Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 147 (2019) 210–216

Procedia Computer Science

www.elsevier.com/locate/procedia

2018 International Conference on Identification, Information and Knowledge in the Internet of Things, IIKI 2018

Challenges and Security Issues in Underwater Wireless Sensor Networks

Guang Yang[a]*, Lie Dai[a], Guannan Si[a], Shuxin Wang[a], Shouqiang Wang[a]

[a], *Shandong Jiaotong University, School of Information Science and Electrical Engineering, 5001 Haitang, Jinan 250357, China*

Abstract

With the advances in technology, there has been an increasing interest from researches and industrial institutions in the use of Underwater Wireless Sensor Networks (UWSNs). Constrained by the open acoustic channel, harsh underwater environment and the particularities of itself, UWSNs are vulnerable to a wide class of security threats and malicious attacks. A survey on threats, challenges and security issues of UWSNs are presented in this paper. In addition, current security researches and mechanisms are presented and discussed.

Peer-review under responsibility of the scientific committee of the 2018 International Conference on Identification, Information and Knowledge in the Internet of Things.

Keywords: underwater communication, underwater wireless sensor networks, security, UWSNs

1. Introduction

Underwater wireless sensor networks (UWSNs) have proven strength in various underwater applications of ocean monitoring, resource exploration, surveillance and military in harsh underwater environment [1][2]. The existing researches are mainly focused on communication, self-organization, connectivity, processing capabilities,

* Corresponding author. Tel.: +86-531-827-35707; fax: +86-531-827-35707
E-mail address: yangguang@sdjtu.edu.cn

Peer-review under responsibility of the scientific committee of the 2018 International Conference on Identification, Information and Knowledge in the Internet of Things.
10.1016/j.procs.2019.01.225

adaptability and low energy consumption. Unfortunately, these researches are constrained for countering against security threats in UWSNs because the resources are much more constrained while security situation is more server due to the characteristics and networking environments [3].

The remainder of this paper is organized as follow. In Section 2, the peculiar characteristics of UWSNs and underwater acoustic network environment are introduced. The threats and challenges in UWSNs are discussed in Section 3. The security requirements are described in Section 4. The current security researches for UWSNs are presented in Section 5. Finally, Section 6 concludes the paper.

2. Particularities and Constraints

As a branch of wireless sensor networks (WSNs), some particularities of UWSNs are similar [4][5]. But due to the harsh working environment, there are some especial particularities and constraints, which are outlined as below.

Extremely Limited in Hardware Resources: Underwater sensor nodes are extremely limited in hardware resources, including energy, computational capability and storage space. Due to higher distances and to more complex signal processing at the receivers to compensate for the attenuation of the signal, the power consumed for underwater acoustic communication is much higher than in terrestrial radio communication. Underwater sensor nodes are deployed in shallow or deep water, where it is inconvenient to charge or replace the nodes' battery. To prolong the network lifetime, the computational capability and storage space are constricted. Hence, virtually all current researches for UWSNs focus on saving energy consumption at the expense of capability and security.

Unreliable Communication Channel: Underwater acoustic channel is temporally, spatially variable, bandwidth limited and dramatically depends on both transmission range and frequency. The farther the communication distance, the lower the bandwidth of acoustic channels, most acoustic systems operate below 30 kHz. The underwater acoustic channel is significantly affected by water temperature, path loss, noise, multipath effect, and Doppler spread [2]. All these factors cause high bit error and delay variance, which result in packet loss probability and high node failure rate. Moreover, the open underwater acoustic channel is shared by nodes within the communication range, which means that an attacker can passively intercept and analysis packets and even worse actively disrupt network services. Hence, it is a great challenge to protect UWSNs from eavesdropping and other malicious attacks.

Dynamic Network Topology: While terrestrial sensor nodes are densely deployed, in underwater, the deployment is deemed to be sparser, due to the cost involved and to the challenges associated to the deployment itself. Majority of underwater sensor nodes are mobile due to water flow. From empirical observations, underwater objects may move at the speed 2-3 knots of or 36 km/h in a typical underwater condition [1], which results in a highly dynamic network topology. Moreover, to expand the monitor and communication region, Autonomous Underwater Vehicles (AUVs) are widely utilized in many applications.

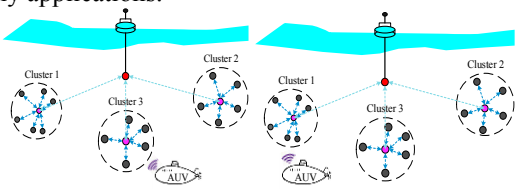

Fig. 1. (a) AUV join in Cluter3; (b) AUV join in Cluter1

The AUVs may frequently join and exit the cluster or network, which also will result in a highly dynamic topology. As shown in Fig.1(a), the AUV joined Cluster 3 as a cluster member node. As shown in Fig.1(b), the AUV is out of the communication range of Cluster 3, and then join Cluster 1 as its member node. These changes of the network topology may change the data routing and influence the accuracy rate of data transmission.

Unsecure Environment and Vulnerability: For some specific fields of application, for example, underwater security monitoring and target tracking, the working environment of UWSNs may not be secure. The underwater sensor nodes are deployed to monitor hostile objects in high seas or hostile sea regions. Consequently, these nodes could become highly vulnerable to threats and malicious attacks.

In general, UWSNs nodes could be physically damaged to be invalid and are also vulnerable to marine organism. As mentioned above, sensor nodes may be deployed at harsh and unattended deep sea, which means that it is unable to guard each node from potential physical damages.

3. Threats and Challenges

As discussed in Section 2, UWSNs are suffer from many constraints. Hence, UWSNs are vulnerable to various threats and malicious attacks. According to actions taken by the malicious attacker, attacks can be passive or active.

3.1. Passive Attacks

The passive attacks refer to the attempts that are made by malicious nodes to perceive the nature of activities and to obtain data transmitted in the network without disrupting the operation. For example, eavesdropping, interfering, leakage of secret information, impersonation, message replay, and message distortion. Moreover, the attacker may capture the packets and then predict the nature of communication by analyse the traffic, observe the exchange of the packets, identify communicating hosts, and determine the location. It is difficult to detect these passive attacks, since the network operation is not affected by passive attacks. To prevent this problem, the best solution is encryption mechanisms which making it hard for eavesdroppers to gain any information.

3.2. Active Attacks

The active attacks attempt to alter, inject, delete or destroy the data transmitted in the network. Active attacks may intercept data, and attempt to modify or drop packets which can be executed by internal or external malicious attackers. The external attacks carried out by nodes that do not belong to the network, which would be easier to detect and defend. The internal attacks are from insider nodes, and can cause considerable damages. It is unfeasible to detect and isolate a malicious node from disrupting the network which disguised as a normal node. Moreover, some internal attacks may come from compromised nodes which are actually part of the network. Hence, internal attacks are more difficult to detect and may cause more severe damages. To prevent this problem, the best solution is using security mechanisms such as encryption, authentication and trust management. According to the aim of attacks, active attacks can be classified as below [6].

Node compromise attacks: In some specific fields of applications, underwater sensor nodes may be deployed in unattended and even worse hostile sea regions. Moreover, the network may consist of tens or hundreds of nodes deployed in large scales, which means that it is unable to ensure the safety of all nodes. An attacker may capture, crack and compromise nodes to read or modify data from memory. And even worse, the compromised nodes may be injected to the network as a legitimate node to monitor or disturb, which can cause more severe damages.

Repudiation attacks: In repudiation attacks, malicious nodes deny having any involvement in particular action or communication with other nodes. Refers to the denial by a node involved in a communication of having participated in all or part of the communication, regardless whether that communication is malicious or not.

Routing attacks: Routing attacks can cause packets unable to be transferred to the destination node, and even worth disrupt the operation of the network. These types of attacks are mounted on the routing protocols, such as routing table overflow, routing table poisoning, packet replication, and rushing attacks. Through these malicious behaviours, attackers can attract packets and analyse or even drop packets at its will. Cryptographic techniques are often used to defend routing attacks. However, the usage of encryption not only increases the size of communication messages but also cause more energy consumption due to high computational complexity.

DoS attacks: DoS is a kind of active attack that attempts to make resources unavailable to the legitimate nodes. The attacker tried to prevent legitimate nodes to access services offered by the network. DoS attacks can be carried out in many different ways, but in the end causing the same problems.

Among these active attacks, DoS attacks are more destructive and hard to detect [7]. To prevent UWSNs from DoS attacks, the attack approaches should be comprehended. DoS attacks can be launched in different ways and at any layer of the protocol stack. Even if UWSNs are well protected by encryption technology, it is still threatened by DoS attacks, which can disrupt communication and cooperation between nodes and decrease availability of the

whole network. Moreover, Dos attacks are low cost, deadly and even worse, hard to detect. Malicious attackers can cause severe damages with very low cost, impersonate as a legitimate node to deceive neighbour nodes, or impose particularly high power cost tasks to legitimate nodes to shorten the nodes lifetime [8]. According to the UWSNs network model, DoS attacks and the solutions for the defence were discussed in our previous work [9].

4. Security Requirements

As a branch of WSNs, the security requirements of UWSNs are similar to terrestrial WSNs [4]. But due to the particularities and constraints of UWSNs, there are also some special security requirements.

Confidentiality: It concerns preventing unauthorized nodes from understanding the contents of the sensitive data (e.g. security credentials and secret keys). Confidentiality is not restricted only to survivability of user's information (e.g. strategic or tactical military information), but also to the survivability of the MAC, routing information, etc. These sensitive data should be prevented from read or tampered by malicious attacker. Confidentiality can be achieved by applying low power efficient encryption technique which is suitable for UWSNs. The Cipher Text Stealing (CTS) technique [10] is a lightweight typical encryption technique used in UWSNs.

Authentication: As discussed above, the acoustic channel is open, moreover, without encryption technique the malicious attacker can easily capture packets and modify the content. Hence, receiving node needs to identify the source of the data to filter malicious attacks. Nodes need to have authorization to access and share channel, services, applications and data on that network. Intrusion detection and trust management mechanism can be utilized to identify abnormal activities to remove malicious nodes from the network. These mechanisms ensure that only the authorized nodes have the permission to perform in the network.

Integrity: Data integrity is to ensures that the received data is not modified, removed, or corrupted in transition by unauthorized nodes either by radio failure or malicious attack. This is most essential in circumstances such as military operations and equipment controls where such changes could cause serious damages. The Message Authentication Code (MAC) [11] for data authentication has been widely applied in WSNs and UWSNs, which has good scalability, low latency, reliability, adaptability and ease of implementation.

Freshness: Freshness is to ensures that the received data is fresh and it is not retransmission of legacy data. Routing updates should be delivered in real time. The delay of the update messages might reflect the wrong state of the network and lead to a large loss in information.

Availability: Availability is to ensures that the network must be robust enough. Even if some nodes failed or the system is attacked, it will still be able to provide services. Proper redundancy tactic and self-adaptive tactic can supply availability for UWSNs.

Isolation: Isolation is to ensures that nodes should be able to identify abnormal activities and remove malicious nodes. Moreover, MAC protocols, routing protocols should be immune to malicious attacks. Proper trust management and lightweight cryptography algorithms should be used to isolate malicious nodes.

Self-stabilization: Self-stabilization is to ensures that nodes should be able to recover from attacks independently in real time without intervention. If node is self-stabilizing to malicious attacks, it can recover to normal state by itself, even if the attacker remained in the network.

Survivability: This is the capability of the system to fulfill its mission in a timely manner, in the presence of accident, failure, intrusion or malicious attacks. It is to ensures that the network can restore and maintain essential services during and after malicious attacks, even if part of the network had been destroyed.

5. Security Issues of UWSNs

As discussed in Section 3, UWSNs are vulnerable to various threats and attacks. To achieve the objectives of the security requirements, a set of mechanisms and security technologies must be proposed to prevent UWSNs from attacks. According to the OSI network, the security issues of UWSNs are logically divided into separate components. As shown in Fig.2, the security architecture of UWSNs can be divided to four layers, physical layer, link layer, transport network layer and application layer. The security issues mainly include: key management, intrusion detection, trust management, secure localization, secure synchronization, and routing security.

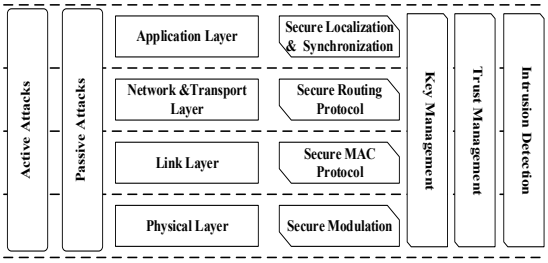

Fig. 2. Security architecture of UWSNs

1) Key management

The main goals of cryptography and key management are confidentiality, authentication, integrity, and non-repudiation. Cryptography enables sensitive information to be stored or delivered in unsecure networks such as the underwater acoustic channel so that it cannot be read or modified by unauthorized users. Due to the peculiar particularities and constraints of UWSNs discussed in Section 2, the encryption and key management mechanisms for WSNs consume bandwidth and energy, and make these primitives unsuitable for very resource-constrained UWSNs. Related researches about cryptography were presented for UWSNs [11-19]. Unfortunately, the existing cryptography and key management mechanisms are suffering from some problems, including cipher text expansion and computational complexity. Message padding and codes increase the length of message after applying cryptography and cause more energy consumption on transmission and computation [20]. Digital signature is usually used for message authentication. A digest is appended to an authenticated message, which will cause expansion and communication overhead [21].

2) Intrusion detection

Intrusion detection mechanisms is to detect, identify and isolate internal or external intruders from the network. However, intrusion detection mechanisms usually work after the malicious attacks took effect and been discovered. It is difficult to detect malicious intruders at the first time that attacks took effect. Hence real-time detection mechanisms need to be researched and improved. Alternatively, intrusion tolerance mechanisms can be used to protect networks while allowing the existence of malicious intruders., which is considered to be an efficient security mechanism. Moreover, algorithms technologies and Intrusion Detection Systems (IDS) have been proposed to further improve UWSNs security. In standalone IDS, there is no data exchanged between nodes; each node runs IDS and detects attacks independently. In distributed and cooperative IDS, every node participates in intrusion detection by having local and global detection decision-making. Hierarchical IDS is suitable for multilayered UWSNs, in which the cluster head nodes perform the task of IDS and act as checkpoints such as routers in wired networks. Among these kinds of IDS, the hierarchical IDS is suitable for UWSNs based on cluster structure.

3) Trust management

As an important complement to security defense based on cryptography, trust management mechanism has significant advantages in intrusion detection. Due to the peculiar particularities and constraints of UWSNs, the research on trust management mechanisms in UWSNs faces more challenges [22]. The existing trust management mechanisms can be classified into three categories: centralized scheme, distributed scheme, and hierarchical scheme. In centralized scheme, a root node or a base station supply trust management for each node in the network. The centralized schemes are inappropriate for UWSNs, because the energy consumption of trust values exchanging between sensor nodes and the base station is an expensive burden. In distributed scheme, each node needs to compute and maintain the trust values of entire network. But it is impossible for UWSNs, because underwater sensor nodes are extremely limited in hardware resources. Hence, the distributed schemes are also inappropriate for UWSNs. As discussed above, it is obvious that neither pure centralized nor pure distributed schemes are suitable for UWSNs. In hierarchical schemes, the computation and transmission of trust value is implemented in a hierarchical way. The trust values are passed and merged from lower layer to upper layer. Therefore, the hierarchical schemes are more appropriate for cluster-based topology which was widely used in UWSNs. In order to broadcast control information and retrieve the readings from the underwater sensor nodes, sink node must be able to authenticate itself.

4) Localization security

Location estimation is a vital component in source detection and tracking applications. The underwater sensor nodes get the location information and speed of mobile nodes during the localization phase, which would be used to select the best relay node to forward data. Without the location information, the sink node cannot identify where the received data comes from. Due to the characteristics of underwater channel, localization protocols proposed for WSNs cannot work in underwater applications [23]. Some localization-specific attacks e.g. Sybil attack, black hole attack and wormhole attack can cause great damages by utilizing or modifying the localization information. Most of existing localization protocols do not take security issues into account when designing. The secure localization scheme should be able to determine the location of sensors even in the presence of Sybil and wormhole attacks, and the scheme should be able to node mobility in UWSNs. To defend against injecting false localization information in UWSNs, effective and efficient cryptographic algorithms need to be developed [24-26].

5) Synchronization security

Synchronization is essential in many underwater applications and scheduling MAC protocols. As discussed in Section 2, due to the characteristics of UWSNs, synchronization security protocols proposed for WSNs are unsuitable for UWSNs. Moreover, it is especially difficult to achieve precise time synchronization in underwater environments. Although it is critical in the UWSNs issues, none of the existing time synchronization schemes [27-28] took security in consideration. To defend time synchronization attacks e.g. masquerade, replay and manipulation attacks, proper cryptographic techniques can be used. However, the countermeasures against delay attacks for WSNs proposed [29-31] are not applicable to UWSNs.

6) Routing security

The routing security consists of basic transports and connectivity security mechanisms applied to routing protocols as well as the individual nodes. Moreover, nodes must exchange information about their neighbors to construct the network topology in order to apply one of the routing protocols (Proactive, Reactive and Hybrid). Routing security involves two aspects: secure routing and secure data forwarding. In secure routing, nodes are required to cooperate in order to share correct routing information, thus keeping the network connected efficiently, whereas in secure data forwarding, data packets must be protected from tampering, dropping, and altering by any unauthorized party. In recent years, some researches are presented to supply routing security for UWSNs [32-34].

6. Conclusion

In this article, the challenges, threats and security issues in UWSNs are discussed. The peculiar particularities and constraints of UWSNs and underwater environment are analyzed. UWSNs are vulnerable to a wide class of security threats and malicious attacks, which severely disturb the communication and cooperation of the network. To avoid these attacks, the security requirements of UWSNs are introduced. Finally, some specific security technologies and security schemes are discussed. As discussed in this article, it is not easy to secure UWANs due to the peculiar particularities and constraints. Moreover, applications may have different requirements on security, and excessive security schemes will be a heavy burden for energy consumption. Hence, how to take into account these features in security scheme design is also an important issue in the future researches.

Acknowledgements

This work is supported by the national Natural Science Foundation of China (Grant no. 61601264) and A Project of Shandong Province Higher Educational Science and Technology Program (Grant no. J15LN13) and Shandong Province Natural Science Foundation (ZR2015FL013).

References

[1] Cui J H, Kong J, Gerla M, et al. Challenges: building scalable and distributed Underwater Wireless Sensor Networks (UWSNs) for aquatic applications[J]. *Channels*, 2005, **45(4)**: 22-35.

[2] Akyildiz I F, Pompili D, Melodia T. Underwater acoustic sensor networks: research challenges[J]. *Ad hoc networks*, 2005, **3(3)**: 257-279.

[3] Heidemann J, Ye W, Wills J, et al. Research challenges and applications for underwater sensor networking[C]//Wireless Communi-cations and Networking Conference, 2006. *WCNC 2006. IEEE*., 2006, 1: 228-235.

[4] Lopez J, Roman R, Alcaraz C. Analysis of security threats, requirements, technologies and standards in wireless sensor networks[M]//*Foundations of Security Analysis and Design V*. Springer, Berlin, Heidelberg, 2009: 289-338.

[5] Perrig A, Stankovic J, Wagner D. Security in wireless sensor networks[J]. *Communications of the ACM*, 2004, **47(6)**: 53-57.

[6] Wood A D, Stankovic J A. Denial of service in sensor networks[J]. *Computer*, 2002, **35(10)**: 54-62.

[7] Raymond D R, Midkiff S F. Denial-of-service in wireless sensor networks: Attacks and defenses[J]. *IEEE Pervasive Computing*, 2008 **(1)**: 74-81.

[8] Hu Y C. A defense against wormhole attacks in wireless networks[J]. *IEEE INFOCOM* 2003, Mar., 2003.

[9] Cong Y, Yang G, Wei Z, et al. Security in underwater sensor network[C]//*Communications and Mobile Computing (CMC)*, 2010 International Conference on. IEEE, 2010, 1: 162-168.

[10] Law Y W, Doumen J, Hartel P. Survey and benchmark of block ciphers for wireless sensor networks[J]. *ACM Transactions on Sensor Networks* (TOSN), 2006, **2(1)**: 65-93.

[11] Bellare M, Canetti R, Krawczyk H. Keying hash functions for message authentication[C]//*Annual International Cryptology Conference*. Springer, Berlin, Heidelberg, 1996: 1-15.

[12] Jiang S M. Securing underwater acoustic networks: a survey[J]. *IEEE Commun. Surv*. Tutorials, 2017.

[13] Souza E, Wong H C, Cunha Í, et al. End-to-end authentication in under-water sensor networks[C]//Computers and Communications (ISCC), *2013 IEEE Symposium on. IEEE*, 2013: 299-304.

[14] Luo Y, Pu L, Peng Z, et al. RSS-based secret key generation in underwater acoustic networks: advantages, challenges, and performance improvements[J]. *IEEE Communications Magazine*, 2016, **54(2)**: 32-38.

[15] Dini G, Duca A L. A cryptographic suite for underwater cooperative applications[C]//Computers and Communications (ISCC), *2011 IEEE Symposium on. IEEE*, 2011: 870-875.

[16] Yuan C, Chen W, Li D. A Hierarchical Identity-Based Signcryption Scheme in Underwater Wireless Sensor Network[C]//*China Conference on Wireless Sensor Networks*. Springer, Singapore, 2017: 44-54.

[17] Hamid M A, Abdullah-Al-Wadud M, Hassan M M, et al. A key distribution scheme for secure communication in acoustic sensor networks[J]. *Future Generation Computer Systems*, 2018, **86**: 1209-1217.

[18] Ateniese G, Capossele A, Gjanci P, et al. SecFUN: Security framework for underwater acoustic sensor networks[C]//*Proceedings of MTS/IEEE OCEANS*. 2015: 1-9.

[19] Capossele A, Petrioli C, Saturni G, et al. Securing Underwater Communications: Key Agreement based on Fully Hashed MQV[C]//*Proceedings of the International Conference on Underwater Networks & Systems*. ACM, 2017: 12.

[20] Dini G, Lo Duca A. A secure communication suite for underwater acoustic sensor networks[J]. *Sensors*, 2012, **12(11)**: 15133-15158.

[21] Jiang S. Wireless Networking Principles: From Terrestrial to Underwater Acoustic[M]. Springer Singapore, 2018.

[22] Goyal N, Dave M, Verma A K. Trust model for cluster head validation in underwater wireless sensor networks[J]. *Underwater Technology*, 2017, **34(3)**.

[23] Chen K, Zhou Y, He J. A localization scheme for underwater wireless sensor networks[J]. *International Journal of Advanced Science and Technology*, 2009, 4.

[24] Han G, Liu L, Jiang J, et al. A collaborative secure localization algorithm based on trust model in underwater wireless sensor networks[J]. *Sensors*, 2016, **16(2)**: 229.

[25] Das A P, Thampi S M. Fault-resilient localization for underwater sensor networks[J]. *Ad Hoc Networks*, 2017, **55**: 132-142.

[26] Varadharajan K. SECURE LOCALIZATION USING COORDINATED GRADIENT DESCENT TECHNIQUE FOR UNDERWATER WIRELESS SENSOR NETWORKS[J]. *ICTACT Journal on Communication Technology*, 2018, 9(1).

[27] Liu J, Wang Z, Zuba M, et al. DA-Sync: A Doppler-assisted time-synchronization scheme for mobile underwater sensor networks[J]. *IEEE Transactions on Mobile Computing*, 2014, **13(3)**: 582-595.

[28] Liu J, Wang Z, Peng Z, et al. TSMU: A time synchronization scheme for mobile underwater sensor networks[C]//*Global Telecommunications Conference (GLOBECOM 2011)*, 2011 IEEE. IEEE, 2011: 1-6.

[29] Song H, Zhu S, Cao G. Attack-resilient time synchronization for wireless sensor networks[J]. *Ad Hoc Networks*, 2007, **5(1)**: 112-125.

[30] Boukerche A, Turgut D. Secure time synchronization protocols for wireless sensor networks[J]. *IEEE Wireless Communications*, 2007, **14(5)**.

[31] Du X, Guizani M, Xiao Y, et al. Secure and efficient time synchronization in heterogeneous sensor networks[J]. *IEEE transactions on vehicular technology*, 2008, **57(4)**: 2387-2394.

[32] Dini G, Duca A L. SeFLOOD: A secure network discovery protocol for Underwater Acoustic Networks[C]//*Computers and Communications (ISCC)*, 2011 IEEE Symposium on. IEEE, 2011: 636-638.

[33] Peng C, Du X. SDBR: A Secure Depth-Based Anonymous Routing Protocol in Underwater Acoustic Networks[J]. *International Journal of Performability Engineering*, 2017, **13(5)**: 731.

[34] Han S Y, Chen Y H, Tang G Y. Fault diagnosis and fault-tolerant tracking control for discrete-time systems with faults and delays in actuator and measurement[J]. *Journal of the Franklin Institute*, 2017, **354(12)**: 4719-4738.