Network Security in Wireless Sensor Networks: Threats and Countermeasures

PROF. DR. PARIN SOMANI
Director, Department of Skill Development, London Organisation of Skills Development Ltd, 27 Old Gloucester Street, London, United Kingdom

Abstract- ***As the number of wireless sensor networks has increased, so has the importance of ensuring the confidentiality of the information that is sent between them. As a result of their malleability and the simplicity with which they may be implemented, sensor networks have found applications in a wide variety of academic and real-world contexts. Due to these qualities, they are vulnerable to a variety of threats that put the confidentiality of their data in jeopardy. As a result of the fact that the data is protected while it is moving through and across networks, the investigators now have access to a novel and fascinating research opportunity that was not available to them in the past. The architecture of these networks, which is focused towards preserving the data, is confined by the networks' own power and processing capabilities. This is the case even if the architecture is geared towards protecting the data. Academics and engineers can have a better understanding of this application field with the aid of our high-level examination of the principles of wireless sensor network security that we present here. The principles of information security are going to be covered in this chapter, with a specific emphasis on wireless sensor networks (WSNs). In addition, the chapter that comes after this one will include an overview of the data security requirements that are required for networks of this type. In addition, this article discusses the dangers that can be posed to the data security of WSNs as well as various preventative measures.***

Indexed Terms- ***Wireless Network, Wireless Security, Wireless Threats***

I. INTRODUCTION

Because wireless sensor networks (WSNs) have such a wide variety of possible applications, more and more researchers and engineers are getting interested in developing and implementing WSNs. These make it possible to create wireless networks with a high number of nodes in a manner that is both simple and adaptable. In addition to this, they make it possible to do this without the need of any cables at all. This makes it possible to implement Wireless Sensor Networks (WSN) in applications that were previously unimaginable. They are being put to use in a diverse array of intelligent and smart systems, including those that are tasked with environmental observation and forecasting, those that are employed in manufacturing and logistics, those that are tasked with monitoring habitats, those that are employed in manufacturing and logistics, those that are employed in manufacturing and logistics, those that are employed in manufacturing and logistics, and those that have military, health, domestic, and industrial applications.[1] The Intelligent Habitat Monitoring System, sometimes known as IHMS, is a system that was developed specifically for the purpose of monitoring natural ecosystems. The topic of multimedia wireless sensor networking is a more recent development within this wider discipline. [2,3] This subfield is able to manage a wide variety of multimedia data types. This category includes a wide variety of data types, some examples of which include audio recordings, video recordings, and still photographs. In a sensor network of this kind, the number of the network's nodes would often range from the hundreds to the thousands, and even more. [4,5] The job of not only receiving information but also processing and disseminating it has been delegated to these nodes. The secrecy of information that is sent by a WSN may be jeopardised in a variety of ways, including eavesdropping, retransmitting packets that have already been sent, adding redundant or nonsensical bits into packets, and many more risks of varied natures. Privacy and protection of data when it is being sent and received over networks are of the utmost significance, which is why information security is one of the most important concerns.[6,7] According to Moore's law, there will not be any substantial improvements in the hardware capacity or processing capabilities of

sensors used in wireless sensor networks any time soon. This is a prediction made by Moore's law. In spite of the predictions made by Moore's law, there has not been an increase in the amount of computer power available. This is an exception to the pattern that has been seen in general. The performance standards have been drastically lowered since it is of the utmost importance to keep the cost of these networks as low as possible.[8]

Sensors that are sold at a lower price point typically have a smaller capacity for storing data, a greater rate of power consumption, and a slower processing rate than their more costly counterparts. This creates a new task for the research community, as it requires the production of information security solutions that are not only effective and unique, but are also suited for sensor networks with little resources. [9,10] This presents a new challenge for the research community since it demands the creation of information security solutions that are effective and creative. Individuals have the opportunity to provide themselves with an authentic challenge as a result of this. It is necessary for the sensors that make up the network to have consistent interactions with the outside environment in order for the network to communicate with either other sensors or with people.[11,12] This is because the network is able to monitor and respond to events as they occur in real time, which is why this is the case. Because there is always a possibility that the physical security of these sensors may be compromised, the total security of the network is currently in jeopardy on a level that has never previously been witnessed. Recent advancements in power analysis and time-based attacks have provided a broad variety of adversarial actors with the capacity to carry out a number of operations that have the potential to do harm to the target.[13] It is possible to make the case that wireless sensor networks have the same unfavorable reputation as wireless channels. Because wireless sensor networks are able to contain a sizeable number of nodes and sinks, there is a natural concern regarding the dependability of the communications that take place inside the network. In order to guarantee that all of the nodes that are taking part in the communications can be trusted, it is important to construct trust models on an individual basis for each node.[14,15] The way that we think about the risk presented by wireless sensor networks needs to be revised in order to take into account all of these different elements. There are risks associated with these networks that do not exist with conventional computer systems, wireless networks, or even high-bandwidth wireless adaptations of these technologies. These risks are unique to these networks and do not apply to other types of computer systems. As a consequence of this, there is a wide range of answers that may be given to the several forms of intimidation. After reading this chapter, the reader will have a higher chance of benefiting from being well-versed in the core principles underpinning security and WSN security. [16]

This will be the case since they will have gained a better understanding of these concepts. When everything is said and done, the reader will have a deeper comprehension of the advantages and disadvantages associated with WSN security. If we look at a variety of well-known and more recent attacks, as well as the preventative measures that were put into place as a response to those attacks, we may be able to learn more about the dangers that we face and improve our capacity to respond to them. This may be the case if we also increase our ability to respond to them.[17,18] The reader will walk away from this chapter with a stronger comprehension of the challenges associated with information security as well as a familiarity with the key ideas that were presented in this chapter. The readers who have either a cursory knowledge or no familiarity at all with information security may find this helpful in gaining an understanding of the topics that are offered here. After finishing this chapter, we anticipate that readers will have a fundamental comprehension of Wireless Sensor Network Security (WSNS). Students will be well on their way to discovering new difficulties and the solutions to them in this fascinating field of study and practical application once they have completed this activity. In addition, we believe that the vast majority of readers will already have a thorough understanding of the fundamental concepts underlying WSNS. In this chapter, we have offered an explanation of the fundamentals, and it is our sincere hope that the readers will have no trouble understanding the ideas.[19,20]

The part of this page titled "General Characteristics of WSN" delves into the distinguishing aspects of the Wireless Sensor Network (WSN). On the other hand, because to these features, there are restrictions placed on the possible responses to the security

vulnerabilities that are present in WSN. These characteristics make these networks the superior option for a wide variety of applications, but they also restrict the range of solutions that are practically possible. The significance of these features with regard to the security of WSNs is the primary subject of the work that is now being carried out.[21,22] In order for wireless sensor networks (WSNs) to be trusted and safe for use in communications, they must first satisfy a variety of security standards. These requirements are included in the mandatory degree of protection that is described in Section 3. In WSN, dangers can present themselves in a broad range of different ways depending on the specific kind. The discussion of many of the most serious threats will take up the most of the time allotted to this chapter's fourth section. In the next section (entitled "Defences"), we will explore potential defences that may be taken against the attacks that were detailed before. The accumulation of knowledge in this field has led to an abundance of fascinating new findings in recent years.[23,24] These discoveries are assisting us in lessening the WSN's susceptibility to attacks and in making secure implementations less taxing on resources like as processing power and memory. In Section 6, we cover the most recent findings of research as well as the actual applications of a variety of various algorithms and schemes. Things will be brought to a close in the seventh and last portion of the chapter. In addition to providing a summary of the information presented in the chapter, it also provides some prospective future research avenues for WSN.[25]

II. OBJECTIVE

1. To conduct research on the topic of network security in wireless sensor networks, including threats and mitigation strategies.
2. Countermeasures To Attacks On Wsn

III. SECURITY REQUIREMENTS IN WSN

Wireless sensor networks are a subset of wireless networks that are referred to by their abbreviation, WSN, which stands for wireless sensor network. Because of the nature of wireless communications, the requirements for the safety of a WSN are fundamentally different from those of traditional computer networks. Because WSN is a network, it has its very own set of requirements that must be complied with on an individual basis. The laws that regulate the safety of WSNs are based on a combination of the standards for the safety of wireless communications and the safety of computer networks.[26,27] These standards have been combined to create the foundation for the regulations. This is done to verify that every WSN-based connection and exchange is safe and does not put the network's integrity at risk in any way.[28] These distinctive traits, which will be investigated in further detail in the following sections, are held by every WSN and help to separate it from the others. These attributes will be discussed in more detail in the following sections. It's probable that their peculiar behaviour may be explained by a number of various factors, such as the large volume that they create, the pattern of dispersion that they adhere to, and the constraints that they confront in terms of the resources that are available to them in terms of availability. The interplay of all of these aspects has directly led to the formation of specific exceedingly granular criteria for the degree of security that must be maintained. These standards must be adhered to at all times. In the following section of this post, we are going to talk about some of the most essential requirements for the security of WSNs.

- Data Confidentiality

The data is traded between the sender and the recipient, and it is possible for it to go via a variety of nodes along the way to reach its final location. It's conceivable that these specifics will be saved in memory for further processing to take place at a later time. [29] This information can be regarded as secret to the extent that it should only be discussed between the sender and the recipient. An adversary may get access to this information in a variety of ways, such by eavesdropping on conversations that take place across wireless networks, gaining access to the storage facility, or engaging in any of a number of other modes of attack. The word "data confidentiality" refers to the fact that the data in issue are only accessible to, and consequently utilised by, those persons or organisations who have been granted permission to do so. This ensures that the data are kept private. If any data is lost as a consequence of negligence or poor security procedures, this can result in identity theft, a loss of business, a breach of privacy, and a range of other activities that can be detrimental to the organisation. It is absolutely necessary for there to be no data broadcast to other networks in the area by the sensor

network itself if the message is to remain completely contained within the network. When travelling to its final destination, data will often pass through a significant number of nodes along the way. Because of this, there is a growing demand for safe communication routes not just between individual nodes but also between individual nodes and base stations.

1. One of the processes that is utilised the most frequently in order to protect the secrecy of data is encryption. Prior to transmission, sensitive data, including keys and user identities, should be encrypted. The nature and kind of protocol that is used to encrypt sensitive information, such as symmetric or asymmetric cryptography, mutual authentication, identity or nonce based encryption, can be used to characterise the information that is sensitive. [30]
2. Prior to putting the sensitive information into memory storage, it is possible to take certain steps towards encrypting the data. This is of utmost importance in situations where the nodes may be subjected to user interaction or in situations involving military applications.

- Threat Models

It is conceivable for an attacker to only have access to a small subset of the nodes in the network that they have successfully hacked. An opponent of this kind is referred to be an attacker of the mote class. Another option is when the adversary is in control of more powerful hardware, such as a laptop; this is the origin of the phrase "laptop class attacker." As a result of the fact that these sorts of attackers have access to powerful central processing units (CPUs), massive amounts of battery capacity, high-power radio transmitters, and sensitive antennas, the network is put under a significantly bigger degree of danger by them. To give you an example, a few nodes can cause interference with a few radio links, while a laptop can cause interference with the entire network.[31] In conclusion, attacks that are carried out on a network may either be carried out by insiders who are a part of the network or by outsiders who are not even a part of the network. When a network is compromised from the outside, the person doing the attacking does not have any special rights or permissions within the network.[32] On the other hand, in the scenario of an insider attack, the offender is considered to be a lawful member of the network in which they committed the crime. These sorts of assaults are carried out either by compromised sensor nodes that are running bad code or by laptops that are using data (cryptographic keys and code) that was stolen from lawful nodes. Either way, the nodes that are being attacked have been hacked. Now that we've gotten that out of the way, let's talk about some of the most serious attacks that were conducted against WSN. The architecture of the WSN leaves the physical layer open to interference and other types of physical assault. The data connection layer of a WSN is susceptible to a variety of assaults, including collision, weariness, and unfairness, among others.[33]

- Denial of Service (DoS)

The use of a wireless sensor network (WSN) is susceptible to experiencing resource depletion and device failures due to a wide range of potential causes. The jamming of network nodes, the transmission of messages that do not comply to the rules that have been set, malicious attacks, and external circumstances are all included in this category. As a direct consequence of this, the performance of the system deteriorates, and it is no longer able to execute the purpose for which it was designed.[34,35] These are some examples of "denial of service," or "DoS," assaults, which are made against WSN in an effort to impair its operations. These assaults are directed against different layers of a WSN's layered architecture, specifically the physical, connection, routing, and transport layers. Because of the constraints placed on the network's resources, it may soon become impossible to cover the costs of defending a WSN against attacks of this kind. Researchers have spent a significant amount of time and effort investigating these attacks and developing techniques for minimising the harm that they do to the network in the process of designing mitigation strategies.[36] After that, we'll quickly go through some of the most prevalent forms of distributed denial of service (DDoS) attacks, broken down into the levels of defence they're intended to overwhelm. Jamming and other forms of physical attack are two of the many ways that the physical layer of WSNs might be compromised. However, there are a number of additional ways as well. Attacks that may be conducted at the network layer of a WSN architecture include those known as neglect and greed, homing, tampering with or falsifying routing information, black holes, and floods. Assaults of this kind might be carried out in a number of different ways.[37]

- Physical Attacks

The nodes that comprise a WSN may be installed in any one of a number of different settings, some of which may be incompatible with the hardware and might cause it to malfunction. In addition, sensor nodes are intentionally kept inexpensive and lightweight, which makes it difficult to make them tamper-proof, resistant to extreme temperatures or conditions, and capable of preventing or controlling physical attacks or more complex side-channel attacks. This is due to the fact that the sensor nodes are kept at a low cost and are very lightweight. This is due to a number of factors, including their inexpensive cost and their low weight. [38]As a consequence of this, the individual nodes that comprise a WSN are exceptionally susceptible to being physically manipulated in any way or being attacked in any other way. By altering the nodes in a certain way, it is possible to extract keys as well as other significant cryptographic parameters.[39] The accurate extraction of these features is essential to the effective operation of any security system. An adversary might potentially gain information relating to a network by extracting the source code. [40] This is certainly a possibility. If an adversary possesses this information, they are able to make changes to the code and gain access to the network. If an adversary is successful in replacing the legitimate nodes in the sensor network with infiltrating nodes that are malicious, the integrity and safety of the operation of the whole sensor network may be compromised. [41 Attackers who are able to get physical access to a network are able to compromise individual nodes and, as a result, the operation of the network as a whole. Because of their low cost and widespread distribution, which are characteristics shared by all WSNs, it is extremely challenging to avoid becoming the victim of such attacks.[42]

- Collisions

Collisions are a kind of link layer jamming that have the effect of lowering network performance.[43] This is because continuous message transmission has the potential to induce collisions in networks. Making use of the fact that continuous message transmission may result in collisions is the method by which this objective is accomplished. In order to achieve this goal, the messages can be transmitted in quick succession. Collisions need the messages to be resent from the beginning, which might cause a node's battery to run out if it happens frequently enough.[44,45] Modifying even a little section of a packet in order to induce the establishment of a MAC mismatch at the receiving end is another sort of attack that can be carried out using this approach. This assault can be used to carry out another type of attack. Each time erroneous packets have to be resent, the total cost of transmission goes up. This cost takes into account the amount of money spent on the energy used and the amount of time it takes. The effectiveness of the network will decrease if this kind of attack is allowed to continue for a considerable length of time without being stopped.[46]

- Neglect and greed Attack

During the process of communication between any two nodes in a WSN, it is possible that packets will need to be routed and re-routed across a large number of nodes. The transmission of data from the source to the destination is dependent on the successful and comprehensive routing of the data packets destined for that destination. [47] A malicious or hacked node that is in the path might impact multi-hopping in the network. This can happen either by the packets being dropped or by the packets being routed towards a fake node. Because of this assault, the functionality of the neighboring nodes is also disrupted, and those nodes may lose their ability to receive or send messages.[48,49]

- Alteration of Routing Information (also known as "spoofing")

During this type of attack, the routing information is tampered with and subjected to changes. As a result, the end-to-end latency may increase due to the creation of new routing pathways, the extension or contraction of current routing paths, respectively. It either turns away or draws in traffic, which lowers the quality of the service. It is also possible for it to create bogus error signals, which either prevent nodes from accessing the channel or increase their latency.[50]

- Flooding

Within the context of this form of resource exhaustion attack, an attacker will repeatedly send connection setup requests to a node. Each one of these requests triggers an allocation of resources on the part of the node in order to fulfill the request. The memory and energy resources of the node that is being attacked might be depleted if a malicious node sends persist requests to that node.[51]

- De-synchronization

An adversary is able to carry out this attack by constructing messages that can include any control flags or sequence numbers of earlier frames, and then transmitting these messages to two linked nodes. The nodes are tricked into thinking that they have lost their synchronization as a result of these bogus messages. Nodes are responsible for resending any supposed lost frames; however, if an adversary is able to maintain the transmission of falsified messages, the resources of the nodes will quickly be drained. In addition, because the linked nodes are preoccupied with the synchronization-recovery procedures during the assault, they are unable to communicate with one another or exchange any information that may be valuable.

- Sybil Attack

An intriguing assault like this one involves a node taking on many identities, which ultimately results in the failure of the redundancy measures that are used by distributed data storage systems in peer-to-peer networks. The functionality of the Sybil attack is based on the capability of concurrently representing several nodes. The Sybil attack has the potential to cause damage to various fault-tolerant systems, including disparity, multi path routing, routing algorithms, data aggregation, voting, equitable resource allocation, and topology maintenance. This attack also has an effect on the geographical routing protocols, in which a malicious node in the network displays many identities to other nodes in the network, giving the impression that it is present in more than one location at the same time. In a similar vein, the malicious node's ability to simultaneously offer many identities allows it to generate more votes while the voting process is in progress. [52] It has the potential to disrupt the routing algorithms by designing multiple routes that only travel via a single node. Requests that appear to come from several entities but are actually being made by a single malicious node are one way that the resources of a node might be depleted.

- Flood Attacks

At the beginning of communication, each node is required to introduce itself to the network by sending a "hello" message to the nodes that are immediately next to it. In addition to this, it verifies that the node that is providing the hello message is located nearby. An adversary can take advantage of this feature by establishing a powerful wireless connection. It is able to reassure all of the nodes in the network that he is their neighbor, which enables it to initiate contact with the nodes. Because the attacker will now have access to the information flow in the network, it should be evident that the security of the information will be jeopardized if they use this assault. A kind of this attack may also be carried out if the nodes utilize a puzzle technique in order to provide access to any node that is seeking a connection. [53] The adversary must have sufficient resources to manage this assault and must be able to offer a high-quality routing path to other nodes in the network in order to be considered a viable threat. This will result in data congestion and a disruption to the hierarchical structure of the network's data flow when traffic decides that this route is desirable enough to use to send packets via it.

- Attack on the Node's Replications

Within the WSN, sensor nodes are uniquely identified by their IDs (which also serve as indices of their locations for geographical routing algorithms). An opponent can create a new node to the sensor network by duplicating the ID of an already existing node and assigning it to the malicious node. This allows the attacker to get access to the network. This assures that the adversary is present in the network, giving the hostile entity the ability to cause harmful effects on the sensor network.

Packets that arrive at the duplicated node are susceptible to being manipulated, discarded, or redirected if the node is used. This causes the contents of the information packet to be erroneous, the connection to be lost, data to be lost, and excessive end-to-end latency to follow. When this attack is carried out, the adversary has the potential to get access to crucial information, such as the cryptographic key, the source code, or other security settings. This has implications for the security of the entire sensor network.

It is possible to carry out coordinated attacks using replicated nodes located in specified locations in order to exert control over certain nodes or areas of the network.

IV. COUNTERMEASURES TO BE TAKEN IN RESPONSE TO ATTACKS ON WSN

- Attacks of a Physical Nature

An adversary is able to get access to vital data held on a node by taking advantage of its physical weaknesses and is also capable of causing damage to or reproducing the nodes. The required degree of security will dictate the specific actions that must be taken in order to guarantee the physical safety of sensor nodes in WSN. When forming WSNs, hundreds or even thousands of nodes are frequently spread out over a significant distance, which makes it impossible to provide a comprehensive and complete assurance of safety for all of the nodes.

To ensure that the integrity of these motes' security is not undermined by cost considerations, it is possible to harden nodes operating in hostile settings. There are further defenses available against physical assaults, such as camouflaging and obscuring sensor nodes.

- Collisions

It is possible for information that has been modified and then sent across a network to make the latency of the network worse. This can result in the dropping and discarding of packets once the corrupted ones have been discovered, which in turn decreases the quality of service that is offered by the network. It is feasible to include collision detection and avoidance tactics to reduce the likelihood of finding oneself in a situation like this. CRC is an abbreviation for cyclic redundancy check, which may be conducted on a message at both the sender's end and the recipient's end to detect whether or not the message has been altered. Error correcting codes can be utilized in a manner analogous to that which was described above in order to prevent communications from being altered or corrupted by a third party. These kinds of codes, which are capable of excellent mistake correction, come at the cost of extra bits, which have to be added to the initial message in order for them to work correctly. Since hostile agents may be able to introduce more defects into the message than the correcting codes are able to remedy, the efficiency of these codes is limited as a result of this fact. If the communication nodes cooperate with one another, it is possible to protect the authenticity of the data that is included inside the packets that are transferred.[54]

- Neglect and greed are to attack

It is impossible to identify this form of assault because, during the attack, only some of the packets are lost, and the malicious node involved behaves in an unpredictable way. Therefore, it is impossible to detect this kind of attack. The most effective action that can be done to lessen the impact of harm that is brought on by the carelessness or avarice of a malicious sensor node is to define alternative routing methods. One further strategy that has been proposed involves the use of duplicate messages, which mitigate the damage that is brought about by rogue nodes.

- Alteration of Routing Information (also known as "spoofing")

In order to reroute the flow of data to its intended destinations, the routing information that is contained inside the packets is either tampered with or fabricated. This may be done in one of two ways. It is feasible for an adversary to conduct an attack against any particular node because the addresses of the nodes may be changed, and also because an attacker can influence the flow of traffic.

Utilizing CRC or MAC approaches enables the secure creation of packets, which in turn makes it easier to easily identify packets that have been tampered with. In a similar vein, link layer authentication is useful as a means of providing protection against this kind of attack. The participation in the information exchange is restricted to just those nodes that have been authorized to do so by the network administrator. In a similar vein, authentication and ant replay protection methods are strategies that may be applied to fight back against the impacts of interrogation attacks.

- De-synchronization

An adversary can induce retransmissions and, eventually, a loss of synchronization between communication nodes by forging the control fields and the transport layer header. A defense against this form of attack on motes is provided by authenticating the crucial components that are used in the transit of the packets. The receiving end is able to identify any bogus communications and is in a position to disregard any instructions included within them.

- Sybil Attack

It is hard to prevent an insider node from carrying out this assault; nevertheless, it is feasible to restrict the activities that it participates in. In order to prevent an insider from connecting within the network and generating shared keys with every node in the network, the base station places limits on the number of neighbors with which a sensor may create a connection and restricts the number of neighbors with which a sensor can establish a connection. In the case that any node makes an effort to go over this limit, an error will be produced as a result of this attempt. When adopting this strategy, a compromised node is prevented from interacting with more than a certain number of other nodes, the majority of which are located in the immediate vicinity of the compromised node. In addition, the identities of the nodes in the network that make requests to build connections are reviewed and validated before the requests are processed. Every node in the network uses the key that is uniquely theirs while communicating with the base station. In order to verify the sincerity of the information being transmitted from one nearby node to another, a shared key is utilized during the information exchange process. Because the compromised node can only communicate with its close neighbors, the amount of damage that can be caused by this assault is restricted to a more manageable level.[55]

- Forwarding with Selectivity

Using multipath routing is the step that must be taken in order to eliminate or avoid this assault, just as it is with the route alteration attack. This safeguard guarantees that the message destined for the destination will, in the end, be delivered to it, although along a path that is distinct from the one followed by the malicious node. [56]The WSN is able to monitor the network on a regular basis, which enables it to follow suspicious behavior by any node. Source routing that makes advantage of the geographical monitoring of the network is another potential preventative technique that may be utilized in response to this kind of assault. Since further attacks on WSN are just versions of the attacks that have been disclosed, it is possible to avoid and counteract them in the same way as the previous attacks.

CONCLUSION

This article may be used as a text for researchers, particularly those who are just starting out in the field, and it will provide them with an overview of the rapidly expanding study field of wireless sensor networks. This chapter offers a concise but comprehensive introduction to the fascinating world of sensors. This chapter covers a wide range of interesting issues, and readers interested in delving further into this research field will discover many more such themes. This chapter has been broken up into a variety of sections, each of which discusses a distinct facet of WSN. The fundamental aspects of WSN are dissected in order to provide the reader with an overview of the network. This, in turn, aids the reader in comprehending the threats posed by WSN and the defenses against them. Following are some of the more significant assaults that have been launched on WSN, along with the preventative and defensive measures that have been taken. The problems that are faced by the area of WSN are one of a kind, as are the security architectures that are used. In the future, we will need to be prepared to acknowledge many more novel designs of WSN, as well as more complex assaults and ways to defend against them.

REFERENCES

[1] V. S. Kumar, M. Sakthivel, D. A. Karras, S. Kant Gupta, S. M. Parambil Gangadharan and B. Haralayya, "Drone Surveillance in Flood Affected Areas using Firefly Algorithm," 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), Chickballapur, India, 2022, pp. 1-5, doi: 10.1109/ICKECS56523.2022.10060857.

[2] Parin Somani, Sunil Kumar Vohra, Subrata Chowdhury, Shashi Kant Gupta. "Implementation of a Blockchain-based Smart Shopping System for Automated Bill Generation Using Smart Carts with Cryptographic Algorithms." CRC Press, 2022. https://doi.org/10.1201/9781003269281-11.

[3] Wagner D. Resilient aggregation in sensor networks. In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks. ACM Press; 2004. p. 78–87. Crossref

[4] Zheng J, Jamalipour A. Wireless Sensor Networks: A Networking Perspective. John Wiley & Sons Publisher; Hoboken, NJ; 2009.

[5] Hu C. International Journal of Future Generation Communication and Networking. 2016;

[6] Arunmozhi S, Venkataramani Y. International Journal of Computer Applications. 2011; Nunoo MH, Boateng K, Gadze J. International Journal of Network Security and its Applications. 2015; 109(11).

[7] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. IEEE Communications Magazine, 40(8):102–114, August 2002.

[8] Mona Sharifnejad, Mohsen Shari, Mansoureh Ghiasabadi and Sareh Beheshti, A Survey on Wireless Sensor Networks Security, SETIT 2007.

[9] Hemanta Kumar Kalita and Avijit Kar, Wireless Sensor Network Security Analysis, International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1, December 2009.

[10] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary. Wireless SensorNetwork Security: A Survey. Security in Distributed, Grid, and Pervasive Computing. YangXiao,(Eds.) 2006.

[11] T. Aura, P. Nikander, and J. Leiwo. Dos-resistant authentication with client puzzles. In Revised Papers from the 8th International Workshop on Security Protocols, pages 170–177.Springer-Verlag, 2001.

[12] R. Anderson and M. Kuhn. Low cost attacks on tamper resistant devices. In IWSP: International Workshop on Security Protocols, LNCS, 1997.

[13] D. Boyle and T. Newe,"Securing Wireless Sensor Networks: Security Architectures", Journalof Networks, 2008.

[14] X. Du and H. Chen. Security in Wireless Sensor Networks. IEEE Wireless Communications,2008.

[15] J. Granjal, R. Silva and J. Silva, Security in Wireless Sensor Networks. CISUC UC, 2008.

[16] Z. Liang and W. Shi. PET: A PErsonalized Trust model with reputation and risk evaluation forP2P resource sharing. In Proceedings of the HICSS-38, Hilton Waikoloa Village Big Island, Hawaii, January 2005.

[17] P. Albers and O. Camp. Security in ad hoc networks: A general intrusion detection architecture enhancing trust based approaches. In First International Workshop on Wireless Information Systems, 4th International Conference on Enterprise Information Systems, 2002.

[18] R. Anderson and M. Kuhn. Tamper resistance - a cautionary note. In The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, 1996.

[19] D. Braginsky and D. Estrin. Rumor routing algorthim for sensor networks. In WSNA '02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, pages 22–31, New York, NY, USA, 2002.

[20] Navaneetha Krishnan Rajagopal, Mankeshva Saini, Rosario Huerta-Soto, Rosa Vílchez-Vásquez, J. N. V. R. Swarup Kumar, Shashi Kant Gupta, Sasikumar Perumal, "Human Resource Demand Prediction and Configuration Model Based on Grey Wolf Optimization and Recurrent Neural Network", Computational Intelligence and Neuroscience, vol. 2022, Article ID 5613407, 11 pages, 2022. https://doi.org/10.1155/2022/5613407

[21] Navaneetha Krishnan Rajagopal, Naila Iqbal Qureshi, S. Durga, Edwin Hernan Ramirez Asis, Rosario Mercedes Huerta Soto, Shashi Kant Gupta, S. Deepak, "Future of Business Culture: An Artificial Intelligence-Driven Digital Framework for Organization Decision-Making Process", Complexity, vol. 2022, Article ID 7796507, 14 pages, 2022. https://doi.org/10.1155/2022/7796507

[22] Eshrag Refaee, Shabana Parveen, Khan Mohamed Jarina Begum, Fatima Parveen, M. Chithik Raja, Shashi Kant Gupta, Santhosh Krishnan, "Secure and Scalable Healthcare Data Transmission in IoT Based on Optimized Routing Protocols for Mobile Computing Applications", Wireless Communications and Mobile Computing, vol. 2022, Article ID 5665408, 12 pages, 2022. https://doi.org/10.1155/2022/5665408

[23] Rajesh Kumar Kaushal, Rajat Bhardwaj, Naveen Kumar, Abeer A. Aljohani, Shashi Kant Gupta, Prabhdeep Singh, Nitin Purohit, "Using Mobile Computing to Provide a Smart and Secure Internet of Things (IoT) Framework for Medical Applications", Wireless Communications and Mobile Computing, vol. 2022, Article ID 8741357, 13

pages, 2022. https://doi.org/10.1155/2022/8741357

[24] Bramah Hazela et al 2022 ECS Trans. 107 2651 https://doi.org/10.1149/10701.2651ecst

[25] Ashish Kumar Pandey et al 2022 ECS Trans. 107 2681 https://doi.org/10.1149/10701.2681ecst

[26] G. S. Jayesh et al 2022 ECS Trans. 107 2715 https://doi.org/10.1149/10701.2715ecst

[27] Shashi Kant Gupta et al 2022 ECS Trans. 107 2927 https://doi.org/10.1149/10701.2927ecst

[28] S. Saxena, D. Yagyasen, C. N. Saranya, R. S. K. Boddu, A. K. Sharma and S. K. Gupta, "Hybrid Cloud Computing for Data Security System," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), 2021, pp. 1-8, doi: 10.1109/ICAECA52838.2021.9675493.

[29] S. K. Gupta, B. Pattnaik, V. Agrawal, R. S. K. Boddu, A. Srivastava and B. Hazela, "Malware Detection Using Genetic Cascaded Support Vector Machine Classifier in Internet of Things," 2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA), 2022, pp. 1-6, doi: 10.1109/ICCSEA54677.2022.9936404.

[30] Natarajan, R.; Lokesh, G.H.; Flammini, F.; Premkumar, A.; Venkatesan, V.K.; Gupta, S.K. A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0. *Infrastructures*2023, *8*, 22. https://doi.org/10.3390/infrastructures8020022

[31] V. S. Kumar, A. Alemran, D. A. Karras, S. Kant Gupta, C. Kumar Dixit and B. Haralayya, "Natural Language Processing using Graph Neural Network for Text Classification," 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), Chickballapur, India, 2022, pp. 1-5, doi: 10.1109/ICKECS56523.2022.10060655.

[32] M. Sakthivel, S. Kant Gupta, D. A. Karras, A. Khang, C. Kumar Dixit and B. Haralayya, "Solving Vehicle Routing Problem for Intelligent Systems using Delaunay Triangulation," 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), Chickballapur, India, 2022, pp. 1-5, doi: 10.1109/ICKECS56523.2022.10060807.

[33] S. Tahilyani, S. Saxena, D. A. Karras, S. Kant Gupta, C. Kumar Dixit and B. Haralayya, "Deployment of Autonomous Vehicles in Agricultural and using Voronoi Partitioning," 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), Chickballapur, India, 2022, pp. 1-5, doi: 10.1109/ICKECS56523.2022.10060773.

[34] V. S. Kumar, A. Alemran, S. K. Gupta, B. Hazela, C. K. Dixit and B. Haralayya, "Extraction of SIFT Features for Identifying Disaster Hit areas using Machine Learning Techniques," 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), Chickballapur, India, 2022, pp. 1-5, doi: 10.1109/ICKECS56523.2022.10060037.

[35] Shivlal Mewada, Dhruva Sreenivasa Chakravarthi, S. J. Sultanuddin, Shashi Kant Gupta. "Design and Implementation of a Smart Healthcare System Using Blockchain Technology with A Dragonfly Optimization-based Blowfish Encryption Algorithm." CRC Press, 2022. https://doi.org/10.1201/9781003269281-10.

[36] Ahmed Muayad Younus, Mohanad S.S. Abumandil, Veer P. Gangwar, Shashi Kant Gupta. " AI-Based Smart Education System for a Smart City Using an Improved Self-Adaptive Leap-Frogging Algorithm." CRC Press, 2022. https://doi.org/10.1201/9781003252542-14.

[37] Rosak-Szyrocka, J., Żywiołek, J., & Shahbaz, M. (Eds.). (2023). Quality Management, Value Creation and the Digital Economy (1st ed.). Routledge. https://doi.org/10.4324/9781003404682

[38] Dr. Shashi Kant Gupta, Hayath T M., Lack of it Infrastructure for ICT Based Education as an Emerging Issue in Online Education, TTAICTE. 2022 July; 1(3): 19-24. Published online 2022 July, doi.org/10.36647/TTAICTE/01.03.A004

[39] Hayath T M., Dr. Shashi Kant Gupta, Pedagogical Principles in Learning and Its Impact on Enhancing Motivation of Students, TTAICTE. 2022 October; 1(2): 19-24. Published online 2022 July, doi.org/10.36647/TTAICTE/01.04.A004

[40] Shaily Malik, Dr. Shashi Kant Gupta, "The Importance of Text Mining for Services Management", TTIDMKD. 2022 November; 2(4): 28-33. Published online 2022 November doi.org/10.36647/TTIDMKD/02.04.A006

[41] Dr. Shashi Kant Gupta, Shaily Malik, "Application of Predictive Analytics in Agriculture", TTIDMKD. 2022 November; 2(4): 1-5. Published online 2022 November doi.org/10.36647/TTIDMKD/02.04.A001

[42] Dr. Shashi Kant Gupta, Budi Artono, "Bioengineering in the Development of Artificial Hips, Knees, and other joints. Ultrasound, MRI, and other Medical Imaging Techniques", TTIRAS. 2022 June; 2(2): 10–15. Published online 2022 June doi.org/10.36647/TTIRAS/02.02.A002

[43] Dr. Shashi Kant Gupta, Dr. A. S. A. Ferdous Alam, "Concept of E Business Standardization and its Overall Process" TJAEE 2022 August; 1(3): 1–8. Published online 2022 August

[44] A. Kishore Kumar, A. Alemran, D. A. Karras, S. Kant Gupta, C. Kumar Dixit and B. Haralayya, "An Enhanced Genetic Algorithm for Solving Trajectory Planning of Autonomous Robots," 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2023, pp. 1-6, doi: 10.1109/ICICACS57338.2023.10099994

[45] S. K. Gupta, V. S. Kumar, A. Khang, B. Hazela, N. T and B. Haralayya, "Detection of Lung Tumor using an efficient Quadratic Discriminant Analysis Model," 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC), Mysore, India, 2023, pp. 1-6, doi: 10.1109/ICRTEC56977.2023.10111903.

[46] S. K. Gupta, A. Alemran, P. Singh, A. Khang, C. K. Dixit and B. Haralayya, "Image Segmentation on Gabor Filtered images using Projective Transformation," 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC), Mysore, India, 2023, pp. 1-6, doi: 10.1109/ICRTEC56977.2023.10111885.

[47] S. K. Gupta, S. Saxena, A. Khang, B. Hazela, C. K. Dixit and B. Haralayya, "Detection of Number Plate in Vehicles using Deep Learning based Image Labeler Model," 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC), Mysore, India, 2023, pp. 1-6, doi: 10.1109/ICRTEC56977.2023.10111862.

[48] S. K. Gupta, W. Ahmad, D. A. Karras, A. Khang, C. K. Dixit and B. Haralayya, "Solving Roulette Wheel Selection Method using Swarm Intelligence for Trajectory Planning of Intelligent Systems," 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC), Mysore, India, 2023, pp. 1-5, doi: 10.1109/ICRTEC56977.2023.10111861.

[49] Shashi Kant Gupta, Olena Hrybiuk, NL Sowjanya Cherukupalli, Arvind Kumar Shukla (2023). Big Data Analytics Tools, Challenges and Its Applications (1st Ed.), CRC Press. ISBN 9781032451114

[50] Shobhna Jeet, Shashi Kant Gupta, Olena Hrybiuk, Nupur Soni (2023). Detection of Cyber Attacks in IoT-based Smart Cities using Integrated Chain Based Multi-Class Support Vector Machine (1st Ed.), CRC Press. ISBN 9781032451114

[51] Parin Somani, Shashi Kant Gupta, Chandra Kumar Dixit, Anchal Pathak (2023). AI-based Competency Model and Design in the Workforce Development System (1st Ed.), CRC Press. https://doi.org/10.1201/9781003357070

[52] Shashi Kant Gupta, Alex Khang, Parin Somani, Chandra Kumar Dixit, Anchal Pathak (2023). Data Mining Processes and Decision-Making Models in Personnel Management System (1st Ed.), CRC Press. https://doi.org/10.1201/9781003357070

[53] Alex Khang, Shashi Kant Gupta, Chandra Kumar Dixit, Parin Somani (2023). Data-driven Application of Human Capital Management Databases, Big Data, and Data Mining (1st Ed.), CRC Press. https://doi.org/10.1201/9781003357070

[54] Chandra Kumar Dixit, Parin Somani, Shashi Kant Gupta, Anchal Pathak (2023). Data-centric Predictive Modelling of Turnover Rate and New Hire in Workforce Management System (1st Ed.), CRC Press. https://doi.org/10.1201/9781003357070

[55] Anchal Pathak, Chandra Kumar Dixit, Parin Somani, Shashi Kant Gupta (2023). Prediction of Employee's Performance Using Machine

Learning (ML) Techniques (1st Ed.), CRC Press. https://doi.org/10.1201/9781003357070

[56] Worakamol Wisetsri, Varinder Kumar, Shashi Kant Gupta, "Managerial Autonomy and Relationship Influence on Service Quality and Human Resource Performance", Turkish Journal of Physiotherapy and Rehabilitation, Vol. 32, pp2, 2021.