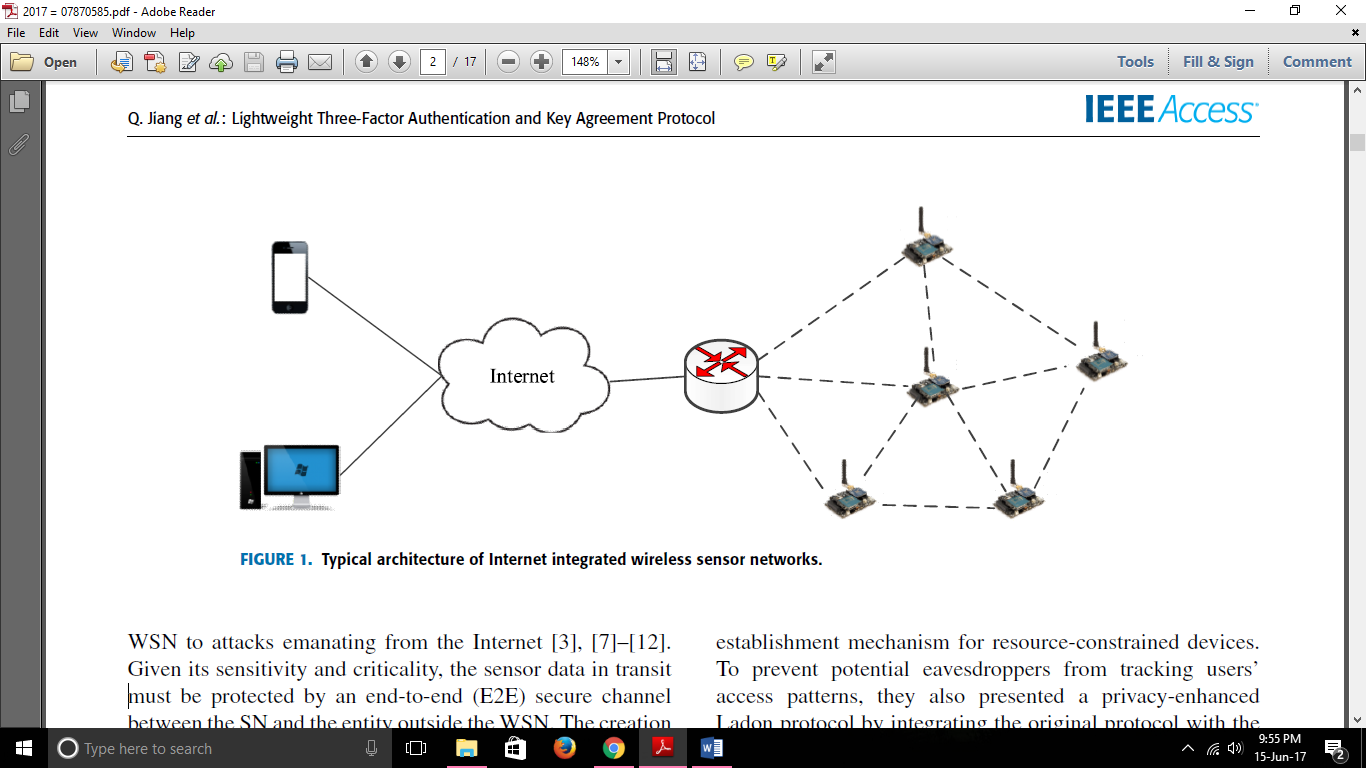
Lightweight Three-Factor Authentication and Key Agreement Protocol for Internet-Integrated Wireless Sensor Networks

INTRODUCTION

* One vision of future Internet is that objects and things with sensing and actuating capabilities will be connected and integrated making up the Internet of Things (IoTs).
* As Wireless Sensor Network (WSN) is one of the core technologies supporting the sensing capabilities required by future applications, the integration of WSN with the Internet will have an active role in the evolution of the architecture of future Internet
* The integration of WSN with the Internet also brings new threats



* Given its sensitivity and criticality, the sensor data in transit must be protected by an end-to-end (E2E) secure channel between the SN and the entity outside the WSN
* The creation of such a channel requires authentication and key agreement mechanisms that allow two remote entities to mutually authenticate and negotiate secret keys that are used to protect the sensor data against various types of active and passive attacks
* The openness of the Internet still requires authentication and key agreement protocols for establishing the E2E secure channel between the two communicating peers
* Amin et al. presented a new secure 3FA protocol, which is claimed to be secure against all the known security attacks
* Weaknesses:
* Type I SCLA - the secret data obtained from the smart card is enough for an adversary to reveal the user password
* Type II SCLA - the transcripts of an authentication session are needed for an attacker, in addition to the secret parameters in the user's smart card
* user identity and password can be exhaustively guessed in an offline manner along with the secrets stored in the stolen smart card and the intercepted authentication messages.
* KSSTIA if the temporal parameters in an authentication session are disclosed
* Is prone to tracking attack and cannot fufill user untraceability.

An efficient and secure 3FA protocol based on the Rabin cryptosystem

Bio Hashing

* Biometric : Verifies identity of user
* Biometric data cannot be replaced
* **Biohashing** : Privacy-preserving biometric schemes
* Stages :

1. Enrollment stage

* Biometric template *B* + random secret key *K* – generates biohash value *BH*(*K*; *B*)
* Preprocessing performed on *B* to make biometric feature invariant to small variations in input biometric
* *BH*(*K*; *B*) generated by comparing inner product of random vector generated from user specific secret key *K* and the feature vector extracted against a predefined threshold

1. Verification stage
   * + *BH*(*K*; *B*0) can be generated from the received biometric signal *B*0 and the secret key given by the user
       - (Same as above)
     + The verification is done by comparing *BH*(*K*; *B*0) with the stored value *BH*(*K*; *B*)

Rabin Cryptosystem

* Public key cryptographic primitive based on integer factorization
* Advantage over other public-key cryptosystems - Rabin has the characteristic of computational asymmetry
* Encryption – very efficient

Decryption – heavyweight

* Includes three algorithms:



Proposed authentication protocol

9 phases

