International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

CRASH DETECTION USING SENSOR DATA ON VANETS

Aishwarya.D. Khannukar[1], P.V. Gopikrishna[2], Praveen.Kalkundri[3]

[1]PG Student Electronics & Communication Department, KLS Gogte Institute of Technology, Belgaum. Karnataka, India.
[2]Associate Professor Electronics & Communication Department, KLS Gogte Institute of Technology, Belgaum. Karnataka, India.
[3]Associate Professor Electronics & Communication Department, KLS Gogte Institute of Technology, Belgaum. Karnataka, India.

Abstract - *VANET is a special category of MANET, which fulfills prospect in the further intelligent transporting system by giving vehicle communication road surveillance, traffic security, road problems and conditions etc. This paper goes with the flow of systematic literature survey to give a comparison between existing methods formally verifying the rightness of VANET. Throughout this paper, we analyze information of research and models done by different researches and understand their contribution and challenges of the existing approaches and come up with the way for improving their solution. This paper describes the implementation of EC Crypto system for wireless sensor network. Elliptical curve digital signature algorithm (ECDSA) is used for the working based on message recognition. In our defined model, MQTT (Message Queuing Telemetry Transport) acts as a server model which is lightweight, publish – subscribe network protocol that transports message between devices. The Raspberry-Pi model generates the key using ECDSA for the cars and then the communication in between the vehicle is done using the MQTT model.*

Key Words: **ECDSA (Elliptical curve digital signature algorithm); MQTT; VANET.**

1. INTRODUCTION

VANET are used in the betterment of street safety control the street traffic and provide emergency as per requirement. Road problems, issues are occurring day by day. Security is main step in VANET, and an important factor in the progress of vigorous VANET application in VANET, and also the roadside infrastructure are nodes connecting [20]. At present many types of applications of VANET are present which concentrate on various types of transport organization like driving aid, control to traffic road, security of public etc. VANET are special branch of network that consist of cars as network modes roadside tower (RST) and on-board sets (OBS). In VANET, each car serves a network mode which communicate with one another and roadside units [11]. Basic purpose of VANET is given excellent routing and good safely for the people. This type of technology is gaining more importance day by day as car accident is increasing rapidly. As in short period VANET can be in between vehicle to vehicle V2V, V2I or I2I as given in figure 1[16].

VANET ask a perfect investigation privacy related issue. Users which use this type of network have to be precluding an attentive from being attacked of their saved data that is being secured from location which is given on different kinds of attacks on their network security. The creators of vehicles and their operators have to identify manufacturing units and privacy and security [4]. Reliability problems because of limited wireless transmission range are introduced by wireless link characteristics. Transmission errors and packet losses are induced by broadcast nature.

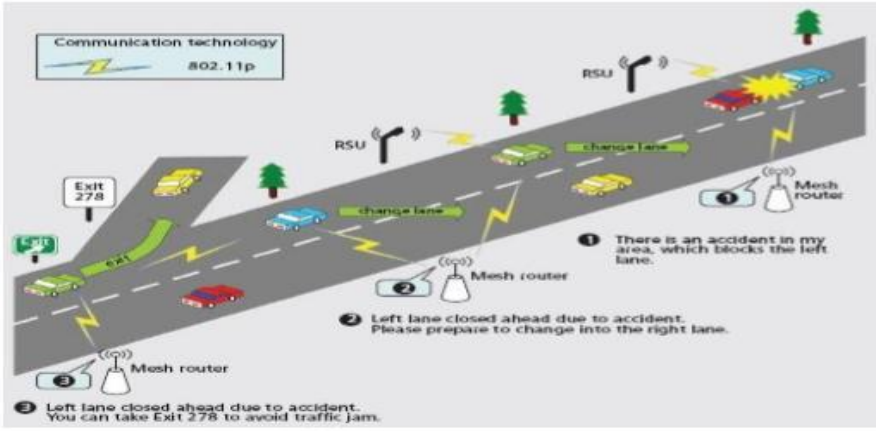

Fig 1: The architecture of VANET.

VANET privacy and security must satisfy the following requirement; message encryption and decryption, message non-repudiation, message confidentiality, privacy, availability and anonymity and liability identification [16]. Because of rapid and fast-growing technology of security threats in VANET they form a highly changing network topology. Application of VANET message sharing, picture, videos parking and toll collection service, accident avoidance, safely driving and traffic control [15[3]. As per the review papers tested, they are many methods in securing data sent through VANET application. Some papers do security using RSS, AES, DES, and RSA. The security of the message is done using the stated algorithm. To encrypt and decrypt the data the induced algorithm is used. The data that is encrypted and decrypted is sent using many different methods like using LORA, MQTT, WIFI, Bluetooth or internet server etc.

In this paper we are serving the other methods proposed by different authors and comparing their algorithm to us. According to this review paper we are using sensor data that detects weather the accident has occurred or not. Once when the data is been collected the same data is encrypted using ECDSA algorithm, that encrypted data is than sent through a MQTT server which protects the data from many attacks. That encrypted sent data is decrypted again using ECDSA decryption algorithm. After the data is been decrypted the sent message is displayed on the console without been attacked by the attackers.

The rest of the sections of this paper are divided into the following concepts: - section II: has a concise research of existing VANET applications for security, section III: defines proposed system, section IV: consist of conclusions and finally section IV has the references.

2. RELATED WORK

Security in communication is a main objective in VANET. If two vehicles are travelling and they try to communicate with each other they try to secure the data that upholds the privacy and safety of the obtained information. Researches in this field have made a great research on how to keep the security that helps in maintaining a safe and user-friendly surrounding for transmission and communication between VANET. To keep safe the data or information in VANET, it is very important task to secure the privacy and authentication of the data.

As the information in VANET transfer in open environment, good security algorithms must be used as they are wide in behavior and travelling of data is in different speed. To transfer text and image file in a network of different sizes in a CRYPTOOL simulator Ravi kalkundri [1] has used standard RSA and ECC-AES algorithm. Authentication, integrity, confidentiality, availability, non-repudiation, hybrid-cryptography, lightweight technique are the safety problems that come into picture when the information is being travelling from V2V, V2I OR I2I. To overcome such issues, they are many security scheme's like symmetric key cryptography, public key cryptography, hybrid

cryptography, lightweight technique that are best suited for VANET, that enhance the security techniques. Thus, this proper explains and compares the RSA algorithm and hybrid ECC-AES is more secure and prompt than RSA, though RSA uses less time to encrypt and decrypt the data security which is required is completely obtained from ECC-AES. The pairing-based algorithm i.e. RSA and ECC-AES shows that it is most feasible for WSN'S that issues battery safety level. Less time and utilization of power in communication used in PCB which is very trivial for wireless sensor kind of networks [1].

Two different types of concepts have been discovered by Romgxing that are based on integrity advances, first concept is anonymous key (BAB) [2][3] group signature type is the second one[4][5]. Non-repudiation, authenticity, revocation and conditional fuzzy are the safety advances that address both the concepts proposed by him [4].Class sign methods are used from class sign category which does not show the existence of the traffic data [6]. The time of securing and authenticating the data is much higher than accepting the public key signature conventionality, which defines the greater drawback in this paper [7][8].

Researcher A. WASEF Grew up with an idea, in which a VANET by itself could create the data for oneself with the help of private, public keys by signing their own self-made keys which could overcome the drawback of Remixing's research [9]. To decrease the overhead of message authentication public key signature concept is been used. Since the vehicles that are travelling around are moving with a very high speed and their bandwidth of travelling is very finite, assigning a certificate data (CRL) to each travelling vehicle is very hard. Here it concludes with the adjustment between the group-based scheme and traditional scheme which concludes with a result of major drawback.

Rajeev Singh uses RSU'S which act as certificate authority (CA) that generates the key using ECC for the car's safety. The connections between vehicle to vehicle are done using ECDH. ECDH is type of a protocol in which both the vehicle agrees on a given secret key which also uses a private key innovation. Here the model is split into two parts communication and registration period for vehicle. The communication phase where ECDH is used to generate shared secret key for communication between vehicle. This process fakes place only when the public is in contact with the CA. The computation cost of this process is too high [16].

In the entire environment which is large space Bhargav Bellur divided this large place into small zones and assigns a certificate number to each divided zone that reduces the problem of public key infrastructure with a time period of each travelling vehicle [7].This proposed concept could overcome the drawback of (CRL). The drawback he faced here was overhead incurred while obtaining new certificates and plus the corresponding specific type of CRL's to assign.

3. PROPOSED APPROACH

3.1 BLOCK DIAGRAM

In this paper we are sending sensor messages to an encryption-oriented model where the received message or the data is been encrypted using ECDSA (Elliptical curve data security algorithm) than the encrypted message is sent to other device using MQTT (Message queuing telemetry transport) module. The data is than decrypted on the other side using the ECDSA (elliptical curve data security algorithm) decryption algorithm. The data which is decrypted is displayed on the display screen which helps the other vehicle to get in control and alters them. Comparing to the researched papers above I am using this method to secure the data sent. As all the companies have their server to protect the data, the data sent through crash of cars must not be attacked and send with complete security we are using the (ECDSA). The sensors used here are vibration and flame. The figure given down shows the block illustration of the project being conducted.

Two sensors vibration and flame sensors are used to detect the changes happened in the VANET. The data sensed may be analog. The analog data is sensed a sent through the analog to digital converter. The description of the sensors used here are given below,

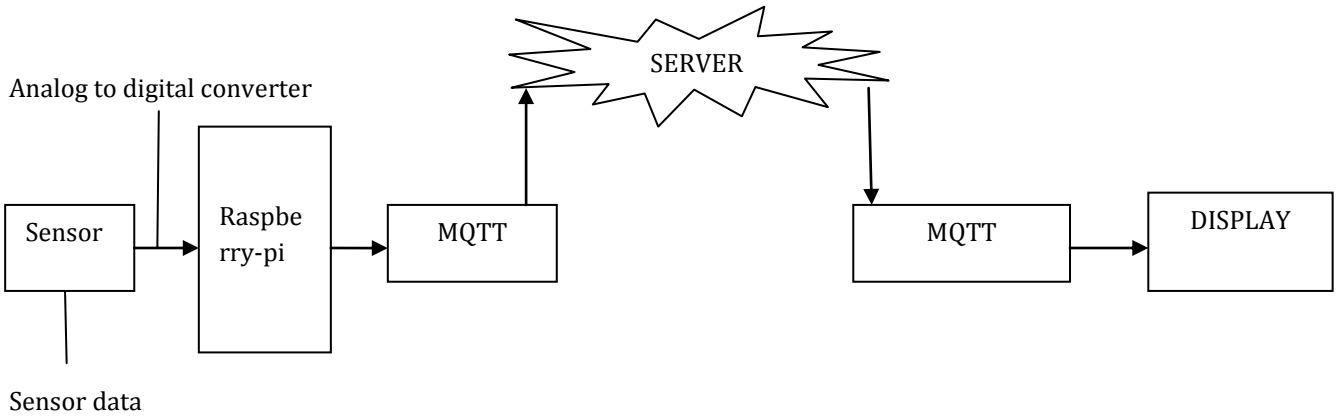

Figure 2: Block diagram.

3.2 SENSORS:

Flame sensor:

Well, this sensor which is also very delicate and sensitive to incoming normal light is defined as a flame sensor therefore this sensor is used as a flame alarm. The flame or fire this sensor detects is in the range between 760nm – 1100nm which is its wavelength range. Sensitivity is adaptable, stable performance. When high temperature is given to this sensor it easily gets damaged hence, this type of sensors is placed at a certain distance to detect. So, the detection has to be done from a distance of 100cm. The output we get from this sensor can be either analog or digital signal.

Features:

Performing voltage in this sensor is in the range from 3.3V-5V.3cm*1.6cm is the mounding of screw whole PCB size. Switch board indicates green and red is identified as power. Comparator chip LM393, is stable and firm. 0.8m is the distance to detect the flame, lighter flame test can be set at this distance if the intensity is more than required the detection distance is increased at a certain distance. Microcontroller is used to directly connect to the output. High temperature may burn down the flame so, keeping a distance with the flame is necessary. This sensor is used here because it can immediately sense the and respond to the occurrence of the fire or flame. The response of this sensor is faster as well as more accurate compared to heat/smoke detector because of its mechanism while detecting the flame.

Figure 3: Flame sensor.

Vibration sensor:

This sensor is piezoelectric accelerometers that can detect vibration. Switch SW–420 unit is used as a vibration switch. To detect the vibration comparator LM393 is used. Pointiometer is used to detect the threshold if it goes beyond the limit. LED light indicates output logic low signal when there is no vibration a vice-versa. On state the vibration switch is closed where it doesn't vibrate, the output goes low which indicates the green light. When the sensor vibrates momentary of vibration switch gets disconnected, the output is given high, and the green light goes off. Microcontroller is used to detect the vibration sense, where the LED goes high and low which detects weather the surrounding environment has vibration or not.

Detection of vibration, earthquake alarm, smart car etc is some of the applications in which this type of vibration sensor is used. These Vibration sensors are flexible in nature. They use the piezoelectric effect to detect the changes with the help of acceleration, force, pressure or strain etc. 10 mV/g to 100 mV/g, is the sensitivity range of these sensors. Switching output between 0 to 1 is used which helps in easy installation. A small board PCB dimension with 3.2cm x 1.4cm is been used along with LM393 voltage comparator.

Accelerometer sensor, velocity sensor, gyroscope sensor, microphone sensor, vibration meter is some of the types.

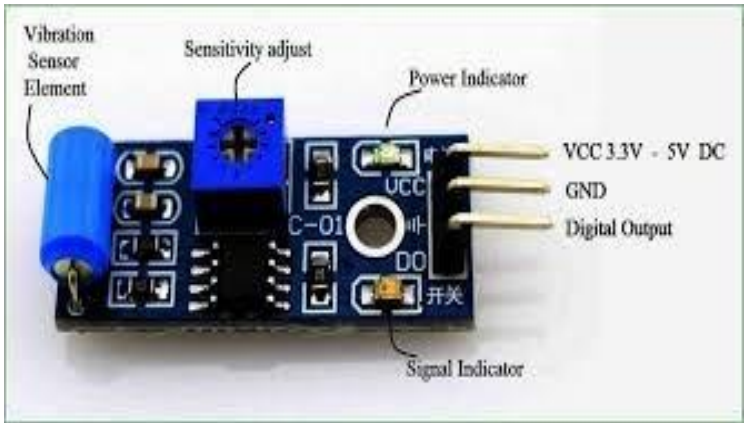

Figure 4: vibration sensor.

3.3 RASPBERRY-PI MODULE

It is a series of small on-board computers whose power is 5V 3A. The raspberry-pi here is used to receive the sensed data and encrypt the data using ECDSA (elliptic curve data signature algorithm). A small SD card of any size is been inserted in the slot which acts as the hard drive. The power is given to it by USB and the output is seen on a modern monitor.

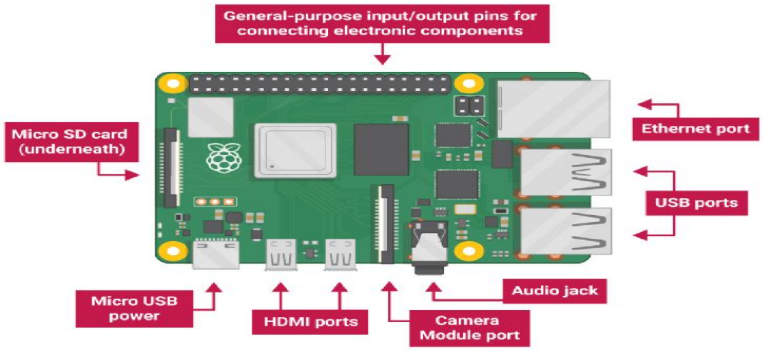

Figure 5: Raspberry-pi Device.

3.4 ECDSA- elliptical curve digital signature algorithm.

A private and public key is present here which is an asymmetric authentication scheme. Transmitter on the transmitting side uses the private key to digitally sign the sending message; where as the receiver on the receiving side uses the public key cryptography to recognize the authenticator. The authentication process fails if the message that is been transmitted is attacked by the attackers while transmission. The algorithm used here is based on elliptical curves which is similar to digital signature algorithm (DSA). The working of ECDSA goes as follows: -

STEP1: Pairs of key generation:

The transmitter known private key used to send message and create a private key as well. Thus, the curve domain parameters are (F_P, a, b, G, n, h). The authenticator's private key is chosen in the internal which is pseudo-random integer. Q= DG, equation is used to compute the public key, where Q here is defined as public key and G is set as the generator point.

STEP2: Creating the key signature

The receiver who is receiving the key created by the transmitter uses the digital signature key to recognize the received message from the exact authenticator who sends the message. Key pair (d, G) which is present near the transmitter which is used for generating a key chooses a pseudo-random number (m) which is in the range between [1, n-1]. r & s are the two keys generated from the key signature, while r is been calculated given in equation (1) and (2).

$$(x1, y1) = m.G \bmod p, p \text{ is a prime no.} \quad (1)$$

$$r = x1 \bmod n, r \text{ should be in the range } [1, n-1] \quad (2)$$

When r is equal to 0, new area is generated again. A secure hash algorithm is converted which can be created in the form of an integer 'e' which is derived to compute s. 's' is generated and is computed by following equation (3):

$$s = m-1\,(e + dr) \bmod n \quad (3)$$

The integer's r & s are regenerated when a random number is selected if 's' is computed to be '0'. The signature of the authenticator is (r, s).

STEP3: Signature verification

Receiver uses the transmitter's domain numbers and the generated public key to authenticate the received key. From this the authenticator's signature (r, s) numbers are also known. Hash algorithm is computed by the receiver to get 'e'. For verifying the number, the given down equations are been computed and analyzed:

$$w = s-1 \bmod n \quad (4)$$

$$u1 = e.w \bmod n \quad (5)$$

$$u2 = r.w \bmod n \quad (6)$$

$$(x2, y2) = u1.G + u2.Q \bmod n \quad (7)$$

When the computed x2 is equal to 'r', the verification process is successful, if the integers (x2, y2) are equal to 'point at infinity' (0), the signature key computed is rejected. The flow working principal graph of ECDSA in ECC algorithm is shown in the figure (6).

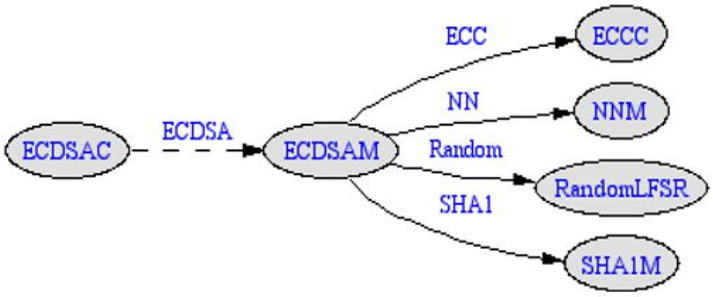

Figure 6: Graph of elliptical curve data signature algorithm.

There MQTT stands for Message Queueing Telementry Transport, protocol which is a medium used to transmit and receive messages across the network to any different device working with it. We know that MQTT can be widely used to internet of things applications. But do you know that MQTT can be a good choice for sending data in local networks too. Instead of juggling with TCP or HTTP request and running webserver, MQTT can be a super simple, yet reliable solution for local network data exchange between raspberry pi to raspberry pi or raspberry pi to computer. The data encrypted is sent through a server to the destination through server using the MQTT protocol. On the receiver side the data is received through MQTT server and decrypted using the ECDSA decryption algorithm. After decrypting the received data, the client gets the sensor message which is displayed on the console that helps the different vehicles to alert themselves from the accident happened ahead through the sensed data received.

4. CONCLUSIONS

VANET i.e. vehicle ad-hoc network is the future of vehicle and the people it still needs a lot of research because of the importance and accuracy and risks involved to the human being. There are still many protocol and researches of VANET which concentrates on different aids of transport system like driving, privacy, protection of people, control of traffic, raising security and system potency is been used. Several attacks on VANET are still present across the communication that leads to incorrect transmission of data at the receiving end. Hence VANET security plays a very important role.

Hence the conclusion we have come up to in this paper is the SLR of the methods concentrating on verifying the correctness of the different VANET protocol. ECDSA algorithm is used in VANET architecture, following processed protocols, upcoming attacks and the solution to secure data from these attacks is been completed. We have done a survey on the previous protocol and results done on VANET and their attacks and drawback. Comparing the previous drawback, we have come up with a different algorithm and protocol that improves the security and accuracy of information in communication with VANET based on the before study done, we have identified some set of challenges that can improve the existing before works. We calculated and researched a better survey which can be used as a start up in doing research in VANET.

REFERENCES

[1] Ravi kalkundri, Dr. Rajashri khanai, Praveen.kalkundri, "Analysis of cryptographic algorithm for secured data transmission in VANET's".

[2] R. Lu, X. Lin, H. Zhu, P-H. Ho, and X. shen, "ECPP; efficient conditional privacy presentation protocol for secure vehicular communication, "In INFOCOM 2008, the 27TH conference on computer communication. IEEE, April 2008, pp.1229 1237.

[3] Y. Jiang, M. Shi, X. shen, and C. Lin "Bat: A robust signature scheme for vehicular network using binary authentication true", wireless communication, IEEE transaction on, Vol.8, no.4, pp. 1974 1983, April 2009.

[4] X.Lin, X. sum, P.-H, Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communication, "vehicular technology, IEEE. Transaction on, Vol. 56, no. b, pp-3442 3456, nov.2007.

[5] G. Calandriello, P. Papadimitratos, J-P Hubaux, and A. lioy, efficient and robut pseudonymous authentication in VANET, in proceeding of the fourth ACM international workshop on vehicular ad hoc network, ser. VANET 07., New York, NY, USA: ACM, 2007,PP.928.[online].Available: Attp: 11doi.acm.org/10. /145/128 7748. 1287752.

[6] D.Boneh and H. Shacham," Group signatures with verified local revocation," in Proceedings of the 11th ACM conference on Computer and communications security, ser. CCS 04. New York, NY, USA: ACM, 2004, pp. 168177. [Online].Available: http://doi.acm.org/10.1145/1030083.1030106

[7] B. Bellur," Certificate assignment strategies for pki-based security architecture in a vehicular network," in Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE, 30 2008-dec. 4 2008, pp. 1 6.

[8] Jung, C. Sur, Y. Park, and K. Rhee," A robust conditional privacy preserving authentication protocol in VANET" in Proceeding of Mobil Sec, June 2009, pp. 3535.

[9] A. Wasef, Y. Jiang, and X. Shen," Dcs: An efficient distributed certificate-service scheme for vehicular networks," Vehicular Technology, IEEE Transactions on, 59, no. 2, pp. 533 549, Feb. 2010.

[10] C.-T. Li, M.-S. Hwang and Y.-P. Chu," A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," Computer Communications vol. 31, no. 12, pp. 2803 2814, 2008, mobility Protocols for ITS/VANET.

[11] Deeksha, Ajay Kumar, Manu Bansal, "A review on VANET security attacks and their countermeasure"., 4TH IEEE international conference on signal processing, computing and control (ISPCC 2K17), Sep 21-23, 2017, Solan, India.

[12] J.M, de Fuemtes, A.I. Gomzales- tables and A. Ribagorda, 'overview of security issues in vehicular ad-hoc n/w," handbook of research on mobility and computing, / GI Global, 2010.

[13] Chem, LI, Tang, H., and Valang, J., "analysis of VANET security based on routing protocol information, "fourth international conference on processing, pp.134-138, June 2013.

[14] Raw, R.S., Kumar, M. and Singh, N., "Security challenges, issues and their solution for VANET ", international journal of network security and its application, 2013.

[15] A.S. Alhasan, Md. Shohrob Hossion, and Mahammed ad hoc network "conference on advances in computing, communication and informatic, pp.21-24, Sept.2016.

[16] Rajeev Singh, Sumit Riglani, "efficient and secure message transfer in VANET" IEEE internal of conference paper, 2016.

[17] AmitDua, Akash Dutta, "A study of application based on elliptic curve cryptography". Proceeding of the third international conference on trends in electronic and informatics (ICOEI 2019) IEEE Explore part number: CFP19J32-ART, ISBN: 978-538b.

[18] Siquan Hu, Yingrui Jia, Chundong she., "performance analysis of VANET routing protocol and implementation of a VANET technical, 2017 internal conference on computer technology, electronics and communication (ICCTEG).

[19] J. Velez, R Trafford, M Pierce., "providing common network services over MQTT. 2018 IEEE sensors. 2018-ieeexplore.ieee.org.

[20] U.Hunkeler, H-L.Teuong, "MQTT-S A publish / subscribe protocol for wireless sensor ". -20083RD international conference paper.2008-ieeexplore.ieee.org.