Abstract

In an unprotected environment of Wireless Sensor Network, the authentication scheme for multicast secure communication has to be designed with limited usage of resources and computation. In Multicast Authentication Based on Batch Signature-Enhanced (MABS-E) scheme, a tree construction to counteract the Denial of Service (DoS) attack requires latency at the sender. This authentication latency leads to the jitter effect on real-time applications at the receiver. In few applications, user mobility is considered for authentication process. And also, due to user mobility, the sensor node is compromised. This paper proposes a technique called Batch based Selective Bin Verification (BSBV), which avoids the construction of merkle tree. It reduces latency and allows the receiver to tolerate DoS attack even in the case where the attack fails to be detected. In order to prevent to compromise a node, re-authentication scheme is employed, can prolong the lifetime of the sensor network is provided. The number of
inspections of each packet is decreased when binning technique is used. In BSBV technique, the packet failure rate is decreased to 0.01 from 0.04 because all are verified with the batch verification, when the chosen bin is two. The Packet Delivery Ratio is 82.95% when fifteen malicious nodes are presented.

References

- Hui Song and Liang Xie, "Sensor Node Compromise Detection: The Location Perspective," In proceedings of International Conference on Wireless Communications
- D. Liu, P. Ning, and R. Li, &quot;Establishing Pairwise Keys in Distributed Sensor Networks,&quot; ACM Transactions on Information and System Security (TISSEC), Vol. 8, No. 1, pp. 41-77, Feb 2005.

Index Terms

Computer Science
Wireless And Security

Keywords
Multicast Authentication Signature Re-authentication Membership verification