# Multi-generations Key Pre-distribution's Technique in Wireless Sensor Network

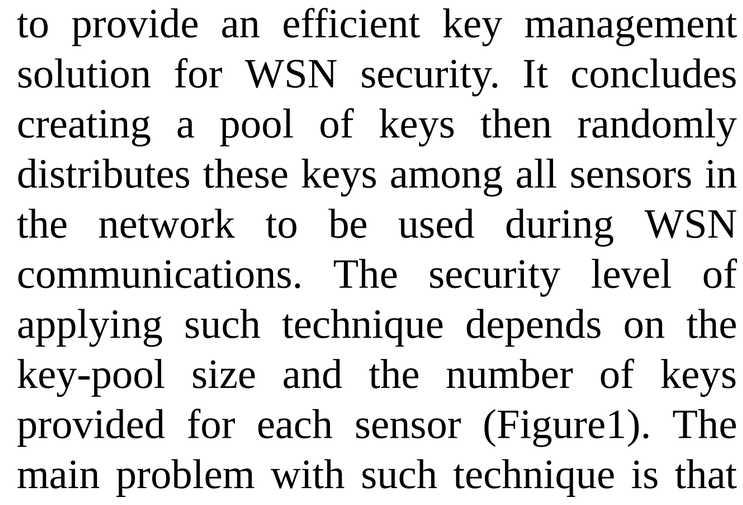
**Mohammed Abuhelaleh and Khaled Elleithy**
**Department of Computer Science and Engineering**
**University of Bridgeport, Bridgeport, CT**

## Abstract

Network future relies nowadays on producing a low-cost and effective network in less cost. One of the most effective network solutions is the Wireless Sensor Networks (WSN). Security is the main challenge of this kind of networks where the nodes in such network are restricted by the power consumption due to limited power source. The main factor of WSN security is the key management part which consists of creating, distributing, and using the keys in the network lifecycle. Key Pre-distribution technique is approved to work efficiently to support WSN security. One of the drawbacks of this technique is that it is not supporting renewing and refreshing keys to support multi-generations sensors. In this work we present a novel technique to reproduce new keys from old pre-distributed keys in efficient way to save the power.

## Introduction

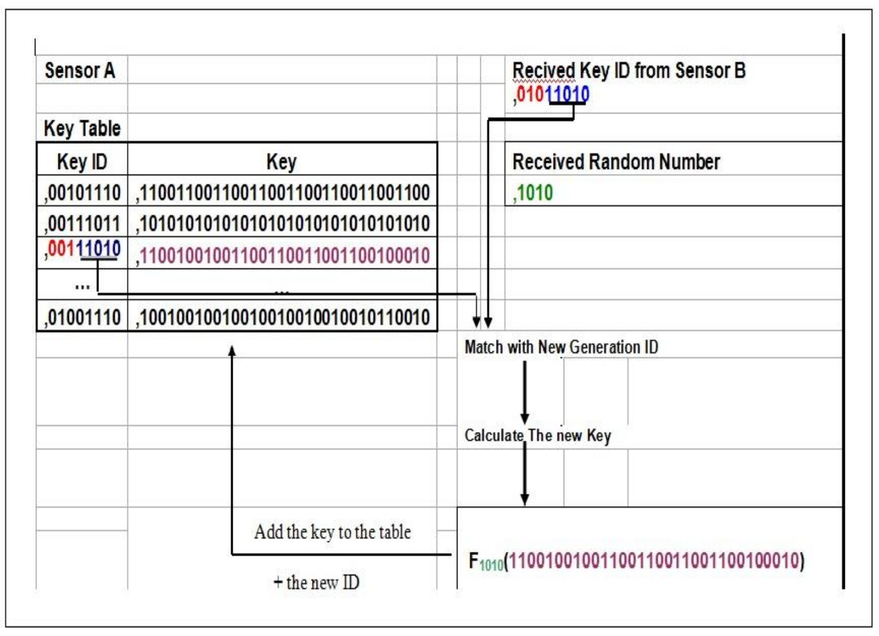
Key Pre-distribution algorithm is proposed to provide an efficient key management solution for WSN security. It concludes creating a pool of keys then randomly distributes these keys among all sensors in the network to be used during WSN communications. The security level of applying such technique depends on the key-pool size and the number of keys provided for each sensor (Figure1). The main problem with such technique is that it is not support the keys renewal or refreshing. This limits the ability of expanding the network by adding new generation of sensors. In our work, we provide a novel and an efficient algorithm to support this weakness of the original protocol. This algorithm is part of a complete solution we are working for to provide an efficient and secure communication for WSN.



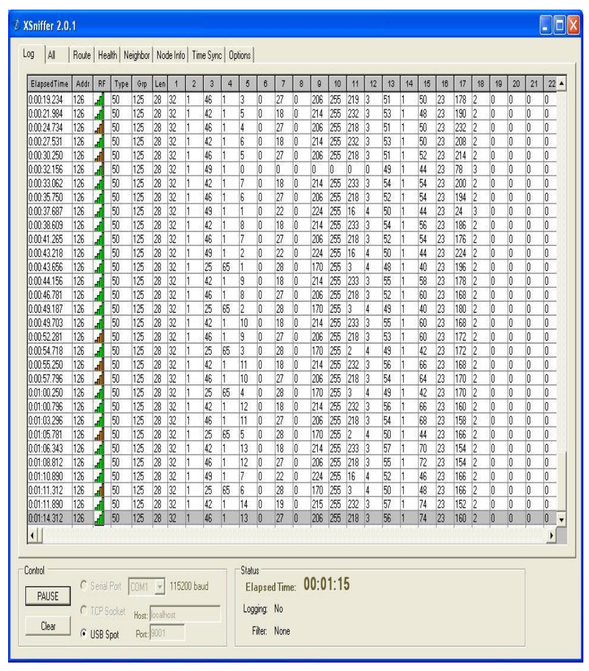

Security level

## Multi-generations Algorithm

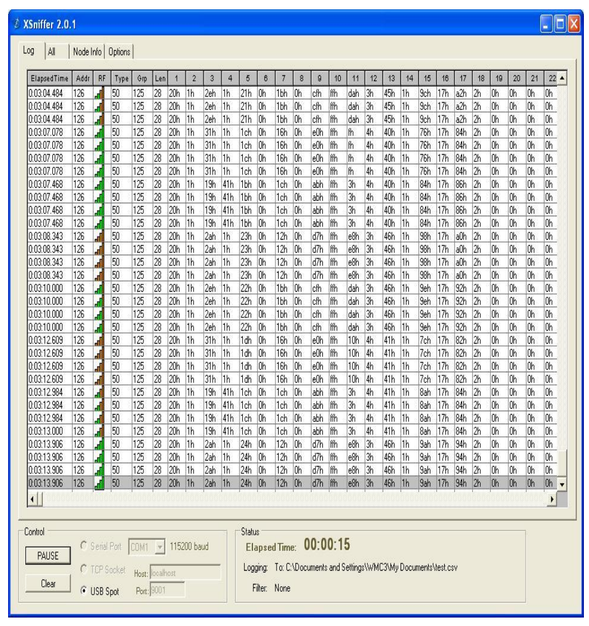
The B.S. randomly generates a number of keys and assigns key ID to each key. The key has to start with a specific flag that represents the first generation of key (i.e. 001 for example). The B.S. then randomly distributes groups of these keys on the sensors, like in KD method, prior to network deployment. The B.S. station also distributes a formula of one way function to all sensors. In addition to that, the B.S. station distributes some random numbers with unique IDs for each number (the formula and the numbers are the same for all sensors). After a period of time, the B.S. may refresh its keys by calculating a new value of each key using its related old key, and one of the numbers that are previously distributed to the sensors. The new ID for the key will be the second generation flag plus the old key (i.e. 0010… for example). B.S. then distributes the new group of keys on its new sensors. Moreover, B.S. may broadcasts some updated keys to the sensors that have been compromised by intruders (using the secret key, or public key of the specific sensor).




## Data Collected



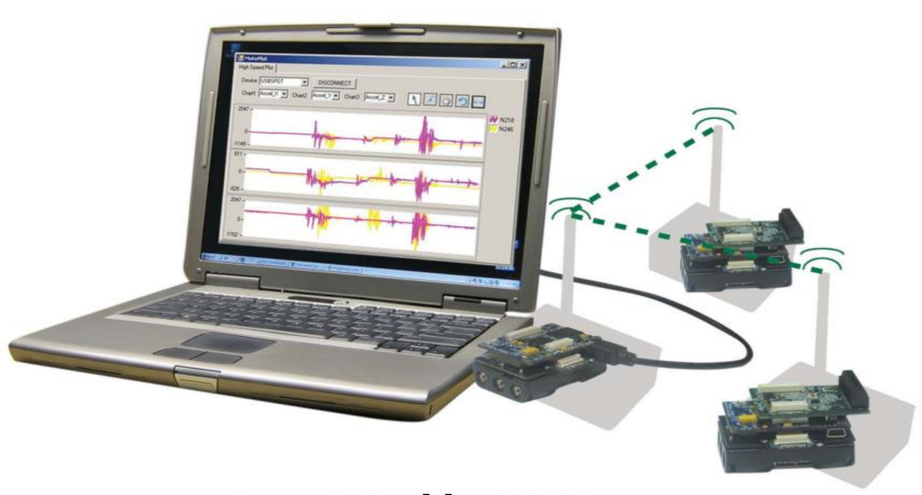

Temperature Collected by sensors (Unencrypted)




Temperature Collected by sensors Unencrypted

## Implementation

We applied this algorithm on a small WSN using Imote2.Builder Sensor with Imot2 sensor board loaded with .NET micro-framework. We programmed these sensor using C#. The experiment is to collect the current temperature from 9 sensors distributed in different places. All the information sent via this network is encrypted using the keys produced by our algorithm



Imote2.Builder WSN setup

## Conclusion

This work presents a novel algorithm to produce new keys from the existing keys in WSN with a low power consumption. In addition, this work shows a real experiment that has been applied on WSN using this algorithm. The experiments verified the efficiency and simplicity of our algorithm. The experiment also approved the ability of our algorithm to be applied in Object Oriented Language which gives this algorithms all the benefits of Object Oriented concepts.