Int. J. Nonlinear Anal. Appl. 14 (2023) 1, 1125–1132
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2022.27417.3593

Security management of wireless sensors network in industrial application

Ali Moradkhani, Ali Broumandnia*, Seyed Javad Mirabedini

Department of Computer Engineering, South Tehran Branch, Islamic Azad University, Tehran, Iran

(Communicated by Madjid Eshaghi Gordji)

Abstract

In this survey, the main and dominant point of pursuit is reviewing some aspects and approaches of networks security that are more appropriate for wireless sensors, by applying effective changes to some details and divisions, and it has been attempted to make them exclusive for the certain wireless sensors network that can be utilized in any particular or crucial industrial fields, like oil and gas pipeline and medical devices for monitoring the patient. Security network algorithms and processing trends are usually accessible and ready to use for everyone, however, it also increases the potential risk and concern of attack for industries that use wireless sensor networks. In this study, basic data has been altered and actually disintegrated before securing; additionally, common algorithms have been employed in order to reduce the risk involved with using wireless sensor networks for maintaining and protecting basic and major industries, and in particular for monitoring pipelines.

Keywords: medical devices, networks security, Security management, wireless sensors
2020 MSC: 68M25, 91G20

1 Introduction

Today most of the critical industries in the world trying to use high-tech monitoring system for preventing any mistake such as human mistake or mistake which comes from low level control system. In other side, Wireless Sensor Networks (WSNs) have been attracting increasing interest for supporting a new generation of ubiquitous computing systems with great potential for many applications such as surveillance, environmental monitoring, health care monitoring or home automation. One of the most important industrial systems in which any small mistake can cause a huge irreparable damage is Oil and Gas pipeline system. Using a wireless sensor networks for monitoring in pipeline could be very helpful and can improve the level of the monitoring and decrease the cost in compare with old system monitoring, but always there is an important question against using wireless sensor concept which is questioning the security of wireless sensors network and also how it can avoid any attack. WSNs, is such a network that normally consisting a large number of distributed nodes that organize themselves into a multi-hop wireless network [2]. Each node has one or more sensors, embedded processors and low-power radios, and is normally battery operated. Typically, these nodes coordinate to perform a common task. Varity of sensors, embedded systems and huge number of data transactions always are the most concern in using WSNs in critical and basic industries of every country [5]. Because,

*Corresponding author
Email addresses: a.moradkhani@gmail.com (Ali Moradkhani), broumandnia@gmail.com (Ali Broumandnia), j.mirabedini@gmail.com (Seyed Javad Mirabedini)

Received: January 2022 *Accepted:* April 2022

in this particular network, the form of distribution and computing ubiquitous, raises many challenges in terms of real-time communication and coordination due to the large number of constraints that must be simultaneously satisfied, including limited power, CPU speed, storage capacity and bandwidth also wireless sensors cannot have a enough computing for security algorithm and this is a big welcome door for anybody or other competing organizations or intruders to inter to a very critical network like oil and gas system. The purpose of this study is using three trustable security algorithms which have been used for wireless sensors network in other industrial systems by changing, mixing and adding some extra parts to the system to design a new high secure, reliable and suitable network for main and basic industries. In this study has been tried to work on networks corrosion detector sensor for Oil and Gas pipeline monitoring system. According to the Fig. 1 in 100 km pipeline, every 2 km of pipe, one corrosion detector sensor can be installed that contains one matrix of pins (probes) for getting the signal from that specific part of pipe which is under monitoring plus one very low power consumption microcontroller and one wireless module for transferring the data over any available wireless network such as GPRS, LTE, 3G, 4G or other network.Another example of sensor networks could be a comprehensive patient monitoring system. As shown in Fig. 2 , various sensors are connected to the patient's body, all connected to the mobile phone wirelessly, and the information is sent to the server via the mobile phone. In fact, the basic concept of all sensor networks is the same.

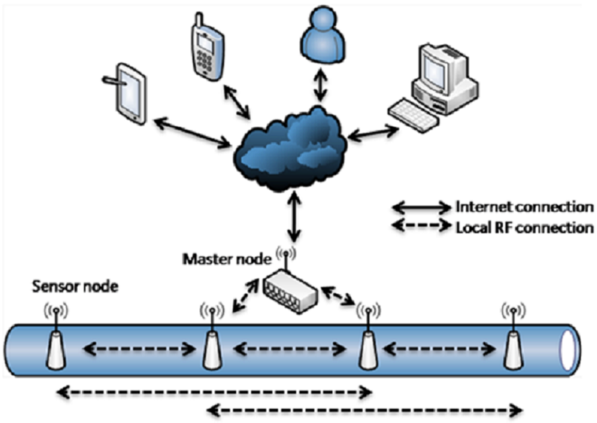

Figure 1: Whole idea of corrosion detector sensor networks for Oil and Gas pipeline monitoring system.

Such as every monitoring system another side of this system is the server and the handhold devices like tablet and cellphone which should understand and decode the data that has been received from network. In this study has been focused on secure transferring data by using very low power computing Consumption of security algorithm, by adding some extra parts for decreasing the risk and increasing the safety level of wireless sensor networks.

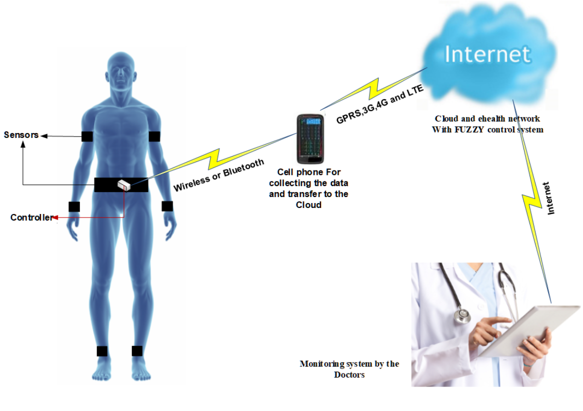
Internet
GPRS,3G,4G and LTE
Cloud and ehealth network
With FUZZY control system
Sensors
Wireless or Bluetooth
Cell phone For collecting the data and transfer to the Cloud
Controller
Internet
Monitoring system by the Doctors

Figure 2: Patient monitoring system by using of sensor networks.

2 Limitation In Corrosion Sensor Networks

The inherent structure of the sensor networks has some limitations with a strong effect on other parts of the system that are essential for any network system [3]. Especially in outdoor systems like pipeline these limitations will be bold and sometimes are the most real reasons that the main industries like Oil and gas pipeline do not have enough propensities in using this system Fig. 3.

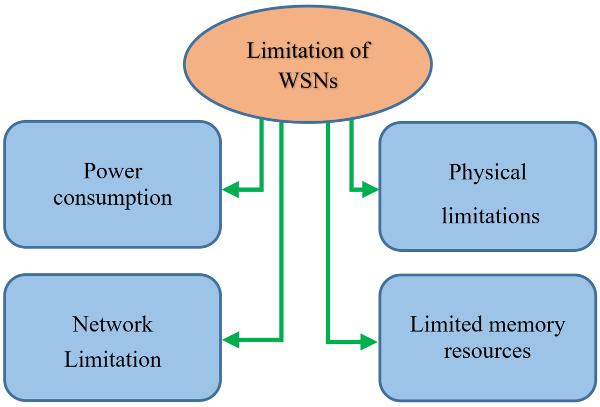

Figure 3: Effective Limitations on Wsns.

For instance, the inherent limitations in sensor networks make the design of security procedures more complicated. So, regarding this study some of these limitations has been listed below and need more consideration in order to have a better design for network security [12].

A.Power consumption

Access limitation to power supply especially in outdoor system like Oil and Gas pipeline force using very simple encryption algorithm. The study is assumed of using solar cell and battery for sensors and master nodes so the power supply source is bounded [8]. Also, the system just can do very simple encrypting in every nodes and master nodes.

B.Network limitations

Beside node limitations, sensor networks bring all the limitations of a mobile ad hoc network where they lack physical infrastructure, and they rely on unsecured wireless media [6].

C.Physical limitations

Sensor networks deployment nature in public and hostile environments in many applications makes them highly vulnerable to capture and vandalism. Physical security of sensor nodes with tamper proof material increases the node [13].

D.Limited memory resources

The amount of key-storage memory in a given node is highly constrained, it does not possess the resources to establish unique keys with every one of the other nodes in the network. This brief explanation could be enough for having a simple but strong security system on every nodes and in addition show that using some private encrypting might be more efficient with few side effect on the system [14].

3 Types Of Attacks in Wireless Sensor Networks

Before reviewing and making the best decision for securing the data of WSNs, should take a viewpoint of the most important way to attack the WSNs. Wireless Sensor networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. Basically attacks are classified as active attacks and passive attacks [10]. But, there are some other types and ways of attacks that are branches of passive and active which have been listed as follows:

A.Passive Attacks

The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. The Attacks against privacy is passive in nature.

B.Node subversion

Capture of a node may reveal its information including disclosure of cryptographic keys hence compromising the whole sensor network [17].

C.False Node

Addition of a malicious node by an adversary to inject the malicious data, false node would be computationally robust to lure other nodes to send data to it [19].

D.Node Malfunction

A malfunctioning node will generate inaccurate data which would jeopardize the integrity of sensor network especially when that node is data aggregation node for example, a cluster leader [21].

E.Node Outage

What happens when a cluster leader stop functioning? Sensor network protocols should be robust enough to mitigate the effects of node outages by providing alternate route [4].

F.Message Corruption

When contents of a message are modified by an attacker at compromises the message integrity [18].

G.Traffic Analysis

Even the message transfer is encrypted in sensor networks, it still leaves the high probability of analysis of communication patterns and sensory activities revealing enough information to enable adversary to cause more malicious harm to sensor networks [1].

H.Active Attacks

The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack [16].

I.Routing loopsctive

In sensor networks routing loops attacks target the information exchanged between nodes. False error messages are generated when an attacker alters and replays the routing information. Routing loops attract or repel the network traffic and increases node to node latency.

J.Selective forwarding

Selective forwarding is a way to influence the network traffic by believing that all the participating nodes in network are reliable to forward the message. In selective forwarding attack malicious nodes simply drop certain messages instead of forwarding every message. Once a malicious node cherry picks on the messages, it reduces the latency and deceives the neighboring nodes that they are on a shorter route. Effectiveness of this attack depends on two factors. First, the location of the malicious node, how they are close to the master node and the amount of traffic will be attracted [16]. Second is the percentage of messages it drops. When selective forwarder drops more messages and forwards less, it retains its energy level thus remaining powerful to trick the neighboring nodes. In one form of the selective forwarding attack, the malicious node can selectively drops the packets coming from a particular node or a group of nodes. This behavior causes a DoS attack for that particular node or a group of nodes as shown in Fig. 4 A forwarding node selectively drops packets that have been originated or forwarded by certain nodes, and forwards other irrelevant packets instead [20]. They also behave like a Black hole in which it refuses to forward every packet. The malicious node may forward the messages to the wrong path, creating unfaithful routing information in the network.

K.Sybil attacks

A type of attacks where a node creates multiple illegitimate identities in sensor networks either by fabricating or stealing the identities of legitimate nodes. Sybil attacks can be used against routing algorithms and topology maintenance; it reduces the effectiveness of fault tolerant schemes such as distributed storage and disparity [7]. Another malicious factor is geographic routing where a Sybil node can appear at more than one place simultaneously.

L.Sinkhole attacks

In sinkhole attacks, adversary attracts the traffic to a compromised node. The simplest way of creating sinkhole is to place a malicious node where it can attract most of the traffic, possibly closer to the base station or malicious node itself deceiving as a base station. One reason for sinkhole attacks is to make selective forwarding possible to attract the traffic towards a compromised node. The nature of sensor networks where all the traffic flows towards one base station makes this type of attacks more susceptible.

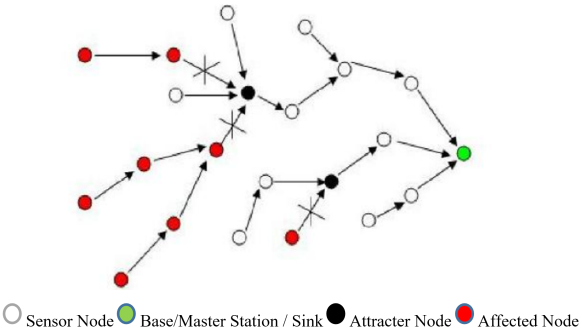

Figure 4: Selective forwarding attacks.

4 Triple Levels of Securing Corrosion Detector Wireless Sensor Networks

Regarding to Fig. 1 all corrosion detector wireless sensors have been installed in one level of priority and among them is no leader and in this structure all sensors have direct connection to master node and have 2 connection to left and right side of themselves. This structure just lets every node has a connection with just 2 others nodes on its left and right sides and helps to enhance the ability of power consumption control and close other ways of attack to the system in first layer of network. Because, all nodes send their id to left and right of itself, for instance, in the future, if they get any packet from others it will be ignored. In fact, every node just expect to have a communication in first layer from left and right nodes Fig. 5.

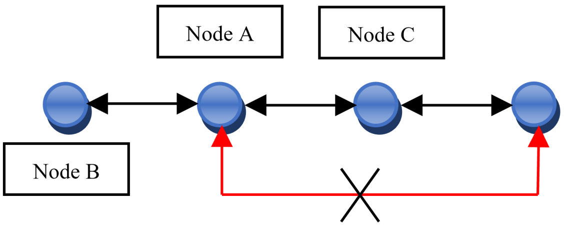

Figure 5: Red communication is not acceptable with node A.

Every node just gets the id of its neighborhood from master node and server and with this method any external attempt for being one of the nodes in network will be extremely impossible. Every node in this project sends the data of corrosion which has been detected during a 24 hours to its left and right node at the specific time during a day. With this procedure if one node cannot send the data to the master node or lose the connection, the left or right node of that can send the last update data to the master node. To increase encrypting data transition among the nodes, pattern of data packet for each side is different. Node A before sending the data to the encrypting algorithm and after that to node B, rotates data 4 times to the left and after that adds it to 8 first bits of node A's id which has been rotated 4 times to the right. This routine will be reversed for sending the data from node A to node C. In this study sending the data between nodes has used random key pre-distribution schemes (RKP). It means that before the deployment of nodes, for each node, a master node randomly chooses a key ring and loads it into the node it is called key pre-distribution [11]. After that each node knows its left and right node and this is the next phase, named shared key discovery. Finally, node A wants to establish a path key with node B. If they are in their communication range and have a shared key, that means, they are on each other's neighbor list, and the shared key can be used as the path key [?]. Otherwise, as it mentioned before they cannot have a communication together because they are not on the left or right node of each other. In fact this part of random key pre-distribution schemes has been changed in this study. As there is a limitation for connecting one node to all nodes in this network, the processing and computation will be decrease in random key pre-distribution schemes algorithm and regarding to wireless sensors network imitation it can be helpful and it is the right choice for only two neighboring nodes with common key. Next level of data transmission is between each nodes and master node, in fact, in this study master node has a role of aggregator node in this network.it means that this structure is the one-aggregator model, in which only one node plays the role of an aggregator and gets the data from each node and after that sends the data to the sever [9]. This is usually deployed in networks with relatively small number of sensor nodes. In this model all nodes are in the same level and actually they are in a flat layer and it is like a tree structure with just master node that can connect to the next level and server. This model has a strong effect on reducing power consumption that is one of the most important limitation of WSNs. As this study is about a very critical system in oil and gas, any attack and accessing to the data can has irreparable damage on whole system so the security of network should be in highest level. For achieving this goal, 3 levels of encryption is involved Fig. 6. The first level is among nodes that has been described and next level is between nodes and master node that has used Localized Encryption and Authentication Protocol (LEAP) which is one the greatest and popular algorithm for encrypting especially in WSNs. LEAP is a key management protocol [15]. It establishes four types of keys which are individual keys, pairwise shared keys, cluster keys and group keys. Individual keys are symmetric keys shared between the master node and each of the nodes. On the other hand, pairwise shared keys are symmetric keys shared between a node and each neighbors. However, neighbors do not share the key with each other. Whereas, in this study, each nodes just can have a communication with left and right nodes of itself, so some parts of this algorithm should be changed. This protocol is inspired by the idea that every message broadcasted between nodes is different from another and comprise of different security requirements. The Individual key is a unique key shared between anode and its corresponding base station in order to provide security between them as they commune. Communication between a node and master node is vital as it allows a node to inform the base station of any abnormal behavior detected from its surrounding nodes. As, the master node being aware of the malicious node, it can use of the key to encrypt the important information such as instructions to a specific node [3]. The individual key can be fabricated using the following equation:

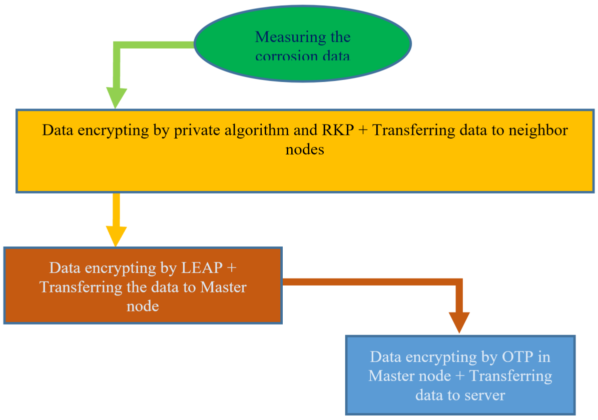
Measuring the corrosion data
Data encrypting by private algorithm and RKP + Transferring data to neighbor nodes
Data encrypting by LEAP + Transferring the data to Master node
Data encrypting by OTP in Master node + Transferring data to server

Figure 6: Three levels of encrypting data.

$$k_u = pk_i(ID_u) \tag{4.1}$$

Where P is the pseudo random function, (k_i)is the initial key, also known as the master key and (ID_u) is the ID of node u. The pair-wise key is a key shared between a node and its neighboring sensor nodes. The establishment of this key ensures protection of communication that longs for privacy or authentication of a source. But, this key is not essential for this project because all nodes just have communication with 2 nodes in their sides and they use of random key pre-distribution schemes for internal communication on sensors level and all nodes have an equal level of communication with master node and they can connect to the master node directly.in this method, there isn't any group and actually nodes with permission to make any group, then group key is not necessary. Therefore, regarding cluster key which is a key shared by a node with multiple of its neighboring sensor nodes, this key is not essential for this structure because all nodes have direct connection to master node. Up to this level there are two level of communication, the first one is among nodes which is separated from master node level another is between each node and master node. But, there is another level of communication between master node and server. Master node in this project is embedded system on ARM9 processor and Linux Angstrom which has an enough power for any encryption algorithm Fig. 7.For increasing safety and reliability in this network and cover any standard of safety in main industries like Oil and Gas pipeline one-time pad encryption has been selected. The one-time pad (OTP) is an encryption technique that cannot be cracked if used correctly. In this technique, a plaintext is paired with a random secret key (also referred to as a one-time pad). Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition. If the key is truly random, is at least as long as the plaintext, is never reused in whole or in part, and is kept completely secret, then the resulting cipher text will be impossible to decrypt or break.

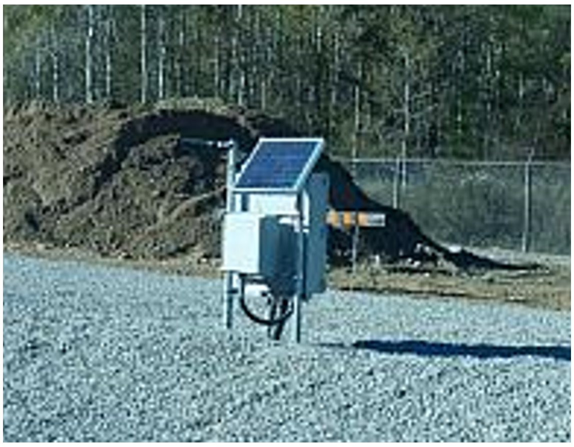

Figure 7: View of master node in oil and gas system

It has also been proven that any cipher with the perfect secrecy property must use keys with effectively the same requirements as OTP keys. However, practical problems have prevented one-time pads from being widely used. These three levels of encryption can cover most limitation of WSNs and warranty extremely safe communication.

5 Experimental Results

During the test, the system was used into one real corrosion monitoring in Oil pipeline with 20 sensors and one master node. The experimental results are as follows:

A. All function performed satisfactory.

However, there were some issues in synchronizing between communication in sensor node level and master node to each sensor nodes. Sometimes there were some delay to response. If master node has a request for getting the data from one node, exactly at the same time the node is working on transferring the data to its neighbor nodes, then delay might be happen.

B.Some WSNs limitation has been covered.

Low power consumption has been covered very well because there is not much computing in nodes for encrypting and this low level of computing does not get much power of the system.as all nodes just have connection with their near neighbors there is no issues on network limitation in WSNs in this structure. Sensors has been packed in a very industrial case and influence of environmental condition are in the lowest level.

C.Stystem has been resitanted for attacks.

Although, system has been tested for attacks but this part needs more considerations and needs some other parties to test the system under more difficult conditions. So under the specific conditions which are extremely important for Oil pipeline industry, the system had acceptable results, because some parts of this method are private and the administrator of the system can change them exactly based on what they need and this flexibility is a significant factor for customers.

6 Conclusions

Using WSNs in some critical industries has some worries, especially related to security because there are a lots of sensors which can be the ways for attacking the whole system and will be a way for leaking. The proposed method has been designed especially for Oil and Gas corrosion wireless network sensor which can cover some limitations of WSNs and also make the attacking to the system more difficult by mixing and changing three algorithms and add one private part to encrypting the data. Although, there are some parts which need more consideration but totally the result of the system was acceptable for Oil pipeline monitoring system and patient monitoring system. The method used in this study could increase the trust level of experts in the use of WSNs in their industry.

References

[1] Mubashir Ali, Muhammad Nadeem, Ayesha Siddique, Shahbaz Ahmad, and Amir Ijaz, *Addressing sinkhole attacks in wireless sensor networks-a review*, Int. J. Sci. Technol. Res. **9** (2020), no. 8.

[2] S. Ali, R.P. Singh, M. Javaid, A. Haleem, H. Pasricha, R. Suman, and J. Karloopia, *A review of the role of smart wireless medical sensor network in covid-19*, J. Ind. Integration Manag. **5** (2020), no. 4, 413–425.

[3] S. Ashraf, *Culminate coverage for sensor network through bodacious-instance mechanism*, J. Wirel. Commun. Netw **8** (2019), no. 3.

[4] A. Bashar and S. Smys, *Physical layer protection against sensor eavesdropper channels in wireless sensor networks*, IRO J. Sustain. Wireless Syst. **3** (2021), no. 2, 59–67.

[5] M.S. BenSaleh, R. Saida, Y.H. Kacem, and M. Abid, *Wireless sensor network design methodologies: A survey*, J. Sensors **2020** (2020).

[6] N. Bhalaji, *A novel hybrid routing algorithm with two fish approach in wireless sensor networks*, J. Trends Comput. Sci. Smart Technol. (TCSST) **2** (2020), no. 3, 134–140.

[7] A.H. Hamza and S.M.K. Al-Alak, *Evaluation key generator of multiple asymmetric methods in wireless sensor network (wsns)*, J. Phys.: Conf. Ser., vol. 1804, IOP Publishing, 2021, p. 012096.

[8] Z. Huanan, X. Suping, and W. Jiannan, *Security and application of wireless sensor network*, Procedia Comput. Sci. **183** (2021), 486–492.

[9] D. Jain, P.K. Shukla, and S. Varma, *Energy efficient architecture for mitigating the hot-spot problem in wireless sensor networks*, J. Ambient Intell. Humanized Comput. (2022), 1–18.

[10] S.A. Jilani, C. Koner, and S. Nandi, *Security in wireless sensor networks: Attacks and evasion*, Nat. Conf. Emerg. Trends Sustain. Technol. Engin. Appl. (NCETSTEA), IEEE, 2020, pp. 1–5.

[11] G. Mehmood, M.S. Khan, A. Waheed, M. Zareei, M. Fayaz, T. Sadad, N. Kama, and A. Azmi, *An efficient and secure session key management scheme in wireless sensor network*, Complexity **2021** (2021).

[12] S.R. Mugunthan, *Wireless rechargeable sensor network fault modeling and stability analysis*, J. Soft Comput. Paradigm (JSCP) **3** (2021), no. 1, 47–54.

[13] Y. NarasimhaRao, P.S. Chandra, V. Revathi, and N.S. Kumar, *Providing enhanced security in iot based smart weather system*, Indonesian J. Electric. Engin. Comput. Sci. **18** (2020), no. 1, 9–15.

[14] D.U. Palani, D. Raghuraman, D.D. StalinDavid, R. Parthiban, S. Usharani, D. Jayakumar, and D. Saravanan, *An energy-efficient trust based secure data scheme in wireless sensor networks*, Eur. J. Molecul. Clinic. Med. **7** (2021), no. 9.

[15] B. Sheng, Q. Li, and W. Mao, *Data storage placement in sensor networks*, Proc. 7th ACM Int. Symp. Mobile ad hoc Network. Comput., 2006, pp. 344–355.

[16] D. Singh, B. Kumar, S. Singh, and S. Chand, *Evaluating authentication schemes for real-time data in wireless sensor network*, Wireless Personal Commun. **114** (2020), no. 1, 629–655.

[17] ———, *A secure iot-based mutual authentication for healthcare applications in wireless sensor networks using ecc*, Int. J. Healthcare Inf. Sys. Inf. (IJHISI) **16** (2021), no. 2, 21–48.

[18] D. Sivaganesan, *A data driven trust mechanism based on blockchain in iot sensor networks for detection and mitigation of attacks*, J. Trends Comput. Sci. Smart Technol. **3** (2021), no. 1, 59–69.

[19] Vikas, B.B. Sagar, and M. Munjul, *Security issues in wireless sensor network–a survey*, J. Discrete Math. Sci. Crypto. **24** (2021), no. 5, 1415–1427.

[20] H. Wang, *Iot based clinical sensor data management and transfer using blockchain technology*, J. ISMAC **2** (2020), no. 3, 154–159.

[21] W. Wang, C. Qiu, Z. Yin, G. Srivastava, T.R. Gadekallu, F. Alsolami, and C. Su, *Blockchain and puf-based lightweight authentication protocol for wireless medical sensor networks*, IEEE Internet Things J. **9** (2021), no. 11, 8883–8891.