. Time stamps in Key Distribution Protocols, Communications of the ACM, **1981**; 24(8): pp. 533-534.
5. Roger M. Needhamand Michael Schroeder, Using Encryption for Authentication in Large Networks of Computers, Communications of the ACM, **1978**; 21(12): pp. 994-995.
6. Alec Yasinsac, Detecting Intrusions in Security Protocols, Proceedings of First Workshop on Intrusion Detection Systems, in the 7th ACM Conference on Computer and communications Security, **2000**; pp. 5-8.
7. National Bureau of Standards (NBS). Data Encryption Standard. Dederal Information Processing Standard, Publication 46, NBS, Washington, D.C., **1977**.
8. R.LRivest, A.Shamir, L.M.Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems, CACM, **1978**; 21(2): pp. 120-126.
9. Otwy D., and Rees O. Efficient and timely mutual authentication. Operating Systems Review, **1987**; 21(1): pp. 8-10.
10. J.Kelsey, B.Schneier, & D.Wagner. Protocol Interactions and the Chosen Protocol Attack, Sec. Protocols, 5th, Internet Workshop Apr.97, Proc. Springer-Verlag, 98, pp. 91-104.
11. Yun Wang, Yoon Kah Leow, and Jun Yin. Is Straight-line Path Always the Best for Intrusion Detection in Wireless Sensor Networks, in 15th International Conference on Parallel and Distributed Systems, **2009**.
12. Yang Xiao, Hui Chen, Yanping Zhang, Xiaojiang Du, Bo Sun, and Kui Wu. Intrusion Objects with Shapes under Randomized Scheduling Algorithm in The 28th International Conference on Distributed Sensor Networks",in Computing Systems Workshops, **2008**.
13. Tran Hoang Hai, Eui-Nam Huh. Optimal Selection and Activation of Intrusion Detection Agents for WSN.
14. Xi Peng, Zheng Wu, Debao Xiao,Yang Yu. Study on Security Management Architecture for Sensor Network based on Intrusion Detection, International Conference on Networks Security, Wireless Communications and Trusted Computing, **2009**.

How to cite this article:

Vintha Rajya Lakshmi, M. Krishna Kanth: Security Protocol in Network Traffic by Intrusion Detection, J. Pharm. Res., 2015; 4(1): 35-37.

Conflict of interest: The authors have declared that no conflict of interest exists.

Source of support: Nil