Vulnerability Analysis of Wireless Sensor Networks via Maximum Flow Interdiction

Keyu Wu[1](✉), Zhou Zhang[2], Xingchen Hu[1], Boliang Sun[1], and Chao Chen[1]

[1] National University of Defense Technology, Changsha 410073, China
keyuwu@nudt.edu.cn
[2] Tianjin Artificial Intelligence Innovation Center, Tianjin, China

Abstract. Due to limited resource and changing environments, wireless sensor networks are susceptible to device failures. In this paper, we evaluate network's vulnerability under potential device failures or attacking. Specifically, we model wireless sensors and their operating procedure as an S-T network, where the information rate regarding the network performance is defined. The network robustness is evaluated via considering how network capacity varies when network changes. The evaluation process turns out to be a maximum flow interdiction problem, which is then solved by transforming into a dual formation and approximating with a linear programming. Lastly, via numerical simulation, the proposed scheme is shown to be well suitable for evaluating network's robustness.

Keywords: Vulnerability analysis · Network interdiction · Maximum flow · Malicious attacking

1 Introduction

Wireless sensor networks consist of widely deployed sensors that sense environment, collect data and route information to interested users, which are essential for the Internet of things. Due to either hardware degradation and or malicious attacking, wireless sensors may fail and be out of service [1]. The performance of an improperly designed network may greatly suffer due to device failures. Therefore, robustness is an important design aspect for wireless sensor networks.

In literature, a network's robustness or vulnerability is mainly investigated from the view of the underlying graph topology. For example, in [2], the connectivity of a network is considered, where two metrics, namely "node-similarity" and "optimal connectivity", are defined to quantify network vulnerability. Similarly, work [3] considers robustness as the redundancy of routing path between two nodes, and defines a metric "natural connectivity" for measuring the network's robustness. Beside connectivity, criticality is another metric that is used for measuring network vulnerability [4,5]. The node critical value is defined via counting the number of paths that flows through a node. The edge critical value

B. Li et al. (Eds.): IoTaaS 2019, LNICST 316, pp. 310–317, 2020.
https://doi.org/10.1007/978-3-030-44751-9_26

is defined similarly. Therefore, a node or edge with higher criticality value contributes more to the network's throughput, and may manifest itself as a vulnerable point of a network. Furthermore, based on the definition of node and edge critical values, network criticality is defined [6,7] via averaging nodes' and edges' critical values. From the perspective of information theory, work [8] studied the vulnerability of network from the topology dissimilarities after network topology changes. The robustness metric is then calculated with the Jenson-Shannon divergence that is original from the information theory.

However, node connectivity or network topology changes does not necessarily well represent the network performance variations caused by node failures. In this paper, we will investigate the network robustness from the capacity of a sensor network. Specifically, we model wireless sensors and their operating procedure as an S-T network, where the maximum supported information rate, i.e., the capacity, of the network performance is defined. Furthermore, an intelligent attacking strategy that aims to minimize the network's capacity is considered, where the attacking strategy is solved with maximum flow interdiction methods. Finally, the network robustness is then measured in terms of capacity variations under such an attacking scheme.

The rest of this paper is organized as follows. Section 2 introduces models for representing a sensor network and its working procedure. Section 3 analyzes the network robustness with a network interdiction problem. Section 4 provides a computationally tractable algorithm for solving the interdiction problem. Section 5 shows simulations result and Sect. 6 concludes the paper.

2 Modeling the Capability of Sensor Networks

2.1 Network Topology Model

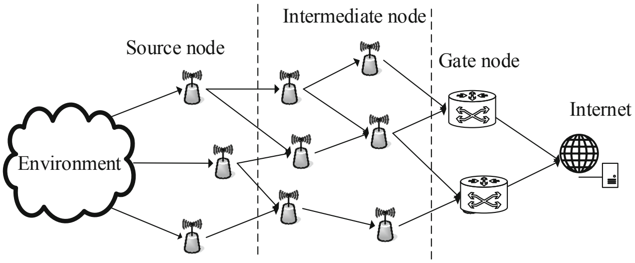

Fig. 1. An example for sensor networks under investigation.

In this paper, we investigate a sensor network as shown in Fig. 1, where some source nodes measure environment and transmit measured packets throughout intermediate nodes to gate nodes that located at the edge of network, and from gate nodes, measured information can be accessed via the Internet. Note that a measured packet can be routed to the Internet through potentially multiple paths, which is determined by underlying routing algorithms. Furthermore, since different tranceiving pairs are associated with different distance and wireless resources, edges of network have different transmission capacities.

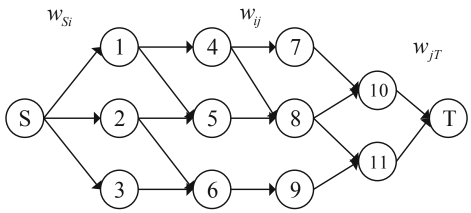

Fig. 2. S-T network induced from the sensor network.

Mathematically, the above sensor network can be modeled as a directional weighted graph, as shown in the S-T network of Fig. 2. Specifically, let $\mathcal{V} = \{1, 2, \cdots, n\} \cup \{\text{S,T}\}$ denote the sensor nodes, where $\{1, 2, \cdots, n\}$ denotes the sensor nodes in the network, S is a virtual node that represents the environment, and T is a virtual node that represents the Internet (destination of information flow). In addition, let $\mathcal{E} = \{(i, j)\}$ denote the edges that connects node i and node j with flow direction specified by underlying routing algorithm. Moreover, there is a weight associated with edge in the S-T network. Specifically, there is a weight w_{Si} associated with node S to a sensor node i, and it represents the maximum information sample rate that sensor node i is able to sense from the environment. The value of w_{Si} with $i \in \{1, 2, ..., n\}$is determined by the capacity of sensors and the design goal of sensing tasks. In addition, there is a weight w_{jT} with $j \in \{1, 2, ..., n\}$ from a gate node j to node T, and it represents the maximum information transmitting rate from a gate node to the Internet. The value of w_{jT} is determined by the capacity of gate node and backhauls. Lastly, there is a weight w_{ij} with $i, j \in \{1, 2, ..., n\}$ from a node j to a node i, and it represents the maximum routing rate that information is transmitted from node i to node j. The value of w_{ij} is determined by nodes' transmission capability and wireless channel condition. In summary, the triple $\mathcal{G} = (\mathcal{V}, \mathcal{E}, W)$ defines a sensor network, and in the following, we evaluate the networks' performance based on the above information.

2.2 Network Capability Model

The S-T graph represented in Fig. 2 captures the network topology and capability of individual nodes (source nodes, intermediate nodes and gate nodes). In this part, we model the capability from the network point of view with network flow model, which integrates the overall ability of sensing environment, routing sensed information, and delivering information to the Internet. Specifically, we investigate the question: what is the maximum information rate can be delivered from the node S (environment) to node T (the Internet) without violating pairwise capability constraints w_{ij} with $i, j \in \{S, T, 1, 2, ..., n\}$?

The network flow model answers the question. We define a flow function $f : \mathcal{V} \times \mathcal{V} \mapsto \mathbb{R}$, such that the function f satisfying following conditions:

1. capacity constraints: for all $i, j \in \mathcal{V}$, we have $f(i, j) \leq w(i, j)$ (which means that the actual data rate cannot exceed the edge rate capacity);
2. skew symmetry: for all i, j, we have $f(i, j) = -f(j, i)$ (because edges are directional);
3. flow conservation: for all $u \in \mathcal{V} \backslash \{S, T\}$, we have $\sum_{v \in \mathcal{V}} f(u, v) = 0$ (flows into a node must equal flows out from a node).

A valid flow function f satisfying above conditions represents an assignment of data rate over different edges. The value of a flow function defined as $|f| = \sum_{i \in \mathcal{V}} f(S, i)$ represents the data rate flow over the network. Among all possible flow functions (assignments), there is an optimal flow f^* that achieve the maximum flow value, which is the best one can get under the network topology and devices' individual capacity. Hence, we can use the value of maximum flow to capture the network capacity.

There exists many algorithms for solving f^*, and Ford-Fulkerson algorithm is perhaps the most well-known one, which can solve f^* with time complexity of $\mathcal{O}(n \cdot |\mathcal{E}|^2)$ [11]. Developing fast algorithms for solving the maximum network flow is an on-going research direction in computer science. Algorithms faster than Ford-Fulkerson algorithm have been developed (see [12] and references therein).

In summary, we have developed a maximum flow model for modeling the overall network capability given sensor networks' topology and individual devices' capacity. In addition, the developed model can be solved efficiently with polynomial time complexity.

3 Vulnerability Analysis via Network Flow Interdiction

In this part, we analyze the network vulnerability under device's potential failures. Specifically, due to device degradation and potential attacks, sensors in the network may be out of service and network capability deteriorates. A robustly designed network is able to tolerate such device failures and reserve network capability as much as possible. In contrast, the performance of a vulnerable network may be severely suffered when devices are out of service.

In order to evaluate the vulnerability, we have to model the pattern of device's failures. In this paper, we analyze the network's performance changes under the worst case device failure pattern. It may correspond to an intelligent attacker that is attempting to deteriorate the network's performance by compromising the most important sensors. This problem can be modeled under network interdiction framework.

Suppose that an attacker is able to compromise k edges among the total $|\mathcal{E}|$ edges, and it selects the k edges in a way such that the maximum flow of the residual network (after removing the selected edges) is minimized. Let $x_{ij} \in \{0, 1\}$, $\forall (i, j) \in \mathcal{E}$, indicates the decision of the attacker, i.e., if $x_{ij} = 1$ the edge (i,j) is removed from the network; $x_{ij} = 0$ otherwise. Hence, the attacker's attacking scheme can be formulated as

$$\text{MFI-K:} \quad \min_{x \in X} \quad \max_{f} \sum_{i \in \mathcal{V}} f(S,i) \tag{1}$$

$$\text{s.t.} \quad \sum_{(i,j) \in \mathcal{E}} x_{ij} = k \tag{2}$$

$$f(i,j) \leq w_{ij}(1 - x_{ij}) \tag{3}$$

$$\sum_{j \in FS(i)} f(i,j) - \sum_{j \in RS(i)} f(j,i) = 0, \tag{4}$$

Note that, in (1), '$\max\limits_{f}$' means to find a flow assignment function that achieves network capacity (i.e., maximizes the overall network flow (see Sect. 2.2)). In addition, '$\min\limits_{x \in X}$' means to find an attacking scheme that minimizes the capacity of residual network. Lastly, constraint (3) means that a flow from node i to node j cannot exceed the capacity w_{ij}, if the edge (i,j) is not chosen by the attacker; the flow equals 0, if the edge is compromised by the attacker.

Denote the results to problem (1) MFI-K is $(\boldsymbol{x}^*(k), \boldsymbol{f}^*(k))$, where $\boldsymbol{x}^*(k)$ means the optimal attacking decisions made by attackers, and $\boldsymbol{f}^*(k)$ means the optimal flow assignment for protecting the network's performance from the attacking. We can repeatedly solve the MFI-K problem for different values of k and obtain a sequence of solutions $\{(\boldsymbol{x}^*(k), \boldsymbol{f}^*(k))\}_{k=1}^{K}$, from which several metrics can be defined to evaluate the network's robustness:

1. Robustness profile $\{|\boldsymbol{f}^*(k)|\}_k$, which describes how the network performance changes under different attacking intensity.
2. $\beta-$quantile point $k(\beta)$ is the maximum number of edges loss such that the network can tolerate before performance drop to β percent, i.e.

$$k^{\beta} = \max \left\{ k \,\middle|\, \frac{|\boldsymbol{f}^*(k)|}{|\boldsymbol{f}^*(0)|} \geq \beta \right\}. \tag{5}$$

   It can be seen that, for a given β, a network with larger k^{β} is more robust.
3. Critical edge set $\mathcal{E}^C$ is the set of edges that are susceptible to attackings, which can be defined as

$$\mathcal{E}^C = \cup_k \boldsymbol{x}^*(k) \tag{6}$$

   The set $\mathcal{E}^C$ describes how the vulnerable edges distributed. Given that other conditions are equivalent, a network with smaller size of $\mathcal{E}^C$ is more robust.

We have shown that the network vulnerability can be analyzed with maximum flow interdiction methods and corresponding evaluation metrics. In the following, we develop a method for solving $(\boldsymbol{x}^*(k), \boldsymbol{f}^*(k))$ of an MFI-K problem.

4 Solving Maximum Flow Interdiction Problems

In this part, we consider the solving of the MFI-K problem (1). It is well known that exactly solving the MFI-K is NP-hard [13], and we restore to linear approximation of MFI-K. However, due to the min-max structure, (1) manifests as a two-stage optimization problem, which hampers the solving process. By transforming the maximum flow problem into its dual formulation, the two-stage optimization problem can be transforming into a minimization problem

$$\text{MFI-K-Dual:} \quad \min_{\boldsymbol{x},\boldsymbol{u},\boldsymbol{\eta}} \sum_{(i,j)\in\mathcal{E}\backslash\{(S,T)\}} w_{ij}(1-x_{ij})\eta_{ij} \tag{7}$$

$$\text{s.t.} \quad \sum_{(i,j)\in\mathcal{E}} x_{ij} = k \tag{8}$$

$$\alpha_i - \alpha_j + \eta_{ij} \geq 0 \quad \forall (i,j) \in \mathcal{E}\backslash\{(S,T)\} \tag{9}$$

$$\alpha_T - \alpha_S \geq 1 \tag{10}$$

$$\boldsymbol{\eta} \geq \mathbf{0} \tag{11}$$

$$\boldsymbol{x} \in [\mathbf{0},\mathbf{1}]^{|\boldsymbol{\mathcal{E}}|}, \tag{12}$$

where $\boldsymbol{\alpha}$ and $\boldsymbol{\eta}$ are the dual variables of the constraints (3) and (4), respectively, and constraint (12) represents the linear approximation of the original problem. It can be seen that problem is a linear programming problem, which can be addressed efficiently with standard LP solver. Furthermore, from its solution, we can get $x^*(k)$, i.e., the selected attacking edges. Lastly, after removing $x^*(k)$ from the network, we can obtain $|f^*(k)|$, i.e., the performance of the residual network, by applying standard maximum flow solver [11].

5 Numerical Results

In this part, we verify our proposed evaluation methods with numerical simulation. A sensor network is generated over an area with 1000 × 1000 m, where the three types of nodes are selected for representing source nodes, gate nodes and intermediate nodes, respectively. Figure 3 shows an instance of generated network. Two nodes are assumed to be able to establish connection if their distance is less than 100 m. The source node's sampling rate is fixed to 0.3 Mbps; the gate node's delivery rate is fixed to 10 Mbps; and the transmission capacity of a link is based on the distance d_{ij} between two nodes, calculated as $w_{ij} = \frac{1}{d_{ij}^2+1}$ Mbps. Links are bidirectional, and for each source node, its routing paths to gate nodes through intermediate nodes are computed via maximum flow routing algorithms [14, 15].

Three different attacking schemes are considered, namely, maximum flow interdiction scheme as shown in (7); random attacking scheme that randomly removes edges in the network; greedy attacking scheme that removes edges with

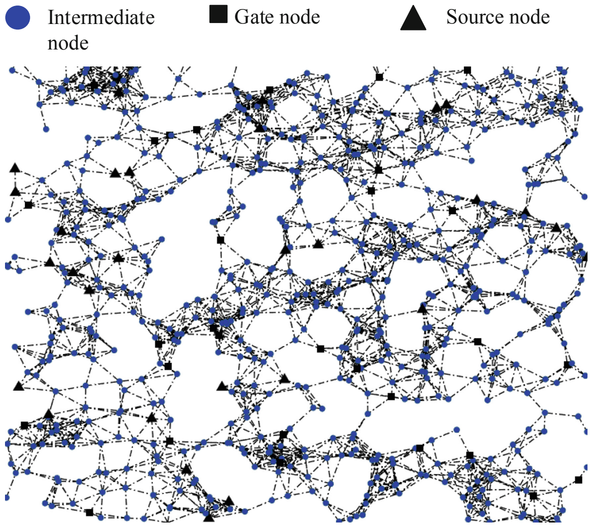

Fig. 3. Topology of a simulated sensor network instance.

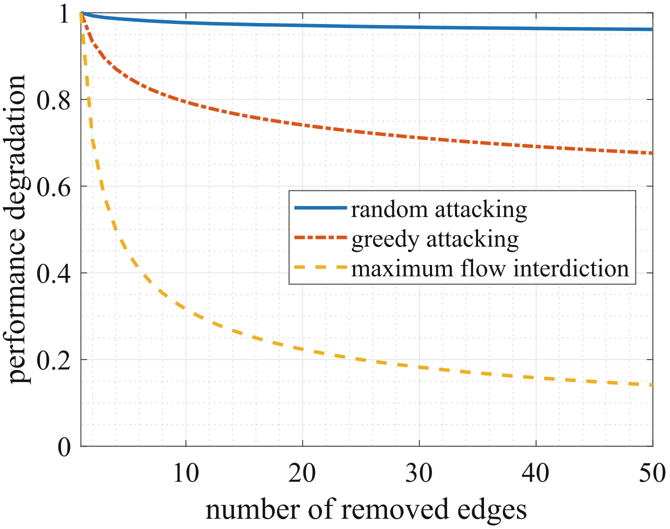

Fig. 4. Network performance degradation under different attacking schemes.

largest transmission capacity. Figure 4 shows the robustness profile of the investigated network under these three schemes averaged over 1000 network realizations. It can be seen that, as the removed edges increases, the network performance drops quickly under the maximum flow interdiction scheme. Furthermore, the network demonstrates a more robust profile against the greedy attacking scheme. Lastly, the network's performance changes slightly under random attacking scheme. In summary, different attacking schemes demonstrate significant robustness profile, while the maximum flow interdiction represents the worst case situation, and is suitable for evaluating networks' robustness.

6 Conclusion

In this paper, we have investigated network vulnerability with maximum flow interdiction methods, from which network robustness profile, the critical edges and quantile points are theoretically defined. As the maximum flow interdiction problem is NP-hard, we consider its linear approximation for solving an attacking strategy and the evaluation metrics. It is interesting to study how these metrics change under typical sensor networks' topology, which is left as future work.

References

1. Akyildiz, I.F.: A survey on sensor networks. IEEE Commun. Mag. **40**(8), 102–114 (2002)
2. Dekker, A.H., Colbert, B.D.: Network robustness and graph topology. In: Proceedings of the 27th Australasian Conference on Computer Science, vol. 26, pp. 359–368 (2004)
3. Jun, W., Barahona, M., Yue-Jin, T.: Natural connectivity of complex networks. Chin. Phys. Lett. **27**(7), 078902 (2010)
4. Tizghadam, A., Leon-Garcia, A.: LSP and back up path setup in MPLS networks based on path criticality index. In: IEEE International Conference on Communications, pp. 441–448 (2007)
5. Tizghadam, A., Leon-Garcia, A.: On congestion in mission critical networks. In: INFOCOM Workshops. IEEE (2008)
6. Tizghadam, A., Leon-Garcia, A.: On robust traffic engineering in transport networks. In: IEEE Globecom IEEE Global Telecommunications Conference. IEEE (2008)
7. Tizghadam, A., Leon-Garcia, A.: Survival value of communication networks. In: INFOCOM Workshops. IEEE (2009)
8. Schieber, T.A., Carpi, L., Frery, A.C., Rosso, O.A.: Information theory perspective on network robustness. Phys. Lett. A **380**(3), 359–364 (2016)
9. Dhuli, S., Gopi, C., Nath Singh, Y.: Analysis of network robustness for finite sized wireless sensor networks. Eprint arXiv (2016)
10. Titouna, C., Nait-Abdesselam, F., Khokhar, A.: A multivariate outlier detection algorithm for wireless sensor networks. In: IEEE ICC 2019, pp. 1–6 (2019)
11. Ford, L.R., Fulkerson, D.R.: Maximal flow through a network. Can. J. Math. **8**(3), 399–404 (1965)
12. Boykov, Y., Kolmogorov, V.: An experimental comparison of min-cut/max-flow algorithms for energy minimization in vision. IEEE Trans. Pattern Anal. Mach. Intell. **26**(9), 1124–1137 (2004)
13. Wood, R.K.: Deterministic network interdiction. Math. Comput. Model. **17**(2), 1–18 (1993)
14. Mahlous, A.R., Fretwell, R.J., Chaourar, B.: MFMP: max flow multipath routing algorithm. In: European Symposium on Computer Modeling and Simulation, Liverpool, pp. 359–368 (2008)
15. Ohara, Y., Imahori, S., Van Meter, R.: MARA: maximum alternative routing algorithm. In: IEEE INFOCOM, Rio de Janeiro, pp. 298–306 (2009)