Abstract. For a network system survivability refers to the ability to provide essential services to end users in the presence of failures and/or attacks. Survivability evaluation focuses on the measurement of this ability. As a dominating way of survivability evaluation, the model-based analysis technology for wireless sensor networks (WSNs) faces three problems. First, the technology assumes that node distribution accords with some statistical regularity, and network has a fixed topology. However, in WSNs the node distribution and topology may change at any time which makes the evaluation result be untrustworthy. Second, survivability indicators are calculated by hand. But the personnel calculation is error prone. Third, there is no a systematic way to compute survivability indicators, i.e., we are not able to perform calculations of indicators by calling fundamental calculation processes. To solve the first problem, we propose a Continuous Time Markov Chain (CTMC) to characterize evolution of behaviors of single nodes under failures and attacks, and a parallel composition of CTMCs to characterize evolution of behaviors of WSN. The parallel composition can characterize links between nodes such that the calculation of survivability indicators does not depend on the node distribution regularity and topology. To solve the second problem, we develop an algorithm to map the initial deployment of WSN to the parallel composition of CTMCs described by the modeling language of the stochastic model checker PRISM. To solve the third problem, we present how to formalize survivability indicators including k-connectivity etc. with Continuous Stochastic Logic (CSL). Finally, we show the effects of node misbehaviors on survivability by numerical analysis.

Keywords: Survivability Wireless Sensor Network Stochastic Model checking: Continuous Time Markov Chain

1 Introduction

Wireless sensor networks [1,2] are communication networks of wireless autonomous nodes that are deployed over a surveillance area, and monitor physical environments through the cooperation of large amount of sensors. WSNs increase people’s capacity to sense the physical world, and are widely used for national military defense, industrial and agricultural production, environment monitoring, disaster relief and other fields. At present, the technological progress of the relevant fields of WSNs promote the constant development of intelligent, miniaturized, low-power, and low-cost sensors. However, cost and size limit resources in sensor nodes such as energy, memory, speed
of computation, bandwidth, etc. The occurrence of faults and attacks are normal because WSNs are usually deployed in adverse and malicious environments, and resources of nodes are limited. It is very important to ensure the ability of WSNs to fulfill critical services in a timely manner to end users in the presence of failures and/or attacks. Survivability is developed to guarantee critical services[3].

Survivability[4-8] is commonly defined as the ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures. In recent years for improving the ability of recovering from failure and attack a variety of survivable approaches are proposed. In order to determine whether these approaches achieve their goal, we need to evaluate them. Evaluation results can be used as a guideline to design or deploy survivable WSNs.

Our motivation is to develop a trusted, fast, and easy-to-use evaluation approach of survivability of WSNs. At present there are two types of evaluation approaches of survivability of WSNs: simulation[9-11], model-based analysis technology[12-26]. The latter usually models the evolution of behavior of WSN as a finite state transition system including Continuous Time Markov Chain(CTMC), Semi-Markov Process(SMP), etc. Two major problems in existing model-based analysis approaches are that:(1) The developed model can only describe the evolution of behavior of a single node, but not the entire network; Computation of survivability indicators depends on the statistical regularity of node distribution and the topology of WSN. However, these two dependent objects change anytime resulting in the invalidity of model. Following evaluation of survivability offers no value for designers of WSNs.

Stochastic model checking[27] is an automatic verification technique of finite state systems. Here, automatic verification means that if the model and the property to be verified are provided, stochastic model checking will call pre-designed algorithms to verify the property automatically. Therefore stochastic model checking is fast, trusted, and easy-to-use. Inspired by stochastic model checking in this paper we will develop an automatic approach to evaluating survivability of WSNs. We summarize the contributions of this work as follows:

1) We propose a CTMC to model the evolution of behaviors of a single node when failure and attack occur. Further a parallel composition of two or more single nodes’ model is proposed to model the entire network. The analysis of survivability of WSNs based on the parallel composition does not depend on the statistical regularity of node distribution and the topology of WSN because it can depict the connectivity between different nodes.

2) PRISM[28] is the best advanced stochastic model checking tool at present. In order to compute survivability indicators automatically with PRISM, we develop an algorithm to map the initial deployment of a WSN to the parallel composition expressed with the modeling language of PRISM.

By using CSL we formalize survivability indicators such as k-connectivity, steady availability, etc. The way to formalize survivability indicators by using logic systems makes us focus on the meaning of indicators, not how to compute these indicators.
2 Related Work

Survivability has been analyzed extensively for wired and infrastructure wireless networks. However, only a few survivability studies were made for WSNs because resources in every sensor node are limited, and the statistical regularity of node distribution and the topology of WSN change anytime.

Petridou et al. are the first to use stochastic model checking to evaluate survivability of WSNs[26]. Their basic idea is the same with us, that is to model the evolution of behavior of network with CTMC, formalize survivability indicators with CSL, and compute survivability indicators with the help of PRISM. Works by Petrido et al. and us are quite different, in two big ways. The first one is that Petrido et al’s work only applies to WSNs with star topologies, while our work is unrelated to topologies, i.e., our work applies to WSN with an arbitrary topology. The second one is that Petrido et al. take an abstract and top-level modeling approach which can not character effects of failure and attack accurately. For example, Petrido et al. think effects of balckhole attack on network connectivity in dense and underdense areas are the same.

Xing et al. focus on the survivability of wireless ad hoc networks with node misbehaviors and failures[14].Topology connectivity is a critical index for the survivability of wireless ad hoc networks. Xing et al. propose a novel SMP to characterize the evolution of node behaviors, and obtain the lower and upper bounds on the topology survivability for k-connected networks by derivation. However, Xing et al. assume that nodes are uniformly and randomly distributed on a 2D, i.e., Poisson distribution. Once node distribution changes or is not a Poisson distribution, i.e., the assumption does not hold, the evaluation of sur- vivability has no value. In addition, although modeling node behavior with SMP avoids the assumption that networks satisfy Markov property, for transient e- valuation indexes the complexity of their calculation is very high. For other evaluation indexes except topology connectivity Xing et al. do not present cor- responding evaluation methods. Zhipeng et al. extend works in [14] by assuming that node distribution satisfies binomial model or negative binomial model.

In summary, models adopted by the existing model-based analysis technol- ogy can be divided into two types: CTMC[12,13,16,17,20,24,25,26] and SM- P[14,15,18,19,21,22]. Both models are just for fixed network topologies, for example, models in [12,16,17,19,20,26] are oriented toward star and flat topologies, models in [13,15,23,24,25] are oriented toward cluster-based structure. However, topology can change anytime such that models no longer apply. Calculation of evaluation indexes also assumes that node distribution satisfies certain statistical regularity. However, in general it is very difficult to find a proper statistical regularity to characterize node distribution. Even if we find this statistical regu- larity, node distribution can change at any moment. We hope that our paper can provide a model which does not depend on the topology and statistical regularity of node distribution, and a method to automatically calculate as many evalua- tion indexes as possible such that ordinary engineers in the field of network can evaluate the survivability of WSNs easily.
3 Problem Formulation

At present there’s no universal definition of survivability. Intuitively survivability refers to the ability for a network system to provide essential services to end users in the presence of failures and/or attacks, and to recover full services in a timely manner. In order to achieve the evaluation of survivability it must be defined mathematically. Knight et al. are the first to give a mathematical definition of survivability[7]. They characterize evolution of behaviors of system as a finite state-system defining tolerable service transitions. Survivability is defined as the degree that tolerable service is satisfied by the finite state-system. However Knight et al. do not present how to model systems, how to evaluate survivability.

The model-based analysis technology consists of two aspects: modeling evolution of behaviors of system, computing survivability indicators. Therefore, modeling and computation are key technologies to perform evaluation of survivability. Inspired by these two key technologies, we give the following mathematical definition of survivability of WSNs.

Definition 1(Survivability Specification of WSN). A survivability specification of WSN is a four-tuple (W, M, I, P), here W is a WSN, M is a finite-state machine characterizing evolution of behaviors of WSN under failure and attack, I is a set of indicators, P is a function computing the probabilities that M satisfies each element of I.

3 Conclusion

This paper develops a framework to evaluate survivability of WSNs automatically. Firstly, we propose a CTMC to characterize evolution of behaviors of single node in WSNs under failure and attack. Then a parallel composition of CTMC is proposed to characterize evolution of behaviors of WSNs under failure and attack. Finally, in order to perform automated calculation of survivability indicators, we develop an algorithm to map the initial deployment of WSN to the evaluation model of network described by the modeling language of PRISM, and present how to use CSL to formalize all kinds of survivability indicators.

References