Advances in Computer, Communication and Computational Sciences pp 87–97

On Confidentiality, Integrity, Authenticity, and Freshness (CIAF) in WSN

Shafiqul Abidin, Vikas Rao Vadi & Ankur Rana

Conference paper | First Online: 28 October 2020

1272 Accesses | **16** Citations

Part of the Advances in Intelligent Systems and Computing book series (AISC,volume 1158)

Abstract

A Wireless sensor network (WSN) comprises several sensor nodes such as magnetic, thermal, and infrared, and the radar is set up in a particular geographical area. The primary aim of sensor network is to transmit reliable, secure data from one node to another node, node to base station and vice versa and from base station to all nodes in a network and

to conserve the energy of sensor nodes. On the other hand, there are several restrictions such as large energy consumption, limited storage/memory and processing ability, higher latency, and insufficient resources. The related security issues in wireless sensor network are authenticity, confidentiality, robustness, integrity, and data freshness. The sensor nodes are susceptible to several attacks such as DOS, Sybil, flood, black hole, selective forwarding which results in the leakage of sensitive and valuable information. It is therefore necessary to provide security against these critical attacks in the network. Wireless sensor network were earlier used for military applications with the objective of monitoring friendly and opposing forces, battlefield surveillance, detection of attacks, but today Wireless Networking have a huge number of applications-environmental, healthcare, home, industrial, commercial and are still counting. This paper is an extensive review of the security requirements, attacks that are to be avoided and resolved for achieving a secure network connection. This paper also emphasizes various limitations and defense strategies to prevent threats and attacks. The issues of applications of wireless sensor network for smooth and reliable transmissions are also discussed. The sensor networks are popular for mission-critical-tasks and security is immensely required for such hostile environment employed networks.

Keywords

Cryptography **Data confidentiality** **Sybil**

Data authentication **Black hole attack**

Attacks on WSN

References

1. G. Lu, B. Krishnamachari, C.S. Raghavendra, An adaptive energy-efficient and low-latency MAC for

data gathering in wireless sensor networks. in *IEEE IPDPS* (2004)

2. B. Heinzelman, A.P. Chandrakasan, H. Balakrishnan, An application-specific protocol architecture for wireless microsensor networks. IEEE Trans. Wireless Commun. **1**(4), 660–670 (2002)

3. S. Abidin, Key agreement protocols and digital signature algorithm. Int. J. Curr. Adv. Res. **6**(8), 5359–5362 (2017)

4. N. Burri, P. von Rickenbach, R. Wattenhofer, Dozer: ultra-low power data gathering in sensor networks. in *ACM/IEEE IPSN* (2007)

5. Z. Jiang, J. Ma, W. Lou, J. Wu, A straightforward path routing in wireless ad hoc sensor networks. in I*EEE International Conference on Distributed Computing Systems Workshops* (2009), pp. 103–108

6. S. Bashyal, G.K. Venayagamoorthy, *Collaborative Routing Algorithm for Wireless Sensor Network Longevity* (IEEE, 2007)

7. J. Burrell, T. Brooke, R. Beckwith, Vineyard computing: sensor networks in agricultural production. Pervas. Comput. IEEE **3**(1), 38–45 (2004)

8. S. Kim, S. Pakzad, D. Culler, J. Demmel, G. Fenves, S. Glaser, M. Turon, *Health Monitoring of Civil Infrastructures using Wireless Sensor Networks*. in *ACM/IEEE IPSN* (2007)

9. M. Ceriotti, L. Mottola, G.P. Picco, A.L. Murphy, S. Guna, M. Corra, M. Pozzi, D. Zonta, P. Zanon, Monitoring heritage buildings with wireless sensor networks: the torre aquila deployment. in *ACM/IEEE IPSN* (2009)

10. K. Lorincz, D. Malan, T.R.F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, S. Moulton, M. Welsh, Sensor networks for emergency response: challenges and opportunities. IEEE Pervas. Comput. Special Issue. Pervas. Comput. First Resp. (2004)

11. S. Abidin, A novel construction of secure RFID authentication protocol. Int. J. Sec. Comput. Sci. J. Malaysia **8**(8), 33–36 (2014)

12. N.M. Durrani, N. Kafi, J. Shamsi, W. Haider, A.M. Abbsi, *Secure Multi-hop Routing Protocols in Wireless Sensor Networks: Requirements, Challenges and Solutions* (IEEE, 2013)

13. V. Bulbenkiene, S. Jakovlev, G. Mumgaudis, G. Priotkas, Energy loss model in Wireless Sensor Networks. in *IEEE Digital Information Processing and communication (ICDIPC), 2012 Second International conference* (2012), pp. 36–38

14. J.H. Chang, L. Tassiulas, Maximum lifetime routing in wireless sensor networks. IEEE/ACM Trans. Netw. **12**(4), 609–619 (2004)

15. M. Zhang, S. Wang, C. Liu, H. Feng, *An Novel Energy-Efficient Minimum Routing Algorithm (EEMR) in Wireless Sensor Networks* (IEEE, 2008)

16. M. Saraogi, *SecurityiIn Wireless Sensor Networks* (University of Tennessee, Knoxville)

17. A. Jain, K. Kant, M.R. Tripathy, Security solutions for wireless sensor networks. in *2012, Second International Conference on Advanced Computing & Communication Technologies*

18. C. Karlof, D. Wanger, Secure routing in wireless sensor network: attacks and countermeasures. in *First IEEE International Workshop on Network Protocols and Applications* (2013), pp. 113–127

19. M. Ahuja, S. Abidin, Performance analysis of vehicular ad-hoc network. Int. J. Comput. Appl. USA **151**(7) 28–30 (2016)

20. N. Kumar, A. Mathuria, *Improved Write Access Control and Stronger Freshness Guarantee to Outsourced Data*. (ICDCN, 2017)

21. W. Feng, J. Liu, Networked wireless sensor data collection: issues, challenges, and approaches. IEEE Commun. Surv. Tutor. (2011)

Author information

Authors and Affiliations

HMR Institute of Technology & Management, (GGSIPU), New Delhi, Delhi, India
Shafiqul Abidin

Bosco Technical Training Society, New Delhi, India
Vikas Rao Vadi

Quantum University, Roorkee, Uttrakhand, India
Ankur Rana

Corresponding author

Correspondence to Shafiqul Abidin .

Editor information

Editors and Affiliations

Department of Mathematics and Computer Science, University of Missouri–St. Louis, Chesterfield, MO, USA

Sanjiv K. Bhatia

Computer Science Engineering Department, ABES Engineering College, Ghaziabad, Uttar Pradesh, India

Shailesh Tiwari

Shanghai Advanced Research Institute, Pudong, China

Su Ruidan

National Institute of Technology Agartala, Agartala, Tripura, India

Munesh Chandra Trivedi

Computer Science Engineering Department, Motilal Nehru National Institute of Technology, Allahabad, Uttar Pradesh, India

K. K. Mishra

Rights and permissions

Copyright information

About this paper

Cite this paper

Abidin, S., Vadi, V.R., Rana, A. (2021). On Confidentiality, Integrity, Authenticity, and Freshness (CIAF) in WSN. In: Bhatia, S.K., Tiwari, S., Ruidan, S., Trivedi, M.C., Mishra, K.K. (eds) Advances in Computer, Communication and Computational Sciences. Advances in Intelligent Systems and Computing, vol 1158. Springer, Singapore. https://doi.org/10.1007/978-981-15-4409-5_8

.RIS .ENW .BIB

DOI	Published	Publisher Name
https://doi.org/10.1007/978-981-15-4409-5_8	28 October 2020	Springer, Singapore

Print ISBN	Online ISBN	eBook Packages
978-981-15-4408-8	978-981-15-4409-5	Intelligent Technologies and Robotics Intelligent Technologies and Robotics (R0)

Publish with us

Policies and ethics