Study of environmentally sustainable security in wireless sensor networks

Aseel Hamoud Hamza[1], Saif M. Kh. Al-Alak[1]
[1]Department of Computer Science, College of Science for Women, University of Babylon, Iraq

ABSTRACT

The popular technology Wireless sensor networks (WSNs) are used in many fields of the application such as the medical, the military, the industry, the agricultural, etc. In this paper, explains the security issues in the WSNs. Firstly explain the challenges of wireless sensor networks, the security requirements such as confidentiality, integrity, authenticity, data freshness, and availability and the attacks in the WSNs, the security issues are accomplished via these classes: [the encryption algorithms (symmetric, asymmetric, hybrid) , the security protocols such as (Tinysec, SPINS, LEDS, Minisec, LEAP, MASA, Lightweight LCG, MiniSec, VEBEK of WSN), the secure data aggregation, and the key management, etc.]. Also, this paper concentrates on the study researches that fulfill the high level of the security in the WSNs.

Keywords: Security, Confidentiality, Integrity, Authentication, Wireless Sensor Networks.

Corresponding Author:
Aseel Hamoud Hamza,
Department of Computer Science,
College of Science for Women,
University of Babylon, Iraq.
Email: aseel.hamod@uobabylon.edu.iq

1. Introduction

Wireless Sensor Networks(WSNs) consists of the number of independent distributed sensors nodes (so-called motes) to monitor physical or environmental status like as (temperature, pressure, light, sound, and humidity), the development of Wireless Sensor Networks was first started by military applications such as battleground observation and yet these are emerged into different fields such as manufacturing process monitoring, good health monitoring and traffic control etc. [1, 2]. WSN composed of a particular node named gateway node (Base Station) rich in storage resources and computing. The sensor nodes transmit information to the gateway among a many nodes using wireless transmission for more processing.

The security requirements for the WSNs are alike to traditional networks, so you must consider the parameters like as (confidentiality, authenticity, integrity, availability, etc.) in the establishment of the network. Because of WSNs network limitations (in energy, memory, and processing) not whole security solutions designed for traditional networks utilized immediately in WSNs. The researchers in the security of the WSNs have suggested many security systems that have been improved for these networks with resource limitations. A number of safe and effective routing protocols [3, 4][5][6] and encryption techniques [7, 8][9] and secure data aggregation [10, 11][12], and the key management [13, 14][15] were suggested by many WSNs security researchers.

The paper is structured as follows. Section 2 present introduction, the section 3 explains challenges of WSNs. Section 4 explain security requirements, the section 5 present cryptography on WSNs, the section 6 present secure data aggregation, section 7 present security protocols in WSNs, the section 8 explain key management, the section 9 and 10 show in brief way a an attacks on WSNs, and in final we conclude the study in the section 11.

2. Challenges of WSNs

The continued progress in micro electro mechanical schemes, the miniaturization and grown communication abilities of sensors has made it possible to exist everywhere and imperceptible anyplace. A sensor network is a foundation involved detecting (measuring), figuring and corresponding components that give a client the capacity to watch instrument and respond to phenomena and events in a specified environment. To design and improve protocols or techniques some challenges are require to be understood [16]. These major challenges are briefed below.

2.1 Limited functional capabilities

The sensor node has small memory, a low processor and a small quantity of the stored energy. This restrains several functional abilities in the communication and the processing.

The best technique should benefit from participating resources inside the organization structure, taking into account the restriction of singular node abilities.

2.2 Limited energy

Sensor node restricted energy storage. Thus, the efficient use of this energy will be critical in determining the scope of utilize of these sensor networks. In utmost cases, renewing energy is not possible or impossible. Sensors are unattended in this area. Limited energy in the sensor contract should be considered as appropriate consumption or use that can minimize the total energy use in the network.

2.3 Network lifetime

Limited energy and resources in the sensor nodes results in a bounded lifetime in the network. Ideally, the network must become ineffective only when all nodes are consumed. In fact, the lifetime of the sensor network is the lesser time when the network is functioning efficiently, the network is efficient, if it can observe the sensor field fully and gather the data sensed with QOS. Appropriate techniques should try to minimize energy use and thus increase network life.

2.4 Scalability

Sensor nodes transferred in the detection zone must be optimum. To suitable some nodes later, scalability is one of the major obstacles to achieving this goal. The scalability of sensor ordering exhibit the ability to handle the development of business standards in a powerful way and easily expand them [17].

2.5 Redundancy

Due to the failure of the recurrent node and unavailable of the failed nodes, the absence of a unique proof in the world because of the large number of sensor nodes in the sensor, the global definition (GID) is mostly impractical. Although, at times, GPS[18] provides location data to hold the sensor, it requires a remarkable path for a few satellites, which are generally inaccessible within the work, under thick foliage, Submerged, when stuck by an enemy or central MARS probe and so forth.

2.6 Storage, search and retrieval

The sensor network can product a large amount of primary data like as continued time series of surveillance on all points in the area covered by the network. Because the data source is persistent, the database is not proper for WSNs.

3. Security requirements

To achieve security for the WSN, the following issues are subject to the following requirements.

3.1 Confidentiality

Securing data during transport from one node to another node or denying unauthorized access is a way to keep your data confidential. Illegal access to sensitive data and eavesdropping utilizing encryption techniques should be prohibited. Because public key encryption is expensive to be utilized in resource-restrict sensor networks, almost of the suggested protocols employ symmetric key encryption technique. Creators of TinySec [19] Discussion that CBC is proper cipher system for sensor networks.

3.2 Integrity

Data integrity for the recipient ensures that the received data is not changed during the transfer by discount; observe that the data authentication can also supply data integrity

3.3 Authenticity

WSN contains the broadcast nature of the connection so that the attacker can instead change the contents of the message from adding useless packages in the native package. To defend this attacker's technique, the receiving node must have the ability to control access by discovering the valid node and which is not allowed. Let the valid message come and end the message that not valid source. Digital signature is a method of authenticate a node [20].

3.4 Data Freshness

In encrypting the shared key in which the keys are updated after a specified period of time to supply guarantee that incoming data is new. This ensures that doesn’t find replay attack, since the attacker take a quantity of data and resend it to generate illegal access. This kind of conservation can be achieved by attaching the timestamp to the message. The receiver node clock and time stamp are compared to determine whether the received data is new or not.

3.5 Availability

The communication and account capabilities are limited in the sensor, so a calculation of more than its capacity results in additional energy usage, but if no additional energy, there will no extra data availability. The collapse of an individual node can impact network arrival. An attack can launch an attack on the usage of the energy or resources, threatening node and DOS attack. The sensor can use its energy in a smart way by getting sleep when there is a steady state for a long time and backup power for situations that demand an account more than usual.

4. Cryptography on WSNs

Use of proper encryption technology is very important for WSN networks because every security services are guaranteed by the cryptography. The encryption techniques utilized in the WSN must check the sensors' constricts, which are also assessed by data size, processing time, and power consuming. In this the section, the concentrate was on utilizing encryption in WSNs. Such as public key encryption, symmetric key encryption and hybrid encryption

4.1Public key cryptography in WSNs

Many researchers use public key techniques such as:

IN[21] The symmetrical cryptography is not proper for WSNs when compare with asymmetrical cryptography due to protect from security risk in effetely. In spite of key administration and security, public key cryptography can be active to WSNs as key administration domain the public key technique solid and productive of key time the public technique are skillful, in security aims implementation when compare with symmetrical key like the public key is employed for encryption and the private key is employed for decipher in this method reduce security risk and attacker cannot find out the private key which it enables it to decrypt information and thus can respect the information and confidentiality of information and validation which allows for safe transport.

IN[22] in this paper ECC and RSA is compared and discover that ECC is more usefulness to RSA, because of low memory use, low CPU consuming and smaller key size compared to RSA. ECC (160bits) is two times better than RSA (1024bits) when code size and power consuming are take into account and carry out in 8051 and AVR programs. ECC (160bits) utilizes four times less energy than RSA (1024bits) in MICA2DOT. A novel system named "Multivariate Quadratic" was suggested that display enhancements over ECC and RSA.

In [23] the suggested method to supply data security will be the bidirectional key Management between the base station to the cluster heads of the block and from cluster heads to the sensor nodes by employing ECC ,in addition to the concept of secret participation a system that will not only avoid a single user authority but enhance data security.

4.2 Symmetric cryptography in WSNs

Many of the studies for WSNs focus on utilizing symmetric key cryptography for encryption of plain text and decryption of cipher text. The main challenge to deployment the key is how to secure distributes the participated key between the two communicating parties". Many works were related to the Symmetric key cryptography such as:

In [24] This research talk about a novel crypto-graphical technique "SCAWSN" evolved for the WSNs to conserve the data of the sensor. In additional to, modulo process, reverse process, inverse process and the conversion are the processes utilized in this technique. This technique is simply designed. The plain text entry is displayed in kilobyte for the technique and the identical output in millisecond is in the outcome table. The outcome displays that the (SCAWSN) technique takes less time to calculate the conversion of unencrypted text to encrypted text and also to encrypted text to unencrypted text as compare with the DES and AES technique. The sensor node is characterized by its restricted capacity, so this technique will be effective because it has less power for the battery and a memory capacity.

In [25] cryptographic algorithm RC4 is an effective to secure the data as it is faster and easy than another techniques. A modified RC4 technique with difference in status table computation was suggested to improve the randomness in the key generation method. The key generation time was faster than the actual RC4 technique. The suggested design was executed in WSN utilizing "TICC 2431" and the outcome was more effective than the actual RC4. As a future work, much security study can be carried out on the suggested technique to test the robust of key generated for WSNs.

In [26] this paper Blowfish technique is utilized for application of security. Three sensors called as ("MQ6 Gas sensor, LM35 Temperature sensor, LDR Light Dependent Resistor sensor") are utilized. The values from the sensor are noticed by (microcontroller Atmega8). Then the values are encrypted via (Atmega microcontroller). The values encrypted are transferred via utilizing (Zigbee module CC2500). The transferred data are received via Zigbee and the values are decrypted via utilizing (Atmega microcontroller). The encrypted values and decrypted are shown in PC. The values are transferred securely by utilizing the Blowfish technique.

4. 3 Hybrid algorithm in WSNs

Hybrid technique means a combination of two or more techniques. The hybrid technique gets the advantages of asymmetric and symmetric techniques. Several hybrid techniques have been suggested. Several researcher selections only asymmetric techniques, another utilize only symmetric techniques and several of them pick combination of them to obtain the advantages of both them**.**

In [27] this paper suggest a hybrid encryption technique for WSNs. It is constructed on stream cipher and Block cipher symmetric key. At the first split message receive from sensor node into left halve which encrypted by utilizing block cipher and Right half encrypted by utilizing stream cipher, the message digests are computed in both sides, at the last encrypted the message and digest values are chain and transferred to next cluster head, hash function is utilized for the Data integrity.

In [28] the hybrid encryption is utilized to give better security for messages. Mixed asymmetric technique, RSA and DES symmetric technique to encrypt messages are used. Compare the different methods and find that the integration of RSA and DES is the most effective. The method is compared encryption time and the key generation, specify the effectiveness of various hybrid techniques relayed on the memory consuming and time. De-anonymization and Data anonymization methods are utilized for suitable security objective.

In [29] suggest a hybrid security protocol of two technique ECC and AES. Three methods of the suggest protocol are application on the secret message. The suggest protocol will increase randomness which executed by a Diehard test means increased security. There is a tradeoff between increase the security and energy consumption. A balance should be made between the complication of the encryption protocol and the quantity of energy exhausted.

In [30] this paper explained the cryptography techniques and methods of cryptographies symmetric and asymmetric, and explain the technique (RSA, AES, Blowfish, Triple DES, RS4, DES), as well as show how chosen of the right cryptographic systems based on time, memory and security. Also demonstrate comparing of the cryptography and the attacks.

5. Security protocols in WSNs

Cryptography is an essential way to fulfill the network security. This found a secure relation between two ending points. The sender encrypts the plain text and the receiver decrypts the cipher text. The diverse kinds of keys are utilized in the encryption method. The various protocols suggested by a several researchers to solve the WSN security problem [31] such as SPINS, Tinysec, Minisec, LEAP, LEDS, Lightweight LCG, MiniSec, MASA, VEBEK of WSN). Related works of the researcher on this aspect**:**

In [32] This work display the first secrecy and integrity of data that try to add security depend on watermarking and crypto graphical mechanisms to watermarking LEACH named enhanced proved watermarking-LEACH to fulfill data secrecy and integrity. The main purpose of this work is to treatment, the privacy and integrity at two level node and the CH level. It has been deduced that suggested protocol is better than Watermarking-LEACH on the level of the security.

In [33] In this study, to preserve energy active security communication for the WSN, a chaotic based security implementation was utilized. The designed system was executed on OPNET simulator and outperforms of the chaotic based encryption method was assessed with Skipjack encryption. Simulation outcomes detected the chaotic-based encryption technique has a lower rate delay, data memory use, program memory and have close energy consumption. Chaotic-based encryption techniques are proper to utilized for the WSNs.

In [34] In this paper WSNs efficiency is improved by using a novel suggested which is employed Leach protocol as the routing protocol for data transport. A Symmetric cryptographic technique had been utilized to improve the WSN security. The malicious nodes are found out and blocked in first work, thus reduce the danger to the network and consume less power .The lifetime is increased by using this technique.

In [35] from the results, the suggested system supply confusion and diffusion, and thus assure The collapse effect occurs. Percentage of sensitivity to normal text and the key sensitivity in the suggested system is better than the Genetic method and RC5 So it is safe. In the future, more technique can be used in WSNs compared to the suggested system.

In [36] the complication of the suggested mechanism rely on the space of the secret key and the number of duplicates in encryption. But rely on (bandwidth, network lifetime, and processing) at the WSNs, a lightweight encryption technique chooses the balance between overhead and security. Then, the suggested technique assures confidentiality of data relay on encryption mechanism and the secret key encryption. In the end, it is deduced that the suggested system achieves the requirements of the current security systems without extra transport costs that confirm the efficiency and supremacy.

6. Secure data aggregation

Data aggregation is the operation by which information is collected and expressed in a summary form to reduce the data connection in the network. To enhance energy efficiency of sensor network, the data aggregation objective to aggregate data packets into many sensors as well as categorize and filter data from compromised nodes.

In [37] this paper, try to suggest a secure data collection framework that protect privacy, confidentiality, integrity and validation at the WSNs. In this method, at the first step the existent TinyECC library is expanding to give props to four the symmetric encryption techniques. Estimate and justify the relative use of EC-OU for privacy and confidentiality in the work. To give integrity support, experimentally evaluate the current EC-DSA variables and display that none of the current EC-DSA variables are proper for use. Thus, also suggested alternative EC-DSA which relies on a probability group membership data structure, which is bloom filter. Results display that the EC-DSA alternative is proper for any proper that needs application integration in WSN-limited resource environments. Also integrating a new variable based on Bloom filters through our proposed framework for SDA, the suggested framework to secure the data collection gives prop for privacy, confidentiality and integration rely on a bloom filter based on (end-to-end) integrity.

In[38] there is two method to increases the life time of network and keep energy in secure data aggregation system, as known the sensor try to sign, encrypt the data and send it to the collector. In method of a hop by hop technique the collector decrypt and validate the whole data it receives, next it collect them and lastly encrypt and sign the collection previously transmission it then. Otherness, the collector in technique only require to add the cipher text, the public keys and digital signatures, then replacement the decryption and validate processes with three additions. This addition processes are exhaust less power and faster than signing and encryption, perform the decryption and validation only at the root node, replacing the validation and decryption for a few additions keep 97.74 mJ at any intermediate node in each round to MICA2 nodes. The collector has first given out of battery, then keeping the energy on collectors increases the whole network lifetime. The prior algorithms begin validation steps to assure the data integrity, when the base station gets the collect data. This phase needed a number of transports and integrity check calculation for nodes. Technique alleviates the nodes from the load of this extra step by utilize of the aggregate digital signatures, which validate the total of the data at the base station without the required of the extra transports and calculation of the validation, thus increase the network lifetime and keep energy.

7. Key management

Key management is a major security in the sensor networks. This is the principle of establishing a secure connection using encryption techniques among sensor nodes in a critical region. It is the operation by which cryptographic keys are generated, protected, stored, loaded, transferred, used, and destroyed. [39] There are several main interests in the key management method:

- Key deployment: the number of the keys is needed to be duplicated in the network.
- Key pre-distribution step: This step executed before the publication of the network, exactly during the node's making time.
- Key establishment: A pair or a set of nodes will form a secure session.
- Network initialization step: Includes the first steps required to set up network security, and they are implemented during network publication.
- Member/node eviction: Remove the node from the network so that it will no longer be able to make secure sessions with any nodes in the network, and will not be capable to decrypt traffic in the network.
- Member node/addition: The node added to the network until it can create secure sessions with nodes in the network, unable to decrypt previous traffic in the network.
-Authentication protocol: It is executed each time you request a novel node to join the network, after the prior step is completed.

The study work related to the key management of the work researchers:

In [40] this paper, the Key Management System "SKMS" was introduced for the hierarchical WSNs. The suggested system utilized for symmetric encryption just relies on the hash function and the XOR process to create session keys between every two nodes. Using Performance valuation, the lengthen network lifetime via consumption less time and less power to create a secure connection between nodes. "SKMS" utilizes the value shared between nodes to create (symmetric session keys) and updates this value at a regular time to evade the node take attack and to make sure that just the valid nodes can be contacted. SKMS is proper for various kinds of the WSN networks, and it operates in both hierarchical and flat WSNs as well as heterogeneous and heterogeneous WSNs. The shared value among the nodes is computed after publishing at the discovery stage, that demands three strides and the key generation stage demands five strides to create the session key and because of this (SKMS), it get less time to compute shared value and create the session keys. However, in (MKMLS), the UAV was used as a key management center. If the two nodes need to connect to them for the first time, the nodes can only create a session key with the help of the UAV. (MKMLS) require eight strides to compute the value shared among the nodes and other five strides to create the session key. Every stride demands negotiation between the nodes and every stride consumes energy and time. Compared to (MKMLS), SKMS demands fewer strides to compute the shared value and to create the session key and, as a outcome, consumes less energy and less time, analysis and simulation display that (SKMS) is energy effective and exhausts less time as compare with another similar systems.
In[41] this project, dynamic key management schemes were used. All major key management plans are identified primarily in the light of the assets held for the sensor nodes and safety. The Key Management WSNs master plan is a very fruitful research so far it can be found. The result is that an invalid key is the network that will appear when the rundown of keys contains an invalid key. The primary objective of this process is the dynamic key that is generated every time after the encryption and decryption process. It utilizes RC5 only to transfer information, verify information and key age in the suggested safe agreement, so the device is difficult to identify and deliver, and operates at low power, time and handling costs. Similarly, given most existent devices that support RC5, the suggested agreement should be ideal with existing devices. The RC5 flow number is a cryptographic encryption strategy to consolidate information in the messaging channel as it is less hard and faster than the many different accounts**.**

8. Security Threats

The main classes of attacks against secrecy in the sensor networks are (eavesdropping, hijacking and disruption). Eavesdropping is used to get the result of sensor networks by showing messages sent from the sensor nodes. There are two ways to get result data by hiding from sensor nodes or transmit queries to the sensor nodes, root nodes, sensor nodes attacks or collecting the points. The previous method is named (the passive eavesdropping) and the subsequent method is named (active eavesdropping). The eavesdropping site plays a key role in obtaining information. This attack impacts the feature of authentication and confidentially in the WSN [42]. For the appropriate encryption technique, the code of the message authentication is requiring before the data is broadcast. The disturbance chiefly impacts the network result. Depending on the attacker's ability, threats in the WSN can be categorized into the next classes.
External Attacks Against Internal Attacks: External attacks come of the nodes that do not be owned by WSN. No external attacker or third party can arrival to the most of the encryption material in the sensor network. External attacks in the passive eavesdropping may cause data transfers, and can expand to injecting fake data into the network to exhaust the network resources and increase the DoS attacks. Conversely, internal attacks happen when the WSN legal node acts in unauthorized or unintended methods. Internal attacker is a certified network sensor participant seeking to disrupt processes or use the organizational assets.

Passive Attacks vs. Active Attacks: Passive attacks contain the eavesdropping or exchanged packets in the WSN while. Active attacks contain several modulations at the data stream or the generation of a wrong stream.

Mote class against laptop class attacks: In the mote class attacks, the opponent attacks the WSN is utilizing a few nodes with abilities to those from network nodes. In the attacks of the laptop class, the opponent can utilize powerful devices such as the laptop, etc., can damage the network more than the sensor node harmful. The devices have a greater transport range, power reserve, and processing power than network nodes. Sensors monitor changes in specific criteria or values and report to the sink as required, during transmission (information, report) which is transport may be attacked to supply wrong data to the base stations. Vulnerability in design, configuration, implementation, restrictions that can be used by attackers is called as a failure 3.2 or weakness.

9. Security attacks

Attacks in a computer scheme or network can be categorized[43] like as "interrupting, intercepting, modifying and manufacturing".

- **The interrupt:** is an attack at the availability network, such as (corruption of the messages, the physical capture of the contract and the introduction of the malicious code,.. etc.) [44] .
- **Objection:** is an attack at the confidentiality. The sensors network can be too compromised by a deduct for unauthorized arrival to the sensor device or data stored in it.
- **Modification**: is an attack at the integrity. Modification refers to unauthorized party not only arrival data, but fills it up, for instance by changing the data packages sent or it cause a denial of service attack, like as flooding the network with fake data.
- **Fabrication:** is an attack at the authentication. In fabrication, the adversary injection the fake data and cause to weak the trustiness of the information sent.

The security attacks aim to compromise the five major security goals for network security Confidentiality, Availability, Authentication, Integrity and Nonrepudiation in the WSNs to improve performances of the network. The researcher introduces their experience in many methodologies that a show good result to avoid attacker and protect data from theft in different related work such as:

In[45] this paper, the main security attacks and their solutions were described in WSNs, classifying threats based on their goal. Based on the various services provided, use defensive technologies to maintain the security of WSN networks, such as service safety and availability, and confidentiality data, and safety data. Also recognizes multiple-layer attacks, which change the threats and appropriate solution defense. The security mechanism should be used for WSN layers.

In[46] this suggested work, data security is improved and defends brute force attacks. Data must be transferred in a secure path between two nodes, so all node information must be encrypted. The Honey Encryption technique is then utilized in the WSN. The seed is utilized, and include different words in it. When attackers encrypt the data utilizing a wrong encryption key, HE displays a honey message (for instance, false plain text). This text may be legal but in fact it is not. So the attacker may finish with the mistake message. Empirical results, explain this Honey Encryption supply better performance compared to other techniques.

In[47] the paper, scheme present a protocol that assist to reduce the network traffic and make randomness for the data path to confound the attacker.

In [48] this paper, we have made some active attacks related WSN also explain the countermeasures identical. However, there are still many open problems to be explored. WSN has not yet fully matured and is yet in advance. Many of the protocols developed so far for WSN did not satisfy security threats accurately. Otherwise, important requirements WSN and protocols make it hard to evolve some solid security schemes while maintaining low support in operation cost. Thus, the security of WSN is an open and productive research direction that must be pursued.

In[49] Safe Protocol is an effective protocol for the treatment of two-layer sensor networks in a manner that preserves confidentiality and integrity. Safe Protocol utilizes authentication mechanisms for prefix membership, encryption by DES techniques, and MD5 technology. For the security, Safe Protocol supports the security of the two phased sensor networks. In contrast to the former, Safe Protocol prohibits the storage node at risk from obtaining a practical assessment of the values of the data elements collected through sensor and sink queries. The result explain that Safe Protocol outdo the prior data in the storage space.

In[50] this work suggest that Secure Force is a security solution for WSN. The Secure Force architecture (64, 128, and 192 bit) was used and the several tests were performed for text and image data. The test result displays that SF works well in computational time and randomization. At the outcome of security analysis for SF (64-bit), there were several specific vulnerabilities that were improved in 128 and 192-bit structures. After the test showed that SF-128 performance works well when compared to SF-64 and SF-192. SF-128 occupies the first place in the list with (35ms encoding/ decoding time, 51.55% avalanche and 11.44% Entropy change).

10. Conclusion

The researcher use encryption, security protocol, secure data aggregation and Key Management in the WSNs, there are several challenges. At first, choose encryption approaches rely on the ability to handle sensor nodes. On the second, the sensors are limits on (memory, energy, bandwidth, and computation capability).

Security services must be designed to achieve these limitations. Thirdly, the protocols suppose (the sensor nodes and base station) are constant. Security issues in WSNs are of special interest such as use the private key processes on the sensor that where the new studies about public key encryption explains the public key processes functional in the sensor. However, private key processes are expensive in holding the sensor. Because the public key encryption can simple security design in the WSNs, enhancing the private key processes on the sensor nodes is much desired.

Continued stream security in the WSNs, Security in WSNs concentrates on separate events like as humidity and temperature and at final Quality of Service and Safety. Current studies on security on the WSN focuses on (secure routing, secure data aggregation, key management), security services and quality of service must be all together valuated in WSNs.

11. References

[1] Younis, M.F., K. Ghumman, and M. Eltoweissy, *"Location-aware combinatorial key management scheme for clustered sensor networks".* IEEE transactions on parallel and distributed systems, vol.**17**,no.8, p. 865-882, 2006.

[2] Zhang, W. and G. Cao. *"Group rekeying for filtering false data in sensor networks: A predistribution and local collaboration-based approach*". in *IEEE INFOCOM*. INSTITUTE OF ELECTRICAL ENGINEERS INC (IEEE), 2005.

[3] Kandru, C.R. and R.S. Sangam, *"A Survey on Routing Protocols of Wireless Sensor Networks: A Reliable Data Transfer Using Multiple Sink for Disaster Management*, in *Next-Generation Wireless Networks Meet Advanced Machine Learning Applications*", IGI Global. p. 84-99, 2019.

[4] Chelbi, S., et al., *"A new hybrid routing protocol for wireless sensor networks".* International Journal of Ad Hoc and Ubiquitous Computing, vol.**28**,no.4, p. 247-257, 2018.

[5] Alabdullah, M.G.K., et al., *"Analysis and simulation of three MANET routing protocols: A research on AODV, DSR & DSDV Characteristics and their performance evaluation".* Periodicals of Engineering and Natural Sciences, vol.**7**, no.3, p. 1228-1238, 2019.

[6] Nagaraj, U. and P. Dhamal, *"Broadcasting routing protocols in VANET".* Network and Complex Systems, vol.**1**,no.2, p. 13-19, 2012.

[7] Dr.K.Sheela Sobana Rani, R.A.N., 3R.Aiswarya, 4 S.Archana and 5M.Divya Bharathi, *"a secure RSA for data transmission in wireless sensor networks".* International Journal of Emerging Technology in Computer Science & Electronics , vol.**13**, no.4, p. 272-277, 2015.

[8] Yi, L., et al., *"A Novel Block Encryption Algorithm Based on Chaotic S-Box for Wireless Sensor Network".* IEEE Access, **7**: p. 53079-53090, 2019..

[9] AL-Swidi, A.A., E.H. Al-Saadi, and L.H. Al-Saadi, *"Soft public key Cipher".* Periodicals of Engineering and Natural Sciences, vol.**7**,no. 3, p. 1433-1438, 2019.

[10] Lakshmi, V. and P. Deepthi, *"A secure channel code‐based scheme for privacy preserving data aggregation in wireless sensor networks".* International Journal of Communication Systems, vol.**32**,no.1, p. e3832, 2019.

[11] Merad Boudia, O.R., S.M. Senouci, and M. Feham, "*Secure and efficient verification for data aggregation in wireless sensor networks".* International Journal of Network Management, vol.**28**, no.1, p. e2000, 2018.

[12] Zheng, J. and A. Jamalipour, *Wireless sensor networks: a networking perspective*. John Wiley & Sons, 2009.

[13] Kamaev, V., et al. *"Key management schemes using routing information frames in secure wireless sensor networks*". in *Journal of Physics: Conference Series*. IOP Publishing, 2017.

[14] Athmani, S., A. Bilami, and D.E. Boubiche, *"EDAK: An Efficient Dynamic Authentication and Key Management Mechanism for heterogeneous WSNs".* Future Generation Computer Systems, **92**: p. 789-799, 2019.

[15] Thigale, S.B., et al., *"Lightweight novel trust based framework for IoT enabled wireless network communications".* Periodicals of Engineering and Natural Sciences, vol.**7**,no.3, p. 1126-1137, 2019.

[16] Gupta, S.K. and P. Sinha, *"Overview of wireless sensor network: a survey".* Telos, vol.**3**,no. 15μW, p. 38mW, 2014.

[17] Masri, W. and Z. Mammeri. "*Middleware for wireless sensor networks: A comparative analysis*". in *2007 IFIP International Conference on Network and Parallel Computing Workshops (NPC 2007)*. IEEE, 2007.

[18] Shen, C.-C., C. Srisathapornphat, and C. Jaikaeo, *"Sensor information networking architecture and applications".* IEEE Personal communications, vol.**8**, no.4, p. 52-59, 2001..

[19] Karlof, C., N. Sastry, and D. Wagner. "*TinySec: a link layer security architecture for wireless sensor networks*". in *Proceedings of the 2nd international conference on Embedded networked sensor systems*. ACM, 2004.

[20] Jain, M.K., *"Wireless sensor networks: Security issues and challenges".* International Journal of Computer and Information Technology, vol.**2**,no.1, p. 62-67, 2011.

[21] Heena Dogra, J.K., *"Asymmetrical Encryption for Wireless Sensor Networks: A Comparative Study".* International Research Journal of Engineering and Technology, vol.**04** ,no. 06, 2017.

[22] Panda, M., *"Security in wireless sensor networks using cryptographic techniques".* American Journal of Engineering Research (AJER), vol.**3**,no.01, p. 50-56, 2014.

[23] Thakare, M.R.S.S.a.P.A.N., "*A Survey on Security in Wireless Sensor Networks Using Elliptical Curves Cryptography".* International Journal of Engineering Research & Technology (IJERT), vol.**2**,no.10, 2013.

[24] M.Rajalakshmi[1], D.C.P., "*A Simple Cryptographic Algorithm for Wireless Sensor Networks".* JASC: Journal of Applied Science and Computations, vol.**5** ,no.9,p. 818-824, 2018.

[25] Kiruthika, B., R. Ezhilarasie, and A. Umamakeswari, *"Implementation of modified rc4 algorithm for wireless sensor networks on cc2431".* Indian Journal of Science and Technology, vol.**8**,no.S9, p. 198-206, 2015.

[26] Priyadharshini, S.P., N. Arumuagam, and K. SangeethaAnanthamani, "*Implementation of security in wireless sensor network using blowfish algorithm".* International Journal of Computer Applications, **975**: p. 8887, 2014..

[27] Sasilatha, M.S.M.a.T., "*A Hybrid Cryptographic algorithm design using Block and Stream cipher based Confidentiality and Integrity in Wireless Sensors Networks".* AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES, vol.**10**,no.1, p. 387-393, 2016..

[28] Kawale, D.S.R., *"Message Security Using RSA-DES Hybrid Cryptography".* IOSR Journal of Computer Engineering (IOSR-JCE), vol.**21**,no.2, p. 07-10, 2019.

[29] Susan Mohammed, S.K.A.-A.a.H.A.L., *"ECC and AES Based Hybrid Security Protocol for Wireless Sensor Networks".* Journal of Engineering and Applied Sciences . vol.**13**,no.24, p. 10356-10363, 2018.

[30] I Yashaswini R, I.H., IIIBindu AThomas, *"Wireless Sensor Network Security using Cryptography".* IJARCST, vol.**4**,no.2, 2016..

[31] Gupta, R., et al. *"Security for wireless sensor networks in military operations*". in *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*. IEEE, 2013.

[32] Manro, R.R.a.R., *"Improved Watermarking Leach Protocol using node level Integrity and Confidentiality in WSN".* International Journal of Computer Sciences and Engineering, vol.**6**,no.11, ISSN: 2347-2693, p. 597-601, 2018..

[33] Bayılmış, C., et al., *"Enhanced secure data transfer for WSN using chaotic-based encryption".* Tehnički vjesnik, vol.**24**,no.4, p. 1065-1069, 2017..

[34] Dalal, S.a.K., *"Security Enhancement in WSN Networks using Cryptography Techniques".* International Journal of Recent Trends in Engineering & Research (IJRTER). vol.**2**,no.6, 2016.

[35] Banerjee, B. and J.T. Patel, "*A Symmetric Key Block Cipher to Provide Confidentiality in Wireless Sensor Networks".* infocomp, vol.**15**,no.1, p. 12-18, 2016.

[36] R, M.S.P.a.M.B., "*Data Confidentiality in Wireless Sensor Networks-A Survey".* International Journal for Scientific Research & Development, vol.**3**,no.12, 2016.

[37] Jariwala, V.J., "*Privacy Preserving Secure Data Aggregation for Wireless Sensor Networks".* Journal of Computers, vol.**13**,no.6, p. 655-678, 2018.

[38] Kumar, V. and S. Madria, *"ENERGY EFFICIENT SECURE DATA AGGREGATION IN WIRELESS SENSOR NETWORKS".* 2011.

[39] Lee, J.C., et al., "*Key management issues in wireless sensor networks: current proposals and future developments".* IEEE Wireless Communications, vol.**14**,no.5, p. 76-84, 2007.

[40] Muhajjar2, M.A.A.-t.a.R.a.A., *"SYMMETRIC KEY MANAGEMENT SCHEME FOR HIERARCHICAL WIRELESS SENSOR NETWORKS".* International Journal of Network Security & Its Applications (IJNSA), 2018. vol.**10**,no.3, p. 17-24.

[41] Krishan Gopal, Y.T., "*a secure approach of data transmission in wsn using RC5 algorithm".* International Journal For Technological Research In Engineering, vol.**5**,no.12, ISSN (Online): 2347 – 4718): p. 4636- 4640, 2018..

[42]Tayebi, A., S. Berber, and A. Swain, *"Wireless Sensor Network Attacks: An Overview and Critical Analysis with Detailed Investigation on Jamming Attack Effects*, in *Sensing Technology: Current Status and Future Trends III*", Springer. p. 201-221, 2015.

[43] Stallings, W., *"Cryptography and network security: principles and practice*". Pearson Upper Saddle River, 2017.

[44] Mohanty, P., et al., *"SECURITY ISSUES IN WIRELESS SENSOR NETWORK DATA GATHERING PROTOCOLS: A SURVEY".* Journal of Theoretical & Applied Information Technology, **13**, 2010.

[45] Khan, M.A.K.a.M., *A Review on Security Attacks and Solution in Wireless Sensor Networks.* American Journal of Computer Science and Information, **Vol.7 No.1,**(2349-3917): p. 1-7, 2019..

[46] Gracy, P.L. and D. Venkatesan, "*AN HONEY ENCRYPTION BASED EFFICIENT SECURITY MECHANISM FOR WIRELESS SENSOR NETWORKS".* International Journal of Pure and Applied Mathematics, vol.**118**,no.20, p. 3157-3164, 2018..

[47] Lavanya Ranganath , K.K.S., Priyanka B M, Shruthi A M and Dr C dyaRaj, *"Security for Source Node Privacy in Wireless Sensor Networks".* International Research Journal of Engineering and Technology, vol.**04** ,no.04, p. 1307- 1309, 2017..

[48] Furrakh Shahzad, M.P.a.A.A., *"A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures".* International Journal of Computer Science and Information Security, vol.**14**,no.12, p. 54-65, 2016.

[49] Pune, N.P.S.Z.s.D., "*Query Confidentiality in Wireless Sensor Networks".* International Journal of Advanced Research in Computer Science and Software Engineering. vol. **5**,no.2,p. 119-123, 2015.

[50] Khan, S., et al., *"Security analysis of secure force algorithm for wireless sensor networks".* arXiv preprint arXiv:1509.00981, 2015.