International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 11, November - 2013

Literature Survey on Intrusion Detection Mechanisms in Network based Applications

Asiya. A.R
Department of Computer Science and Engineering,
Akshaya College of Engineering and Technology,
Coimbatore.

Rameeza Banu. S
Department of Computer Science and Engineering,
Akshaya College of Engineering and Technology,
Coimbatore.

***Abstract*- The detection of intruders in network based application is very challenge in task. Several methods and algorithms have been proposed to detect intrusion in a network. But none of them finds satisfactory solution. Still an investigation is going on for efficient routing mechanism in the wireless sensor network. The use of internet and the services provided by the internet are in a great demand, and because of its popularity, the complexity of web services also increased. The ubiquitous usage of personal and corporate data makes the web services and easy target for different types of attacks. The leakage of data from the databases in an organization is another major problem. To reduce this continuous monitoring of database activity is necessary, which results in wastage of time. The Existing technique has drawbacks that need to be focused. The survey presents very recent research on different attacks occurring in a network and recommends Entropy based Anomaly Detection System could be applied to get a better performance.**

Introduction

The internet facilities have grown up rapidly. With the help of internet infrastructure, the host not only share the information that are needed but also helps in completing the task by using the resources provided by the internet. So the security of the networking environment from the intruders and also from the different types of attack should be considered as one of the most important issue. The existing intrusion detection system does not address in the case of any encrypted traffic for attack detection. So it will become better to use Entropy based Anomaly detection algorithm for detecting the encrypted traffic and prevent the multilevel DDoS attack in the network based application. Moreover, the detection accuracy can be increased by incorporating the host based intrusion detection system solutions in virtual network systems.

1. Mitigating DDoS Attack in Multiparty Application

In a networking environment, the network based applications open some of the communication port which makes themselves to be easily attacked by DDoS. So to avoid that a port hopping technique is used means acknowledgements are exchanges between the pair of processes. But in that case, if the acknowledgement is lost, the port should remain open for a longer period of time not knowing that the acknowledgement is lost which becomes an easy target to DDoS attack.

In the BIGWHEEL algorithm, if it assume that a specific port p, is open as a worker port, then the probability of p is open continuously for IL time units,

$$R(x,y,z) = \begin{cases} 1, & y < x \\ z\sum_{i=1}^{x} R(x,y-i).(1-z)^{i-1}, & y \geq x \end{cases}$$

Eqn.1: BIGWHEELalgorithm [1]

Table1: Continuous Open Probability [1]

W	IL=3L	IL=4L	IL=5L
2	3.9998E-12	5.0000E-16	6.0005E-20
5	3.4995E-11	7.0013E-15	1.2610E-18
7	8.3982E-14	2.1008E-14	4.6268E-18

But the port hopping is extended by applying BIGWHEEL algorithm for all the network based applications, which helps the server to communicate with multiple clients without any synchronization. This hopping pattern should be enabled with an adaptive algorithm called HOPERAA that helps to communicate with different parties with clock drift which become a simple collection that help the clients to interact with the server independently of the any other client.

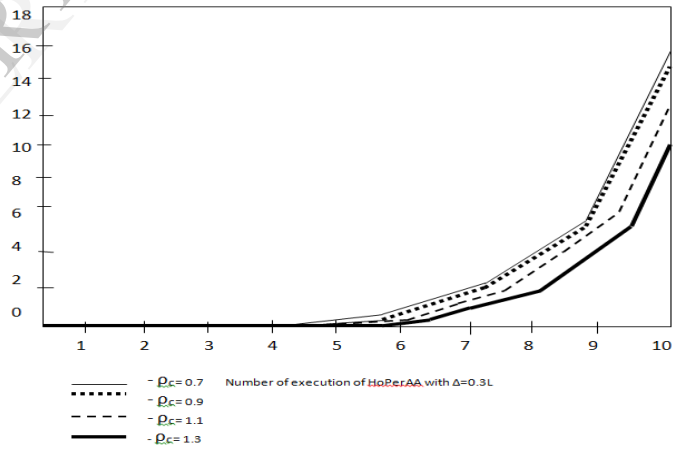

Fig.1: The length of HOPERAA execution interval grows with the number of HOPERAA executions [1]

Drawbacks: The main drawback is that the inclusion of hopping method in the multiparty applications should be dominate in a scalable way because of not having any group synchronization also this adaptive algorithm should work under fixed clock drift and it should not be able to address the variable clock drift and variable hopping frequencies.

2. Implementation of an Intrusion Response System for Relational Database

The intrusion response component is responsible for providing a appropriate response in the case of any anomalous request. The database response policy supports the intrusion response system for database management system. This response policy helps the database administrators to specify suitable responses for the different anomalous request

depending upon their nature and also under some different circumstances.

Here policy matching and policy administration should be considered as the major issue. For policy matching, an algorithm was generated that find matches of policy database with an anomalous request. The algorithm should be extended by including PostgeeSQL DBMS and experiments should be done which produces an efficient result.

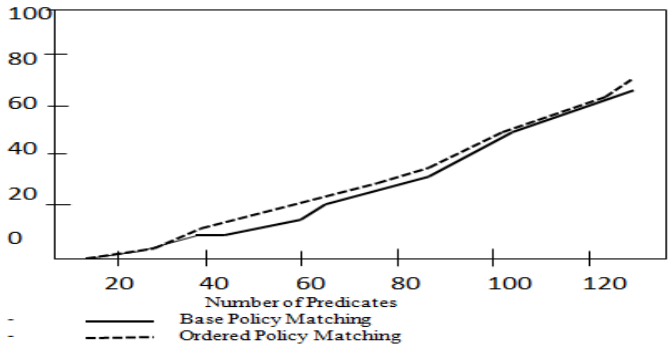

Fig.2: Number of predicate versus number of predicates skipped [2]

The policy administration, in order to prevent any malicious modification from legitimate users a new technique called Join Threshold Administration Model (JTAM) was implemented, which was based on the separation of duty. The key factor here is JTAM is administered by K DBA's, that means the policy object should not be considered as valid if it has been authorized by K DB's.

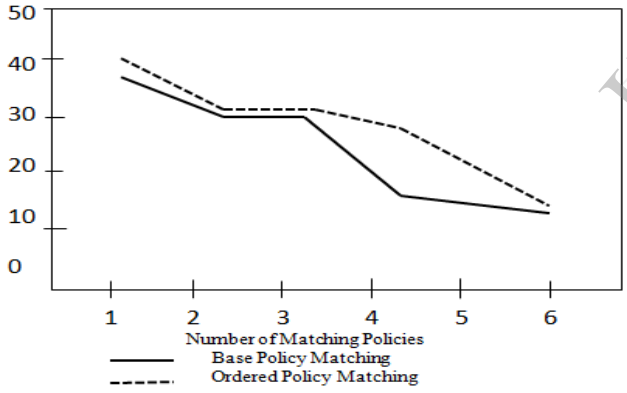

Fig.3: Number of matching policies versus number of predicates skipped [2]

The future work is related to the provision of authentication which will provide another defense layer for certain anomalous activity that are critical to the system resources.

3. Detecting Intrusion in Multitier Web Applications

Internet and the usage of services provided by the internet are increasing which helps to enable communication and the management of all types of information that are received from anywhere. Because of its increased applications and complexity, the web services have extended to the multitier design in which the application in the web server run the front-end logic and data are moved to the database or any other file server.

A DoubleGuard Intrusion detection system models that behavior of the network from both the front-end webserver and back-end database. The attack should be ferret by monitoring both the web and the database request which should be able to done by an individual intrusion detection system.

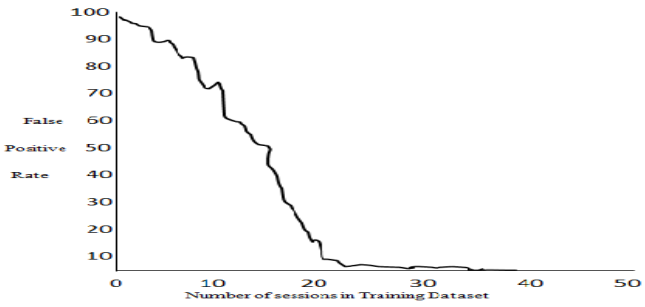

Fig.4: False positives versus training time in static website [3]

DoubleGuard was implemented using an Apache webserver with MYSQL. It should be processed on real world traffic in both the static and dynamic web applications which should able to expose out a wide range of attacks with high accuracy.

4. Adaptive Deadlock Free Routing Algorithm

A deadlock free routing algorithm called CLUE was proved for switched torus which requires two virtual channels. One channel is used for the mesh sub network in the deadlock free routing algorithm. The other channel is an adaptive channel.

Other two algorithms called flow controlled clue which is fully adaptive and has not virtual channel. It uses a well-defined flow control function to avoid the deadlocks. Wormhole clue was implemented for wormhole- switched tori which are partially adaptive because it requires the addition of some constraints to the adaptive channel for the avoidance of deadlock.

Table 2: Output Channel State Fields [4]

Field	Name	Description
G	Global state	Idle (I), active (A) or waiting (C)
C	Credit count	No. of free buffers
S	Safe packet count	No. of safe packets

5. Detection of Clone Attack in WSN

Wireless Sensor Network which is a collection of sensors that was deployed in hostile environment in which the adversary can capture the nodes reprogram and replicate them in a difference number of clones which gets an easy control of the network. A number of solutions was found out to address this problem but was not satisfactory, because their solution requires high energy and memory demanding.

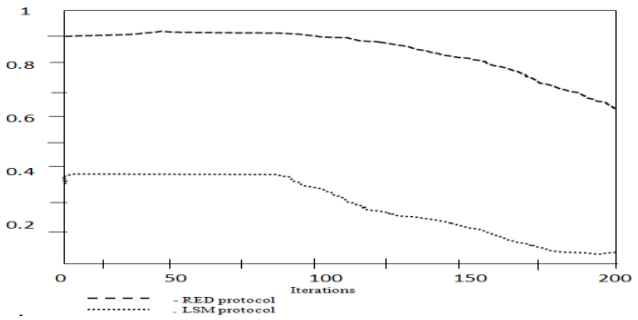

Fig.5: Detection probability for both RED and LSM. N=1,000, r=0.1, g=1, and p=0.1. [5]

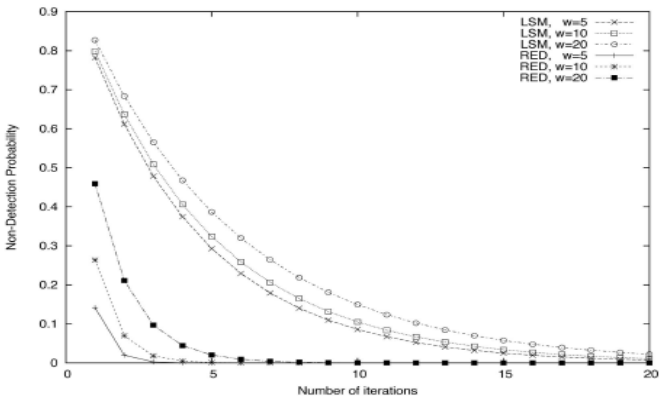

Fig.6: Nondetection probability (n=1,000 and c=0.5) [5]

A new self-healing randomized, efficient and distributed protocol for the detection of node replication attack for this the properties of distributed mechanism was analyzed which provides on efficient way to resist different kinds of attack.

6. Risk Mitigation of Mobile Ad hoc Network

Because of the changing nature of the network infrastructure, the mobile ad hoc networks are likely to be attacked very soon. The problem of routing attack must also be addressed because it cause a severe damage to the mobile ad hoc network. One of the solution suggested to the above problem is the isolation of malicious nodes by binary or naïve fuzzy response decisions.

Table 3: Risk Assessment and Decision Making [6]

		Node		
Approaches	Index	0	4	6
BINARY	Decision	Isolation	Isolation	Isolation
DRC	$Risk_A$ $Risk_C$ Risk Decision	0.00011 0.00164 -0.00153 Isolation	0.0000057 0.00164 -0.00163 Isolation	0.0000057 0.0144 -0.0143943 No isolation
DRCIF	$Risk_A$ $Risk_C$ Risk Decision Time	0.467 0.0136 0.4534 Isolation 300ms	0.00355 0.0136 -0.01005 No isolation 0	0.00355 0.1 -0.096 No isolation 0

But both the binary and naive fuzzy response decision results in unexpected network partition and uncertainty in countering the routing attack which was occurring in mobile ad hoc network. So a new technique, risk aware response mechanism based on Dempster-Shafer theory of evidence was suggested to give a better performance than the existing system.

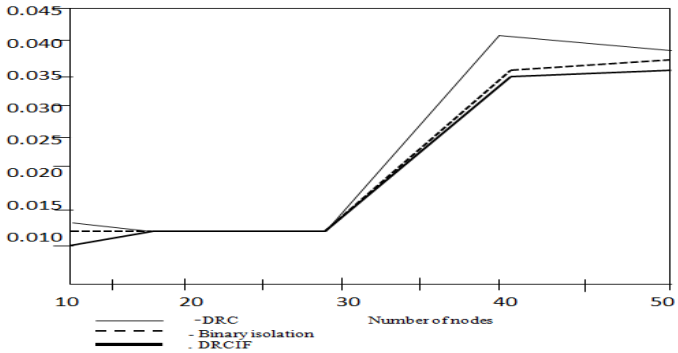

Fig.7: Mean Latency (Seconds) [6]

The suggested scheme should be extended by adding adaptive decision model in future.

Conclusion

Since the detection and prevention of attack is very challenging task and is commonly found in all the network based application, the solution for this problem is very necessary. By the concept of entropy based anomalous detection algorithm the attacks can be prevented and also reduce false positive rate and false negative rate.

References

[1] Zhang Fu, Marina Papatriantafilou, and Philippas Tsigas "Mitigating Distributed Denial of Service Attacks in Multiparty Applications in the Presence of Clock Drifts" IEEE Transactions on Dependable and Secure Computing, vol. 9, No. 3, May/June 2012

[2] Ashish Kamra and Elisa Bertino, Fellow, IEEE "Design and Implementation of an Intrusion Response System for Relational Databases" IEEE Transactions on Knowledge and Data Engineering, vol. 23, No. 6, June 2011

[3] Meixing Le, Angelos Stavrou, Member, IEEE, and Brent ByungHoon Kang, Member, IEEE "DoubleGuard: Detecting Intrusions in Multitier Web Applications" IEEE Transactions on Dependable and Secure Computing, vol. 9, No. 4, July/August 2012

[4] Wei Luo and Dong Xiang, Senior Member, IEEE " An Efficient Adaptive Deadlock- Free Routing Algorithm for Torus Networks" IEEE Transactions on Parallel and Distributed Systems, vol. 23, No. 5, May 2012

[5] Mauro Conti, Member, IEEE, Roberto Di Pietro, Luigi Vincenzo Mancini, and Alessandro Mei, Member, IEEE " Distributed Detection of Clone Attacks in Wireless Sensor Networks" IEEE Transactions on Dependable and Secure Computing, vol. 8, No. 5, September/October 2011

[6] Ziming Zhao, Student Member, IEEE, Hongxin Hu, Student Member, IEEE, Gail-Joon Ahn, Senior Member, IEEE, and Ruoyu Wu, Student Member, IEEE "Risk-Aware Mitigation for MANET Routing Attacks" IEEE Transactions on Dependable and Secure Computing, vol. 9, No. 2, March/April 2012

[7] Dan Li, Member, IEEE, Yuanjie Li, Jianping Wu, Senior Member, IEEE, Sen Su, and Jiangwei Yu "ESM: Efficient and Scalable Data CenterMulticast Routing" IEEE/ACM Transactions on Networking, vol. 20, no. 3, June 2012

[8] Zhenhai Duan, Senior Member, IEEE, Peng Chen, Fernando Sanchez,Yingfei Dong, Member, IEEE, Mary Stephenson, and James Michael Barker "Detecting Spam Zombies byMonitoring Outgoing Messages"IEEE

Transactions on Dependable and Secure Computing, vol. 9, No. 2, March/April 2012

[9] Nayot Poolsappasit, Member, IEEE, Rinku Dewri, Member, IEEE, and Indrajit Ray, Member, IEEE "Dynamic Security Risk Management Using Bayesian Attack Graphs" IEEE Transactions on Dependable and Secure Computing, vol. 9, No. 1, January/February 2012

[10] Abdalkarim Awad, Reinhard German, and Falko Dressler, Senior Member, IEEE "Exploiting Virtual Coordinates for Improved Routing Performance in Sensor Networks" IEEE Transactions on Mobile Computing, vol. 10, No. 9, September 2011