# Air pollution monitoring with secure low-cost Vehicular Sensor Networks

*György* KOLUMBÁN-ANTAL[1], *Vladko* LASAK[1], *Razvan* BOGDAN[1, *], and *Bogdan* GROZA[1]

[1]Politehnica University of Timisoara, Pta. Victoriei, no. 2, 300006, Timisoara, Romania

**Abstract.** Counteracting the effects of air quality degradation is one of the main challenges in large cities today. To achieve such a goal, the first step is to control the emissions of various pollutant gases which in turn requires their concentrations to be measured such that proper methods can be applied. In this work we present a low cost urban air pollution monitoring system which we developed as proof-of-concept in Timisoara, Romania. The proposed solution is a Vehicular Sensor Network (VSN), with affordable mid-class sensor nodes being installed on moving vehicles, ideally on the public transportation busses. The system measures temperature, humidity, the concentration of CO2 and dust, along with Volatile Organic Compounds (VOC). The aim of collecting weather data is to build correlations between air pollution levels and different weather conditions. In addition to technical constraints for measuring air quality, one of the challenges that we address is to implement secure transmissions between the devices. This raises several difficulties on microcontrollers that we use due to their low memory and computational resources. To answer both privacy and security issues, the proposed data transmission protocol of the measuring system, builds upon a modified version of the Station to Station (STS) protocol which allows secure tunnelling in an anonymous manner.

## 1 Introduction

Air quality of urban environments has recently become one of the serious issues in our society due to its clear implications on population's health. Authorities seek to not only to monitor the quality of air, but also to find specific measures which can counteract the effects of different pollutants. A number of fixed stations have been placed around the big cities of the world, but the cost associated with those are high [1]. An alternative to this is the implementation of mobile solutions. The idea on which these systems rely is that a single node covers a large urban space and retains the location of every single measurement. Such solutions rely on high precision gas sensors that come with increased deployment and maintenance costs. An alternative to this type of sensors is the low-cost mid-class sensors which are designed for indoor air quality measurements, but can be successfully used for outdoor operation.

This paper presents a low cost mobile urban air pollution monitoring system based on mobile sensor nodes and mid-class sensors. The solution forms a Vehicular Sensor Network (VSN), in which the used sensor nodes are placed on moving vehicles. It has been previously demonstrated [1], that public transportation fleet presents the most appropriate vehicles to be used in a city because they cover a large geographical area in a short time. This paper presents experimental set-up and results in the town of Timisoara, situated in the West part of Romania. Giving the fact that the data is transmitted wirelessly by the sensors forming the network, in order to assure the security of privacy in the VSN, a modified version of the Station to Station (STS) protocol is implemented.

Our work is structured as follows: section II presents the state-of-the-art regarding VSN, while section III offers the architecture of the system. Results are presented in section IV and further developments are highlighted in section V.

## 2 Previous work

In order to control the emissions of different pollutants, different systems have been developed around the world. Previous results on air pollution monitoring for the town of Timisoara, in Romania exists in [2]. The proposed solution comprises of hand-held mobile devices which are covering different parts of the city, but the dataset is limited since monitoring was manual. Based on the gathered data, different predictions are offered for the uncovered areas. Taking into account the advantage of mobility, Vehicular Sensor Networks have been offered as monitoring solution by different authors. Such networks are formed by mobile sensor nodes. In [3], VSN are combined with Vehicular Ad-hoc NETworks (VANET) in order to reduce the costs associated with communication. In [1] the urban air quality measurement is accomplished by using a VANET. The bus fleet of Palermo, in Italy, was used to accommodate the sensor nodes. The data regarding air quality is gathered during bus trips, but this solution is not providing real time pollution monitoring due to the fact that

[*] Corresponding author: razvan.bogdan@cs.upt.ro

the data is uploaded to a central server when the bus arrives to each station. In [4] is presented a VSN air pollution monitoring network based on low-cost gas sensors. This approach does not discuss any security issues involved in the deployment of such solution.

The problem of security in Wireless Sensor Network has been largely addressed in the literature. One of the central issues is how to securely exchange a session key that can be later use to perform encryption and message authentication. Pair-wise key sharing and pre-distribution of secret keys has been extensively studied for WSN, e.g. [5]. To facilitate an interactive key exchange between sensor nodes, the use of asymmetric cryptography is the only alternative. Elliptic curve cryptography has been previously deployed for sensor networks in [6]. The advantage coming from the use of elliptic curves stems from the small key sizes that are more convenient for WSN.

## 3 Secure data transmission

The proposed system (Figure 1) has several sensor modules equipped with air quality sensors and low cost microcontrollers. These modules are uploading the collected data to the central server. Because the data is being sent over the Internet, encryption and authentication are mandatory. However, not all of the existing communication protocols are designed for the low computational power and constrained memory of common microcontrollers. Therefore, we had to design a custom communication protocol to assure security for our setup.

The communication between the sensor modules and the central server is performed in two phases. During the first phase, authentication and secure key exchange is performed between the parties. The second phase is the actual encrypted data transfer.

The authenticated session key exchange is done with the Diffie-Hellman key exchange inside the Station-To-Station (STS) protocol [7]. The STS protocol is implemented by the use of Elliptic Curves Cryptography (ECC) [8] for the underlying asymmetric key exchange. ECC is the preferred choice for our system because it offers high security, with relatively low key sizes (256 bit instead of 1024-2048 bits in case of the regular RSA). This way the memory usage is considerably reduced.

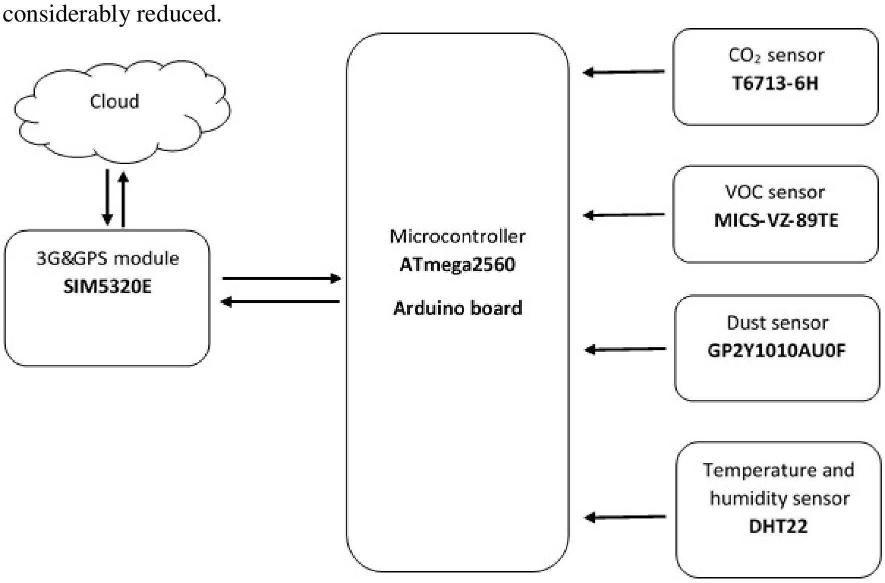

**Figure 1:** The proposed system

We use STS to achieve a secure instantiation of the Diffie-Hellman key exchange, which otherwise is susceptible to Man In The Middle (MITM) attacks. To achieve this, STS provides authenticity for the messages exchanged by the use of digital signatures. The original version of the STS protocol involves a Trusted Third Party (TTP) that assures the authenticity of the public keys. Since our devices share a common production history, the nature of the system makes it possible to share the public keys before the deployment. In this way the public authentication are hardcoded for the central server and the sensor modules.

Since these are public-keys, keeping them secret is not a requirement but it implicitly makes it harder for an adversary to obtains the private authentication keys. The key exchange in general is a time consuming operation and it is not performed before each data transfer session. Instead each session key exchanged is identified by a session key identifier and using this identifier the sensor module can reuse the session key for multiple data transfers.

After the key exchange is performed, the second phase of the protocol starts. This data transfer phase is based in the Encrypt-than-MAC paradigm [9]. First, an encryption key and a Message Authentication MAC key are computed from the secret session key. Then, the data to be transferred is symmetrically encrypted using the encryption key. In order to prevent tampering on the encrypted data, the HMAC code is computed with the newly obtained MAC key. Finally, the encrypted message and the HMAC code are concatenated and a message is sent to the central server. The central server provides his response in a similar way. As an extension to the basic Encrypt-than-MAC paradigm, a counter value is also encrypted together with the data. The encrypted counter is required in order to prevent reply attacks.

The proposed method has been implemented on a low-cost microcontroller having a clock speed of 16Mhz and 8kb RAM. Elliptic curve secp256k1 has been selected for the ECC algorithms. This way, the proposed protocol offers authenticated and encrypted data transfer for microcontrollers with low computing performance and low memory.

## 4 Experimental results

Measurements have been taken on two consecutive days on the streets of Timisoara. On the first day (Saturday 19.05.2018) the traffic was usual. On the second day (Sunday 20.05.2018) the traffic was reduced. The used sensor module had been equipped with multiple sensors. The T6713 sensor was used to measure the $CO_2$ concentration in the air. The measurements were visualized using two representations: histograms and pollution maps. The histograms show the distribution of measured values for each sensor. The number of measured values is represented on the vertical axis. The horizontal axis divides the measurement interval into subranges having equal lengths. Pollution maps illustrates the measured values together with their location. Colours from red to green are used to represent the pollution level. These colours distinguish between the degree of pollution as follows: green stands for the minimal measured value and red stands for the maximal measured value.

The $CO_2$ levels are represented in Figure 2. It can be observed that most of the $CO_2$ levels are situated between 508 ppm and 532 ppm during Saturday.

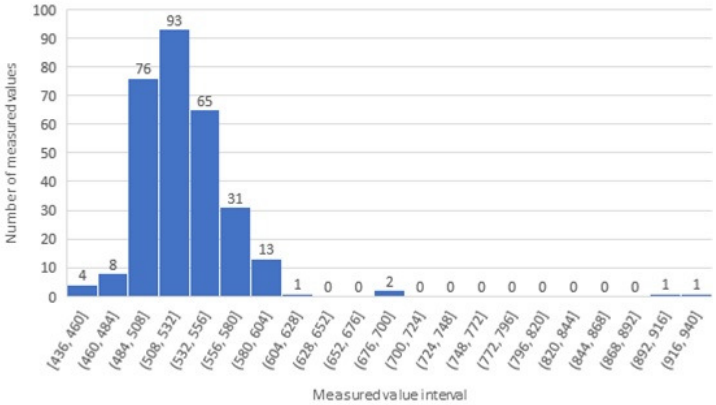

**Figure 2: CO2 concentration histogram for 19.05.2018**

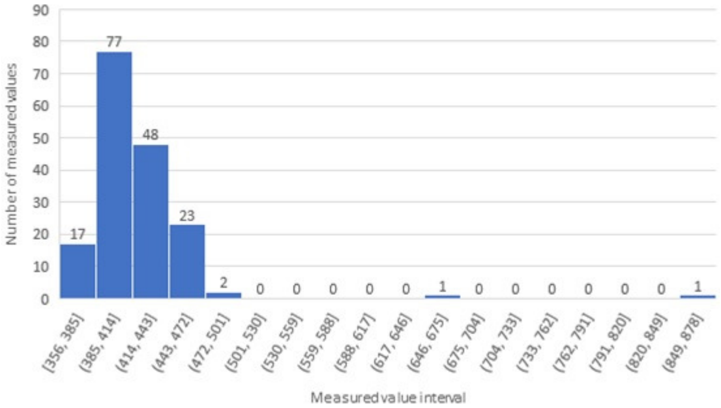

**Figure 3:** CO2 concentration histogram 20.05.2018

The $CO_2$ levels dropped on Sunday (Figure 3). Most of the measured values were between 385 ppm and 414 ppm. Currently the average concentration of atmospheric $CO_2$ is 408 ppm according to [10]. During the two days, the measured $CO_2$ concentrations were relatively close to this average value.

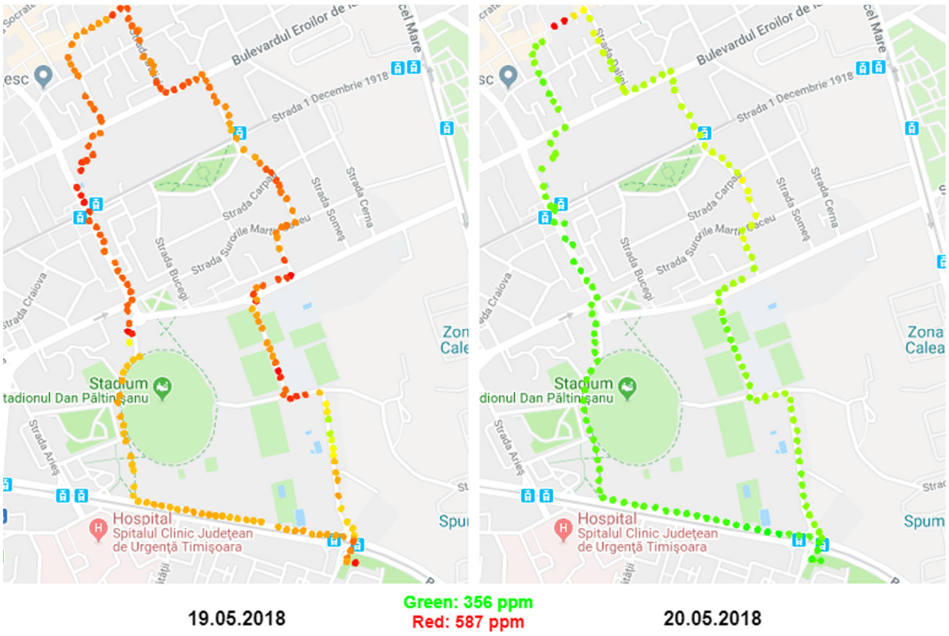

**Figure 4:** CO2 concentration maps

It can be noticed that there is a difference between the two datasets, which is highlighted by the pollution map (Figure 4). Slight variation of the $CO_2$ concentration is observable between the different measurement locations.

The sensor module was also equipped with: GP2Y1010AU0 sensor, used to measure the dust concentration; MICS-VZ-89TE sensor, used to measure VOCs (Volatile organic compounds); DHT22 sensor, used to measure the temperature and humidity.

| Measured parameter | Minimum | Average | Maximum | Measurement unit |
|---|---|---|---|---|
| Carbon dioxide ($CO_2$) | 356 | 489.51 | 587 | ppm |
| Dust concentration | 0 | 98.61 | 177 | µg/m$^3$ |
| VOC | 0 | 10.97 | 20 | isobutylene equivalent |
| Temperature | 20.2 | 25.44 | 32.1 | C$^o$ |
| Humidity | 25.7 | 34.9 | 44.4 | % |

**Table 1:** Minimum, average and maximum sensor values

The GP2Y1010AU0 sensor and the MICS-VZ-89TE sensor are measuring total dust concentration, respectively total VOC. Statistical results for each measured parameter are represented in Table 1.

## 5 Conclusion

Our work presents a low cost system for urban air pollution monitoring. The advantages of our system are twofold. First, the system uses mobile sensor nodes, so the number of sensors requires is lower compared to the fixed stations alternative. Secondly, the sensor modules were equipped with mid-class sensors which are able to measure urban pollution ($CO_2$, dust and VOC) with sufficient accuracy. Furthermore, the price of the mid-class sensors is considerably lower compared to their high-end counterparts. Finally, authenticated and encrypted data transfer has been implemented on the low cost microcontrollers from our setup. Using the ECC variant of the STS protocol, even 8 bit microcontrollers were able to perform secure data transfer using standard 256-bit elliptic curves.

## References

[1] G. Lo Re, D. Peri, S. D. Vassallo, "Urban Air Quality Monitoring Using Vehicular Sensor Networks," in *Advances onto the Internet of Things. Advances in Intelligent Systems and Computing*, Springer, 2014, pp. 311-323.

[2] M. Lungu, N. Stefu, "Study on particulate matter dispersion by correlating direct measurements with numerical simulations: Case study—Timisoara urban area," *International Journal of Environmental Science and Technology,* vol. 15, no. 7, pp. 1441-1452, 2017.

[3] S.-C. Hu, Y.-C. Wang, C.-Y. Huanga, Y.-C. Tseng, "Measuring air quality in city areas by vehicular wireless sensor networks," *Journal of Systems and Software,* vol. 84, no. 11, pp. 2005-2012, 2011.

[4] S. Devarakonda, P. Sevusu, H. Liu, R. Liu, L. Iftode, B. Nath, "Real-time air quality monitoring through mobile sensing in metropolitan areas," in *2nd ACM SIGKDD International Workshop on Urban Computing (UrbComp '13)*, New York, NY, USA, 2013.

[5] D. Liu, P. Ning, "Establishing pairwise keys in distributed sensor networks," *Proceedings of the 10th ACM conference on Computer and communications security,* pp. 52-61, 2003.

[6] A. Liu, P. Ning, "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks," in *International Conference on Information Processing in Sensor Networks*, 2008.

[7] W. Diffie, P. C. Van Oorschot, M. J. Wiener, "Authentication and authenticated key exchanges," *Designs, Codes and Cryptography,* vol. 2, no. 2, pp. 107-125, 1992.

[8] V. S. Miller, "Use of Elliptic Curves in Cryptography," in *Advances in Cryptology — CRYPTO '85 Proceedings. CRYPTO*, 1985.

[9] M. Bellare, C. Namprempre, "Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm," in *International Conference on the Theory and Application of Cryptology and Information Security*, Berlin, 2000.

[10] "CO2Earth," 19 05 2018. [Online]. Available: www.co2.earth.