Cybersecurity Attacks On Wireless Sensor Networks In Smart Cities: An Exposition

Hind Alshambri, Mohammed A. AlZain, Ben Soh, Mehedi Masud, Jehad Al-Amri

Abstract: The smart city concept is a link between digital world and the physical world. The smart city is designed and constructed by using advanced techniques which consist of sensors, electronics and networks. However, automatic information flow and connection between IoT devices creates new security risks. If data can be accessed remotely, it means that a cybercriminal could also access it. Moreover, connectivity is the essence of IoT. If multiple devices are connected to the same network, it means that cybercriminals have multiple access points. Understanding how wireless sensor technology works is crucial before deploying IoT applications. In this article, we explore the understanding through: (1) vulnerabilities on wireless sensors and techniques to avoid them, (2) emerging wireless standards for sensors, and (3) what role these standards will play in the future.

Keywords : Cybersecurity, wireless sensor, smart city.

1. INTRODUCTION

Today, the Internet of Things (IoT) represents a major part of our daily life. Billions of intelligent and autonomous objects around the world are connected and communicate with each other. According to statista.com [1], more than 50 billion objects will be connected in 2020. The International Telecommunication Union (ITU) defines IoT as: "A global infrastructure for the information society, enabling the provision of advanced services by interconnecting physical and virtual objects. it is based on existing, advanced and interoperable information and communication technologies" [2]. This revolutionary paradigm creates a new dimension that removes the boundaries between the real world and the virtual world. Its success is due to the evolution of hardware equipment and communication technologies including wireless. IoT is the result of the development and combination of different technologies. It encompasses almost all areas of current information technology (IT) such as smart cities, machine (Machine to Machine), connected vehicles, wireless sensor networks (Wireless Sensor Networks (WSN)), etc. And it also exploits other advanced technologies, such as cloud computing, big data, or blockchains. The great power of IoT lies in the fact that its objects communicate, analyze, process and manage data in an autonomous way and without any human intervention. However, security issues are the rise due to rapid deployment of this high technology. Identity theft, theft of information and the modification of the data represent a real danger for IoT systems.

The flaws in the lock authentication mechanisms of connected doors, computers or phones are causing several cyber attacks. In 2016, a certain Anna Senpai created a malicious program, called Mirai [3], which takes control of vulnerable connected objects such as surveillance cameras and routers, and generate distributed denial of service attacks (DDos) in a massive manner. Mirai transforms infected objects into bots, that is, it transforms them into autonomous and intelligent IT agents controlled remotely. In 2017, another malware named BrickerBot appeared. The bot forcibly attacks objects using the classic pass of word identification systems [4] to kill them and thus delete their data. Widespread use of IoT can only be achieved when there is good security for objects and communication networks. It is essential to put in place a policy of security that prevents any malicious or unauthorized object from accessing IoT systems, to read their data or modify it. For an object to have the opportunity to exploit a service or to associate with a network, it must first prove its identity and have the rights for necessary access. Connected objects in IoT are generally very limited in their ability to perform calculation and storage. They are also constrained by energy consumption. For this reason, we can not use traditional security mechanisms, such as authentication with digital certificates or the use of asymmetrical cryptographic algorithms like Rivest Shamir Adleman (RSA) or Diffie-Hellman [5] as they are energy-intensive and not even supported by objects. As a result, a new, lightweight and robust mechanism is needed to provide object authentication and data protection services.

2. BACKGROUND

2.1 What is a Wireless Sensor Network?

Wireless Sensor Networks (WSN) are networks consisting of small devices, sensors, base station. The sensors exchange information by wireless communications, using protocols such as those defined in the IEEE 802.11 stack. Packet routing in the network can use one of the many protocols developed for this purpose (eg example: AODV, OLSR), based on a centralized algorithm (directed by a single entity) or distributed (executed by each entity of the network). The sensors collect information about their environment and bring them back to the base station. This base station, or BS (for Base Station), or sometimes well (sink in English), is responsible for collecting and processing the data from the sensors. Once the sensors are deployed, the administrator no longer interacts with the network except through the station basic. It is rare that

- *College of Computers and Information Technology, Taif University, Saudi Arabia*
- **La Trobe University, Bundoora 3086, Australia*.

all WSN sensors are directly connected to each other. The topology of a given network is therefore very often associated with the graph network connectivity. For this reason, sensors are often referred to under the term of nodes.

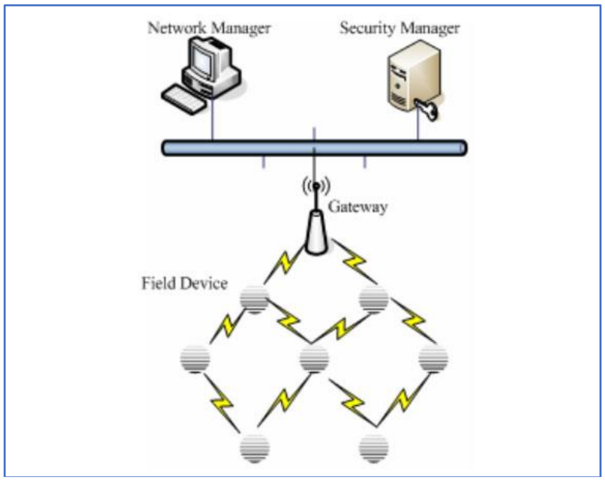

Figure 1: *Basic Architecture of Wireless Sensor Network [21]*

2.2 Applications of WSN in smart cities

In smart cities, the scope of the WSN is very wide, and continues to grow over the course of time and technological advances. Not all are the subject of scientific publications, but some are regularly referred to as examples, or news in the field of new technologies or the commercial field:

Environmental applications

Management of the environment needs more and more recourses for distributed measurements based on the use of sensors. The weather forecasts (based on measurements of hygrometry, pressure of air, et cetera) were one of the first fields of application of the sensors. Measurements of air quality and pollution rates, both in cities and in the countryside, are gradually becoming more widespread. Sensor networks even make it possible to push the measurement to new environments, such as glaciers [6] or the oceans. Agriculture is also likely to use sensors: tests are conducted on the realization of measurements made by microsensors sown at the same time as cultures, to better monitor their development conditions. Judiciously placed in the natural habitat of some species, sensors can be used to track and analyze the behavior of the fauna of an environment [7][22].

Monitoring and detection

Wireless sensor networks are also used to check on safety or security, for example to monitor the structural integrity of certain architectures (railway, aerospace, maritime, or more simply in the building: structural work, structures) and this can allow effective prevention of material failures [8].

Intelligent transport system applications

WSN are used to support intelligent transport system and there are three major areas: roadside unit, and vehicular sensor network.

3. ATTACKS ON WIRELESS SENSOR NETWORKS

3.1 Different types of attacks

Using the TCP/IP layered model (Physical, Data Link, Network, Transport and Application), we explore the cybersecurity attacks on WSN.

Physical layer

The physical layer of the network corresponds to the physical medium used for the data transmission between two nodes, and how the signal is transmitted through this medium. In the case of wireless networks, the signal is propagated under form of electromagnetic waves that move in a vacuum (or, without being affected, through the atmosphere). Unless a directional antenna is used for the broadcast, these waves are sent in all directions, and any device in range equipped with a receiver is therefore able to receive the packets issued. The frequency interference is for the attacker to emit a spurious signal, an electromagnetic "noise" on the frequencies concerned, so that the intended target cannot receive correctly the packets sent to it by the legal nodes [9]. Interference can be achieved using a directional antenna to target a particular node; but in the case of a network of sensors, the attacker generally tries to make a noise in all directions in order to affect the most large number of nodes possible. The attack can be sporadic to produce a partial or full denial of service. If the machine emitting the unwanted signal has enough range to cover the entire geographical extent of the network, all the sensors can find it impossible to use scrambled frequencies. If, moreover, the interference is conducted over the entire frequency range accessible to the sensors, communications become totally impossible to be established in the network. It should be noted that conducting such an attack can be costly in equipment especially if it targets several frequencies and/or a continuous interference in time. Typically, a corrupted sensor will not be able to conduct this attack without exhausting its battery very quickly [23].

Data link layer

The data link layer provides the functional and procedural means for the transfer of data between two entities of the network. It also often detects and possibly corrects some errors on the physical layer (in case of disturbance or degradation of the electromagnetic tick) [10]. Of the two sublayers LLC and MAC, it is mainly the second one in which we are interested here: the protocol used at this level defines how the different agents in the network access the transmission medium in order to limit collisions, and to guarantee an access more often and fair to the medium for all the nodes. These rules can be bypassed, so the MAC layer will end up associated with several types of attacks. Creation of "intelligent" collisions and jamming is another possible cyber security attack on WSN. When several nodes on overlapping staves emit simultaneously using the same frequency (on the same channel), there are collisions. Most of the MAC protocols employed with the sensor networks introduce into the frames a field containing a checksum, which checks the integrity of the frame. But this checksum does not, most of the time, make it possible to correct errors because none of the IEEE 802.11 (Wi-Fi), IEEE 802.15.1 (Bluetooth) or IEEE 802.15.4 (ZigBee, 6LoWPAN) includes error correction code). If one bit of the frame is altered, it is rejected by the recipient. An attacker can therefore seek to produce collisions by emitting a signal at the same time as a legitimate node does, so that the recipient cannot properly receive the weft for it. This collision principle is identical to the jamming conducted on the physical layer; but when the attacker knows about the MAC layer protocol used, it is possible for them to refine their attack, and to replace a jamming "Raw", continuously and expensive though, with an "intelligent" interference.

Network layer

The IP protocol is the most used on the network layer in the control network operators to ensure the addressing of the packets essential for the establishment of a routing algorithm that determines how these are retransmitted from one node to another node in the network. In the case of a clustered network, it happens that all sensors are within range of their cluster head, and that the latter can directly reach the base station. The routing is then very simple. But in other cases, it is necessary to establish a structure for the network allowing the routing of packets to their recipient. An efficient routing protocol must minimize the packet losses as well as retransmission costs and avoid creating loops in the network. Conversely, an attacker can try to lead a denial attack of service by hindering as much as possible the routing of these packets.

Black Hole

In a "black hole" attack, a compromised node performs no retransmission of packets which are sent to it. The node acknowledges the packet from the transmitter, but never forwards the packet for the next hop planned for that packet by the routing protocol. All paths that pass through this compromised node therefore experience removal of their packets during transit [25].

Falsification of routing information

This involves grabbing of the transmission channel and creation of loops. An attack can be conducted as soon as the deployment of the network by transmitting false information when setting up the rules of routing [11]. This information will then seek to hinder the routing of packets, creating cyclic loops in the routing structure, by partitioning the network and by misleading traffic to a corrupt node (for example to exploit data and an attack on confidentiality) or to a legitimate node (for overloading its processing capabilities). Such attacks can also be carried out when a clustering protocol is implemented with the aim of hindering the structural organization of the cluster (since setting up clusters most often defines how packets will be routed in the network). Several other attacks presented below are based on the falsification of routing information. Well (sinkhole) is the combination of "black hole" attack type with the dissemination of false routing information, with a view to attracting as many packets as possible to the attacking node [12]. Concretely, a corrupt node can declare itself a direct neighbor of the base station and announce a zero-cost route to the latter. Its neighbors will estimate that this is the shortest way to get the packets to the base station and are going to put the information in turn. In the end, an important part of the routing paths is created, and consequently the routed traffic will go through this compromised node, which can lead to congestion in the network. Then go into play is the black hole attack, which removes all received packets rather than retransmitting them to their legitimate recipient. An additional consequence of this attack is the depletion of the battery of the neighboring nodes of the attacker - as this node declares itself very close to the base station, a lot of routes will redirect the packets towards it, and its neighbors are going to therefore find themselves heavily solicited by more distant nodes to transmit packages to it [24].

Wormhole

When two or more agents of the network are compromised by an attacker, it is possible for them to conduct a "wormhole" type attack. This attack is to capture traffic at a point giving the network to re-inject it to another point. It takes at least two accomplices, one who captures and the other who injects the traffic, and who communicate with each other through an auxiliary channel generally distinct from the legitimate channels on the network - a tunnel or "wormhole" gives its name to the attack [13]. It is interesting for the nodes leading the attack to retransmit, for example routing information, from a neighborhood of the base station at a point away from the network. In this manner, the tunnel is a good path to the base station for carrying out attacks using selective retransmission. Or more simply, the injection at another point of the used path for the discovery of other paths without the knowledge of the neighbors during the establishment of the routing table can be very detrimental to the organization of the network.

Transport layer

Transport layer protocols are not always implemented in wireless sensor buckets, but when present, attacks can take advantage of their specifications.

Deluge of SYN packets

Existing denial of service attacks on conventional networks at the transport layer level can also be applied in sensor networks: for example, if the TCP protocol is used in the network, an attacker can flood the network with SYN packets used to initiate connections between two nodes. Although this attack requires a more powerful device (especially with better power supply) than a sensor, it allows both to create congestions in the network, and to saturate the capabilities of the sensors by opening too many TCP sessions.

TCP desynchronization

In the same registry, an attacker can forge desynchronization requests to terminate established TCP sessions between two legitimate entities. The exchanges of these sessions are therefore interrupted to then re-establish a new connection: this connection involves the sending of control data that consume a precious amount of energy for the sensors. More generally, if a transport protocol is used, TCP by example, then denial of service attacks based on this protocol [14] are applicable in the network.

Application layer

The application layer optionally implements an application used at the highest through the sensor network to provide a service. The protocols used at this layer are totally dependent on the final objective of the network - there is no standard here strictly speaking. Some attacks are nevertheless applicable at the application level.

Wrong data

A compromised node has the ability to send data in perfect contradiction to the measured physical values in WNS (or even, it can betake measurements and save energy). The values transmitted to the application will then distort the results obtained by the operator of the bucket [15].

Deluge of packages

Depending on the application set up, it may be possible for an attacker to flood the network with useful data (maybe actually measured or otherwise) in an attempt to either distort the results obtained by the base station by averaging the values reported by all of the sensors, or create congestions in the network [16].

3.2 The communication attacks

Neutralize communications

An easy way to lead a denial of service attack against a network is to blur its signal, at the physical level. The installation can be expensive in equipment, but it is very easy to put in place. From outside the network, it requires no knowledge of the internal functioning of it. The attacker needs to know only the beach frequencies to be neutralized, and to calculate the necessary transmission power. For these reasons, it is therefore one of the most widely used methods in the field of military. "Intelligent" scrambling attacks at the data link layer need to listen to the frames sent in the network and to know which moment to trigger collisions. These attacks can be carried out on the network protocols in a simple and widespread manner, but it would be long to adapt them to less "standard" protocols. They can also be conducted since outside the network, which avoids having to compromise an agent. This advantage is important, because diverting a sensor from its original purpose can be very costly in time. Also, because of its simplicity the jamming (an external attack) seems preferable to a good number of more complex attacks that need set up and require access in the network. It therefore seems more cost-effective than an attack on or higher layer (such as by desynchronization or creation of congestion) in order to render the network out of service.

Destroy the network

The two main ways to destroy the network are the physical traction of the sensors, and the attacks aimed at the exhaustion of the batteries. The physical destruction requires knowing the location of the sensors. If these sensors are relatively few and easy to access, it is possible to search by triangulation of the signal and proceed directly to their decommissioning. If they are numerous, or if it is difficult to reach them (in a natural area – but militarily hostile, for example), this operation can be very long, even impossible to lead. A battery-powered depletion attack on a handful of compromised nodes can be more cost effective than to go physically destroy the nodes, or even to scramble the signal on a very long period. On the other hand, it is necessary to acquire enough knowledge thoroughly detailed on the internal functioning of the network to effectively lead the attack.

Redirect data

Exfiltration of data collected off the network can be conducted in a variety of ways, although it is not clear whether it will penalize the good functioning of the network. On the other hand, parasite collection itself can go through attacks on the routing protocol to divert the most useful data to the corrupted node. Broadcast of false paths – a result of typical attacks - are particularly suitable for the fraudulent collection of packets.

Ranking of attacks by paradigm

Paradigm	Possible attacks
Collection and simple transmission	Jamming, collision creation, destruction of sensors, alteration of measurements, alteration of data (application)
Routing of data in the network	Selective retransmission, black holes, resource depletion (battery, network congestion), data corruption (during the retransmission), grabbing of the transmission, transport layer attacks
Reception and treatment of orders	Previous attacks, identity theft (and Sybil attack) used to issue fake orders
Autonomous organization of the network	Previous attacks, false routing information (loops ...), wells, wormholes, deluge of "hello" packets
Aggregation of data	Previous attacks, especially those based on replay Emitted or captured packets
Model Optimization	Previous Attacks

Table1: *showing the order of attacks by model*

4. MITIGATION STRATEGIES

4.1 Prevention approach

Authentication and similar issues

Security is transversal to all fields of study in computer science and protection against denial of service, which is itself related to other safety problems. This means that if there are failures in the compromising system, agent authentication or data integrity can also be exploited in one way or another to impede the proper functioning of the network, including denial of service. More concretely, ensuring the correct authentication of the nodes of the network will prevent an attacker from conducting attacks based on the theft of the identity of another node. With the correct authentication, attacks by desynchronization or the falsification of routing information become inapplicable. If mechanisms that allow to limit the replay of captured packets are added, the scale of attacks, such as Sybil as well as wormhole attacks will be greatly reduced. The protection of data integrity ensures the failure of any attempt to tamper with values passed during routing operations.

Specific routing protocols

Always with the aim of preventing attacks, it is possible to use routing protocols specifically designed for WNS to limit risks. Thus, the protocol, On-demand Distance Vector Routing (AODV), widely used in networks of sensors, has been the subject of proposals aimed at improving its resistance against black hole and sinkhole denial-of-service attacks. In [17], a routing protocol is proposed to have each node checked that its neighbors' neighbors (second degree courses) are well and truly accessible when creating the routes. So for each node x having a neighbor n proposing a route to a given destination, x asks n what the next hop n +1 node is on this route and tries to contact that node n +1 to verify that it is actually accessible. If n + 1 answers, then n is worthy of trust for this route; since n is trustworthy, it will its turn to check the accessibility of the node n + 2 through the jump announced by n + 1, and so on all along the route taken for the data. Other methods based on mechanisms of redundancy and resilience are also used to ensure that if any of the paths proves defective, other copies of packets sent by path scan can proceed to their destination. Mechanisms such as sharing secret can be used for this redundancy mechanism to limit the increase of the volume of data sent [18].

Preventing the compromise of the sensors

It is ultimately very difficult to hide the geographical location of a sensor to a determined attacker. Mechanisms clustering and false sources for messages can be used in order to complicate sensor access and the task to the attacker [19]. The use of directional antenna scan can also make localizing nodes more complex, but this method is not suitable to all uses of sensor networks. In the end, an attacker correctly equipped can always find a sensor by triangulating the electromagnetic signal. Under this circumstance, the next best move is to hide from the attacker the critical nodes using decoy. An example of this is the game of "hunters of panda": sensors scattered in the natural habitat of a panda follow the animal's movements, which are reported to the base station. But poachers search for the animal and attempt to use the network data for localization. If it is impossible to hide the signal from the sensors and prevent attackers to gain direct access to the machines, it is however possible to devise mechanisms to prevent hunters from knowing which sensor referring at a given moment to information about the presence of the panda. A mechanism for disseminating information, based on the epidemic model, has been proposed in this example [20]. If we focus only on denial of service, it is quite possible to imagine the use of similar techniques to conceal from the attacker the critical nodes that could be compromised to inflict a maximum damage to the functioning of the network.

4.2 Fault-tolerance approach: intrusion detection systems

Different intrusion detection systems

The detection of denial of service attacks involves setting up a specific system, capable of collecting clues to determine whether an attack has taken place and, if possible, what is its origin. Here, we are talking about "intrusion detection system", or IDS for Intrusion Detection System. To be precise, it should be noted that these systems are used for detecting all types of attacks not limited to that of denial of service. Uses and specifications of IDS are therefore multiple: the figure above summarizes the different existing categories, which we will briefly describe - there are different ways to distinguish them:

Depending on the origin of the attack

An intrusion detection system may be focused on the attacks coming from outside the network, led by an attacker who would seek to scramble the frequencies used or, indeed, to penetrate the network. Conversely, other systems will monitor the internal activity of the network, in order to detect potential corrupt nodes, or that they seek to monopolize resources on their own account, or that they seek to destroy **network resources.**

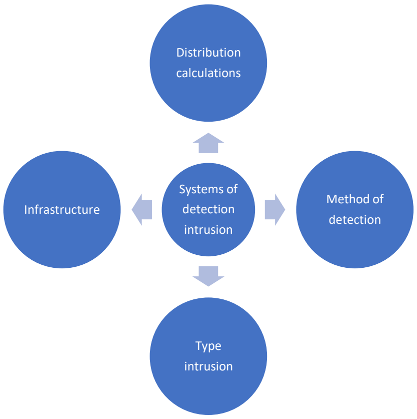

Figure 2: *Different Intrusion Detection System*

Depending on the purpose of the monitoring

An IDS may have the task of monitoring the activity of the network, by analyzing the traffic: the number of transmitted packets, their origin or their destination, their content, the success rate of transmissions. This traffic information gives as many clues as to determine if the network is operating under normal conditions. In parallel, other systems can be oriented towards host security on which they are executed. Their purpose is to detect possible attempts to compromise mission of the machine. Operations carried out for this purpose may include:

- the verification of the integrity of the system, for example, by calculating the condensate (checksum) of critical executable files, in order to compare them with the condensate of their original version;
- monitoring logs for connection attempts, in order to detect repetitive system access failures;
- detection of unusual activity at the CPU activity level, memory allowances, or inflows, which could penalize the operating system in terms of performance and energy consumption

Depending on the type of intrusion to detect

IDSs are used to fight against all types of "intrusions" (or attacks in the more general sense), not just against denial of service although this is the point that concerns us the most in this work. There are various types of IDSs to detect:

- attempts to access the network by an external attacker (who seeks for example by compromising a node or by obtaining cryptographic material); this step used by the attacker is often just a prelude to other attacks (including denial of service);
- access to unauthorized resources, for example when a sensor tries to perform certain operations in a cluster that are not authorized;
- data leaks, which can be difficult to detect if the attack is passive (e.g. simple listening to data circulating on the network), but can otherwise be identified when retrieving these data out of the network;
- greedy sensors' behavior causing the blocking of resources;
- other denial of service attacks with destructive behavior using Tors to affect the operation of the network by the annihilation of the resources - be they virtual

(decommissioning of transmissions) or physical (exhaustion of the battery of the sensors).

5. CONCLUSION

The Internet of Things (IoT) has upset the world of information technology. This new phenomenon becomes inevitable and already affects almost all areas, from watchmaking to automated factories. IoT simplifies our daily lives and creates value for individuals and companies. Objects, also called entities, are very heterogeneous, use different communication technologies and are usually devices with capacity limited. Therefore, securing such systems raises many challenges. The entities in communication must authenticate mutually and protect the integrity and confidentiality of the data they exchange, while using lightweight, fast algorithms and energy efficient. In this manuscript we have listed the different attacks and how to prevent from them.

[1] REFERENCES

[2] statista.com, "online statistics portal, and one of the world’s most successful statistics databases," 2016.

[3] ITU, "Internet of Things Global Standards Initiative. Recommendation ITU-T Y.2060," 2015.

[4] John, Biggs, "Hackers release source code for a powerful DDoS app called Mirai," 2016.

[5] Lagane, Christophe, "BrickerBot, destrector of connected objects," 2017.

[6] Kocher, Paul C., "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS,," Springer Berlin Heidelberg, Berlin, Heidelberg, 1996.

[7] Kirk Martinez, Paritosh Padhy, Alistair Riddoch, Royan Ong and Jane Hart, "Glacial Environment Monitoring using Sensor Networks," 2005.

[8] Kazatzopoulos, Leonidas, "WSN Location Privacy Scheme Enhancement through Epidemical Information Dissemination," 2014.

[9] Wissam Sammouri, Étienne Côme, Latifa Oukhellou et Patrice Aknin, "« Mining Floating Train Data Sequences for Temporal Association Rules within a Predictive Maintenance Framework," 2013.

[10] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler and J. D. Tygar, "SPINS : Security Protocols for Sensor Networks," 2002.

[11] David, Andrew S. Tanenbaum , "Computer Networks, 5/E. Prentice Hall," 2010.

[12] Debashis, Sahabul Alam, "Analysis of Security Threats in Wireless Sensor Network," 2014.

[13] Tseng, Benjamin J. Culpepper and H. Chris, "Sinkhole Intrusion Indicators in DSR MANETs," 2004.

[14] Najma Farooq, Irwa Zahoor and Sandip Mandal, "Recovering from In-Band Wormhole Based Denial of Service in Wireless Sensor Networks," 2014.

[15] (IETF), Internet Engineering Task Force, "Internet-Draft : Survey of Security Hardening Methods for Transmission Control Protocol (TCP) Implementations," 2012.

[16] Fangmin Sun, Zhan Zhao, Zhen Fang, Lidong Du, Zhihong Xu, "A Review of Attacks and Security Protocols for Wireless Sensor Networks," 2014.

[17] Jahangir, Laleh Arshadi and Amir Hossein, "« Entropy Based SYN Flooding Detection," 2011.

[18] Hongmei Deng, Wei Li and Dharma P. Agrawal, Routing Security in Wireless, 2002.

[19] Quentin Monnet, Lynda Mokdad and Jalel Ben-Othman, Data Protection in Multipaths WSNs, 2013.

[20] Kumar, Chinnu Mary George and Manoj, Cluster Based Location Privacy in Wireless Sensor Networks Against a Universal Adversary, 2013.

[21] Leonidas Kazatzopoulos, Costas Delakouridis and Christos Anagnostopoulos, WSN Location Privacy Scheme Enhancement through Epidemical Information Dissemination, 2014.

[22] Rupam Sherma and Nidhi Tripathi, Comprehensive Review on Wireless Sensor Networks, 2015

[23] A.J. Watt,M.R. Phillips,C.E-A. Campbell,I. Wells,S. Hole " Wireless Sensor Networks for monitoring underwater sediment transport"2019

[24] Ribhu Chopra ; Chandra R. Murthy ; Ramesh Annavajjala "Physical Layer Security in Wireless Sensor Networks Using Distributed Co-Phasing" 2019

[25] Guangjie Han ; Xu Miao ; Hao Wang ; Mohsen Guizani ; Wenbo Zhang "A Cloud-Based Scheme for Protecting Source Location Privacy in Wireless Sensor Networks Using Multi-Sinks"2019

[26] Shoukat Ali ; Muazzam A Khan ; Jawad Ahmad ; Asad W. Malik ; Anis ur Rehman" Detection and prevention of Black Hole Attacks in IOT & WSN"2018