Journal Engineering Sciences
& Information Technology
Issue (1), Volume (3)
March 2019
ISSN: 2522-3321

المجلة العربية للعلوم و نشر الأبحاث
Arab Journal of Sciences & Research Publishing
AJSRP

Networks Security models Scalability Analysis

Kamal Aldin Yousif Yaseen

Sadara institute || IT || sultanate of Oman

Abstract: There is an emerging scalability problem with existing security models as the size of the networked systems becoming larger, especially when analyzing all possible attack scenarios. presented the worst case computational complexity analyses based on fully connected topology, but real life networked systems run on various network topologies, and other factors that affect the overall performances of security models. In this research, the scalability of existing security models is evaluated and compared with the HARM in realistic scenarios. Two main tasks in this research are (1) formulating key questions that need to be answered to assess the scalability of security models, and (2) evaluate and compare the scalability of security models using simulations.

Keywords: scalability problem, security models, complexity analyses, HARM.

1. Introduction:

Cyber-attacks have significant effects in our daily lives, where they target from critical infrastructures down to small home networks. Cyber-attacks are becoming more complex (in terms of their attack patterns, types and methods), which makes harder to defend our networked systems against them.

This thesis aims to address the inefficiencies of security models and their analysis methods for modern networked systems, To do so scalable and adaptable security modeling and analysis methods are developed, efficient security assessment methods are developed to formulate countermeasures, and the combined effects of unknown attacks are analyzed to formulate mitigation strategies, A comparative analysis of hierarchical security model and existing security models taking into account their complexities and performances is presented, which showed significant improvements in scalability and adaptability using the hierarchical security model. Next, efficient security assessment methods based on importance measures (i.e., network-centric) are presented, which enhanced the operability (i.e., can be used in other security models) of the security evaluations without functional constraints of models and metrics. Finally, this thesis presents methods to incorporate unknown attacks into the hierarchical security model, analyses the combined effects of unknown attacks in the networked systems, and provide efficient algorithms to formulate mitigation strategies.

2. Problem definition:

Scalability problem with existing security models as the size of the networked systems becoming larger, especially when analyzing all possible attack scenarios.

3. Research Goals:

The main goal of this research is to advance security assessment of large sized and

dynamic networked systems and establish efficient and effective security assessment method, Develop security modeling and analysis methods to improve scalability and Adaptability .

4. Research methodology:

This thesis followed the scientific descriptive approach in this research, from the stage of data collection and analysis, design and implementation of programs and mathematical algorithms, processing and proving supposition.

5. Key Questions to Compare Scalability

Scalability is a growing concern for security assessment as it becomes difficultto manage the size of security models when the networked system becomes toolarge. Existing security models and their studies lack in comparative analysis toshow the scalability of security models in various environments and attack scenarios. To address this problem, five key questions are formulated to compare the scalability of security models:

Q1 Was the computational complexity analysis performed؟

Q2 Was the security model compared with other security models؟

Q3 Were different network topologies considered؟

Q4 Were the effects of variable number of vulnerabilities for hosts considered؟

Q5 Were the different types of vulnerabilities (e.g., user and root) considered؟

Scalability in the generation and the evaluation phases are taken into account for analyzing the performance of security models, where answers to the key ques- tions are shown in Table 1 and 2 for generation and evaluation phases respec-tively. The preprocessing phase generally requires the same efforts for all security models (i.e., information gathering in the networked system), and the representa-tion phase does not involve any computational methods (i.e., only for storage and visualisation purposes).

Table (1) answers to key questions in the generation phase

Security models	AG	TLAG	LAG	MPG	HARM
Q1	Yes	Yes	Yes	Yes	Yes
Q2	Yes	No	Yes	Yes	Yes
Q3	No	No	Yes	No	Yes
Q4	No	No	Yes	No	Yes
Q5	No	No	No	Yes	Yes

6. Generation Phase

The main task of the generation phase is to retrieve the network information and generating the relationships between network components specific to the re-quirements of security models (e.g., connecting a vulnerability node to its sub-sequent vulnerabilities or hosts based on the reachability, application, and port information).

Generating AG: Computational complexity of generating the AG has been conducted in and it is compared against the HARM as shown in Figure 2, However, various network topologies are not taken into account when generating AGs. Furthermore, the effect of variable number of vulnerabilities, as well as different types، are not considered.

Key properties of generating the AG is that the connections between vulnera- bilities and hosts in the AG are independent. As a result, the computational com- plexity of generating the AG is greater than the HARM as shown in [2]. More- over, because there are a larger number of edges, traversing the AG to compute all possible attack paths have worse computational complexity than the HARM[8].

Generating TLAG: Only the computational complexity of generating theTLAG is shown in [3]. There is no comparison with other security models in terms of performance, and only a fixed network topology was taken into account،which had a fixed number of vulnerabilities with the same properties (i.e., homo- generous).

Generating the TLAG is not described in [4], but if the same generation method as the HARM is assumed, it would have the same computational com- plexity as the HARM. However, the number of lower layer models is determined based on the number of host pairs (i.e., edges in the upper layer), which has the upper bound of $O(n^2)$. This is greater than the HARM with the upper bound of O(n).

Generating LAG: Computational analysis of the LAG is conducted in[23]،which is also compared against the AG in terms of generating both LAG and AG.

Various network topologies are also taken into account, with a varying number of vulnerabilities. However, different types of vulnerabilities are not taken into account, The LAG has a generation complexity of O(δ n), where n is the number of hosts in the networked system and δ is the time to find the host in the lookup table All vulnerabilities are assumed to be remote to exploits. Since each derivation node is an AND node, repeated nodes are required for each exploit if there are multiple sources it could be exploited from. If the derivation nodes are allowed as OR nodes, the number of repeated nodes (and the size of the LAG in the representation phase) will be reduced. Therefore, the HARM (linear size) has better size complexity than the LAG (polynomial size).

Generating MPG: Computational complexity of the MPG is conducted in[5] which also compared its performance with an AG while taking into account different types of vulnerabilities. However, a fixed network topology was used throughout experiments and a fixed number of vulnerabilities was used for each host.

The MPG has the number of components linearly proportional to the num- ber of hosts and vulnerabilities in the networked system [6]. Additionally, it also requires the use of prerequisite nodes, which decreases the number of inde - pendent connections between hosts and vulnerabilities, but increases the size of the MPG. However, their experimental results showed that the number of total nodes in the MPG is negligible compared to the AG when generating the MPG.

Their performance in the simulation showed almost linear relationship between the computational time for generating the MPG with respect to the number of hosts. In [7], the client-side attacks using the reverse reachability calculations are captured in the MPG as an additional feature.

Table (2) answers to key questions in the evolution phase

Security models	AG	TLAG	LAG	MPG	HARM
Q1	Yes	Yes	Estimated	Estimated	Yes
Q2	Yes	No	No	Yes	Yes
Q3	No	No	No	No	Yes
Q4	No	No	No	No	Yes
Q5	No	No	No	Yes	Yes

7. Evaluation Phase

Computing all possible attack scenarios is taken into account in the evalu-ation phase for reasons described in this research. Existing methods of assessing the security can be used (e.g., graph simplification [9, 10] and heuristic meth-ods [11, 12]), but only specific attack scenarios and the subset of all possible at- tacks

are considered. Matrix evaluation can be used to compute the overall se-curity of the networked system, but it lacks in detailed analysis of the individual attack path.

Evaluating AG: Computational complexity of evaluating the AG and compar- ing its performance against the HARM is shown in [14,15] and [8] respectively.

However, previous studies on the AG did not take into account the performance of evaluating the AG with various network topologies and vulnerability information.

The AG generates edges between vulnerabilities, where there are total O(n2 m2) number of edges. Hence, evaluating such graph becomes O((n2 m2)!), which is highly exponential. In contrast, the HARM captures relationship between vulner-abilities in the upper layer, reducing the total number of edges to O(nm2 + n2).

This is shown in this research via simulations which using Akaroa2 tools .

Evaluating TLAG: Only the computational complexity of evaluating the TLAG is presented in [13] based on matrix evaluation. There is no comparison with other security models, and only fixed topology and number of vulnerabilities are used in the experiment.

The evaluation of the TLAG computes the overall security of the networked system using the matrix evaluation with probability of an attack. However, this method lacks in assessing different attack paths and their effects. It is shown in [14] that the number of host-pair attack graphs (i.e., the number of lower layer security models) was not linearly proportional to the number of hosts, which is larger than the HARM with a linearly proportional number of lower layer security models.

Evaluating LAG: Evaluating the LAG is not shown in [15], and graph sim- plification and approximation algorithms are used to evaluate the LAG in] 16.[Moreover, the performance is not compared with other security models, as well as using a fixed network topology with a fixed number of identical vulnerabilities.

If all possible attack scenarios are computed using the LAG, then the computational complexity of the LAG is equivalent with the AG. Because each fact node (e.g., hosts) makes an independent connection to derivation nodes (e.g., vulnera- bilities), the conceptual structure of the LAG is identical to the AG. The number of paths from each fact node increases exponentially as the number of choices increases in the attack path, which is the same property found in the AG.

Evaluating MPG: Performance of evaluating the MPG uses a graph simpli- fication method, which has almost linear scalability performance in respect to the number of hosts. This is compared with the AG in [17]. However, the perfor - mance analysis did not consider different network topologies or variable number of vulnerabilities that may affect how reachability groups are formed.

Evaluating the MPG utilises graph simplification. As a result, their evaluation complexity is almost linear with respect to the number of nodes. But taking into account computing all possible attack scenarios, the worst case scenario of eval-uating the MPG is equivalent to the AG (e.g., consisting of only a single reachability group). If there are multiple prerequisite nodes, then connections between hosts and vulnerabilities are grouped by the prerequisite nodes, and it reduces the complexity in the evaluation phase.

8. Experiment A: Simple Network Topologies

The performance of the HARM is compared with the AG for various cases.

The attack scenario used in the simulation is similar to that in the experiment con- ducted in [13],The networked system used in the simulation is shown in Figure1 .A network has four sites (i.e., four identical networked systems connected via firewalls), where each site has three subnets demilitarized zone (DMZ) shown in figure 1, as Internal Networks, and Database such as in Figure 3. In each DMZ, there are five hosts and five administrative LAN hosts, and each Internal Network is divided into ten subnets with hosts connected with a bus topology, The port information and the firewall rules are abstracted.

Ten remote-to-other vulnerabilities are assigned to half of the hosts in each subnet, and the other half with one remote-to-root and nine remote-to-other vul- nerabilities. The attack scenario was to compromise a host in the DMZ, an ad-ministrative LAN host, and all hosts in the network that has a remote-to-root vulnerability. Hosts that are not directly reachable from the attacker are com- promised using other hosts as a stepping stones, The number of hosts in each subnet was increased to compare the scalability between the AG and the HARM.

The comparison of scalability is shown in Figures 2 and 3 for generation and evaluation phases respectively. The simulation is conducted using an automated network simulation tool named Akaroa2 [18, 19], where the results are collected with the confidence level of 0.95 and the relative error of 0.03. The simulation program was coded using Python, and it was conducted in a Linux environment with Intel(R) Core2 Quad CPU 2.66GHz with 3.24GB of RAM.

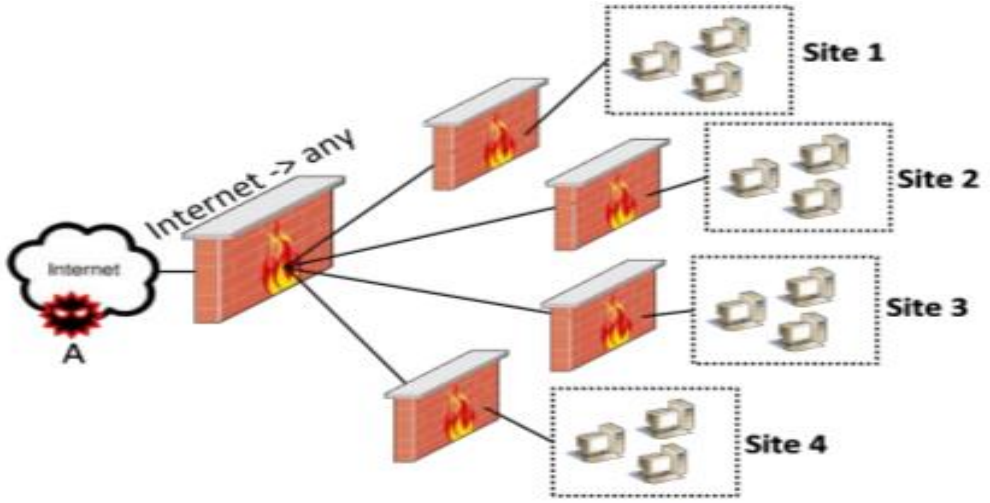
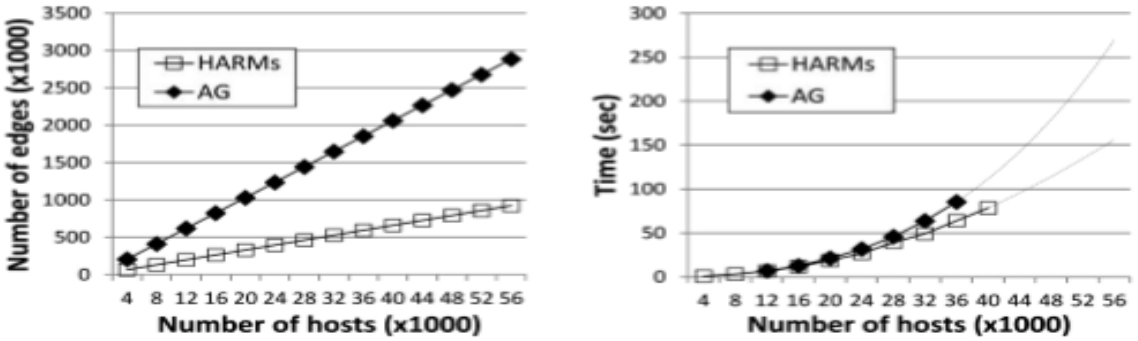


Figure (1) A Networked System for Experiment 4A

Performance Analysis with Fixed Variables: Figure 2 shows the performances of the AG and the HARM in the generation phase. This shows that the



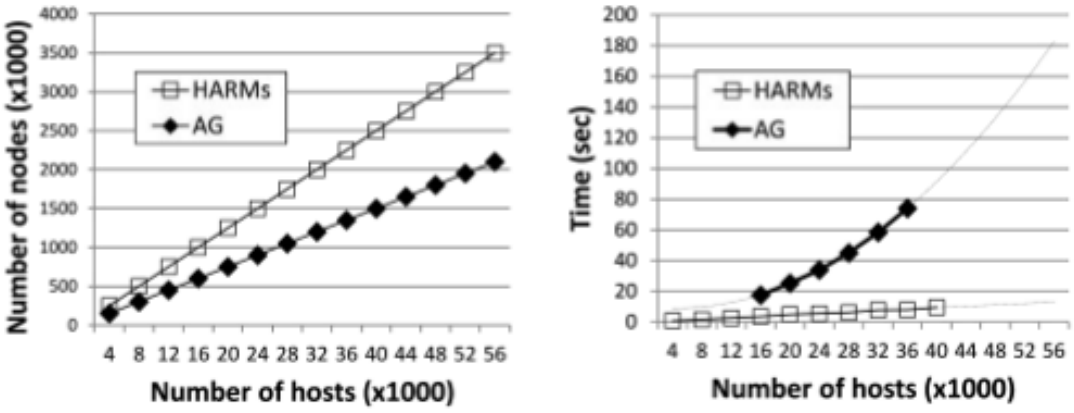
(a) Number of Edges **(b) Generation Time Measurement**

Figure (2) A Comparison between AG and HARM in the Generation Phase

number of edges in the AG increases quicker than the HARM. However, genera- tion times for the AG and the HARM do not have a significant difference. Thisindicates that the number of edges has little influence on the generation time. Both security models have linear growth of the edge numbers, but the number of edges for the HARM was always less than that of the AG.

The trend observed from the simulation is comparable with the simulation result of the MPG [20]. The time comparison shows that the time for the evalu-ation increases rapidly for the AG, but almost linearly for the HARM as shown in Figure 3(b). In contrast, the number of nodes computed in the HARM is much greater than that of the AG. The AG constructs the attack paths using vulnerability sequences only, but the HARM also analyses the sequence of hosts. Therefore, an extra space of memory is required to store the information.

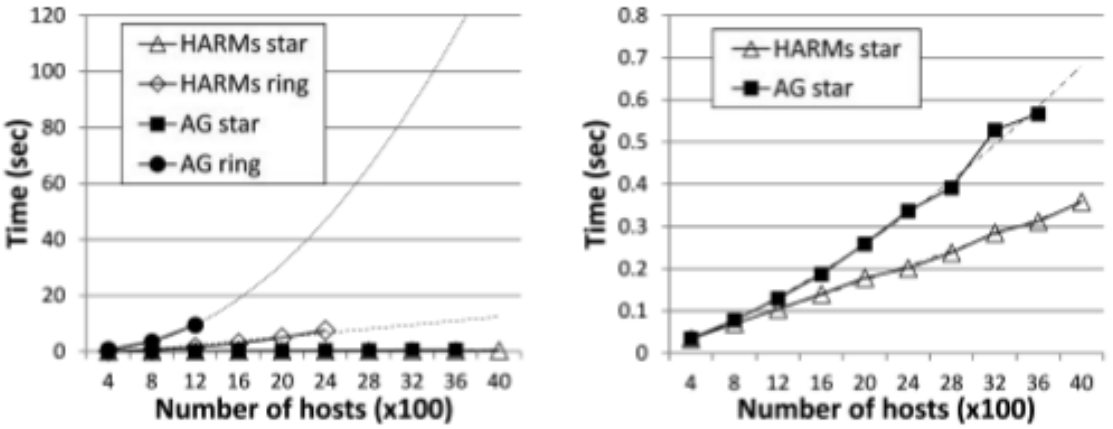
Performance Analysis with Non-fixed Variables: Various network topolo- gies and variable number of vulnerabilities are taken into account. Bus (fully connected), ring, and star topologies are considered to connect hosts in each inter-nal network, where the number of vulnerabilities for each host is varied from 10 to 150 .The number of hosts is fixed at 1200 when simulating the variable number of vulnerabilities. For this experiment, the goal of the attacker is changed to compro-mise a single host selected in the one of the subnets in the Internal Network (e.g.،a host in the 10th subnet in each internal networks). The bridging hosts (i.e., head hosts that connect to other subnets) are not selected as the target host. In order to



(a)Number of Nodes Computed **(b) Evaluation Time Measurement**

Figure (3) A Comparison between AG and HARM in the Evaluation Phase

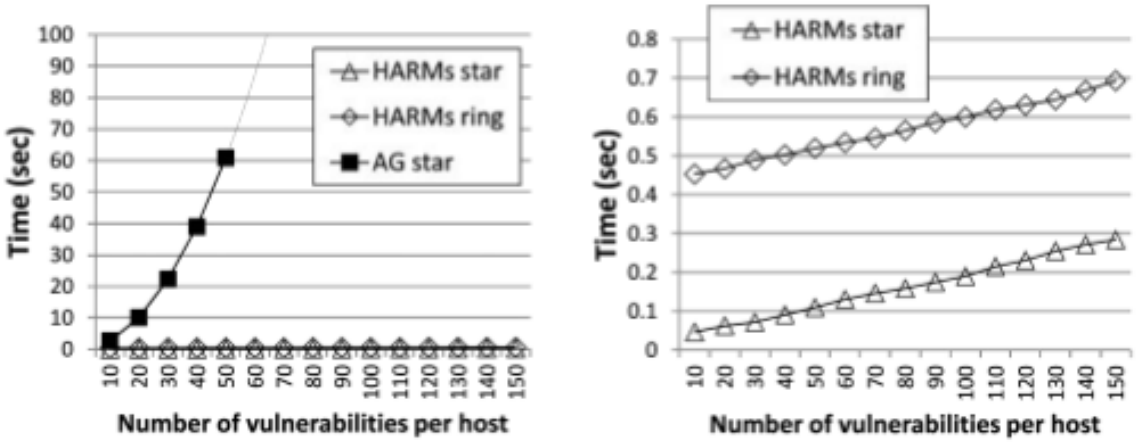
simulate different topologies, a single vulnerability to each host is assigned that is enough to gain the root access, Scalability Difference of Network Topologies in the Evaluation Phase shown in Figure 4.



(a) Scalability of Different Network Topologies **(b) Scalability of Star Topology**

Figure (4) Scalability Difference of Network Topologies in the Evaluation Phase

The simulation result of different topologies is shown in Figure 3. Since the performances of generating the HARM and the AG are similar, only the differ-ences in the evaluation phase are compared. Note that evaluating fully connected topology suffered from the scalability problem, where the evaluation of 400 hosts timed out (i.e., it took longer than three hours). However, the AG is significantly slower than the HARM when other topologies are taken into account.



(a) Evaluation Time **(b) HARM Star and Ring Topologies**

Figure (5) Scalability Difference with Varying Number of Vulnerabilities

Scalability Difference with Varying Number of Vulnerabilities show the evaluation time and topologies as shown in Figure5.

The simulation result of varying the number of vulnerabilities is shown in Figure 3 The number of hosts was fixed at 1200. The fully connected topology for both security models could not be evaluated for 1200 hosts. In addition, the ring topology for the AG reached the time out during the simulation (i.e., it took longer than three hours to evaluate). The comparison in the evaluation phase shows that as the number of vulnerabilities increases, the growth rate of the AG is much greater than the HARM for all network topologies. The performance increase is almost linear using the HARM for all topologies, indicating the number of vulnerabilities is also a constant factor in the evaluation phase.

9. Experiment B: Combined Network Topologies

In this section, the scalability of AG, 2-HARM and 3-HARM in terms of generation and evaluation are compared using a networked system with various number of hosts, topologies, vulnerabilities and network densities. The same net- worked system shown in Figure 2 is used.

10. Complex Network Topologies:

The number of hosts in the DMZ and Internal Network was increased to com -pare the scalability between the AG, 2-HARM and 3-HARM. Figure 6 shows that generating these models are almost equivalent because their generating al-gorithm is the same, which generates linearly proportional number of nodes in respect to the number of hosts in the networked system.

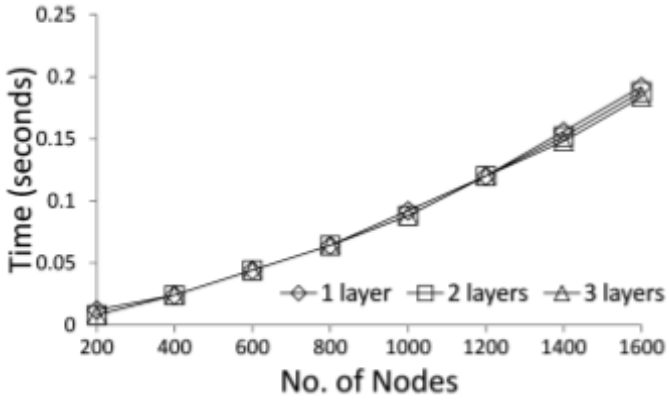


Figure (6) Generation of AG, 2-HARM, and 3-HARM

In case of an evaluation, four combined network topologies are considered: (i) star-star, (ii) tree-star.(iii) ring-star, and (iv) mesh-star, which are shown in Figure 7. Each combined topology creates a complex mesh structure as a result of mixing topologies. Figure 7(a) shows the performance of security models evaluating the star-star topology.

It shows that all models have a similar trend in performance, but the 3-HARM outperforms the AG and 2-HARM. Similarly, in Figure 7(b), 7(c) and 7(d). the 3-HARM performs the best. Also, an observation is that the evaluation time is significantly increased for the ring-star and mesh-star topologies.

Different performance of different network topologies are presented in Figure 5. It shows that as the network density increases, the time taken to evaluate the network increases. The network density is the measure of network connections between hosts in the Networked system (i.e., a normalised degree centrality measure, which measures the number of edges).

11. Varying Number of Vulnerabilities:

An experiment is conducted to observe the effect of varying number of vul-nerabilities as shown in Figure 3. Figure 9(a) shows that it affects the AG significantly compared to the HARM, where it is almost negligible to notice any changes in the HARM. Because the AG creates connections between individual vulnerabilities, the time taken to evaluate becomes significantly longer as the num- ber of vulnerabilities is

increased (as shown in Figure 5(a)). A larger number of vulnerabilities are used in Figure 9(b) to distinguish the performance difference between 2-HARM and 3-HARM. The result shows that the evaluation time for the

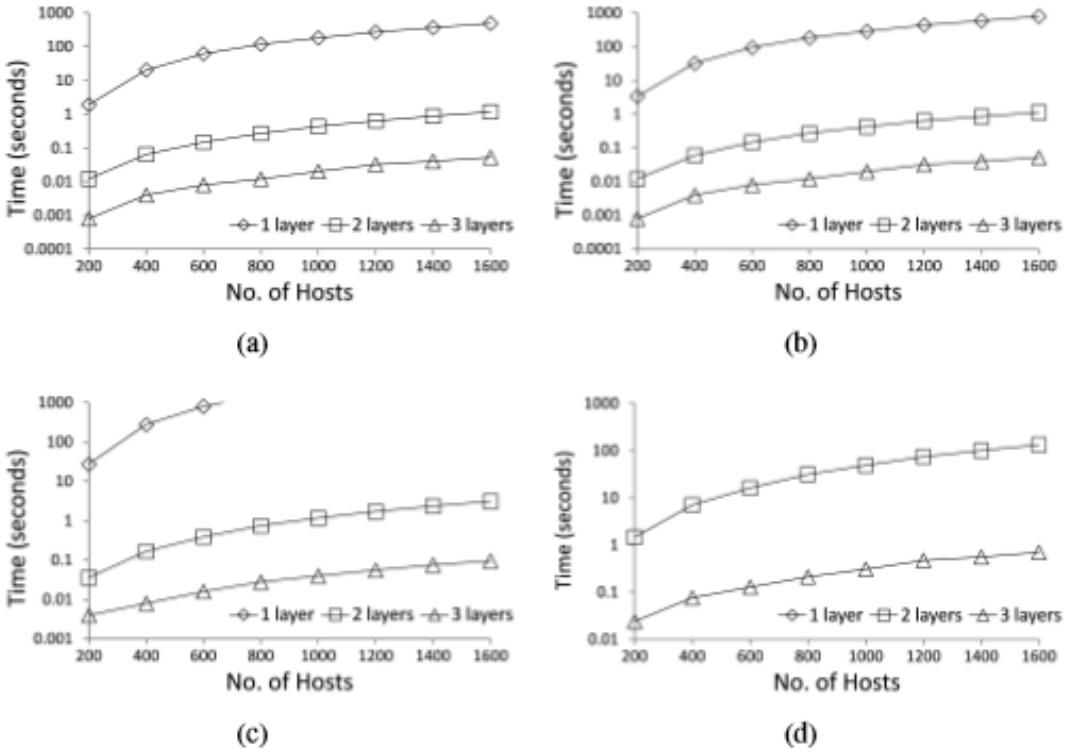


Figure (7) Performance of evaluating combined network topologies in the order of star-star, tree-star, ring-star and mesh-star topologies respectively

2-HARM is increasing gradually, whereas that of the increase of the 3-HARM is relatively constant.

12. **Varying Network Density:** A further simulation is conducted to investigate the effect of network density when analyzing the security of networked systems.

    For this experiment, a mesh topology is used with various network density values.

    Figure 7 shows the performance of AG (i.e., 1 layer), 2-HARM (i.e., 2 layers)**.** and 3-HARM (i.e., 3 layers) with respect to the network density, Figure 7(a) shows that the performances of the AG and 2-HARM are significantly worse than the 3-HARM. Figure 7 shows that both AG and 2-HARM converges to the worst case performance when the network density is greater than 0.3. The propor- tion represents the performance proportionality compared to when density equals to 1. Also, the proportionality of 3-HARM converges to the worst case perfor- mance is significantly slower than the AG and 2-HARM. For the network density at 0.5, the AG reached 93.7% of the worst case performance, while 2-HARM reached 93.8%, and 3-HARM only reached 90.0%. It shows that modelling with higher hierarchy may improve the

performance of analysing the security of the Networked system, figure 8 show the Performance of 2-HARM and 3-HARM Evaluating Various Network Topologies.

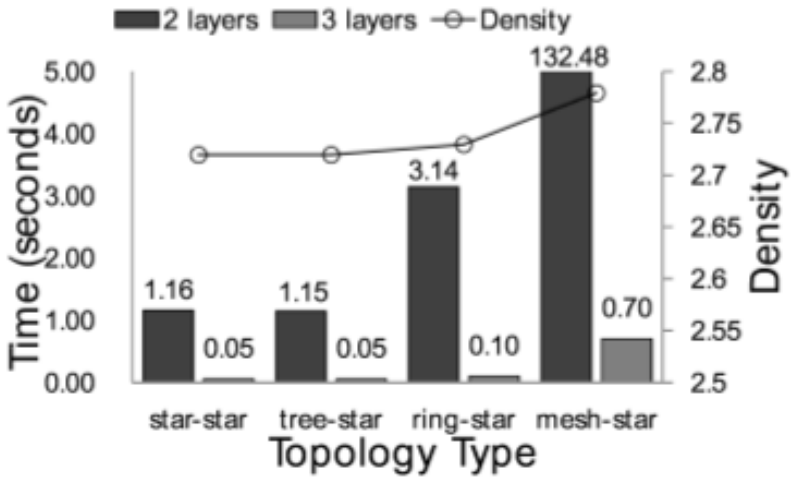


Figure (8) Performance of 2-HARM and 3-HARM Evaluating Various Network Topologies

13. Scalability of Security Models in the Lifecycle Phases

Only a few studies conducted scalability analysis comparing the efficiency of various security models, and none of them considered the efficiency of security models in the modification phase. The similarity between the AG, LAG, and the MPG is that they are represented in a single layer. As a result, they suffer the scalability problem not only in the evaluation phase but also in the representation

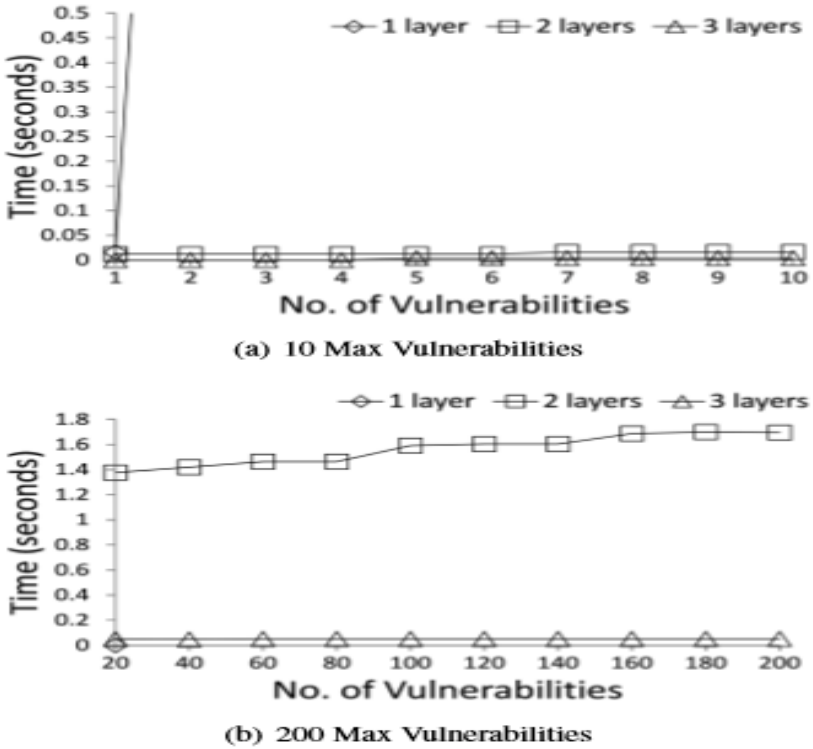


Figure (9) Performance of AG, 2-HARM, and 3-HARM Evaluating Various Numbers of Vulnerabilities

phase (e.g., as shown in Figure (7). The AG suffered the scalability problem due to independent connections between the model components (e.g., vulnera- bilities), where the representation of the AG had more edges compared with the HARM. The number of nodes was the same, but the number of edges was greater in the AG. On the other hand, security models using hierarchy (e.g., the HARM and TLAG) are less complex to represent. Moreover, in the case of updates in the networked system, single layered security models (e.g., AG, LAG and MPG) may affect many components in security models, whereas using hierarchy only affects specific layers and corresponding lower layers. However, there is a lack of scalability and adaptability analysis in the modification phase in the lifecycle of security models, figure 10 show the Performance of AG, 2-HARM, and 3-HARM Evaluating Various Network Density.

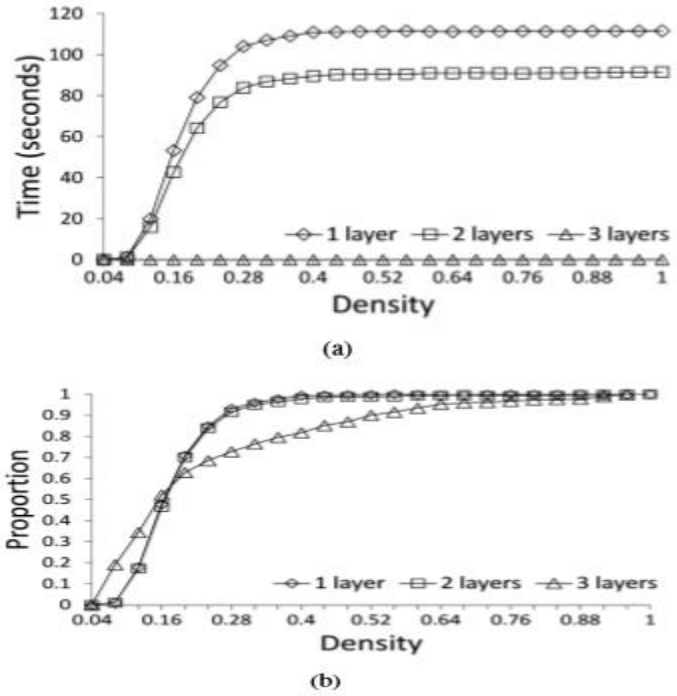


Figure (10) Performance of AG, 2-HARM, and 3-HARM Evaluating Various Network Density

14. Network Structure and Attack Scenarios

In a real life networked system, network topologies are complex with many combinations of simple topologies (e.g., combinations of star, tree, ring and mesh topologies). The worst case complexity defined by analysing a fully connected topology gives the upper bound performance. Although a few complex network topologies are taken into account in the experiment, it is difficult to evaluate the scalability of security models. However, as shown in the density analysis above, the performance of security analysis can be estimated based on the density of the networked system in respect to the worst case performance. Thus، the complexity analysis and experimental results are a reasonable estimation for the performances of using security models. Moreover, such assessment can be used to design networked systems that are secure as well as efficient to analyse the security to mitigate attacks.

15. Real Testbed Experiments

One of the limitations is a lack of experimenting on a real system. Although the observed performance in the simulation would be linearly proportional to the real systems, the complexities in real systems are difficult to estimate in a simula- tion, Also, other scalability factors are not taken into account (e.g., performance factors such as QoS, delay, and delivery rate), which may affect the performance of security analysis

16. Comparisons with Other Security Models

The results obtained in the experiments were comparable with some of the existing security models and their analyses [21, 22, 23]. The comparison between the HARM and the AG shows the performance of the HARM was always better than the AG. The variation of vulnerabilities affected the AG significantly, show- ing an almost exponential growth in the evaluation phase. In contrast, the HARM showed a linear growth of the evaluation time, which is practically computable for a large number of vulnerabilities. Because the underlying algorithms are the same (e.g., generation algorithm, full path search algorithm), the improvement of scalability comes from the structural advantages of the HARM.

17. Differences between the AG and HARM

The experimental results show the HARM with better performances against the AG even when the same underlying security models and algorithms are used.

Their performances in the generation phase were similar, but the AG showed that it created more edges than the HARM. Consequently, their performances in the evaluation phase showed that the AG had an exponential computational complex-ity while the HARM had a linear computational complexity with respect to the AG. The underlying algorithm to evaluate attack scenarios was the same, but the performance of the HARM is more efficient than the AG. Therefore, the struc-ture of the HARM reduces the total number of edges in the security model, which resulted in fewer computations during the evaluation phase.

On the other hand, the number of memory space required in the representation phase for the HARM is greater than the AG, because the upper layer components of the HARM are also required in the evaluation, However, an extra memory space required by the HARM can be reduced with memory management.

18. Security Evaluation and Overhead

The complexity analyses and experimental results show a significant scalabil-ity improvement using the HARM over traditional security models (e.g., an AG).

Using the hierarchy improves the performance because multiple computations can be grouped in the HARM, whereas a single layered security model does not have such properties. However, if an output of all possible attack scenarios is required، then there is an overhead associated with using the HARM, which requires a top- down correlation with lower layer components (i.e., mapping out all components into a single layer). This overhead is not taken into account, which may have a significant effect on security analysis.

3. Results:

1. The Hierarchical Security Model (HARM) improves the efficiency of the security model by reducing the Number of independent connections between hosts and vulnerabilities.
2. Further performance analysis is conducted in this Research to validate the improvements achieved using the HARM.
3. The experiment is divided into two parts: (i) performance analysis using simple network topologies and (ii) performance analysis using combined network topologies.
4. a new scalable and adaptable security model based on hierarchy developed, and a formal definition of its structures and functionality.

4. Discussion:

Key questions are listed to compare the scalability of security models, and The experimental results showed the efficiency of the HARM by answering these Questions. The experimental results showed the efficiency of the HARM in com-parison to the attack graph(AG), especially the 3-HARM which is also much scalable than the -2HARM (i.e., More scalable using more hierarchy). However, there is still a lack of understanding various attack scenarios which should be reflected in the security Models.

The variation of vulnerabilities affected the AG significantly, show-ing an almost exponential growth in the evaluation phase. In contrast, the HARM showed a linear growth of the evaluation time, which is practically computable for a large number of vulnerabilities. Because the underlying algorithms are the same (e.g., generation algorithm, full path search algorithm), the improvement of scalability comes from the structural advantages of the HARM.

5. Conclusions and recommendations:

Existing studies did not take into account analyzing the scalability of these Models (SAG, MPAG, TVA, HAT)in various network scenarios. As networked systems are becoming large and dynamic (e.g., a Cloud network), traditional solutions are facing scalability and adaptability problems. Structural modification solutions (e.g., Multiple Prerequisite Graph (LAG), Logical Attack Graph (MPG), and Two-Layer Attack Graph (TLAG)) cannot evaluate all possible attack scenarios in a scalable manner، and heuristic solutions may lose security information. As a result, network and Security administrators are facing difficulty determining the security posture to Efficiently deploy defense strategies.

This research shows the scalability of security models used for a large sized Networked system, A performance analysis was conducted to demonstrate how Different security models, namely the HARM and the AG, performed in various Network scenarios. The experimental results show that even when using the

same algorithm to evaluate the security of networked systems, the performance of the HARM is much better than existing security models, Moreover, regardless of The network scenario, the HARM showed better or equal performance in terms of Generation and evaluation phases.

References:

[1] 15408-1:2005, I. Common criteria for information technology security evaluation - part 1: Introduction and general model, 2003.

[2] INTERNATIONAL TELECOMMUNICATION UNION, T. S. S. Security architecture for systems providing end-to-end communications. Tech. rep., ITU-T Rec. X.805, Oct. 2003.

[3] ISLAM, T., AND WANG, L. A Heuristic Approach to Minimum-Cost Network Hardening Using Attack Graph. In Proc. of New Technologies, Mobility and Security (NTMS 2008) (2008), pp. 1–3.

[4] JACKSON, T., SALAMAT, B., HOMESCU, A., MANIVANNAN, K., WAGNER, G., GAL, A., BRUNTHALER, S., WIMMER, C., AND FRANZ, M. Compiler-Generated Software Diversity. In Moving Target Defense, S. Jajodia, A. K. Ghosh, V. Swarup, C. Wang, and X. S. Wang, Eds., vol. 54 of Advances in Information Security. Springer New York, 2011, pp. 77–93.

[5] JAFARIAN, J., AL-SHAER, E., AND DUAN, Q. Openflow Random Host Mutation: Transparent Moving Target Defense Using Software Defined Networking. In Proc. of the 1st Workshop on Hot Topics in Software Defined Networks (HotSDN 2012) (New York, NY, USA, 2012), ACM, pp. 127–133.

[6] JAJODIA, S., NOEL, S., AND OBERRY, B. Topological Analysis of Network Attack Vulnerability. In Managing Cyber Threats, V. Kumar, J. Srivastava,andA.Lazarevic,Eds.,vol.5ofMassiveComputing.SpringerUS, 2005, pp. 247–263.

[7] JAQUITH, A. Security metrics blog. http://www.securitymetrics.org.

[8] JHA, S., SHEYNER, O., AND WING, J. Minimization and Reliability Analyses of Attack Graphs. Tech. Rep. CMU-CS-02-109, School of Computer Science, Carnegie Mellon University, Feb. 2003.

[9] JHA, S., SHEYNER, O., AND WING, J. Two Formal Analyses of Attack Graphs. In Proc. of the 15th IEEE Computer Security Foundations Workshop (CSFW 2002) (2002), pp. 49 – 63.

[10] JIA, Q., SUN, K., AND STAVROU, A. MOTAG: Moving Target Defense against Internet Denial of Service Attacks. In Proc. of the 22nd International Conference on Computer Communications and Networks (ICCCN 2013) (2013), pp. 1–3.

[11] JIA, Q., WANG, H., FLECK, D., LI, F., STAVROU, A., AND POWELL, W. Catch Me if You Can: ACloud-Enabled DDoSDefense. InProc. Of the 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2014) (Jun 2014).

[12] JIN, C., WANG, X., AND TAN, H. Dynamic Attack Tree and Its Applications on Trojan Horse Detection. InProc.of the Second International Conference on Multimedia and Information Technology (MMIT 2010) (2010), vol. 1, pp. 56–53.

[13] J¨URGENSON, A., AND WILLEMSON, J. Processing Multi-parameter Attacktrees with Estimated Parameter Values. In Advances in Information and Computer Security. Springer, 2007, pp. 308–313.

[14] KANG, U., TSOURAKAKIS, C., AND FALOUTSOS, C. Pegasus: A Petascale Graph Mining System Implementation and Observations. In Proc. of 9th IEEE International Conference on Data Mining (ICDM 2009) (2009), IEEE, pp. 229–233.

[15] KARGL, F., KLENK, A., SCHLOTT, S., AND WEBER, M. Advanced Detection of Selfish or Malicious Nodes in Ad Hoc Networks. In Security in Ad-hoc and Sensor Networks, C. Castelluccia, H. Hartenstein, C. Paar, and D. Westh off, Eds., vol. 3313 of Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2005, pp. 152–163.

[16] KARYPIS, G., AND KUMAR, V. Parallel Multilevel k-way Partitioning Scheme for Irregular Graphs. In Proc. of ACM/IEEE Conference on Supercomputing (ICS 1996) (1996), vol. 42, pp. 278–300.

[17] KING, S. Science of cyber security, 203. http://www.fas.org/irp/agency/dod/jason/cyber.pdf.

[18] KIRRMANN, H., AND DZUNG, D. Selecting a Standard Redundancy Method for Highly Available Industrial Networks. InProc.ofthe3rdIEEE International Workshop on Factory Communication Systems (WFCS 2006) (2006), pp. 386–390.197

[19] KORDY, B., MAUW, S., RADOMIROVI´ C, S., AND SCHWEITZER, P. Foundations of Attack–Defense Trees. In Formal Aspects of Security and Trust, P. Degano, S. Etalle, and J. Guttman, Eds., vol. 6561 of Lecture Notes in Computer Science. Springer, 2011, pp. 80–93.

[20] KORDY, B., MAUW, S., RADOMIROVIC, S., AND SCHWEITZER, P. Attack Defense Trees. Journal of Logic and Computation (2012).

[21] KORDY, B., PIETRE-CAMBACEDES, L., AND SCHWEITZER, P. DAGBased Attack and Defense Modeling: Don't Miss the Forest for the Attack Trees. CoRR abs/1303.7397 (2013).

[22] LANTZ, B., HELLER, B., AND MCKEOWN, N. A Network in a Laptop: Rapid Proto typing for Software-defined Networks. InProc.ofthe9thACM SIGCOMM Workshop on Hot Topics in Networks (New York, NY, USA, 2010), Hotnets-IX, ACM, pp. 19:1–19:3.

[23] LEMAY, E., FORD, M., KEEFE, K., SANDERS, W., AND MUEHRCKE, C. Model-based Security Metrics Using Adversary View Security Evaluation (ADVISE). In Quantitative Evaluation of Systems (QEST), 2011 Eighth International Conference on (Sept 2011), pp. 191–200.

نماذج أمان الشبكات تحليل القابلية للتوسع

الملخص: هناك مشكلة في قابلية التوسع في النماذج الأمنية الحالية حيث يصبح حجم الأنظمة الشبكية أكبر، خاصة عند تحليل جميع سيناريوهات الهجوم المحتملة. عرض تحليلات التعقيد الحسابي للحالة الأسوأ استنادًا إلى الطوبولوجيا المترابطة بشكل كامل، ولكن الأنظمة الشبكية الحقيقية تعمل على العديد من طبولوجيا الشبكات وعوامل أخرى تؤثر على الأداء العام لنماذج الأمان. في هذا البحث، يتم تقييم قابلية تطوير نماذج الأمن الحالية ومقارنتها مع HARM في سيناريوهات واقعية. تتمثل مهمتان رئيسيتان في هذا البحث في: (1) صياغة الأسئلة الرئيسية التي تحتاج إلى إجابة لتقييم قابلية تطوير نماذج الأمن، و (2) تقييم وقابلية تطوير نماذج الأمن باستخدام عمليات المحاكاة.

الكلمات المفتاحية: مشكلة قابلية التوسع، نماذج الأمان، تحليلات التعقيد، النموذج الهرمي لأمن المعلومات.