

{tag} International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

[Volume 153](#)

-
[Number 2](#)

Year of Publication: 2016

Authors:

Kyu-hyun Song, Tae-ho Cho

10.5120/ijca2016911978

{bibtex}2016911978.bib{/bibtex}

Abstract

Wireless Sensor Networks (WSNs) are composed of many sensor nodes and a base station for collecting event information from a wide local area. However, an attacker can easily intrude into a network through external nodes by exploiting characteristics of wireless communication and the limited hardware resources of sensor nodes. Specifically, an attacker can intrude into a sensor network and launch a sinkhole attack in order to capture and redirect event reports of WSNs. Intrusion-tolerant routing for wireless sensor networks (INSENS) has been proposed to prevent sinkhole attacks via intrusion of an external node. INSENS blocks the intrusion of an external node using three symmetric keys to prevent the sinkhole attack. However, even in the presence of INSENS, a sinkhole attack can again be launched by the compromised node because the network does not account for compromised nodes. In this paper, proposed method with three steps involving the interactive authentication method prevent sinkhole attacks by a compromised node. The proposed method detects fake route request messages and drops the compromised node. Proposed method improves the number of the delivered event reports to the base station (BS) by around 65.72% when compared to INSENS. Thus, it improves the

reliability of the network and reduces the average energy consumption by around 22.32% because it prevents internal sinkhole attacks.

References

1. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," *Communications Magazine*, IEEE, vol. 40, pp. 102-114, 2002.
2. K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks*, vol. 3, pp. 325-349, 2005.
3. X. Du and H. Chen, "Security in wireless sensor networks," *Wireless Communications*, IEEE, vol. 15, pp. 60-66, 2008.
4. J. Deng, R. Han and S. Mishra, "INSENS: Intrusion-tolerant routing for wireless sensor networks," *Comput. Commun.*, vol. 29, pp. 216-230, 2006.
5. E. Shi and A. Perrig, "Designing secure sensor networks," *Wireless Communications*, IEEE, vol. 11, pp. 38-43, 2004.
6. F. Ye, H. Luo, S. Lu and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," *Selected Areas in Communications*, IEEE Journal On, vol. 23, pp. 839-850, 2005.
7. S. Zhu, S. Setia and S. Jajodia, "LEAP : Efficient security mechanisms for large-scale distributed sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 2, pp. 500-528, 2006.
8. (Accessed: Jan. 11, 2016). MICAz: wireless measurement system. Available: <http://trl.iba.edu.pk/Memsic-set-2.pdf>.
9. I. Krontiris, T. Giannetsos and T. Dimitriou, "Launching a sinkhole attack in wireless sensor networks; the intruder side," in *2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 2008, pp. 526-531.
10. N. Gandhewar and R. Patel, "Detection and prevention of sinkhole attack on AODV protocol in mobile adhoc network," in *Computational Intelligence and Communication Networks (CICN)*, 2012 Fourth International Conference On, 2012, pp. 714-718.
11. E. C. Ngai, J. Liu and M. R. Lyu, "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks," *Comput. Commun.*, vol. 30, pp. 2353-2364, 2007.
12. Kyu-Hyun Song and Tae-Ho Cho. Secure route determination method to prevent sinkhole attacks in INSENS based wireless sensor networks. *Journal of Korean Institute of Intelligent Systems* 26(4), pp. 267-272. 2016.
- 13.

Index Terms

Computer Science

Networks

Keywords

Wireless sensor networks, Sinkhole attack, Intrusion tolerance, Secure routing, Interactive authentication.