IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# Sensor Authentication in Sensor Networks That Collaborate

[1]Mona, [2] Ms. Paridhi Tutlani
[1]MTech (CSE), [2]Asst. Prof. of CSE DEPTT
[1]Computer Science of Engineering
[1]RPS College of Engineering &Technology,
Balana, Mahendergarh (Haryana)

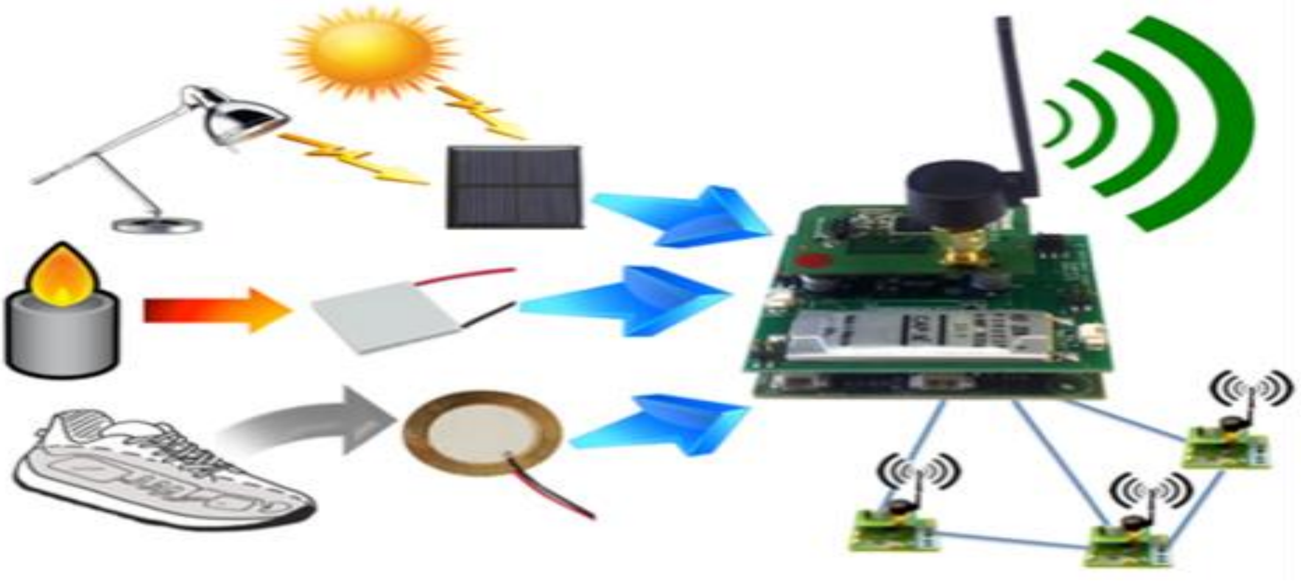
*Abstract:* In this thesis, we have a tendency to address a brand new security drawback within the realm of collaborating device networks. By collaborating device networks, we have a tendency to discuss with the networks of device networks collaborating on a mission, with every device network is severally closely-held and operated by separate entities. Such networks square measure sensible wherever variety of freelance entities will deploy their own device networks in multi-national, commercial, and environmental situations, and a few of those networks can integrate complementary functionalities for a mission. Within the state of affairs, we have a tendency to address associate degree authentication drawback whereby the goal is for the Operator Oi of device Network Si to properly confirm the quantity of active sensors in Network Si. Such a retardant is difficult in collaborating device networks wherever different device networks, despite showing associate degree intent to collaborate, might not be fully trustworthy and will compromise the authentication method. We have a tendency to propose 2 authentication protocols to deal with this drawback. Our protocols place confidence in Physically Unclonable Functions, that square measure a hardware based mostly authentication primitive exploiting inherent randomness in circuit fabrication. Our protocols square measure light-weight, energy economical, and extremely secure against variety of attacks. To the simplest of our information, ours is that the 1st to addresses a sensible security drawback in collaborating device networks.

**Keywords**: Sensor, Path. Routing, Algorithms

## Introduction

The Wireless Sensor Network (WSN) is an infrastructure-free wireless network that uses an ad-hoc deployment of a large number of wireless sensors to monitor system, physical, and environmental factors.

WSN uses sensor nodes with an inbuilt processor to manage and monitor the environment in a specific area. As WSN system's base station is connected to the Internet to share data. They are linked to the Base Station, which serves as the WSN System's processing unit. A WSN system's base station is connected to the Internet to share data.



Wireless Sensor Network

In many military and commercial environments, wireless sensor networks are proving to be critical technology. Practical requirements in both military and civilian contexts imply that sensor networks will not operate totally independently in the near future, but will instead collaborate on mission duties with peer networks owned and maintained by other groups. Complete trust across collaborating networks is not practical when missions involve different countries and/or business viewpoints. Consider the two circumstances below:

**Multi-Country Scenario**

There are numerous natural events that can occur and influence multiple countries. Earthquakes can wreak havoc over various countries, volcanic ash can blanket hundreds of square miles, and tsunamis can wipe out entire coastlines. Detecting these events in order to provide early warning and relief is critical for all countries vulnerable to such a calamity, and larger sensor nets can be deployed by working with neighboring countries to identify such phenomena as they form and occur at greater distances. However, perfect trust is unlikely because each country will have its own interests and agendas that may or may not be beneficial to the other cooperating countries (pollution and climate policies, etc.).

A Business/Environmental Scenario

With commercial and environmental applications of sensor networks, such as soil monitoring, weather prediction, healthcare, and so on, there is now interest in sensor-clouds [1, 2, 3, 4], which combine multiple independent sensor networks into a cloud framework to provide services that a single sensor network cannot provide. Individual networks from competing enterprises and organizations are likely to damage overall network and service functionality for selfish reasons.

## ***SMART OBJECTES***

Sensor Networks: Wireless and Ubiquitous. Small wireless sensors can be used to collect information from the physical world in a wide range of situations, from wildfire tracking and animal observation to agriculture management and industrial monitoring, and wireless sensor networks have emerged from this principle. Each sensor sends data to a base station through wireless transmission. As shown in Figure 1.5, sensors assist one another in relaying information to the base station. Since the early 2000s, the topic of wireless sensor networks research has been quite busy, with multiple yearly conferences, numerous journals, and a huge number of annual workshops. To emphasise the sensors' ubiquity, wireless sensor networks are frequently referred to as ubiquitous sensor networks.

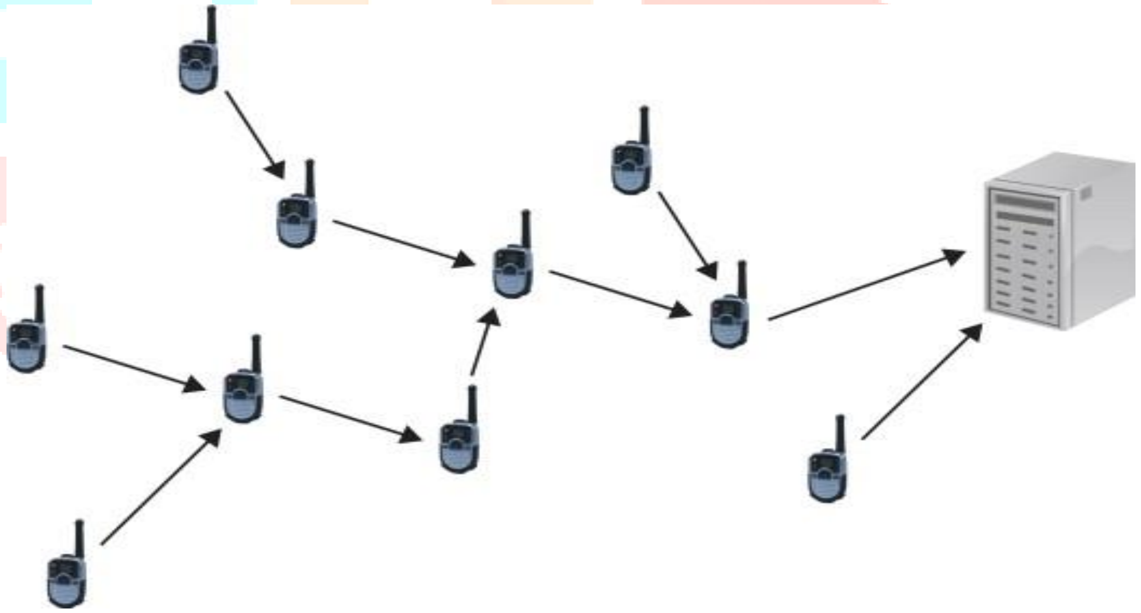


Figure 1.5. Wireless sensor networks provide large-scale measurements of physical properties using large amounts of sensors that transport their data wirelessly to a base station.

## PROBLEM SOLVED

The following issue is addressed in this thesis:

How can the Operator Oi of Network Si correctly authenticate active sensors in its network given n cooperating S1, S2, S3,..., Sn? This problem is clearly peculiar to scenarios in which different sensor networks collaborate, and it is practical because network operators need to know which sensors are active (i.e., operating) in their own network. In the existence of other untrusted sensor networks, the solution to this problem is not simple. Sensors in another network Sj can masquerade as sensors in Network Si, packets can be dropped, corrupted, or replayed during forwarding, and packets can be dropped, corrupted, or replayed when Operator Oi of Network Si submits a query requesting sensors that are active in its network to report.

## PRELIMINARIES OUTLINE

We offer crucial preliminaries about our authentication problem and proposed protocols in this section. The general system model is presented in presents the problem formulation. A number of attacks that compromise the authentication problem are discussed in gives a quick description of Physically Unclonable Functions, which are the key technology employed in our authentication protocols.

## SYSTEM MODEL

This thesis is about a network of sensor networks that are operated independently but collaborate. Figure 1 depicts a simplified scenario in which three sensor networks work together in a deployment field. These sensor networks will be referred to as S1, S2, and S3. As an example, consider S1 to be a network of temperature sensors, S2 to be a network of infrared sensors, and S3 to be a network of seismic sensors. These three sensor networks are owned and operated independently by O1, O2, and O3, and are anticipated to work together in the field and interact with one another. Intruder detection using information from numerous sensors in different networks, despite each sensor network autonomously executing its own, is a feasible application in this scenario mission.

## OUR CONTRIBUTIONS

In this thesis, we suggest two handshaking protocols to overcome the difficulty mentioned above.

Physically Unclonable Functions are used in our protocols (PUFs). PUFs are hardware circuits that allow hardware-based device authentication. A PUF circuit generates a verified response in response to a challenge. The most notable feature of the PUF design is that, because its behaviour is based on the intrinsic unpredictability of physical hardware during creation, it is neither predictable nor clonable. PUFs have been designed with a large number of challenge response pairs up to 264 with minimal increases in circuit overhead and latency, depending on the hardware characteristics and physical properties exploited, such as circuit delays, voltage values at power-up, and ring oscillator frequencies [5]. To overcome the authentication challenge, our protocols combine PUF answers, XOR encryption, and aggregation while being immune to a range of attacks.

## BIBLIOGRAPHY

[1] L. Kulseng, Z. Yu, Y. Wei, and Y. Guan, “Lightweight secure search protocols for low-cost rfid systems,” in Distributed Computing Systems, 2009. ICDCS’09. 29th IEEE International Confferent on. IEEE, 2009, pp. 40-48.

[2] D. Liu and P. Ning, “Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks,” in Network and Distributed System Security Symposium (NDSS), San Diego, February 2003.

[3] D. Liu and P. Ning, “Establishing pairwise keys in distributed sensor networks,” in Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), October 2003.

[4] W. Gu, N. Dutta, S. Chellappan, and X. Bai, “Providing end-to-end secure communications in wireless sensor networks,” IEEE Transactions on Network and Service Management (TNSM), to appear.

[5] D. Malan, M. Welsh, and M. Smith, “Implementing public-key infrastructure for sensor networks,” ACM Transactions on Sensor Networks (TOSN), vol. 4, no. 4, p. 22, 2008. 21

[6] L. Yao, Z. Yu, T. Zhang, and F. Gao, “Dynamic window based multihop authentication for wsn,” in Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010, pp. 744-746.

[7] S. Srivathsa, “Secure and energy efficient physical unclonable functions,” Ph.D. dissertation, University of Massachusetts Amherst, 2012.

[8] I. Verbauwhede and R. Maes, “Physically unclonable functions: manufacturing variability an unclonable device identifier,” in Proceedings of the 21st edition of the great lakes symposium on Great lakes symposium on VLSI. ACM, 2011, pp.455-460.