Poster: Limiting Damage Spread in the IoT Using Features-based Immunisation.

Farell Folly

folly.farell@unibw.de

1. Introduction

With the advent of Internet of Things (IoT), smart applications create an Interconnection of hundreds of thousands or even higher number of devices that leads to a complex and mostly unpredictable network structure. Incontestably, apart from the privacy issues associated with most of the new devices that comprise the IoT, they often lack strong security features, therefore, present a high exposure factor to attacks. Consequently, an exploit on a device or an application can lead to a worldwide epidemic [1], since an IoT network usually exhibits a large-scale network structure where a computer infection can rapidly spread across the globe.

2. Contribution

During our research, we've identified three main issues. Firstly, Traditional graph metrics are inefficient because they are only locally meaningful [2–5], and do not take the nodes' attributes into account. Secondly, computing graph metrics in complex networks is an intractable problem [6]. Lastly, existing diffusion or propagation models are based on randomly chosen nodes, while infection spread is not totally random[7, 8]. Our main contribution lies with the modelling of an IoT network. Each layer, group or cluster will be treated as a separate graph based on the nodes characteristics and features. Among the advantages, one can easily visualize details that are normally difficult to perceive with a "normal eye" [9, 10] or even by a computer that hasn't been given sufficient information about the properties of the nodes.

Compare to a flat graph, where only traditional metrics based only on the existence of links and paths, we see that from the rich graph in fig.1,we can aggregate the nodes based on different features. For instance, we group nodes together per network, to study how networks interact within one another from a damage spread point of view. Then, grouping nodes based on the application that they use, helps visualize nodes that are high likely to spread an infection from one application to application, given that an infection can spread through various applications.

No previous work, to our knowledge, focused on a group and attributes-based representation of an IoT network for the purpose of its security analysis as we present here. Our novelty resides in the fact that we transform any given IoT network into a k-partite[1] graph that reveals many critical security aspects that can be used to analyze an infection spread and make important high-level decisions for immunisation and vaccine distribution.

2.1. Security-relevant features for IoT

There are many interesting features that could influence the vulnerability of an IoT network are important to take into into for a security analysis. The first interesting thing here is that some features are very specific to the IoT and were not taken into account in traditional networks as security relevant. For example, before the advent of IoT, safety matters only in the industrial sector. Nevertheless, today it is becoming very important in the IT field as well. In fact, some cyberattacks have been able to compromise devices and cause physical injuries to their users. We can group the security-relevant features int two groups: those which are rather technical and usual in the IT field (localisation, attack vectors, propagation vectors, etc.) and some others which are operational (safety, users behaviours, costs, etc.)

Let's show that through the following two simple scenarios, considering the basics features: applications, and networks. Therefore we'll try to group the devices according to the applications that they use and also to the networks they belong to.

2.2. Example of Use case: Nodes vs Apps

By putting the nodes into relation with the apps they use (fig.2), and grouping them into a super "node", we

[1] In this paper, we only consider k = 2, for simplicity.

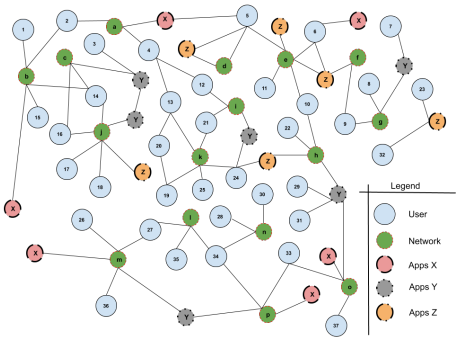


Figure 1: Rich IoT Graph with nodes' attributes and features

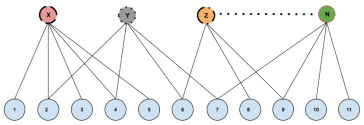


Figure 2: Bipartite graph matching application providers (top) to all other nodes.

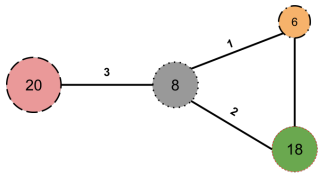


Figure 3: IoT resulting compressed graph given an original rich graph in fig. 1.

can compress the graph (fig.3) and still retain [11] all the security-relevant aspects of the original graph in fig.1 for a security analysis which reveals here that apps Y, although used by a very few number of nodes, is the most critical [12] propagation vector.

3. Conclusion

In summary, we showed that taking attributes into account for the security analysis of IoT has multiple advantages. Firstly, during an infection spread attributes can help ignore certain nodes or weight their importance differently. For instance, when a virus only attacks a particular version of software, nodes that do not use that version can't get or transmit or transmit. Secondly, it is possible to transform the IoT into a k-partite graph and apply the results of many previous works.

4. References

References

[1] B. Castle, The Internet of things (IoT) and Cloud Fundamentals, Cisco IoT Pathfinder (2016).

[2] F. Bauer, J. T. Lizier, Identifying influential spreaders and efficiently estimating infection numbers in epidemic models: A walk counting approach, EPL (Europhysics Letters) 99 (2012) 68007.

[3] G. Lawyer, Understanding the influence of all nodes in a network, Scientific reports 5 (2015) 8665.

[4] S. P. Borgatti, Centrality and network flow, Social Networks 27 (2005) 55 – 71.

[5] R. A. P. da Silva, M. P. Viana, L. da Fontoura Costa, Predicting epidemic outbreak from individual features of the spreaders, Journal of Statistical Mechanics: Theory and Experiment 2012 (2012) P07005.

[6] C. Schulz, Graph Partitioning and Graph Clustering in Theory and Practice, Karlsruhe Institute of Technology (KIT), Institute for Theoretical Informatics, 2016.

[7] C. Gao, J. Liu, N. Zhong, Network immunization and virus propagation in email networks: Experimental evaluation and analysis, Knowl. Inf. Syst. 27 (2011) 253–279.

[8] C. Chen, H. Tong, B. A. Prakash, C. E. Tsourakakis, T. Eliassi-Rad, C. Faloutsos, D. H. Chau, Node immunization on large graphs: Theory and algorithms, IEEE Transactions on Knowledge and Data Engineering 28 (2016) 113–126.

[9] Y. Liu, T. Safavi, A. Dighe, D. Koutra, Graph summarization methods and applications: A survey, ACM Comput. Surv. 51 (2018).

[10] Y. Tian, R. A. Hankins, J. M. Patel, Efficient aggregation for graph summarization, in: Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data, SIGMOD '08, Association for Computing Machinery, New York, NY, USA, 2008, p. 567–580.

[11] M. Burgess, G. Canright, K. Engø-Monsen, A Graph-theoretical Model of Computer Security, International Journal of Information Security Vol. 3 (2004) pp. 70–85.

[12] Y. Zhang, A. Adiga, S. Saha, A. Vullikanti, B. A. Prakash, Near-optimal algorithms for controlling propagation at group scale on networks, IEEE Transactions on Knowledge and Data Engineering 28 (2016) 3339–3352.

Forschungsinstitut Cyber Defence
Universität der Bundeswehr München

der Bundeswehr Universität München

Poster: Limiting Damage Spread in the Internet of Things Using Features-based Immunisation Techniques

Security Challenges

- IoT has a large number of devices, is highly heterogeneous and very dynamic
- Not all vulnerabilities are known and attacks are unpredictable
- Cybercriminal keep improving their techniques, leveraging zero-day attacks
- IoT devices can easily be turned into botnets for a worldwide DDoS attack

Graph Theory Challenges

1. Traditional graph vulnerability metrics are inefficient, only locally meaningful, and do not take the nodes' attributes into account
2. Computing graph metrics in complex networks is an intractable problem

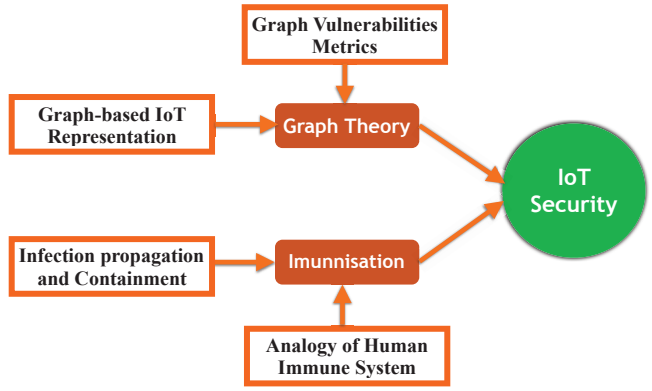
Immunisation Challenges

1. Existing diffusion or propagation models are based on randomly chosen nodes, while infection spread is not totally random.
2. Nodes selection for vaccines distribution is an intractable problem
3. Vaccine distribution process depends on type of attack

... Hard to plan for a systematic security approach

In this research work, we are proposing a new approach that aims at considering the intrinsic properties of the nodes to build a layered network that can support the design of more realistic propagation models and build a compact network by aggregating nodes based on those properties. In addition, such a compact view will ease analysis and requires less computation resources.

"Since we can never produce a 100% secure general system or network, we need methods to mitigate the spread of damage."



We propose to group the security-relevant features into two categories:

A. those which are rather technical and common in the IT field (localisation, attack vectors, propagation vectors, etc.)

B. and some others which are rather operational (safety, users behaviours, costs, etc.).

For example, by putting the nodes into relation with the applications they use (fig.2), and grouping them into a super "node", we produce a compressed graph (fig.3) which still contains all the security-relevant aspects of the original graph in fig.1. Here, it reveals that application Y, although used by a very few number of nodes, is the most critical propagation vector.

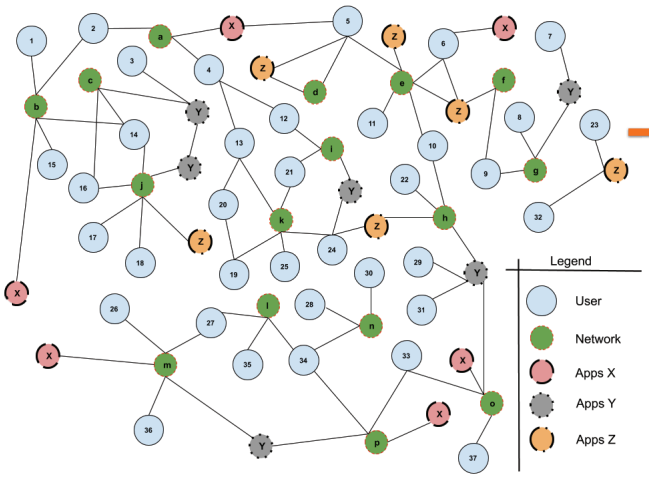


Figure 1: Rich IoT graph with nodes' attributes

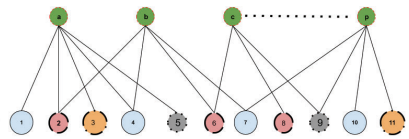


Figure 2: Bi-partite graph based on nodes' attributes

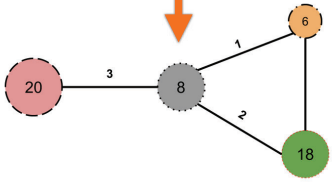


Figure 3: Compressed IoT graph for rapid and high level decision-making processes

Farell FOLLY, folly.farell@unibw.de