POSTER: An Approach to Assess Security, Capacity and Reachability for Heterogeneous Industrial Networks

Apala Ray[1,3(✉)], Johan Åkerberg[2,3], Mats Björkman[3], and Mikael Gidlund[4]

[1] ABB Corporate Research, Bangalore, India
apala.ray@in.abb.com
[2] ABB AB; Corporate Research, Vasteras, Sweden
[3] School of Innovation, Design, and Technology, Mälardalen University, Vasteras, Sweden
[4] Mid Sweden University, Sundsvall, Sweden

Abstract. Industrial plants are heterogeneous networks with different computation and communication capabilities along with different security properties. The optimal operation of a plant requires a balance between communication capabilities and security features. A secure communication data flow with high latency and low bandwidth does not provide the required efficiency in a plant. Therefore, we focus on assessing the relation of security, capacity and timeliness properties of an industrial network for overall network performance.

Keywords: Security modeling · Network assessment · Routing · Path planning

1 Introduction

The goal of industrial automation is to automate the operations involved in industrial processes with minimal or reduced human intervention. Technological advances in terms of computing power and communication capabilities bring operational benefits inside plants, but also increase the exposure of cyber security attacks. Therefore, industrial automation security has constantly gained attention over the last years both in academia and in industry. Along with cyber security requirements on industrial plants, it is also necessary to consider other important requirements of plants in terms of availability and timeliness. Therefore, it is important to understand the network capabilities during network design to avail the required network performance in a heterogeneous network system. The network planning phase should capture the properties of the system and identify constraints on the network to achieve an overall secure solution. In this work, we explore how a network path can be chosen inside a plant between two devices, where the network will consider the required levels of communication security, capacity and timeliness. In a multi-hop heterogeneous network, data communication between source and destination can be possible through multiple paths involving devices with varying capabilities. The problem is that, some

B. Thuraisingham et al. (Eds.): SecureComm 2015, LNICST 164, pp. 577–580, 2015.
DOI: 10.1007/978-3-319-28865-9_34

devices can score high on one particular performance parameter, whereas, score very low on other performance parameters. If the decision of choosing a flow path between a source and destination is done based on one performance criteria only, such as, security or path reachability or link capacity, then one segment of a network may be overloaded.

There is a set of work where different models are used to assess network security. Security monitoring and incident modeling by combing automated analysis of data from security monitors and system logs with human expertise is shown in [1]. There are some research on attack graph construction and performance evaluation [2]. in [3], two layers attack graph is proposed. Attack models also can be used to assess network security. A hierarchical attack representation model is proposed in [4], where a two-layer hierarchy is proposed to separate the network topology information from the vulnerability information of each host. A ranking scheme to identify a relevant portion of the attack graph is proposed in [5]. In [6], a framework for an experimentation environment for network industrial control system is proposed which can reproduce concurrently physical and cyber systems. Most of these work focus on run-time analysis of network traffic or generate attack graphs. In this paper, we provide a model which can be used during network design to identify optimized network paths.

2 Proposed Idea

To assess security, capacity and reachability for heterogeneous industrial networks, we propose to analyze the systems globally, identifying flow paths based on application requirements and directing resources efficiently to increase the confidence in the system. For an efficient flow path estimation, our model requires the topology of the system along with the performance related attributes as input. The key performance indicators required for successful operations of a network are also identified. Once we have a mathematical model, then we can

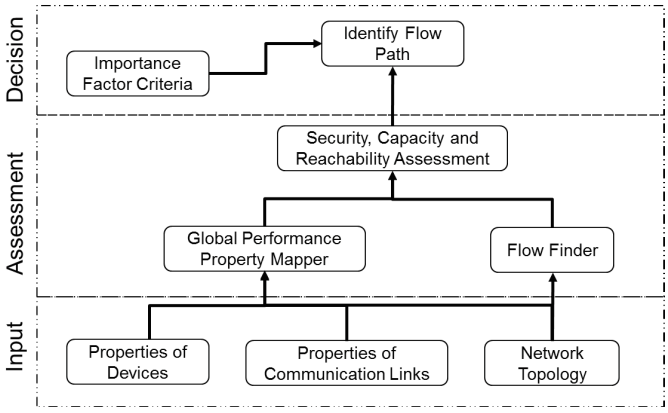

Fig. 1. Architecture for Secure and Robust Path Identification

individually analyze the effect of each key performance indicator on a network flow. Based on this analysis, we can study the effects of a local performance indicator of each node on the global performance indicator of a flow path keeping overall security, capacity and timeliness in the system. This helps us to rank the each communication flow path based on the key performance indicators of the network. This information is useful when designing a plant with a service level agreement. Figure 1, presents the architecture of the component required for path identification.

3 Results

Figure 2 shows the result from our proposed model. We apply the proposed idea on an example network to analyze the network flow value. We consider a small network and estimate the flow value of each flow path. Then we present how the flow value between two devices changes based on the change in local performance metrics *node assurance value*, *link capacity* and *hop count*.

We can see from the graph that with an increase of *node assurance value* the *flow value* gradually increases until the *node assurance value* reaches maximum allowed limit. With the increase of *link capacity*, the *flow value* increases until it reaches the minimum of the rest of *link capacity* set in the flow path. Once the *link capacity* reaches the minimum of the set, there is no change in the flow value. The increase of *hop count* decreases the *flow reachability* and in turn decreases the *flow value*.

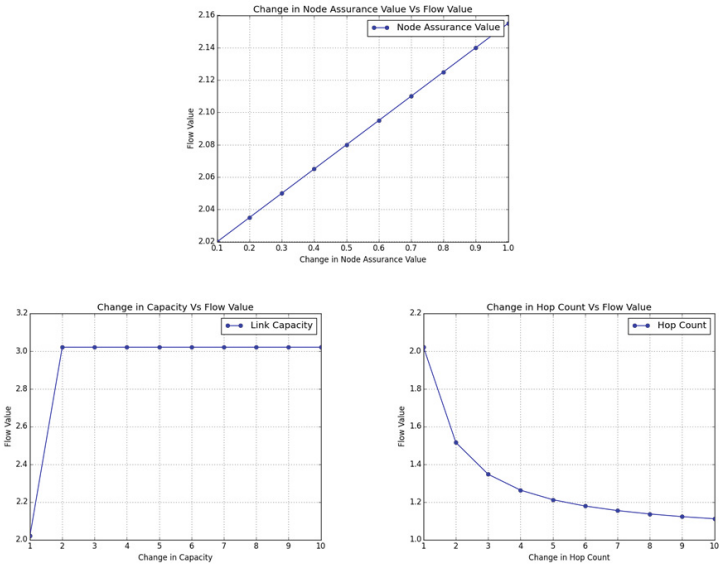

Fig. 2. Change in Flow Value with change in Node Assurance Value, Link Capacity Value and Hop Count

4 Conclusions

We introduce a concept to balance secure, high capacity and reachable flow path in a heterogeneous industrial network during planning phase. We use the concept of *flow awareness value* to determine the trustworthiness of a network. This value is a probabilistic measure of confidence in the security properties of devices and communication flows. The *flow awareness value* captures the risk of a flow path getting affected from the nodes in the flow path. We also introduce the concept of link bandwidth and hop count to model the *flow capacity* and *flow reachability*. This model can assist plant operators to rank each communication flow path based on security, capacity and reachability. We have observed that, if there is a bottleneck with a low capacity link in the network, the increase of trustworthiness of nodes will not improve the flow path value. Similarly, if we have a high number of intermediate nodes with low capacity and high security between the source node and destination node, we might not get a high rank flow path. This type of information is useful when designing a plant with a service level agreement.

In this network model, we do not consider the throughput of the system which can be an average rate of successful message delivery over a communication link. This throughput can only be available to the network operator during run-time when the message sending rate is also available along with the fixed topology. Therefore, we need to analyze the working flow paths rather than all possible flow paths. Then we can validate the performance of a network after choosing the identified flow path as described in our model. We plan to explore this option in our next work.

References

1. Sharma, A., Kalbarczyk, Z., Barlow, J., Iyer, R.: Analysis of security data from a large computing organization. In: 2011 IEEE/IFIP 41st International Conference on Dependable Systems Networks (DSN), June 2011
2. Sheyner, O., Haines, J., Jha, S., Wing, R.: Automated generation and analysis of attack graphs. In: Technical Report CMU (2002)
3. Xie, A., Cai, Z., Tang, C., Hu, J., Chen, Z.: Evaluating network security with two-layer attack graphs. In: Proc. of Annual Computer Security Applications Conference (ACSAC 2009) (2009)
4. Hong, J., Kim, D.-S.: Harms: hierarchical attack representation models for network security analysis. In: Proceedings of the 10th Australian Information Security Management Conference, Western Australia, December 2012
5. Mehta, V., Bartzis, C., Zhu, H., Clarke, E.: Ranking attack graphs. In: Zamboni, D., Kruegel, C. (eds.) RAID 2006. LNCS, vol. 4219, pp. 127–144. Springer, Heidelberg (2006)
6. Genge, B., Siaterlis, C., Fovino, I.N., Masera, M.: A cyber-physical experimentation environment for the security analysis of networked industrial control systems. Computers and Electrical Engineering (2012)