INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

# User Authentication in Wireless Sensor Networks


**Dr. Ashok Kumar Das**

**IEEE Senior Member**
**Associate Professor**
Center for Security, Theory and Algorithmic Research
(Department of Computer Science and Engineering)
International Institute of Information Technology, Hyderabad
(Formerly **Indian Institute of Information Technology, Hyderabad**)

E-mail: *ashok.das@iiit.ac.in*
Homepage: http://www.iiit.ac.in/people/faculty/ashokkdas
Personal Homepage: https://sites.google.com/view/iitkgpakdas/


September 11, 2022

# Temporal credential-based three-factor user authentication for distributed wireless sensor networks

This work is published in the paper:

**Ashok Kumar Das. "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks," in *Peer-to-Peer Networking and Applications (Springer)*, Vol. 9, No. 1, pp. 223-244, 2016, DOI: 10.1007/s12083-014- 0324-9. (2021 SCI Impact Factor: 3.488)**

[This article is one of the top five most popular downloaded articles during December 2014 to January 2015 of the Peer-to-Peer Networking and Applications]

**Necessity for user authentication**

- Most queries in wireless sensor network (WSN) applications are issued at the point of the base station or gateway node of the network.
- However, for critical applications of WSNs (e.g., battle field, healthcare application) there is a great need to access the real time data inside the WSN from the nodes, because the real-time data may no longer be accessed through the base station only.
- The real-time data can be given access directly to the external users (parties) those who are authorized to access data as and when they demand.
- The user authentication plays a vital role for this purpose.

# User authentication in DWSNs

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

## Three factors used in the designed scheme

- Smart card
- Password
- Personal biometrics (for example, fingerprints, faces, irises, hand geometry and palm-prints, etc.)

# Biometrics and Fuzzy Extractor

- Uses the user's personal biometrics along with traditional password to design user authentication protocols in WSNs.
- The biometric verification allows one to confirm or establish an individual's identity.
- There are major advantages of using biometric keys (for example, fingerprints, faces, irises, hand geometry and palm-prints, etc.):
  - Biometric keys can not be lost or forgotten.
  - Biometric keys are very difficult to copy or share.
  - Biometric keys are extremely hard to forge or distribute.
  - Biometric keys can not be guessed easily.
  - Someone's biometrics is not easy to break than others.

# Biometrics and Fuzzy Extractor

- The output of a conventional hash function $h(\cdot)$ is sensitive and it may also return completely different outputs even if there is a little variation in inputs.
- The biometric information is prone to various noises during data acquisition, and the reproduction of actual biometric is hard in common practice.
- To avoid such problem, a fuzzy extractor method is preferred, which can extract a uniformly random string and a public information from the biometric template with a given error tolerance $t$.

# Biometrics and Fuzzy Extractor

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

## Definition

The fuzzy extractor is a tuple $(\mathcal{M}, l, t)$, which is composed of the following two algorithms, called *Gen* and *Rep*:

- **Gen:** It is a probabilistic algorithm, which takes a biometric information $B_i \in \mathcal{M}$ as input, and then outputs a secret key data $\sigma_i \in \{0,1\}^l$ and a public reproduction parameter $\tau_i$, where $Gen(B_i) = \{\sigma_i, \tau_i\}$.
- **Rep:** This is a deterministic algorithm, which takes a noisy biometric information $B_i' \in \mathcal{M}$ and a public parameter $\tau_i$ and $t$ related to $B_i$, and then it reproduces (recovers) the biometric key data $\sigma_i$. In other words, we have $Rep(B_i', \tau_i) = \sigma_i$ provided that the condition $d(B_i, B_i') \leq t$ is met.

# Biometrics and Fuzzy Extractor

- The probability to guess the biometric key data $\sigma \in \{0,1\}^l$ by an attacker is approximately $\frac{1}{2^l}$, where $l = m - 2\log(\frac{1}{\epsilon}) + O(1)$, where $\epsilon$ is the statistical distance between two given probability distributions, and $m$ is the min-entropy given as follows.
  the min-entropy $H_\infty(A)$ of a random variable $A$ is $-log(max_a Pr[A = a])$.
  **Vanga Odelu, Ashok Kumar Das, and Adrijit Goswami. "A Secure Biometrics-Based Multi-Server Authentication Protocol using Smart Cards," in *IEEE Transactions on Information Forensics and Security*, Vol. 10, No. 9, pp. 1953 - 1966, 2015, DOI: 10.1109/ TIFS.2015.2439964. (2021 SCI Impact Factor: 7.231) [This article is one of the top 50 most frequently downloaded documents for Popular Articles (June - November 2015)]**

# User authentication in DWSNs

**Threat Model** In the following we consider the three types of models:

- **Honest-but-Curious adversary model**: This model [HCAM] is a passive adversarial model where the adversary $\mathcal{A}$ will behave like a legitimate entity and follow the specified protocol. However, $\mathcal{A}$ can read all the transmitting information between the corrupted entities in the network.
- **Dolev-Yao (DY) threat model**: This model is known as the DY model [DYM]. In the DY model, an adversary $\mathcal{A}$ has the potential ability to eavesdrop, intercept, modify and delete messages that are being communicated among various agents through a wireless network.
- **Canetti and Krawczyk's model**: This model is also known as the "CK-adversary model" [CKM]. Keeping all the fundamental assumptions used in the DY model, the CK-adversary model empowers $\mathcal{A}$ to compromise secret keys, secret credentials, and session states through the session hijacking attacks. Thus, leakage of the short term secrets from the *UE* node's memory can lead to disclosure of session key and other secrets.

# User authentication in DWSNs

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

## Threat Model


- [HCAM]: B. Narwal and A. K. Mohapatra, "A survey on security and authentication in wireless body area networks," *Journal of Systems Architecture*, vol. 113, p. 101883, 2021. https://www.sciencedirect.com/science/article/pii/S1383762120301600
- [DYM]: D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198208, 1983. https://ieeexplore.ieee.org/document/1056650
- [CKM]: R. Canetti and H. Krawczyk, "Universally Composable Notions of Key Exchange and Secure Channels," in *International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'02)*, Amsterdam, The Netherlands, 2002, pp. 337–351. https://link.springer.com/chapter/10.1007/3-540-46035-7_22

# User authentication in DWSNs

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

## Threat Model

- Due to the hostile environments in the deployment field, nodes can be physically captured by an attacker.
- Sensor nodes as well as cluster heads can be compromised or captured by an attacker. Usually, nodes are not equipped with tamper-resistant hardware due to cost constraints and hence we assume that once a node is captured by an attacker, all the stored sensitive data as well as cryptographic information are revealed to the attacker.
- In any case, the *GWN* will not be compromised by an attacker.
- Finally, we make use of the famous Dolev-Yao threat model in which two communicating parties (nodes) communicate over an insecure channel. We adopt the similar threat model for WSNs where the channel is insecure and the end-points (users, sensor nodes) cannot in general be trustworthy.

# User authentication in DWSNs



Table: Notations used

| Symbol | Description |
|---|---|
| $GWN$ | WSN gateway node (base station) |
| $U_i$ | $i^{th}$ user |
| $SC_i$ | Smart card of $U_i$ |
| $ID_i$ | Identity of user $U_i$ |
| $PW_i$ | Password of user $U_i$ |
| $B_i$ | Biometric information of $U_i$ |
| $K$ | 1024-bit secret number known to $U_i$ only |
| $h(\cdot)$ | Secure collision-free one-way hash function |
| $X_s$ | 1024-bit secret master key of $GWN$ |
| $SN_j$ | $j^{th}$ sensor node in WSN |
| $ID_{SN_j}$ | Identity of $SN_j$ |
| $TE_i$ | Expiration time of $U_i$'s temporal credential |
| $TS_X$ | Current timestamp of an entity $X$ |
| $Gen(\cdot)$ | Fuzzy generator function |
| $Rep(\cdot)$ | Fuzzy reproduction function |
| $t$ | Error tolerance threshold used in fuzzy extractor |
| $\Delta T$ | Maximum transmission delay |
| $A \oplus B$ | Bitwise XORed of data $A$ with data $B$ |
| $A\|\|B$ | Data $A$ concatenates with data $B$ |

# User authentication in DWSNs

**Pre-Deployment Phase**

Before deployment of nodes in the network, the *GWN* does the following steps.

- Step PD1. For each deployed sensor node $SN_j$, the GWN selects a unique identifier $ID_{SN_j}$.
- Step PD2. The GWN generates randomly a large 1024-bit number $K_{GWN-S}$, which is considered as the GWN's private key only known to the GWN. After that for each deployed sensor node $SN_j$, the GWN computes $TC_j = h(K_{GWN-S} || ID_{SN_j})$, which is the temporal credential for $SN_j$.
- Step PD3. Finally, each deployed sensor node $SN_j$ is pre-loaded with the information $TC_j$ as its temporal credential prior to its deployment in the target field.

# User authentication in DWSNs

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

**Pre-Deployment Phase**

| $ID_{SN_j}$ | $TC_j = h(K_{GWN-S} \|\| ID_{SN_j})$ |
|---|---|

Figure: Pre-loaded information into $SN_j$'s memory.

# User authentication in DWSNs

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

## Registration Phase

- Before accessing data from a particular sensor node in the sensor network, the user $U_i$ needs to register with the *GWN* of the network.
- $U_i$ first selects a unique identity $ID_i$ and chooses a password $PW_i$.
- $U_i$ generates randomly a large 1024-bit secret number $K$. $U_i$ computes the masked password $RPW_i = h(ID_i||K||PW_i)$ and sends the registration request message $\langle ID_i, RPW_i \rangle$ to the GWN via a secure channel.
- The remaining steps are summarized in the following table.

# User authentication in DWSNs

| User ($U_i$)/Smart Card ($SC_i$) | GWN |
|---|---|
| Inputs $ID_i$, $PW_i$, $B_i$.<br>Generates a random secret number $K$.<br>Computes $RPW_i = h(ID_i \|\| K \|\| PW_i)$.<br>$\langle ID_i, RPW_i \rangle$ $\rightarrow$<br>(via a secure channel) | Generates private key $K_{GWN-U}$.<br>Computes $TC_i = h(K_{GWN-U} \|\| ID_i \|\| TE_i)$,<br>$PTC_i = TC_i \oplus RPW_i$.<br>Generates secret information $X_s$ and<br>computes $r_i = h(ID_i \|\| X_s)$.<br>Selects temporary identity $TID_i$ of $U_i$<br>and initializes it.<br>Stores the tuple $(TID_i, ID_i, TE_i)$<br>in its verification table.<br>$\langle Smart\ Card(h(\cdot), TID_i, TE_i, PTC_i, r_i) \rangle$ $\leftarrow$<br>(via a secure channel) |
| Computes $Gen(B_i) = (\sigma_i, \tau_i)$,<br>$e_i = h(ID_i \|\| \sigma_i) \oplus K$,<br>$f_i = h(ID_i \|\| RPW_i \|\| \sigma_i)$,<br>$r_i^* = r_i \oplus h(ID_i \|\| K)$.<br>Replaces $r_i$ with $r_i^*$ in smart card.<br>Stores $e_i$, $f_i$, $Gen(\cdot)$, $Rep(\cdot)$, $t$<br>and $\tau_i$ in smart card. | |

# User authentication in DWSNs

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

## Registration Phase

$$h(\cdot), TID_i, TE_i, PTC_i, r_i^*, f_i, e_i, Gen(\cdot), \text{Rep}(\cdot), t, \tau_i.$$

Figure: Information stored into $SC_i$'s memory.