Advanced IoT Solution for Smart City Eco-monitoring System

Sergey Bezzateev, Natalia Voloshina, Konstantin Zhidanov
Department of Information Security Technologies, Saint Petersburg State University of Aerospace Instrumentation
St. Petersburg, Russia
bsv@aanet.ru, natali@vu.spb.ru, konstantin.zhidanov@gmail.com

***Abstract*—Adaptive, scalable and secure smart city eco-monitoring system is considered. This eco-monitoring system is based on use of sensors that support wireless communications (WiFi protocol). In this system each sensor controls several eco-monitoring parameters and also transfers collected eco-data to the base station using network infrastructure. For this purpose several eco-sensors are connected to each sensor. Also each sensor could transfer data from other sensors of its network to the base station. This approach allows to get good scalability and adaptive reconstruction of the eco-monitoring network. All mentioned above means that for the purpose of eco-monitoring the IoT approach is suggested. The system of sensors, work status control, sensors initialization and network topology change was designed by specially developed software platform 'Galouis'.The platform allows users to create efficient software for such systems. Proposed approach also provides secure work of eco-monitoring system by sensor authentication and secure data of authorized sensors transmission through created eco-monitoring network. Important feature of proposed system is that secure adding of new sensors is realized for earlier created eco-monitoring network. This feature makes possible to provide secure and flexible scaling for such systems. Also for the purpose of security and scalability special protocols of secure sensor extraction was proposed. Ultimately this approach makes it possible to move sensors from one eco-monitoring network to another either from one network segment to another segment in secure way.**

I. Introduction

Nowadays a lot of different applications are looked at as applications of eco-monitoring on IoT approach. For smart city applications could be mentioned such global tasks [1]:

- **Cities eco-monitoring:**
  - Structural health: monitoring of vibrations and material conditions in buildings, bridges and historical monuments,
  - Noise urban maps: sound monitoring in bar areas and centric zones in real time,
  - Smart lightning: intelligent and weather adaptive lighting in street lights,
  - Waste management: detection of rubbish levels in containers to optimize the trash collection routes,
- **Environment eco-monitoring:**
  - Forest fire detection: monitoring of combustion gases and preemptive fire conditions to define alert zones,
  - Air pollution: control of CO_2 emissions of factories, pollution emitted by cars and toxic gases generated in farms,
  - Landslide and avalanche prevention: monitoring of soil moisture, vibrations and earth density to detect dangerous patterns in land conditions,
  - Earthquake early detection: distributed control in specific places of tremors,
- **Water:**
  - Water quality: study of water suitability in rivers and the sea for fauna and eligibility for drinkable use,
  - Water leakages: detection of liquid presence outside tanks and pressure variations along pipes,
  - River floods: monitoring of water level variations in rivers, dams and reservoirs,
- **Security and emergencies:**
  - Perimeter access control: access control to restricted areas and detection of people in non-authorized areas.
  - Liquid presence: liquid detection in data centers, warehouses and sensitive building grounds to prevent break downs and corrosion,
  - Radiation levels: distributed measurement of radiation levels in nuclear power stations surroundings to generate leakage alerts,
  - Explosive and hazardous gases: detection of gas levels and leakages in industrial environments, surroundings of chemical factories and inside mines,
- **Industrial control:**
  - Indoor air quality: monitoring of toxic gas and oxygen levels inside chemical plants to ensure workers and goods safety,
  - Temperature monitoring: control of temperature inside industrial and medical fridges with sensitive merchandiser,
  - Ozone presence: monitoring of ozone levels during the drying meat process in food factories,
  - Indoor location: asset indoor location by using active (ZigBee, UWB) and passive tags (RFID/NFC).
- **Agriculture:**
  - Wine quality enhancing: monitoring soil moisture and trunk diameter in vineyards to control

the amount of sugar in grapes and grapevine health,
  - Green houses: control micro-climate conditions to maximize the production of fruits and vegetables and its quality,
  - Golf courses: selective irrigation in dry zones to reduce the water resources required in the green,
  - Meteorological station network: study of weather conditions in fields to forecast ice formation, rain, drought, snow or wind changes,
  - Compost: control of humidity and temperature levels in alfalfa, hay, straw, etc. to prevent fungus and other microbial contaminants,

- **Animal farming:**
  - Offspring care: control of growing conditions of the offspring in animal farms to ensure its survival and health,
  - Animal tracking: location and identification of animals grazing in open pastures or location in big stables,
  - Toxic gas levels: study of ventilation and air quality in farms and detection of harmful gases from excrements.

A secure IoT eco-monitoring sensor network approach could be used to solve some of tasks mentioned above. An example of such eco-monitoring sensor network is shown on Fig. 1. It could be noted that the distance between sensors should be less that the radius of their radiochannel range. Important to notice that geometry structure of sensor network is not fixed and is rather flexible. Nodes could disconnect from network and connect again or move to another segment of network. Such actions could change sensor network topology. Obviously usage of distributed sensor networks with flexible topology (Fig.1) causes necessity to connect, move and change location of its sensors. This entails necessity to use simple and secure sensor authentication protocol.

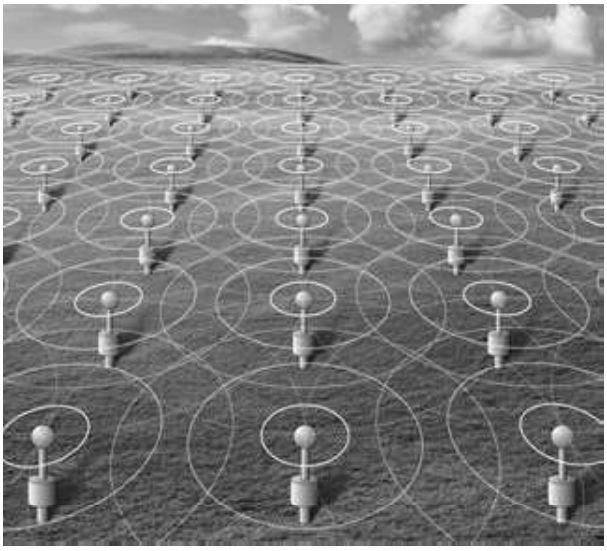

Fig. 1. Wireless sensor network for eco-monitoring

The main problem for flexible sensor networks is that there is no single authentication center. Such center should provide storage, treatment and delivery of authentication certificates to sensor network nodes. Such single authentication center allows to get public key infrastructure (PKI). If single authentication center could be obtained it is easy to perform mutual nodes authentication and secret key generation for secure data transmission. If there is no possibility to get single authentication center (for example if sensor network topology is flexible) a great demand to create and use reliable authentication protocol is appear. The same situation is also for software that makes it easy and effective to control such secure sensor networks for which their elements could be simple and resource limited devices like Arduino, Intel Edison ,etc.

II. Related works

In [2] one type of a distributed sensor network construction with the possibility of information received from the other sensor retransmission is proposed. This variant is used when there is no direct connection with the base station. This approach make it possible to configure sensor network with complex topology. So it becomes possible to transmit a lot of eco-monitoring data collected on a large territory with reduced number of base stations. One of the most important disadvantages of the system proposed in [2] is that there are no approaches for secure transition. In this situation any illegal sensor could be connected to the sensor network and fake data could be sent to the eco-monitoring system. As a result the problem of information security for such sensor network based eco-monitoring systems becomes actual. And an initialization and mutual sensors authentication protocols should be realized for these systems.

III. Security and scalability for eco-monitoring sensor networks

When constructing special kind of sensor networks with variable topology critical issues of security in the transmission and data processing appear. Also a very critical problem is to provide secure connection of new devices to the already existing network.

In the situation when certificate infrastructure supported by trusted authority is unavailable the system of mutual network device authentication becomes much more complicated [3].

This section is focused at possible solutions for such sensor networks creation and supporting with secure mutual authentication of their sensors (devices) that could be used for smart city eco-monitoring goals.

For simplicity we assume that network components could be classified at only two types of devices:

- Gateway or access point(AP) that is used for collecting sensor data. In common approach access point could also perform preprocessing of incoming sensor data and its retranslation to some cloud storage where information from eco-sensors should be stored, processed and issued on user requests.
- Sensors are network devices that are equipped with eco-sensors to collect specified environmental parameters (for example temperature, humidity, noise level

etc.). Such sensor could have other direct connection with access point (AP) or could transfer data through the network (neighbor devices) to AP.

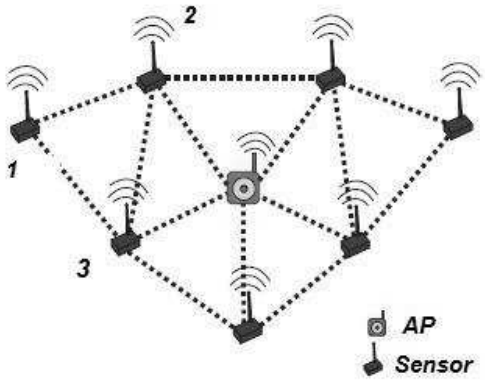

Fig. 2. Wireless sensor network structure

There are main steps in the process of flexible sensor network creation and its support taking into account that this network should be secure:

1) **Sensor initialization.** It means that new sensor should be connected to any available sensor from the network or access point (network devices). The availability means that such network device should be located in radio channel radius of new sensor. Let's assume that both type of devices have similar features from information security point of view. In this case we can consider two possible scenarios in general:
   - First initialization of several sensors (simultaneously) in one secure network. This situation is common for initial network deployment when number of devices (sensors) is more than two $k > 2$.
   - Adding new sensor to the existing secure sensor network.
2) **Stable sensor network functioning.** In this case sensors are not added, not excluded and their position is not changed in respect to their neighbor sensors (position is an appearance in radio channel radius).
3) **Removal sensor from the sensor network.** In this case there could be two situations:
   - Removed sensor is excluded from particular secure sensor network and could be used in the future only after new network initialization.
   - Removed sensor will be added to another segment of existing secure sensor network.

Let's look more precisely at each of mentioned scenarios based on the group of protocols that use master key of sensor network [4], [5], [6], [7] for initial authentication. At the first step of the sensor network initialization it is necessary to provide mutual authentication of the sensors of single network segment. The segment is specified by the radio channel radius of defined data transfer protocol (NFC, Bluetooth, ZigBee,

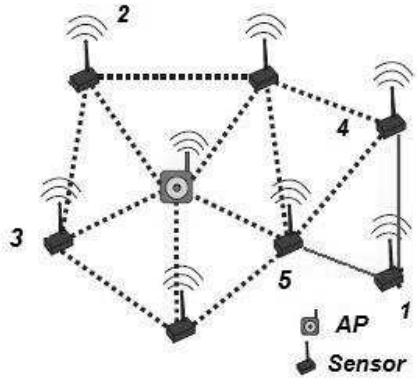

Fig. 3. Sensor moving to another network segment

WiFi, etc.). The main difference between common mutual authentication protocols for sensor networks on the stage of initialization is a level of master key protection on the next steps of network life cycle:

1) Master key that was used on the step of initialization is not destroyed and it is kept in the so called "tamper resistance memory" of network device (sensor) [6], [5]. This approach makes it easy to change the configuration of the network by simple displacement of the earlier installed sensor from the one segment of the secure network to another (3). Displaced sensor can easy authenticate with any other "neighbor"sensor in the same sensor network if this sensors have the same master key. However this feature becomes disadvantage in case if it is necessary to prevent illegal movement (for example if we want to be sure about geo-location of the eco-sensors). In this case we should have additional user authentication protocol for user who want to make legal movement. It means that only authenticated user should have possibility to move sensor from one segment of the secure network to another. Any movement of sensors should be prohibited for unauthenticated user in secure sensor network.
2) Master key that was used on the step of initialization is destroyed after predefined time interval that calculated from the moment when initialization step is completed [7]. This scenario strongly limits the possibility of earlier installed sensor movement from the initial sensor network segment to another part of the same network. This feature of the protocol makes it possible to obtain rather stable structure of secure sensor network. In this case the probability to get false information from the network sensors if this information is false because of sensor location change is significantly reduced.

Obviously for the smart city eco-monitoring purposes the second protocol should be preferred from the point of view to get reliable information about ecological situation in different parts of the city.

This protocol could be described in common way as written

below:

A. First initialization of several sensors for new secure sensor network

- At the beginning the master MK key is defined for new secure sensor network. Each of sensors i that should be installed should have its own unique identification number ID_i.Here we assume that $ID_i > ID_j$ $i > j$. Next we should define one-way function - $H(*)$.
- While the first initialization of sensor network sensors exchange their unique identification n umbers with each other only with those sensors who are inside their radio channel radius. This situation is shown on the Fig.2 where sensors $1, 2$ and 3 exchange their unique identification numbers $ID_1, I\ D_2 ID_3$.
- Each of them uses information about unique identification numbers of other sensors and master key MK to calculate pair keys for mutual authentication. For example sensor 1 calculates pair keys for sensors $2, 3$:

$$K_{1,2} = H(ID_1||ID_2||MK),$$
$$K_{1,3} = H(ID_1||ID_3||MK),$$

where $x||y$ means concatenation of verbless x and y.

Consequentially sensors $2, 3$ also calculate the same pair keys for sensor 1:

$$K_{2,1} = H(ID_1||ID_2||MK) = K_{1,2},$$
$$K_{3,1} = H(ID_1||ID_3||MK) = K_{1,3}.$$

- To obtain the scalability feature for this secure sensor network each sensor also calculates auxiliary key $K_{i,i} = H(ID_1||MK)$ for adding new sensors in future.
- Each sensor deletes its master key MK after predefined time T_{kill} from beginning of the first initialization process. In this way sensor 1 on the Fig. 2 should save such information $\{K_{1,1}, K_{1,2}, K_{1,3}\}$. after the end of the first initialization.

B. Stable sensor network work

In the working process for mutual authentication and generation of session key sensors use pair keys that they obtain while first initialization. For example sensors 1 and 2 use pair keys $K_{1,2}$ and $K_{2,1}$ consequently.

C. Adding new sensor to existing secure sensor network

According to the scheme that is represented on the Fig. 4 new sensor new appears in the radio network radius of sensors 1 and 2 of existing stable secure sensor network.

New sensor should create pair keys for neighbor sensors 1 and 2. To create such pair keys the new sensor uses master key MK that was preinstalled earlier and calculates new pair keys

$$K_{new,1} = H(ID_1||MK) = K_{1,1}$$

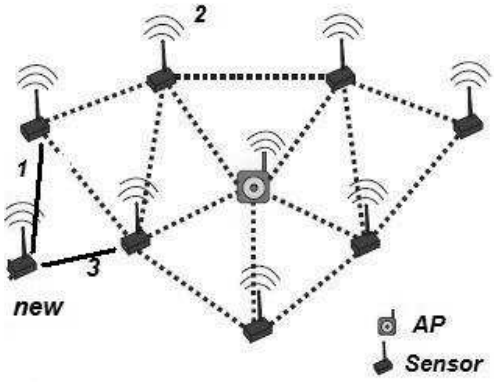

Fig. 4. New sensor connecting

and

$$K_{new,2} = H(ID_2||MK) = K_{2,2}$$

to get connection with sensors 1 and 2 consequently. These generated pair keys make possible to work in secure way through existing secure sensor network for new device. In this case new device could be mentioned as legally added.

On the next step sensor new should delete its master key MK. But before deletion of master key a new auxiliary key $K_{new,new}$ should be created by new device. As a result new added sensor will store following key sequence $\{K_{new,new}, K_{new,1}, K_{new,2}\}$ after initialization process for existing secure sensor network (Fig.4).

D. Illegal sensor moving to another secure sensor network segment of existing network

In case of illegal movement of sensor from initial secure sensor network segment to the new one (Fig. 3) without rewriting of its master key MK the process of authentication will be failed.This authentication failure will occur because pairwise key that was generated on the initialization step could not be used for new neighbor sensors of new segment due to unique properties of pairwise keys. This property of authentication protocol seriously decrease probability of getting incorrect eco-data when geo-location of legal sensor changes illegally.

IV. "GALOUIS" PLATFORM FOR ECO-MONITORING SECURE NETWORK DEVELOPMENT

To improve efficiency and to make the process of development of IoT secure eco-monitoring systems easier there was developed a special platform "Galouis". This platform makes process of program coding more clear and easier and therefore it takes less time to create such secure eco-monitoring systems. Additionally this platform improves the initialization process by the mechanism of writing master keys MK on sensors. Also it is possible to allocate sensors geo-location on virtual map. Common scheme of proposed secure sensor network including sensors, Smartphone that is used for initialization process, cloud storage that collects, processes and visualizes stored eco-data is shown on Fig. 5.

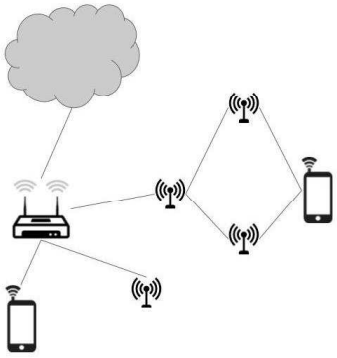

Fig. 5. General scheme for platform ”Galouis” using

”Galouis” platform is a set of components which allows any developers easily build IoT solutions based on ESP8266 module. Platform components are(Fig. 6):

- Firmware (binary image for ESP8266 chip),
- Android software (Java libraries and sample applications),
- Web software (JavaScript library and sample pages),
- Server-side services (user interface, data processing scripts, DB access scripts),
- Database (MySQL schema).

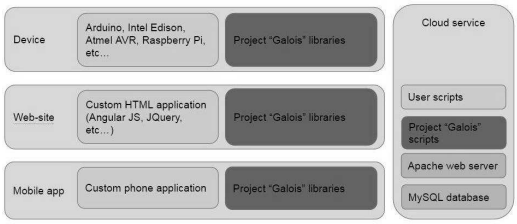

Fig. 6. Components of platform ”Galouis”

Main idea is that any developer only designs a device, web site/mobile appearance, and data processing algorithms. All issues related to security, connectivity and access management are under the hood of ”Galouis” platform. Platform is transparent for developers to perform following actions:

- ”duckling”[11] devices by using any possible channel of user Smartphone (Bluetooth, WiFi, IF, or NFC). For example for NFC it is possible to use OPACITY [8] protocol as a part of duckling procedure.
- access sharing,
- traffic routing between devices,
- web access to devices,
- setting up WiFi credentials at devices.

Device with factory settings doesn’t carry any WiFi credential or user encryption keys. So, device should be initialized before first use - this process is called ”duckling”[11].

Using Java library one can rapidly develop Smartphone user application, so the end-user can easily do following actions:

- Register at server and generate his own encryption key. In this case generated encryption key is stored only on user Smartphone. Also the encryption key can be backed up on server.
- Perform devices initialization (for example by ”duckling” secure protocol).
- Interact with his initialized devices directly when they are located in his Smartphone WiFi range.
- Interact with his devices via system server. In this case all transferred data are protected with end-to-end encryption. As a result data couldn’t be compromised by server.
- Specify WiFi credentials of known access points and deliver them to all his devices.

When initialized, ESP8266 can be accessed by UART. So, it could be used to securely send/receive arbitrary JSON-packed data to/from server or user Smartphone.

According to the proposed approach with ”Galouis” platform and described above protocols there was created prototype of secure eco-monitoring smart city system based on microcontroller $ESP8266$ (Fig. 7). Developed sensors are

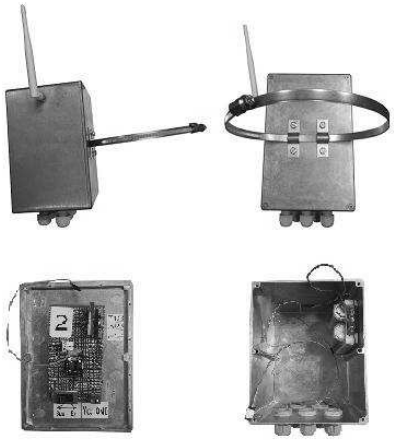

Fig. 7. Sensor box

equipped by eco-sensors of three type: CO_2, radiation and noise level (Fig. 8).

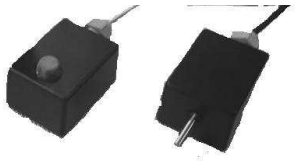

Fig. 8. Data sensors

The usage of retranslation protocols for sensor network jointly with secure pairwise authentication protocols for legal

network sensors makes it possible to cover a large part of controlled territory reliably without additional access points (Fig. 9). That decreases operational cost of the system.

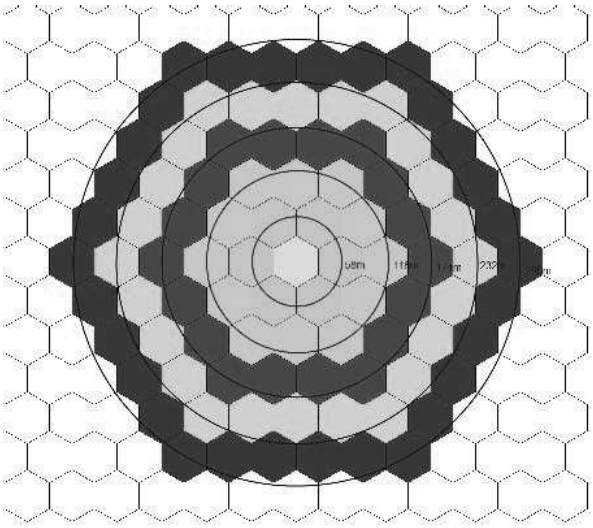

Fig. 9. Covering territory

In developed prototype of eco-monitoring IoT system the maximum speed of data transfer from sensors is not exceeding $800bit/s$ in case when no more then three eco-sensors are connected to each sensor. For such proposed secure eco-monitoring system the territory about $3.5m^2$ could be covered by eco-monitoring system even when sensors are closely located (Table I).

TABLE I. SENSORS NUMBER FOR ECO MONITORING

Zone radius (m)	Covering radius (km^2)	Sensors number
58	0.01	6
116	0.04	18
174	0.10	36
...	...	...
1044	3.42	1026

V. CONCLUSION

The possibility of eco-monitoring network-based system with self-organizing sensors constructing is considered. For sensor mutual authentication in such network a protocol similar to LEAP [7] is used. Such protocol allows to protect a sensor network from unauthorized change it topology and makes it securely scalable. For efficient and fast network initialization, received information processing and for the challenges of changing it configuration platform "Galouis" is developed. Using a mutual authentication secure protocol together with the "Galouis" platform helps to build an efficient, safe and easily scalable sensor network to collect and process ecological information. Proposed approach could be enhanced in a purpose of power optimization. For example one if the secure scheduling could be proposed and investigated.

VI. ACKNOWLEDGMENT

This work was partially financially supported by Dell-EMC corporation. The prototype of developed secure eco-monitoring IoT system was successfully approved in Saint-Petersburg and Novosibirsk cities in current eco-monitoring Smart City programs.

REFERENCES

[1] O. Vermesan , P. Friess, *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*, River Publishers, 2013.

[2] E. Unsal1, M. Milli, Y. Cebi, "Low cost wireless sensor networks for environment monitoring", *The Online Journal of Science and Technology*, v. 6, i.2, 2016, p.61-67.

[3] A. Ometov, K. Zhidanov, S. Bezzateev, R. Florea, S. Andreev, Y. Koucheryavy, "Securing network-assisted direct communication: the case of unreliable cellular connectivity", *InTrustcom/BigDataSE/ISPA, 2015 IEEE*, 2015, Aug 20, vol. 1, pp.826-833.

[4] J. Lee and D. R. Stinson, "Deterministic Key Pre-Distribution Schemes for Distributed Sensor Networks", *ACM Symposium on Applied Computing 2004, Lecture Notes in Computer Science*, vol. 3357, Waterloo, Canada, 2004, pp. 294307.

[5] W. Zhang, M. Tran, S. Zhu and G. Cao, "A Random Perturbation-Based Scheme for Pairwise Key Establishment in Sensor Networks", *Proceedings of MOBIHOC07* (2007), Montreal, Quibec, Canada.

[6] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: efficient security mechanisms for large-scale distributed sensor networks", *ACM Transactions on Sensor Networks*, vol. 2, no. 4, 2006, pp. 500528.

[7] J. Jang, T. Kwon and J. Song, "A Time-Based Key Management Protocol for Wireless Sensor Networks", *Proceedings of ISPEC*, 2007, LNCS 4464, pp. 314328.

[8] V. Petrov, S.Bezzateev, V. Zybin, "Wireless authentication using OPACITY protocol", *InUltra Modern Telecommunications and Control Systems and Workshops (ICUMT), 7th International Congress*, 2015, Oct. 6, pp. 253-258.

[9] "The LOSANT IoT Platform" , Web: https://www.losant.com/iot-platform

[10] "Wio Link", Web: https://www.kickstarter.com/projects/seeed/wio-link-3-steps-5-minutes-build-your-iot-applicat

[11] F. Stajano, R. Anderson, "The Resurrecting Ducking: Security Issues for Ad-Hoc Wireless Networks",*Proc. Seventh Security Proto- cols Workshop, Lecture Notes in Computer Science 1796*, Springer- Verlag, Berlin, 2000, p. 172–182, 1999.