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

Volume 171
-
Number 3

Year of Publication: 2017

Authors:

Sang-hyeok Lim, Tae-ho Cho

10.5120/ijca2017914992

{bibtex}2017914992.bib{/bibtex}

Abstract

Wireless sensor networks (WSNs) consist of several sensor nodes and base stations and collect information through sensors located over a large area. However, they can easily be compromised by an attacker because of their random placement in an open environment, where individual management is difficult. An attacker can execute a false report injection attack and a false vote injection attack through compromised nodes. The probabilistic voting-based filtering scheme (PVFS) is a scheme to prevent these two kinds of attacks. Before sending the report, the proposed method selects the validation node, judges the validity of the report, and filters it based on a set of threshold values. In this paper, the proposed method detects and filters false reports generated from compromised member nodes of event clusters early and improves both the detection rate of false reports and the energy efficiency of nodes compared with PVFS. It's experiments show that the maximum energy efficiency increased by about 17%, and a nearly 30% increase in detection performance was observed.

References

1. Perrig, Adrian, John Stankovic, and David Wagner. "Security in wireless sensor networks." Communications of the ACM 47.6 (2004): 53-57.
2. Zhang, Wensheng, and Guohong Cao. "Group rekeying for filtering false data in sensor networks: A predistribution and local collaboration-based approach." INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE. Vol. 1. IEEE, 2005.
3. Al-Karaki, Jamal N., and Ahmed E. Kamal. "Routing techniques in wireless sensor networks: a survey." IEEE wireless communications 11.6 (2004): 6-28.
4. Perrig, Adrian, John Stankovic, and David Wagner. "Security in wireless sensor networks." Communications of the ACM 47.6.
5. Li, Feng, and Jie Wu. "A probabilistic voting-based filtering scheme in wireless sensor networks." Proceedings of the 2006 international conference on Wireless communications and mobile computing.ACM, 2006.
6. Yu, Zhen, and Yong Guan. "A dynamic en-route scheme for filtering false data injection in wireless sensor networks." SenSys. Vol. 5. 2005.
7. Ye, Fan, et al. "Statistical en-route filtering of injected false data in sensor networks." IEEE Journal on Selected Areas in Communications 23.4 (2005): 839-850.
8. Yang, Hao, and Songwu Lu. "Commutative cipher based en-route filtering in wireless sensor networks." Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th. Vol. 2. IEEE, 2004.
9. Zhu, Sencun, et al. "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks." Security and privacy, 2004. Proceedings. 2004 IEEE symposium on. IEEE, 2004.
10. Lu, Rongxing, et al. "BECAN: a bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks." IEEE transactions on parallel and distributed systems 23.1 (2012): 32-43.
11. Jeba, S. A., and B. Paramasivan. "False data injection attack and its countermeasures in wireless sensor networks." European Journal of Scientific Research 82.2 (2012): 248-257.
12. Jeba, S. A., and B. Paramasivan. "An evaluation of en-route filtering schemes on wireless sensor networks." International Journal of Computer Engineering & Technology (IJCET) 3 (2012): 62-73.

Index Terms

Computer Science Wireless

Keywords

Wireless sensor networks, False report injection attack, False vote injection attack, Secure routing.