Abstract

Wireless sensor networks establish a specific type of wireless data communication networks. WSNs have acknowledged remarkable deliberation in current years due to probable applications in armed sensing, fitness care, wildlife tracking, traffic investigation, building constructions monitoring, atmosphere monitoring etc. The central of trust route deceits in gaining trust. Conversely, the present-day trust-based route approaches have some challenging concerns. Finding the trust of a sensor node is most difficult, and just how it can be completed is still uncertain. Routing rules of wireless sensor network naturally adjust themselves with the current environments which may vary with high mobility to low mobility in extremes along with high bandwidth. Detection of malicious node and information safety in a wireless sensor network is an essential work in any sensor network. To achieve availability, integrity and reliability routing rules should be robust against malevolent attacks. We proposed a secure trust value which helps authenticate the sensor node and similarly preserve and safe the sensor network from malicious nodes. We also proposed a novel approach to detect the black hole attack and also keep safe the network from malicious nodes. The network lifetime will improve
and energy consumption reduced. Experimental outcomes demonstrate that our scheme is
good for wireless sensor network security.

References

1. Yuxin Liu, Mianxiong Dong, Kaoru Ota, and Anfeng Liu, ActiveTrust: Secure and
Trustable Routing in Wireless Sensor Networks, IEEE Transactions on Information Forensics
And Security, Vol. 11, No. 9, pp-2013-2018, September 2016,
under reliability constraint wireless sensor networks,” IEEE Trans. Parallel Distrib. Syst., vol. 27,
3. X. Liu, M. Dong, K. Ota, P. Hung, and A. Liu, “Service pricing decision in cyber-physical
Mar./Apr. 2016.
energy-efficient trust system through watchdog optimization for WSNs,” IEEE Trans. Inf.
6. Vittorio P. Illiano and Emil C. Lupu, Detecting Malicious Data Injections in Event Detection
Wireless Sensor Networks, IEEE Transactions 0n Network And Service Management, Vol. 12,
No. 3, September 2015, pp-496-512
7. Qiang Ma, Kebin Liu, Zhichao Cao, Tong Zhu, Yunhao Liu, Link Scanner: Faulty Link
14, pp 4428-4438, Aug 2015
delivery performance in a large-scale sensor network,” IEEE/ACM Trans. Netw., vol. 22, no. 6,
10. X. Li, Q. Ma, Z. Cao, K. Liu, and Y. Liu, “Enhancing visibility of network performance in
11. Z. Li, Y. Liu, M. Li, J. Wang, and Z. Cao, “Exploiting ubiquitous data collection for mobile
12. Q. Ma, K. Liu, X. Miao, and Y. Liu, “Sherlock is around: Detecting network failures with
13. Y. Liu et al. Does wireless sensor network scale? A measurement study on greenorbs,”
15. E. Magistretti, O. Gurewitz, and E. Knightly, “Inferring and mitigating a link’s hindering
transmissions in managed 802.11 wireless networks,” in Proc. ACM MobiCom, Chicago, IL,
An Improved Trustable Routing and Security in Wireless Sensor Network


**Index Terms**

Computer Science  Wireless

**Keywords**