Comparative Analysis on Survivability Issues of Wireless Sensor Networks

Haitao Wang[1a], Lihua Song[2], Hui Chen[1], Shicai Zhu[3], Qiang Hu[3]

[1] Information Management Center, PLAUST, Nanjing 210007

[2] College of Command Information Systems, PLAUST, Nanjing 210007

[3] College of Communications Engineering, PLAUST, Nanjing 210007

[a]E-mail:haitmail@126.com

Keywords: Wireless Sensor Network; Network Survivability; Ad hoc Network; Fault Tolerance

Abstract. Survivability of wireless sensor network (WSN) is not limited to traditional network security and reliability issues, but from a new perspective of wireless sensor network in a variety of network services and security capabilities. In this article wireless sensor networks and their applications are introduced firstly. Then relevant works on the survivability problems of WSN are summed up and the characteristics of WSN survivability are discussed. Next, comparison and analysis on survivability of Ad hoc network and wireless sensor network is given. Finally, technical challenges WSN face and possible solutions are expatiated.

Introduction

Wireless sensor network (WSN) is a special wireless network, integrating network technology, communications technology, embedded computing and sensor technology. In WSN nodes have information sensing, processing and carrying capacities, and they can collaborate to monitor particular object areas and complete special data collection tasks. In addition, WSNS can interconnect with other networks via sink nodes to achieve information share and transfer. The general framework of WSNs is shown in figure 1.

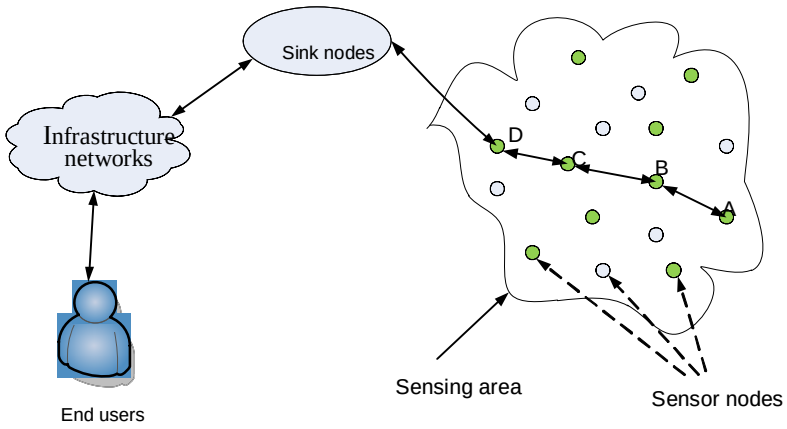

Fig.1 General framework of wireless sensor networks

With the extensive applications of WSNs [1], user requirements for network services performance (including security, reliability, security and so on) are becoming higher than before, especially for military applications. Currently, most of security works of WSN are limited to

traditional security technologies, such as information encryption, invasion prevention and invasion detection, etc. However, nodes in WSN are often deployed in remote or danger areas, and energy, storage space and processing capacity of the sensor node is very limited. These features make sensor nodes suffer from attacks and faults easily, and even cause network paralysis, thus inevitably affecting network availability and security. Therefore, how to provide basic network services under the conditions of wireless sensor networks are suffering from attacks, malfunctions and accidents is vital, that is to ensure the survivability of wireless sensor networks.

Basic definitions and relevant works

Research works on network security has experienced three phases: intrusion prevention, intrusion detection and survivability studies [2]. For survivability, there is no clear definition in academic circles, but a popular definition is given by CMU/SEI research group [3]: Survivability means at the time of attacks, failures or accidents, the system have the ability that it can complete its critical mission in time. The central idea of network survivability is that the system can tolerate a variety of potential threats, including a variety of attacks, failures and accidents and when the system suffered failure or after a short interruption it can restore basic services within a certain response time, guaranteeing the basic properties of the system and ensuring the capability of key services. That is to say, network survivability is not limited to traditional network security and reliability, but from a new perspective to examine the ability to provide service and ensure security in a variety of circumstances.

To date, researches on survivability of WSN have some achievement, mainly including network structure, secure routing protocol, survivability evaluation methods and evaluation models. Currently, works on wireless sensor network survivability mainly concentrate on two aspects: security issues and efficient energy-saving schemes [4]. In security field, encryption, message authentication and security protocols are adopted to ensure data confidentiality and integrity and improve the anti-invasion capacity of the system [6]. For example, SPINS security solution used SNEP (Secure Network Encryption Protocols) and μTESLA protocols to improve network security. In μTESLA protocol, the exposure time of the symmetric key is delayed, providing a efficient broadcast authentication method. In literature [7], the circular wireless sensor network is divided into concentric circles of different radii, and the strategy of mixing single-hop transmission and multiple-hop transmission is proposed. This scheme achieved energy balanced consumption and solved the energy hollow problem existed in wireless sensor network, thus extending the lifetime of the WSN greatly. However, wireless sensor network suffers from a variety of security attacks and the network environment is complex, these factors make traditional security technologies cannot effectively resist external threats and attacks. When WSN is attacked and destroyed, high survivable wireless sensor network should still complete basic missions and offer vital services, such as collecting sensed data and transmitting data to outside users in a safe way. In brief, architecture design, modeling technologies, assessment methods and the enhancement strategies of WSN are in initial stage.

Characteristics of WSN survivability

Compared to other networks, survivability of wireless sensor network must consider the following factors:

1) Lifetime: Sensor nodes mainly rely on the limited battery energy, and the battery cannot be replaced or charged easily in many circumstances. Thus, the most important factor to consider is the

lifetime of the network.

2) Fault tolerance and invulnerability: In WSN the number of sensor nodes is very large, the node density is high and the environment of those nodes is very severe. Further, most nodes must operate autonomously and adjust their behaviors adaptively. Therefore, WSN demands high fault tolerance and invulnerability.

3) Self-healing ability: WSN should detect the damage state timely and can delay or prevent the system failure caused by internal and external attacks. In addition, it can automatically reconfigure e resources after parts of the network paralysis to restore the fundamental service of WSN.

4) Robustness and scalability: In WSN robust channel access and routing protocols are needed to improve network service ability under the limited energy, various hardware and software faults and unreliable communication links. Besides, clustering and hierarchical network structure should be adopted considering the network scalability and coverage areas.

5) Response time: No matter whether WSN is suffered from attacks, faults or accidents, the missions should be completed within the time required by the system or users.

In different applications, factors impacting wireless sensor network survivability are different. Appropriate survivable technologies should be selected to improve the survivability of the system accordingly. In particular, main factors influencing WSN survivability different applications are depicted in table 1.

Table 1 Main factors impacting WSN survivability in various applications

Applications	**Main factors**
military surveillance	Security, reliability, robustness, fault tolerance, information timeliness and self-healing ability
logistics tracking	Reliability, scalability and security
environment monitoring	Reliability, lifetime, invulnerability, robustness and self-healing ability
medical health	Reliability, timeliness, security and privacy

The survivability of WSN focuses on the integrated performance of the system. Different form traditional networks, high survivable WSN has the following distinct traits.

1) Resilience: Resilience reflects the recovery capability of network system. The greater the resilience of a system, its recovery ability is more powerful. WSNs are usually deployed in dangerous or harsh environments, vulnerable to attacks, damages or accidents, high resilience can assure that the network recovers its service capability in time after the attack, destroy or accident, and continue to provide key services for users.

2) Collaboration: Many tasks need collaboration among sensor nodes to complete in WSN. Collaboration ensures nodes can communicate and share data each other to collect comprehensive and accurate data. Then, nodes process and relay these data to outside users. Meanwhile, even when WSN suffers from faults or attacks, collaboration among sensor nodes can facilitate network reorganize and reconfigure to restore network connectivity and maintain basic services.

3) Adaptability: Adaptability is the key to improve the self-healing ability of WSN. Based on cognition, WSN can reasonably allocate tasks according to different characteristics and abilities of various nodes to improve network survivability. In addition, network topology and node transmission power can also be adjusted in terms of application environment and user requirements.

Comparison of MANET and WSN survivability

The operating environments of wireless sensor network are usually adverse without user intervenes, and sensor nodes are powered by battery which cannot be recharged or replaced easily. So the most important performance index of WSN is to minimize energy consumption or maximize the lifetime of the network [7]. However, energy is not a big issue in mobile ad hoc network (MANET), it tries to pursuit minimal data transmission delay and higher quality of service (QoS). Therefore, there is a significant difference between survivability of WSN and MANET [8], as explained in the following.

1) The number of nodes in WSN is very large and the network environment is more complex, so the probability of some nodes fail is high. Sensor nodes are deployed in special regions to collect environmental data and they usually need to work for months even several years, so network scalability and stable working conditions are particularly important.

2) Energy of nodes in MANET can be provided continuously, but sensor nodes are limited by energy supply, processing power and storage space. The primary factor of WSN survivability is to take most advantage of the limited energy to maximize the network lifetime.

3) WSN is faced with more serious security problems and even can be captured. High collaboration among nodes and dynamic system reconfiguration are needed to ensure the completion of basic network tasks.

4) Compared to MANET, most nodes in WSN are stationary and network topology changes infrequently. So clustering network structure is more suitable for WSN to reduce system overheads and improve network scalability.

5) Unlike MANET, point to point communication mode is not adopted in WSN. In order to speed up information transmission rate and save energy, multicast and broadcast communication modes are popular in WSN, leading to severe channel access competition, influencing communications effectiveness and reliability.

Technical challenges and countermeasures of WSN survivability

As depicted above, the limited energy, serve working environment and high node density make the survivability of WSN is faced with more technical challenges, mainly reflected in the following aspects.

1) The limited energy, short communication distance and low processing and storage capacity which have negative impacts on the survivability of the WSN. Therefore, how to utilize Nash equilibrium in game theory to coordination behaviors of sensor nodes and various protocols of different network layers to maximize network service performance is one of the challenges faced by WSN survivability.

2) Open wireless transmission media and harsh network environment make sensor nodes are vulnerable to hostile electromagnetic interference leading to intermittent network connectivity. Thus how to improve anti-interference ability is one of WSN survivability challenge.

3) WSN suffers from failure and intrusion more easily and parts of the system can be destroyed or paralyzed. So, how to continuously offer basic network services within specified response time, improve fault tolerance and self-healing ability of WSN is another challenge.

In order to overcome the survivability challenges faced by wireless sensor network, the following strategies can be adopted to improve the survivability of WSN.

Firstly, sensor nodes can increase the capacity of battery and improve the performance of CPU, memory and functions of wireless communication chip to reduce power consumption. Further,

energy saving aware network encoding and channel access technologies can be developed.

Secondly, at the network layer, low power consumption and high adaptive routing protocols and sleep-wake switch mechanism are designed to achieve energy dynamic management and adapt to the complex network environment of WSN. Redundant nodes can work alternately to prolong the network lifetime. On the other hand, the effective network coverage, topology control and data aggregation technologies are proposed to meet the requirement of network connectivity, coverage and the information transfer reliability.

Thirdly, network security technologies are adopted to improve the intrusion detection and defense abilities, such as anti-jamming communication at physical layer, the encryption technology at network layer, the authentication technology at transport layer. These methods are integrated reasonably to ensure the availability, data integrity, confidentiality and non-repudiation of network.

In addition, data caching and replication mechanisms can be utilized to prevent data corruption or loss caused by network failures or attacks. Efficient multi-path routing protocols can be taken to enhance the robustness of network. When the network topology changes it can update the route (select other available route) immediately to continue offering network services.

Conclusions

So far, researches on WSN have made great progress, but relevant achievements on survivability are relative less [9]. The survivability of WSN goes beyond traditional security issues, emphasizing continuous provision of network services even when the network are attacked or destroyed. Due to limited energy, open transmission medium and vulnerable to security attacks, how to enhance network intrusion tolerance and self-healing capability to improve network survivability still need to be studied systematically in future.

Acknowledgment

This paper is supported by NSFC (NO: 61072043) and Pre-research Project of PLAUST.

References

[1] Xu Yi. Wireless sensing network theory and method[M]. Beijing: Tsinghua University publishing house, 2012.

[2] Hongzhi Zhang,Yu Qing, Li Xuegan. Research progress of the network survivability [J]. Computer Engineering, 2005(10):3—5.

[3] Vickie R，Westmark．A Definition for information System Survivability [C]．In：Proceeding of the 37th Hawaii Internal Conference on System Science (HICSS'4)，Track 9．

[4] Xueping Li, IEEE, and Dengfeng Yang．A Quantitative Survivability Evaluation Model for Wireless Sensor Networks[J]．IEEE,2006:727—732．

[5] Akyildiz I F, Su Weilian．A survey on sensor networks [J], IEEE Commun Mag，2002,40(8) :

104-112 .

[6] Liu Hao, Tang Peihe. Energy balanced transmission strategies in WSN [J], Computer Engineering and applications, 2010,46(33):112—114 .

[7] LU Gang, ZHOU Ming-Tian, SHE Kun, et al. Lifetime Analysis on Routing Protocols of Wireless Sensor Networks[J]. Journal of Software, 2009,20(2):375-393.

[8] Chan H, Perrig A, Song D. Random key pre-distribution schemes for sensor networks[C]. In Proceedings of the IEEE Computer Society Symposium on Security and Privacy. Piscataway, USA: IEEE, 2003:197-213.

[9] Vahid Mavaji, Bahareh Abbasi. Survivability Evaluation in Wireless Sensor Network[C]. 2011 3rd International Conference on Advanced Management Science, IACSIT Press, Singapore, 2011(19):212-216.