Abstract

Sensor Network has gained the reputation of becoming the most promising technology of 21st century due to its low cost and ability to traverse longer distances in unattended hostile environments. However, security has still remained a burning and an unresolved issue for both centralized and decentralized wireless sensor networks. Using rigorous theoretical and practical analysis, we have traced numerous security challenges, security attacks and have designed an efficient timestamp-based protocol called "SET-CTA" to provide defense against variety of security attacks in non-clustered wireless sensor deployment environments. Previously proposed TESLA and ?-TESLA [40] schemes were limited in scope; those schemes were only able to provide protection against basic security attacks like non-repudiation. But SETCTA scheme gives a flexibility to provide protection against numerous security attacks like (e.g. eavesdropping, node capture, man in the middle attack, concurrency attacks, trust attacks and many more [40]) by considering various timestamp based parameters like current-timestamp, sending time-stamp, timestamp-difference(?t) etc. To the best of my knowledge, this is the only end-to-end timestamp based scheme that can provide secure and efficient transmission in centralized wireless sensor environments and can also assure protection against different range of security attacks.
References


Centralized Timestamp based Approach for Wireless Sensor Networks


Centralized Timestamp based Approach for Wireless Sensor Networks


Index Terms

Computer Science

Wireless
Centralized Timestamp based Approach for Wireless Sensor Networks

Keywords

Centralized Current-timestamp Sending-timestamp secure and efficient data transmission protocol FND (First Node Dies) time

LND (Last Node Dies) time

Elliptic Curve Cryptography.