[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks : a survey. Computer Networks 38(4):393–422, March 2002

[2] J. Yick, B. Mukherjee, and D. Ghosal. Wireless sensor network survey. Computer Networks, 52(12):2292–2330, August 2008

[3] X. Du and Y. Xiao. Chapter 17: A survey on sensor network security Springer Wireless Sensor Networks and Applications, 2008

[4] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Networks Journal, 1(2-3):293–315, September 2003

[5] A. D. Wood and J. A. Stankovic. Denial of service in sensor networks. IEEE Computer 35(10):54–62, 2002

[6] S. Madria and J. Yin. SeRWA: a secure routing protocol against wormhole attacks in sensor networks. Ad Hoc Networks Journal, Article in Press

[7] B. Parno, M. Luk, E. Gaustad, and A. Perrig. Secure sensor network routing: a cleanslate approach. In ACM CoNEXT, December 2006.

[8] F. Ye, H. Luo, S. Lu, and L. Zhang. Statistical en-route filtering of injected false data in sensor networks. In IEEE INFOCOM, Pages:2446–2457, 2004.

[9] L. Yu and J. Li. Grouping-based resilient statistical en-route filtering for sensor networks. In IEEE INFOCOM, Pages:1782–1790, April 2009.

[10] S. Zhu, S. Setia, S. Jajodia, and P. Ning. An interleaved by hop-by-hop authentication scheme for filtering injected false data in sensor networks. In IEEE Symposium on Security and Privacy, Pages:259–271, May 2004.

[11] H. Chan, A. Perrig, and D. Song. Secure hierarchical in-network aggregation in sensor networks . In ACM CCS, Pages:278–287, October 2006.

[12] J. Deng, R. Han, and S. Mishra. Security support for in-network processing in wireless sensor networks. In ACM SASN, Pages:83–93, October 2003

[13] L. Hu and D. Evans. Secure aggregation for wireless networks. In Workshop on Security and Assurance in Ad Hoc Networks, Pages:384–391, January 2003

[14] B. Przydatek, D. Song, and A. Perrig. {SIA}: secure information aggregation in sensor networks. In ACM SenSys, Pages:69–102, November 2003

[15] Y. Yang, X. Wang, S. Zhu, and G. Cao. {SDAP}: a secure hop-by-hop data aggregation protocol for sensor networks. In ACM MOBIHOC, Pages:356–367, 2006

[16] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks : a survey. Computer Networks 38(4):393–422, March 2002

[17] T. Abuhmed, N.Nyamaa, and D. Nyang. Software-Based Remote Code Attestation in Wireless Sensor Network. In IEEE GLOBECOM, December 2009.

[18] S. Ganeriwal and M. Srivastava. Reputation-based framework for high integrity sensor networks. In ACM SASN, October 2004.

[19] F. Li and J. Wu. Mobility reduces uncertainty in {MANET}. In IEEE INFOCOM, May 2007.

[20] T. Park and K. G. Shin. Soft tamper-proofing via program integrity verification in wireless sensor networks. IEEE Trans. Mob. Comput.

[21] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla. SWATT: SoftWarebased ATTestation for embedded devices. In IEEE S&P, May 2004.

[22] Y. Sun, Z. Han, W. Yu, and K. Liu. A trust evaluation framework in distributed networks: vulnerability analysis and defense against attacks. In IEEE INFOCOM, April 2006. 4(3):297-309, 2005.

[23] Y. Yang, X. Wang, S. Zhu, and G. Cao. Distributed software-based attestation for node compromise detection in sensor networks. In IEEE SRDS, October 2007.

[24] Jun-Won, H., et al. (2012). "ZoneTrust: Fast Zone-Based Node Compromise Detection and Revocation in Wireless Sensor Networks Using Sequential Hypothesis Testing." IEEE Transactions on Dependable and Secure Computing 9(4): 494-511.

[25] Thaile, M. and O. B. V. Ramanaiah (2016). Node Compromise Detection based on NodeTrust in Wireless Sensor Networks. 2016 International Conference on Computer Communication and Informatics (ICCCI).

[26] J. Ho, D. Liu, M. Wright, and S.K. Das. Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks. In Elsevier Ad Hoc Networks Journal, 7(8):1476–1488, 2009

[27] D.B. Faria and D.R. Cheriton. Radio Layer Security: Detecting identity-based attacks in wireless networks using signalprints. In ACM WiSe, Pages:43–52, September 2006.

[28] Z. Li, W. Xu, R. Miller, and W. Trappe. Securing wireless systems via low layer enforcements. In ACM WiSe, Pages:33–42, September 2006

[29] N. Patwari and S. K. Kasera. Robust location distinction using temporal link signatures. In ACM MobiCom, Pages:111–122, September 2007.

[30] J. Zhang, M. Firooz, N. Patwari, and S. K. Kasera. Advancing wireless link signatures for location distinction. In ACM MobiCom, Pages:26–37, September 2008.

[31] J.-W. Ho, ‘‘A framework for robust detection and prevention of wide-spread node compromise in wireless sensor networks,’’ Doctoral dissertation, Dept. Comput. Sci. Eng., Univ. Texas Arlington, Arlington, TX, USA, 2010.

[32] Al-Riyami, A., et al. (2016). "An Adaptive Early Node Compromise Detection Scheme for Hierarchical WSNs." IEEE Access 4: 4183-4206.

[33] Geedhabhanu, S. and P. Latha (2015). Excluding compromised node by tracing false data injected messages in Wireless Sensor Network. International Confernce on Innovation Information in Computing Technologies.

[34] M. Conti, R.D. Pietro, L.V. Mancini, and A. Mei. A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks. In ACM Mobihoc, pages:80-89, 2007.

[35] B. Parno, A. Perrig, and V.D. Gligor. Distributed Detection of Node Replication Attacks in Sensor Networks. In IEEE Symposium on Security and Privacy, pages:49-63, May 2005

[36] K. Xing, F. Liu, X. Cheng, and H.C. Du. Real-time Detection of Clone Attacks in Wireless Sensor Networks. In IEEE ICDCS, pages:3-10, 2008

[37] H.-A. Kim and B. Karp, ‘‘Autograph: Toward automated, distributed worm signature detection,’’ in Proc. 13th USENIX Secur. Symp., 2004, pp. 271–286.

[38] D. Moore, C. Shannon, G. M. Voelker, and S. Savage, ‘‘Internet quarantine: Requirements for containing self-propagating code,’’ in Proc. IEEE INFOCOM, Mar. 2003, pp. 1901–1910.

[39] J. Newsome, B. Karp, and D. Song, ‘‘Polygraph: Automatically generating signatures for polymorphic worms,’’ in Proc. IEEE Symp. Secur. Privacy, May 2005, pp. 226–241.

[40] S. E. Schechter, J. Jung, and A. W. Berger, ‘‘Fast detection of scanning worm infections,’’ in Proc. RAID, Sep. 2004, pp. 59–81

[41] Y. Yang, S. Zhu, and G. Cao, ‘‘Improving sensor network immunity under worm attacks: A software diversity approach,’’ in Proc. ACM MobiHoc, May 2008, pp. 149–158

[42] Y. Yang, S. Zhu, and G. Cao, ‘‘Improving sensor network immunity under worm attacks,’’ Ad hoc Netw., vol. 47, no. 1, pp. 26–40, Sep. 2016

[43] N. Gui, E. Zhai, J. Hu, and Z. Chen, ‘‘SWORDS: Improving sensor networks immunity under worm attacks,’’ in Proc. Web-Age Inf. Manage. (WAIM), Jul. 2010, pp. 86–96.

[44] Y. Liu, W. Zhang, S. Bai, and C. Wang, ‘‘Defending sensor worm attack using software diversity approach,’’ in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2011, pp. 1–5

[45] T. Abuhmed, N. Nyamaa, and D. Nyang, ‘‘Software-based remote code attestation in wireless sensor network,’’ in Proc. IEEE GLOBECOM, Nov. 2009, pp. 1–8.

[46] X. Kovah, C. Kallenberg, C. Weathers, A. Herzog, M. Albin, and J. Butterworth, ‘‘New results for timing-based attestation,’’ in Proc. IEEE Symp. Secur. Privacy, May 2012, pp. 239–253.

[47] A.-R. Sadeghi, S. Schulz, and C. Wachsmann, ‘‘Lightweight remote attestation using physical functions,’’ in Proc. ACM WiSec, Jun. 2011, pp. 109–114.

[48] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla, ‘‘SWATT: Software-based attestation for embedded devices,’’ in Proc. IEEE Symp. Secur. Privacy, May 2004, pp. 272–282

[49] Y. Yang, X. Wang, S. Zhu, and G. Cao, ‘‘Distributed software-based attestation for node compromise detection in sensor networks,’’ in Proc. IEEE SRDS, Oct. 2007, pp. 219–230.

[50] Distributed Software-Attestation Defense against Sensor Worm Propagation,(2015)

[51] Haque, M. A. and H. Mineno (2018). Contextual Outlier Detection in Sensor Data Using Minimum Spanning Tree Based Clustering. 2018 International Conference on Computer, Communication, Chemical, Material and Electronic Engineering (IC4ME2).

[52] Patil, S. D. and B. P. Vijayakumar (2017). A Novel Outlier Detection Scheme (ODS) in Wireless Sensor Networks. Computing and Network Sustainability, Singapore, Springer Singapore.

[53] Abid, A., et al. (2017). "Outlier Detection in Wireless Sensor Networks Based on OPTICS Method for Events and Errors Identification." Wireless Personal Communications 97(1): 1503-1515.

[54] W. Wu, X. Cheng, M. Ding, K. Xing, F. Liu, and P. Deng, Localized Outlying and Boundary Data Detection in Sensor Networks, IEEE Trans. Knowl. Data Eng., Vol. 19, No. 8, pp. 1145-1157, 2007.

[55] T. Palpanas, D. Papadopoulos, V. Kalogeraki, and D. Gunopulos, Distributed Deviation Detection in Sensor Networks, ACM Special Interest Group on Management of Data, pp. 77-82, 2003

[56] E. Knorr and R. Ng, Algorithms for Mining Distance-Based Outliers in Large Data Sets, International Journal of Very Large Data Bases, pp. 392-403, 1998

[57] S. Ramaswamy, R. Rastogi, and K. Shim, Efficient Algorithms for Mining Outliers from Large Data Sets, ACM Special Interest Group on Management of Data, pp. 427-438, 2000.

[58] J. Branch, B. Szymanski, C. Giannella, and R. Wolff, In-Network Outlier Detection in Wireless Sensor Networks, Proc. IEEE ICDCS, 2006.

[59] K. Zhang, S. Shi, H. Gao, and J. Li, Unsupervised Outlier Detection in Sensor Networks using Aggregation Tree, Proc. ADMA, 2007

[60] Andrade, A. T. C., et al. (2016). Outlier detection using k-means clustering and lightweight methods for Wireless Sensor Networks. IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society.

[61] Shahid, N., et al. (2015). "One-class support vector machines: analysis of outlier detection for wireless sensor networks in harsh environments." Artificial Intelligence Review 43(4): 515-563.

[62] Zhang, Y., et al. (2013). "Distributed online outlier detection in wireless sensor networks using ellipsoidal support vector machine." Ad Hoc Networks 11(3): 1062-1074.

[63] Shahid, N., et al. (2012). Quarter-Sphere SVM: Attribute and Spatio-Temporal correlations based Outlier &amp; Event Detection in wireless sensor networks. 2012 IEEE Wireless Communications and Networking Conference (WCNC).

[64] Rajasegarar, S., et al. (2010). "Centered Hyperspherical and Hyperellipsoidal One-Class Support Vector Machines for Anomaly Detection in Sensor Networks." IEEE Transactions on Information Forensics and Security (TIFS) 5(3): 518-533.

[65] Hao, Y., et al. (2015). A Distributed Bayesian Algorithm for data fault detection in wireless sensor networks. 2015 International Conference on Information Networking (ICOIN).

[66] Titouna, C., et al. (2015). "Outlier Detection Approach Using Bayes Classifiers in Wireless Sensor Networks." Wireless Personal Communications 85(3): 1009-1023.

[67] Feng, H., et al. (2017). "Distributed outlier detection algorithm based on credibility feedback in wireless sensor networks." IET Communications 11(8): 1291-1296.

[68] V. Chatzigiannakis and S. Papavassiliou, " Diagnosing anomalies and identifying faulty nodes

in sensor networks," IEEE Sensors J., vol. 7, pp. 637–645, 2007

[69] Livani, M. A. and M. Abadi (2010). Distributed PCA-based anomaly detection in wireless sensor networks. 2010 International Conference for Internet Technology and Secured Transactions.

[70] Rassam, M. A., et al. (2012). One-Class Principal Component Classifier for anomaly detection in wireless sensor network. 2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN).

[71] K, Kapitanova, S.H , Son and K. D, Kang. Event Detection in Wireless Sensor Networks. Second International Conference, ADHOCNETS 2010, Victoria, BC, Canada, August 2010.

[72] Y, Zhang, N, Meratnia, P. J.M, Havinga. Distributed online outlier detection in wireless sensor networks using ellipsoidal support vector machineǁ. Ad Hoc Networks , December 2012

[73] Y, Zhang, N.A.S, Hammb, N, Meratnia, A, Steinb, M, Voorta. And P.J.M , Havinga. Statistics-based outlier detection for wireless sensor networksǁ, Volume 26, Issue 8, April 2012

[74] Fernandes Jr, G., et al. (2015). "Autonomous profile-based anomaly detection system using principal component analysis and flow analysis." Applied Soft Computing 34: 513-525.

[75] Ghorbel, O., et al. (2015). A Novel Outlier Detection Model Based on One Class Principal Component Classifier in Wireless Sensor Networks. 2015 IEEE 29th International Conference on Advanced Information Networking and Applications.

[76] A. Francillon and C. Castelluccia. Code Injection Attacks on HarvardArchitecture Devices. In ACM CCS, Pages:15–26, October 2008

[77] Patil SD, Vijayakumar BP (2016) Clustering in mobile wireless sensor networks. In: International conference on innovations in computing and networking

[78] <https://blog.csdn.net/baimafujinji/article/details/79376378>

[79] C. Zou, L. Gao, W. Gong, and D. Towsley, ‘‘Monitoring and early warning for Internet worms,’’ in Proc. ACM CCS, Oct. 2003, pp. 190–199

[80] T. Park and K. G. Shin. Soft tamper-proofing via program integrity verification in wireless sensor networks. In IEEE Trans. Mob. Comput., 4(3):297–309, 2005

[78] McDonald, D., et al. (2015). "A Survey of Methods for Finding Outliers in Wireless Sensor Networks." Journal of Network and Systems Management 23(1): 163-182.

[79] Haque, M. A. and H. Mineno (2018). Contextual Outlier Detection in Sensor Data Using Minimum Spanning Tree Based Clustering. 2018 International Conference on Computer, Communication, Chemical, Material and Electronic Engineering (IC4ME2).

最近邻居方案的参考文献：