DOI: 10.15849/IJASCA.211128.13

Int. J. Advance Soft Compu. Appl, Vol. 12, No. 3, November 2021
ISSN 2074-8523; Copyright © ICSRS Publication, 2021
www.i-csrs.org

Potential Security Vulnerabilities of the IEEE 802.15.4 Standard and a Proposed Solution Against the Dissociation Process

ABDULLAH ALABDULATIF

Department of Computer, College of Sciences and Arts in Al-Rass,
Qassim University, Al-Rass, Saudi Arabia.
e-mail: a.alabdulatif@qu.edu.sa

Abstract

Many different networks that rely on short-distance wireless technology for their functions utilize the IEEE 802.15.4 Standard, especially in the case of systems that experience a low level of traffic. The networks using this standard are typically based on the Low-Rate Wireless Personal Area Network, herein called the LR-WPAN; this network is used for the provision of both the physical layer, herein referred to as the PHY, and the media access control, herein abbreviated as the MAC. There are four security features in the IEEE 802.15.4 Standard that are designed to ensure the safe and secure transmission of data through the network. Disconnection from the network is managed and controlled by the message authentication code, herein referred to as the MAC, while the coordinator personal area network, herein abbreviated as the PAN, is also able to trigger the disconnection. However, the process of disconnection from the network is one area of vulnerability to denial-of-service attacks, herein referred to as DoS; this highlights a major shortcoming of the IEEE 802.15.4 Standard's security features. This paper is intended to contribute to the improvement of security for the IEEE network by conducting a specific and in-depth review of available literature as well as conducting an analysis of the disassociation process. In doing so, potential new threats will be highlighted, and this data can be used to improve the security of the IEEE 802.15.4 Standard. Overall, in this paper, the role of the Castalia tool in the OMNET++ environment is analysed and interpreted for these potential new threats. Also, this paper proposes a solution to such threats to improve the security IEEE 802.15.4 disassociation process.

Keywords: *Disassociation vulnerability of IEEE 802.15.4 Standard, DoS attack, IoT security*.

1 Introduction

For researchers and developers of software and networks alike, there is a great level of importance assigned to protecting networks from the risk of attacks, such as eavesdropping, which is often conducted through the use of radio receivers with specific built-in software and technology. Attacks of this nature can be difficult to detect by the system when conducted in the wireless environment [1]. As such, the IEEE 802.15.4 Standard is continually being updated with the aim of enhancing the existing safety features to prevent such attacks from exposing and taking advantage of defects and weaknesses in the system [2].

Both the MAC and PHY layers were given for the LR-WPAN in 2003 in the first approved version of the IEEE 802.15.4 Standard [3]. This original version was subsequently modified in 2006, 2011, 2016, and 2018. Meanwhile, in 2015, the title of the Standard was also updated and is now referred to as the Low-Rate Wireless Network, herein referred to as the LRWN [4]. The Standard adheres to the requirements established by minimal power consumption without supervision of the system Internet of Things (herein abbreviated to IoT). The IEEE 802.15.4 Standard is thus highly relevant in numerous fields, which include (but are not limited to) military, healthcare, industrial, and residential. Low-quality service (herein referred to as QoS) and data are examples of features that make this standard relevant for use in these fields [5]. Congestion of the network or other such failures and errors could lead to latency, which, in turn, could increase the likelihood of an attack, such as the injection of forged frames of spyware on the WLANs by attackers [6]. Thus, the two layers of the Standard could both be at risk of coming under attack. The open and unprotected network is one of the major risk areas of the IEEE 802.15.4 Standard. However, the danger posed by the attacker will depend on their target as well as the type of attack being conducted; however, the openness of the network is arguably a blatant flaw in comparison to the closed nature of a wired network.

The IEEE 802.15.4 Standard uses different frames (Beacon, Command, Data, and Acknowledgement) to facilitate the exchange of data between the nodes and the PAN coordinator. Each of these aforementioned frames possesses different information specific to its function and format, which is variable depending on the action that is being carried out [7],[8].

Because the IEEE 802.15.4 Standard relies on the effective transmission of frames by radio waves, it actively engages with a wireless environment and is thus at risk of attack by hackers who, should they gain access to the network, could intercept, track, or obtain the frames to create a sniffing attack that would provide with highly sensitive data [9],[10].

A DoS attack could be created by a single hacker or a group of hackers collaborating for a common goal, which would result in the collapse of the network for a period of time either temporarily or, in some cases, permanently [11]. The collapse of the network would prevent legitimate users from being able to access it is re-secured

and re-established; oftentimes, this type of action may be achieved by flooding the network with illegal data [11]. Another method that is often utilized by hackers to gain access to a network like the IEEE 802.15.4 Standard is emitting radio signals at an increasing signal-to-noise ratio (SNR) level, which makes the signals intended to be sent distorted and corrupted; this process is known as radio jamming [12]. The MAC layer could be an alternative target for hackers, where they could use DoS methods against CAP Maintenance or GTS requests [11] or even against the transmission of data entirely [13].

The process of disassociation depends largely on the method by which nodes are disconnected from the network; however, a successful disconnection procedure culminates with the target node being securely disconnected. This process can also be used as a means of attacking the network; if legitimate nodes are the target of a DoS attack as a result of weaknesses in the disassociation procedure, then association nodes may also be forcibly disassociated. The Rogue Access Point attack was discovered by Nzabahimana (2018) and is characterized by the attacker use of the disassociation procedure to launch a DoS attack on the entire network. First, in this process, an access point must be installed into the network that is being targeted by the attacker; following this, the original access point is removed from the network through the use of connecting association nodes, thereby leaving only the rogue node as the functional access point and giving the hacker full power over the network as a whole [14].

The IEEE 802.15.4 Standard is associated with extensive amounts of related research aiming to help improve the security of the system and uncovering attacks to which the Standard could be likely to fall victim or which it has otherwise experienced in the past. This paper primarily focuses on the disassociation procedure, with the goal being to provide protection for the network's nodes. This will primarily be carried out by determining weaknesses and areas hackers could exploit in order to impact the security of the entire network.

This section has outlined a summarized version of the IEEE 802.15.4 Standard and how it functions. Section 2 explains the MAC layer. The different security roles in regards to the disassociation packet are analysed in detail in Section 3. Section 4 covers the weaknesses of the IEEE 802.15.4 Standard and how these weaknesses could lead to potential attacks on the system, including scenarios in which these attacks might be seen. The implementation procedure for these attacks is then detailed in Section 5, and the results following this are expressed in Section 6. Section 7 proposes a solution for disassociation packet attacks. Finally, Section 8 contains the conclusion for the paper.

2 Networks and Security for the IEEE 801.15.4 Standard

The IEEE 802.15.4 Standard needs to ensure that messages and packets being transferred using its system are kept secure for the sake of message integrity, the confidentiality of the content within the message, and ensuring that message replay

is as it was. The MAC layer of the standard serves to organize the frames being transferred prior to sending them to the PHY layer, making it important that the security of the MAC layer is protected and updated regularly [4].

2.1. Access Controls

Unauthorized nodes should be detected and prevented access by the access controls, which are based on the access point service. Unauthorized nodes must be disconnected from the network prior to the transfer of any frames, before malicious behaviours can be exhibited [15],[16].

2.2. Message Integrity

A number of techniques are in place in the IEEE 802.15.4 Standard that allow for the detection of changes made to a message that is being transmitted; the message integrity service is responsible for this action. Any messages that have had their content altered during the transmission process should be discarded by the authorized nodes by following the MAC technique. A shared but secret cryptographic can be used in this instance to ensure that both the sending and receiving nodes are capable of distinguishing between unaltered and altered messages. This allows the MAC to determine whether a message is liable for deletion due to its being altered during the transmission process [15],[16].

2.3. Message Confidentiality

Message confidentiality is of the utmost importance for a network. Message confidentiality involves the concealment of the content contained within a message, and, for the IEEE 802.15.4 Standard, this is carried out using two methods: encryption and Nonce. Using the Nonce method provides non-repetitive results, thereby serving to further complexify the encryption of the message being sent [15],[16].

2.4. Replay Protection

It is relatively easy for an attacker to create an eavesdropping attack against the network if said network is wireless in nature, meaning that messages being transferred over the aforementioned network will potentially be compromised in their security. If a message should be captured by an attacker, it could then be utilized for devious or malicious purposes. However, in the case of the IEEE Standard, these types of attack are protected through the use of a sequence number technique that serves to number each packet being sent, which means that the network is able to determine the authenticity of the packet and reject instances where the packet value does not correlate with the sequence number [15],[16].

3 The IEEE 802.15.4 Networks Security Packet

Security is controlled and applied by the MAC layer in the case of the IEEE 802.15.4 Standard, which means that the appropriate measures need to be established in order for the correct control parameters to be specified. This information can then be used to provide support against weaknesses; this, in turn, ensures that the data field is protected by the beacon, data, and control frames while unsupported by the Acknowledgement frames. The Acknowledgement frames' lack of protection means that it is possible for their information to be transferred in an unprotected manner [17].

If security is to be provided for the IEEE Standard, first, a specific and relevant security suite needs to be selected. Oftentimes, the high degree of protection provided by the AES-CCM makes it a suitable option for the encryption and authentication of the data frame; meanwhile the AES-CBC-MAC can provide authentication services for other frames. Finally, the AES-CTR is useful for providing encryption security. However, in cases where there is no need for an exchange of data between the application and a specific frame, a null suite is instead selected [3],[4].

Disassociation packet: When disassociation is requested by the PAN coordinator or an associated node, a command is directly transferred between these two functions, which enables the disconnection process from the network [4].

An example of a generic MAC frame is demonstrated in Figure 1, where a fixed arrangement is utilized for the fields of the frame; however, it is not possible for all fields to be added as part of the MAC header. This is due to the variability that can exist between two different frames. Parameters in the frame control field serve to determine the type of frame in question. A key area of importance in this process is the security-enabled field, which provides protection for the frame that is being transferred. If the level of security is set to 0, the frame will have no protection assigned to it. As such, the auxiliary security header will only be present in the MAC frame's MHR if value one is not determined in the security-enabled field [1].

4 Disassociation Packet and the Risk Posed by Attacks

In this section, we discuss the role of security in the Standard's disassociation process and highlight any weaknesses found in the system that could predispose it to the threat of a hacker attack with the aim of causing malicious activities to the network. The weakness in question is potentially utilizable by attackers using a DoS attack in multiple manners, which should be understood first. At the initiation of the attack, data regarding the network is gathered through the use of a disassociation process attack; then, information can be collected by the attacker, which could compromise the security of the IEEE 802.15.4 Standard. First, a sniffing attack is used to obtain access to sensitive records and information that is sent during the process of frame transfer; the attacker in this instance will not engage in altering

field values and the like at this stage [18]. As a result, the attacker has completed the gathering stage and possesses a file with important and sensitive information about the target network. This information allows the attacker to move on to the next stage.

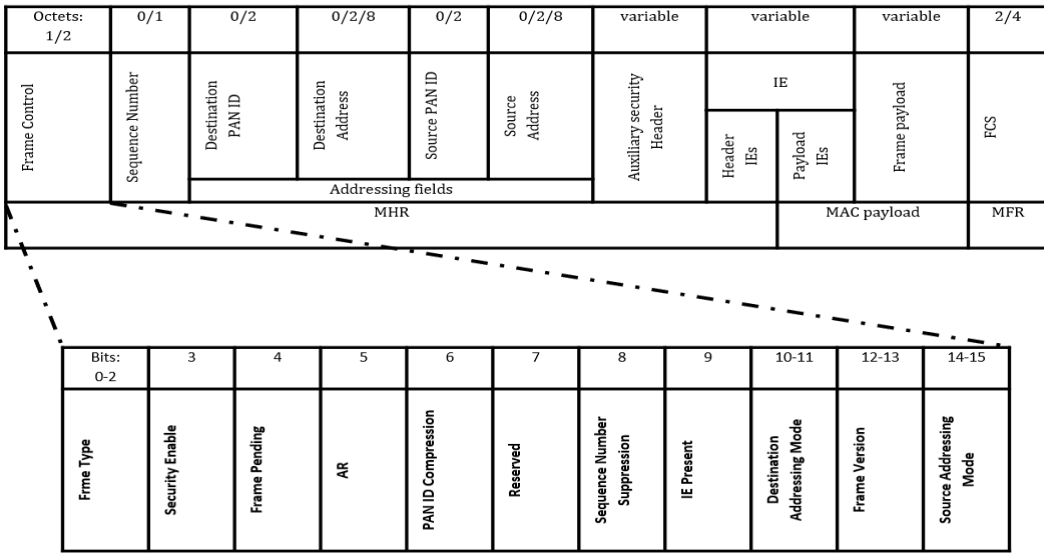

Figure 1: General MAC frame format.

Following this, the attacker can launch an active attack through the initiation of the disassociation procedure either targeting the PAN coordinator or the associated nodes themselves, which causes associated nodes to be removed from the network. In the first case, targeting associated nodes, a fake disassociation notification command is generated and directed by the attacker to the association node(s) that has been targeted. In doing so, the association node must then return an acknowledgement packet to the PAN coordinator, which serves to finalize the process of disassociation. This causes the PAN coordinator to interpret this as the association node being disconnected. In the other case, targeting the PAN coordinator, a fake disassociation notification command is generated and directed by the attacker by impersonating the association node sent to the PAN coordinator, which is demonstrated visually in Figure 2. As before, an Acknowledgement packet is returned, but, this time, it is returned by the PAN coordinator to the association node. Both of these methods will have the same result: preventing the associated node from being able to communicate with the network; thus, disassociation will be complete.

In both cases, regardless of the target (either the PAN coordinator or associated nodes), it is proven that the attacker can generate and direct a fake disassociation notification command. Then, the PAN coordinator and associated nodes can

complete the disassociation process of the IEEE 802.15.4 Standard. In other words, the attacker uses the disassociation notification command that is not secure to launch an active DoS attack over the network.

There is a weakness found within this disassociation process that attackers could use to trigger an attack on the IEEE 802.15.4 Standard. This potential for attack could endanger the safety of the files being transferred through the system and could result in the standard being at risk of malicious hacker intentions. Therefore, actions must be taken to understand the risks posed by this weakness, and, furthermore, steps must be taken to prevent the weakness from being harnessed for malicious purposes by triggering the commencement of the disassociation process. Conversely, the same could be carried out by harnessing the association nodes to disconnect them from the network and trigger the disassociation processes. Regardless of the disassociation method used, this would then expose a major weakness, which would allow for further DoS attacks to be made against the IEEE 802.15.4 Standard itself.

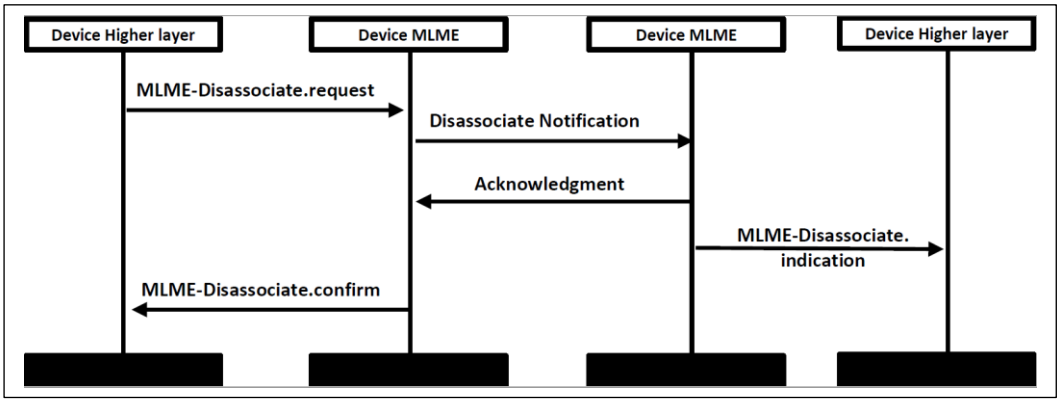

Figure 2: Message sequence chart of disassociation.

4.1. Disassociation Attacks Targeting Nodes

As can be seen below in Figure 3, the PAN coordinator and the associate nodes are the primary components of networks that apply the IEEE 802.15.4 Standard. In addition to the associated nodes (A, B, and C), one other type of node (D) can be seen in the diagram—unassociated nodes, which serve to connect and associate with the PAN coordinator. The attacker (hacker) node that has been maliciously integrated into the system and is intended to carry out an attack on the network. This attacker node conducts a sniffing attack, as previously mentioned, which allows the attacker node to uncover the necessary information for an attack to take place. This attacker node searches for an association packet, meaning there is a node in the network desiring to legally join with the PAN coordinator; should they discover one, which would have been sent from any unassociated node in the system to the PAN coordinator. This attack can be achieved in two steps as follows:

Step 1: When the attacker node detects any association packet throughout the network, it sends to the PAN coordinator to attempt to associate with the network; then, it will create a disassociation packet to send back to the unassociated node, as shown in Figure 3 (step 1).

Step 2: This unassociated node, upon receiving the disassociation command, will respond with an Acknowledgement packet (as detailed previously) for apologies for the link with network. As a result, the node (D) will have failed to successfully complete the association process with the PAN coordinator to join the network, as shown in Figure 3 (step 1).

The attacker node will need to gather all of the relevant information to create a fake disassociation command through a sniffing attack prior to this event. This information will include details regarding the unassociated node that sent the original association packet request as well as a destination and source address for the node and PAN coordinator. Since, in this instance, the node has received information from what it interprets to be the PAN coordinator, it will complete the disassociation process as requested and send out the acknowledgement packet. This causes an incorrect disassociation to be carried out and the node, at the end of the process, to be no longer associated with the network. However, it was not an intended action and was the result of the fraudulent attack node altering the commands sent between the node and the PAN coordinator.

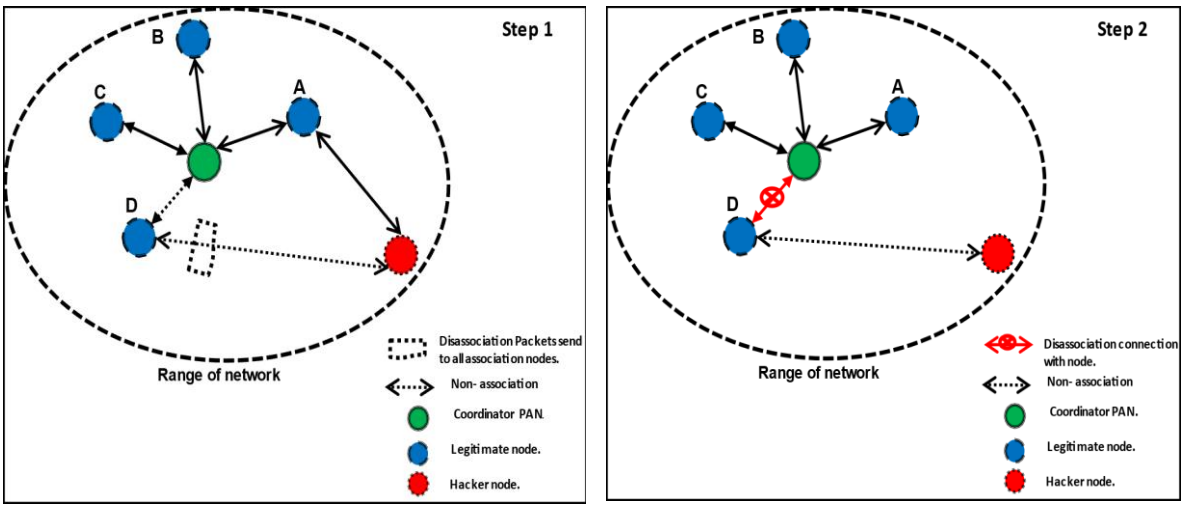

Figure 3: A disassociation attack targeting the nodes.

4.2. Disassociation Attack Toward the PAN Coordinator

As can be seen in Figure 4, for networks implementing the IEEE 802.15.4 Standard, there are numerous associate nodes (A, B, C, and D) as well as the PAN coordinator, both of which can be hacked by a hacker and attacked to interfere with their functioning. Additionally, there are also uncoordinated nodes that are not associated

with the system (but can request to become associated with the PAN coordinator) as well as attacker node that can also be seen in the network and serve the role of attempting to hack into the system and cause malicious intentions. An attacker node that is attempting to hack into the system launches the sniffing attack by collecting data and information on the system, which includes information such as the source address, destination address, etc. Once the attack node has retrieved its information, it is then able to begin the next sniffing attack stage to identify an association packet response sent out by the PAN in response to a request made by the unassociated nodes to join the system. After that This attack can be achieved in two steps as follows:

Step 1: Once the attacker node has detected this association packet response, it is then able to create its own falsified disassociation packet in order to hijack the system; the destination address for this malicious disassociation packet is set to the PAN coordinator so that, when it is received, an acknowledgement packet is then sent out. However, at this time, the attacker node once more interferes with the system so that the destination and source addresses are switched out, meaning that the command is sent to the wrong recipients, as shown in Figure 4 (step 1).

Step 2: The PAN coordinator receives the malicious disassociation packet, interprets it as the node (C), and makes a request to disconnect from the network. As a result, the node is then sent an acknowledgement packet and is removed from the network as a result of the attacker node's actions, as shows in Figure 4 (step 2).

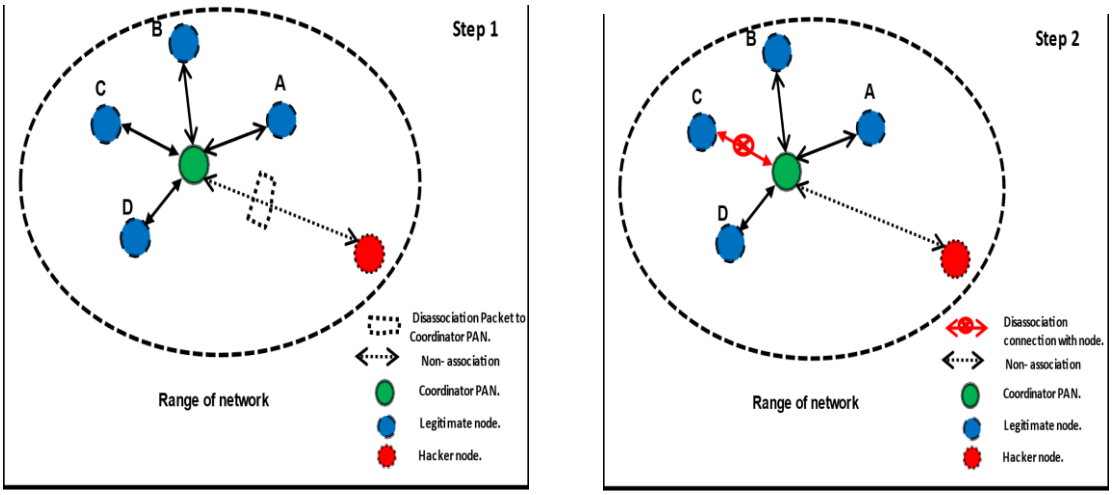

Figure 4: Disassociation attack toward the PAN coordinator.

5 Implementation of Disassociation Attacks on the Network

In section V, we examine the processes undertaken during a disassociation attack process and how such attacks are carried out, including considering the requirements that must be witnessed in order to create an environment in which the attack can be carried out. Indeed, there are certain considerations that will impact whether or not the attacker node will be able to conduct a successful attack on the network based on certain potential weaknesses in the systems but that, if eliminated, would help prevent attacker nodes from being able to carry out their function and thereby promote the security of the network. For the IEEE 802.15.4 Standard, this should be maintained and is considered a point of utmost importance, as failing to do so could leave the Standard with serious weaknesses that, upon discovery by hackers, could be used as a means of hacking into the system and causing damage to the Standard or compromising the confidentiality of the information being shared on the network.

An attack on the IEEE Standard can be simulated with the Castalia-3.2 tool, which allows for the weaknesses of the system to be determined and analysed. In so doing, it is possible to gain insight into areas that could be targeted by attackers, and, subsequently, steps can thus be taken to promote the safety of these weak areas in order to strengthen them and reduce the likelihood of the network being compromised. The primary configuration file used in this analysis process is omnetpp.ini, which contains the majority of the parameters needed in order to create the network simulation. This process can be carried out in such a way that ensures that the network is set up in a manner that is relevant to the simulation in question. Below, the parameters included in the file are explained, including how the Castalia-3.2 tool can be best utilized for monitoring or testing the security of a network like the IEEE 802.15.4 Standard.

First, the main configuration code is considered, which is found within the file, omnetpp.ini. This is needed for setting the correct value for the parameters in question, which should be carried out to meet the requirements of the simulation scenario. These values need to be defined and set, since, as a standard, they have no default figures and values attached to them. Examples of parameters that would need to be defined at this stage include the number of nodes in the simulation or the amount of time for which the simulation is expected to run. In this study on the IEEE 802.15.4 Standard, we generally have five nodes that are legitimate, as well as an extra attacker node that serves as the hacker in the simulation. One of the nodes is the PAN coordinator. The attacker node serves as the malicious entity within this simulation, and its role is to simulate how a real hacker could attempt to infiltrate and damage the network based on the existing parameters for the real Standard; it targets both the nodes and the PAN coordinator to conduct its attack on the system. As such, there are six nodes that are defined as part of this simulation, five of which are legitimate nodes and one of which is the illegitimate attacker node:

```
SN.node[*].Communication.MACProtocolName = "Mac802154"
SN.node[0].Communication.MAC.isFFD = true
SN.node[0].Communication.MAC.isPANCoordinator = true
SN.node[*].Communication.MAC.phyDataRate = 1024
SN.node[1].Communication.MAC.ishack = true
```

The codes serve an important role in the definition and creation of the MAC layer for the simulation, and this is carried out in line with the implementation requirements of the system. The primary parameter above, 'MACProtocolName', is used as a means of determining the specific type of protocol that was implemented during the implementation process by the MAC layer. This is important, as will be subsequently seen, for the success of the simulation from a reliability perspective. Next, there is the 'isFFD' parameter, which serves to distinguish between and identify the network's fully functioning nodes; it also serves to set the names for each of the legitimate nodes, where node '0' is one of the fully functioning nodes present in the network itself. Third, the control of the nodes in terms of which node will be the PAN coordinator node for the network simulation is determined by the parameter, 'isPANcoordinator'. This differentiates between the five nodes in the system that are legitimate, leaving one PAN coordinator node and four legitimate nodes. Fourth, there is the 'phyDataRate' parameter, which is responsible for controlling the speed of transmission during the implementation phase of the simulation, with the value of this parameter being set in Kbps units. Finally, the 'ishack' parameter is responsible for identifying and determining the attacker node from the other nodes, with the attacker node being the node responsible for carrying out the malicious attack on the simulation network of the IEEE 802.15.4 Standard.

During an attack on the IEEE 802.15.4 Standard by a disassociation packet attack, the is for interfering with the normal functioning of the nodes and the PAN coordinator, with the association and disassociation processes being interfered with and controlled by the attacker node. During an attack on the network by the attacker node, the attacker node interferes with these processes, altering the source and destination addresses for the disassociation packets that are sent between the node and the PAN coordinator, which, in turn, forces a node to disassociate from the system. Attacks of this nature by attacker nodes are characterized as being active attacks due to the fact that the attacker node's role during the attack is to actively carry out behaviour that is malicious in nature. The attacker node's behaviour is coded as shown below:

```
void Mac802154::fromRadioLayer(cPacket * pkt, double rssi,
double lqi)
{  if (ishack){
    if (rcvPacket->getMac802154PacketType() ==
   MAC_802154_ASSOCIATE_PACKET){
    int PANaddr = rcvPacket->getPANid();
    nextPacket = new Mac802154Packet("PAN disassociate
    request", MAC_LAYER_PACKET);
    nextPacket->setDstID(rcvPacket->getSrcID());
    nextPacket->setPANid(PANaddr);
    nextPacket->setMac802154PacketType(MAC_802154_
    DISASSOCIATE_PACKET_REQUEST);
    nextPacket->setSrcID(rcvPacket->getDstID());
    nextPacket->setByteLength(COMMAND_PKT_SIZE);
    }
    if (rcvPacket->getMac802154PacketType() == MAC_
    802154_ACK_PACKET){
    int PANaddr = rcvPacket->getPANid();
    sniff() << " The packet is: MAC_802145_Ack_PACKET "
    << (rcvPacket->getSrcID())<< "To node "<< (rcvPacket->
    getDstID());
    nextPacket = new Mac802154Packet("PAN disassociate request
     node", MAC_LAYER_PACKET);
    nextPacket->setDstID(rcvPacket->getSrcID());
     node", MAC_LAYER_PACKET);
    nextPacket->setDstID(rcvPacket->getSrcID());
    nextPacket->setPANid(PANaddr);
    nextPacket->setMac802154PacketType(MAC_802154_DISASSOCIATE_
    PACKET_REQUEST);
    nextPacket->setSrcID(rcvPacket->getDstID());
    nextPacket->setByteLength(COMMAND_PKT_SIZE);
```

A disassociation packet can be launched through one of two methods, which is shown in the above code. These two methods are shown as follows:

Method A: In this method, the attacker node conducts a sniffing attack into the network and, if the 'MAC_802154_ASSOCIATE_PACKET' is detected on the system, the attacker node will complete the following steps in order to launch its attack:

1) A disassociation packet is first built following the plans and information contained within the original packet. This is called: 'MAC_802154_DISASSOCIATE_ PACKET_REQUEST'.

2) For the maliciously created packet, 'MAC_802154 _DISASSOCIATE_PACKET_REQUEST', the destination address will be set as the same as the source address from the 'MAC_802154_ASSOCIATE_ PACKET'.

3) For the maliciously created packet, 'MAC_80154_ DISASSOCIATE_PACKET', the source address will be set as the same as the destination address from the 'MAC_80154_ASSOCIATE_PACKET'.

4) The PAN id will be set as the same for both the attacker packet and the original associate packet that was sent out.

5) Finally, the type of packet is determined by the attacker node. and the 'MAC_80154_ DISASSOCIATE _PACKET_REQUEST' can be sent out over the network to its intended recipient, which, in turn, will trigger the recipient to commence the disassociation process.

Method B: Alternatively, if an acknowledgement packet is sniffed over the network during the attacker node's sniffing attack, the following method is followed for the attacker node to cause malicious intent on the network.

1) A disassociation packet is first built following the plans and information contained within the original packet. This is called 'MAC_802154_DISASSOCIATE_ PACKET_REQUEST'.

2) For the maliciously created packet, 'MAC_802154_ DISASSOCIATE_PACKET_REQUEST', the destination address will be set as the same as the source address from 'MAC_802154_ACK_PACKET'.

3) For the maliciously created packet, 'MAC_80154_ DISASSOCIATE_PACKET', the source address will be set as the same as the destination address from the 'MAC_80154_ACK_PACKET'.

4) The PAN id will be set as the same for both the attacker packet and the original associate packet that was sent out.

5) Finally, the type of packet is determined by the attacker node and the 'MAC_80154_ACK_ PACKET' can be sent out over the network to its intended recipient, which, in turn, will trigger the recipient to commence the disassociation process.

6 Discussion and Rrsults

In this section, the output process for the implementation that was carried out as part of the study for this paper is explained and discussed while further serving to identify and represent the results obtained as a result of this implementation experiment.

During the study, the Castalia tool was utilized to simulate a real attack on the IEEE 802.15.4 Standard, which allowed for accurate results to be determined based on how a real attack on the network might be carried out; this could then be analysed to determine areas of strength and weakness in the existing framework. The means by which the sniffing attack was conducted using the Castalia tool were explained previously in Section 4. When run in the simulation model, the results of the sniff attack can be seen in Figure 5, which were saved under the name of 'Sniffing-trace-txt' by the attacker node itself. From this data, the following information can be obtained:

- The name of the node carrying out the sniffing attack on the packets; in this instance for the simulation, the node was the attacker node itself.

- The type of packet that has been uncovered during the sniffing attack by the attacker node; see Table 1 for examples of the types of packets that can be sniffed out during the attack.
- The network name, which also corresponds to the PAN id.
- The addresses of the sender and destination for the packet.

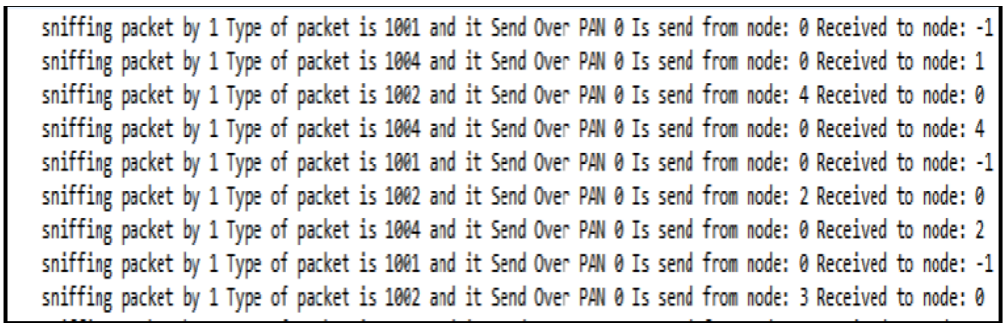

Figure 5: Snippet of the file 'Sniffing-Trace.txt' as a result of sniffing by the hacker node.

Table 1: Type of packet in the Castalia tool

Type of packet	Code
MAC_802154_BEACON_PACKET	1001
MAC_802154_ASSOCIATE_PACKET	1002
MAC_802154_DATA_PACKET	1003
MAC_802154_ACK_PACKET	1004
MAC_802154_GTS_REQUEST	1005
MAC_802154_DISASSOCIATE	1006
MAC_802154_DISASSOCIATE	1007

As a summary for the experiment, it can be said that any attacker node can easily launch an attack against the disassociation process. The disassociation command sent over the network is unencrypted, which is a command type that is easy to detect, manipulate, and resend over the network again. Also, it can create a disassociation command and then send it over the network to force the target node or PAN coordinator to complete the disassociation process. As a result, the disassociation process in the IEEE 802.15.4 Standard lacks a security policy that makes the disassociation process more secure.

As is observed in Figure 6, which shows content from the file 'Sniffing-trace.txt', there is a record kept of the attacks that are carried out, including the type of packet and the destination and source nodes. This file shows the activities in the network,

with two cases clearly visible from this part of the file. In this first case, it can be seen how node 4 was converted into node 1, which indicates that the node has been disassociated from the rest of the network and is thus disconnected, indicating a successful hacking attempt of the simulation system. Therefore, the association process failed to be carried out as a result of the attacking node's infiltration of the system and the creation of false files, leading to an incorrect disassociation of the node in question. This case proves that the attacker is able to attack any node it desires to associate with the PAN coordinator and join the network. Therefore, the attacker can control the network and ban every node in order to associate in the network, which leads to a DoS attack against the network.

7 Proposed Solution for Disassociation Packet Attacks

In this paper, a new type of attack has been identified, analysed, and implemented against the disassociation processes using two methods. This section introduces the proposed solution to overcome the disassociation process attack.

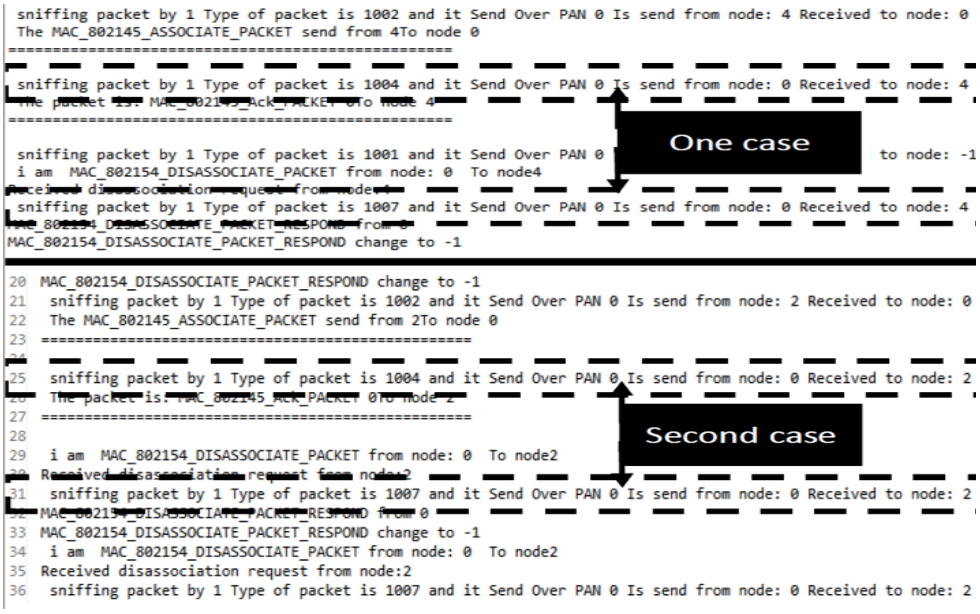

Figure 6: Results of the disassociation attack.

The proposed solution is based on the Disassociation Nonce for each session, with the nonce being the value that is sent to the node requesting association within the association response message. The nonce value should be different between the node and PAN coordinator for each session. So, when the PAN coordinator wants

the node to leave the network or the node desires to leave the network, the PAN coordinator should include the specific Disassociation Nonce for the session in the Disassociation notification message. Therefore, the PAN coordinator or the node has to generate the Disassociation Nonce, which is included in the association response command for each session in the network, and the disassociation process is not successfully completed unless the Disassociation Nonce provides correctly for the node's desire to disassociate from the network. Otherwise, any attempt to initiate the disassociation process will be discarded and assume this is type of attack.

As Figure 7 shows, there are two ways to initiate the association process in the IEEE 802.15.4 Standard. Figure 7a shows the first method, in which the PAN coordinator sends an Association Request message to the node and then sends a Data request. After that, the node sends an association response message to confirm the association with the PAN coordinator. At this stage, both the PAN coordinator and the node are associated and can exchange the encrypted data. In the second method, as shown in Figure 7b, the node sends an Association Request message to the PAN coordinator and then sends a further Data request. Subsequently, the PAN coordinator sends an association response message to confirm the association with the node. As with the first method, both the PAN coordinator and the node are associated and can exchange the encrypted data [4].

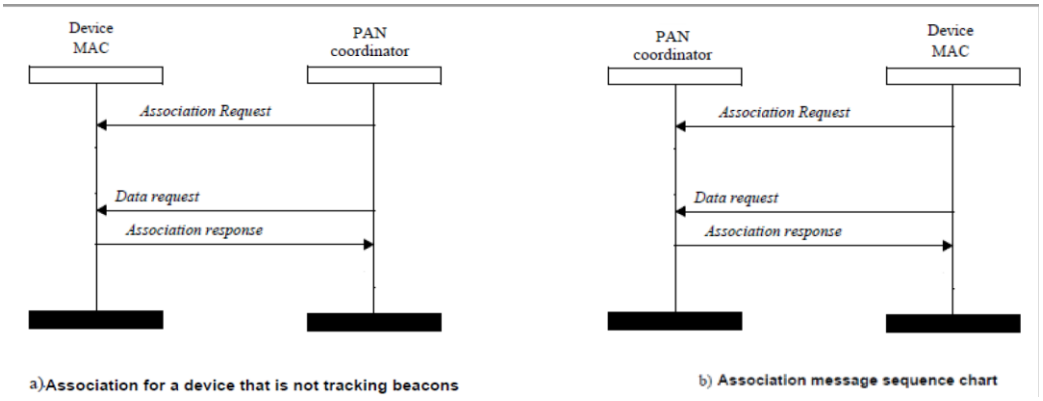

Figure 7. Association process message (two ways) in the IEEE 802.15.4 Standards.

To implement the proposed solution, the association response message can be sent either from the PAN coordinator or node based on the type of the required association. So, the association response message must be modified and add an extra field in the content, called the Disassociation Nonce, as shown in Figure 8. Thus, in both cases of initiating the association process, either the PAN coordinator or the node that sends the association response message has to generate a Disassociation Nonce. The Disassociation Nonce is generated only when the association status value is (0 x 00), which means the association was successful; otherwise, the Disassociation Nonce will not be generated. After the association process is successfully completed, both the PAN coordinator and the node have a

Disassociation Nonce for this session only. The advantage for including the Disassociation Nonce value in the association response message is that, in the IEEE 802.15.4 Standard, the association response message is sent encrypted. So, the value of the Disassociation Nonce will be secure and the attacker will not have the chance to launch the DoS attack against the Disassociation process.

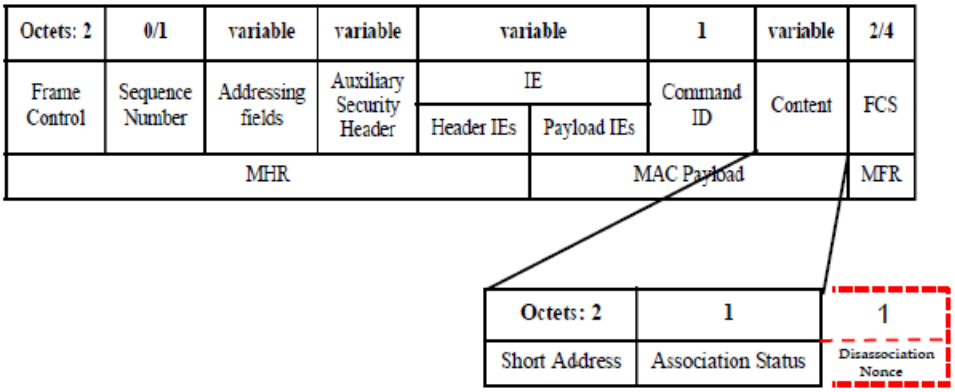

Figure. 8. Proposed Association Response Command Content field format.

During the Disassociation process, when the PAN coordinator desires the node to leave the network or the node desires to leave the network, the disassociation notification message must change by adding a field called the Disassociation Nonce in the Disassociation notification message, as shown in Figure 9. So, any participant that wants to send a Disassociation notification message should include the Disassociation Nonce in this message. Thus, when the message is received, the receiver can obtain the Disassociation value and compare it with the Disassociation value for the current session. If both are equal, it can safely disconnect from the network; otherwise, it will ignore the Disassociation notification message.

The Disassociation Nonce is a proposed solution in this paper for eliminating a potential attack by an attacker against the Disassociation process. In the case of a reply attack, the attacker node is unable to launch this type of attack against the Disassociation process, because the value of the Disassociation Nonce will be different between the node association node and the PAN coordinator. Moreover, the value of the Disassociation Nonce for the node itself will be different between sessions, since the security rule for the Disassociation Nonce is to not reuse the Nonce value for long period of time.

The Disassociation Nonce provides greater protection for the disassociation process against a Modification attack. Both the PAN coordinator and association node have Nonces for specific sessions, which means that, if the attacker node attempts to modify any message of the disassociation process and send it, this message will be discarded. So, the value of the Disassociation Nonce is linked by a number of factors, including the PAN coordinator address and association node address and

the session id. Therefore, it will be easy to define any modification in the message during any stage of disassociation process.

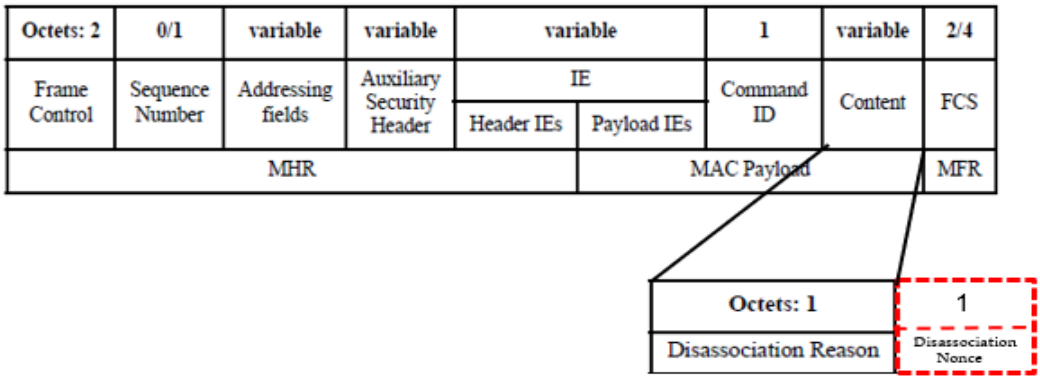

Figure 9. Disassociation Notification command Content field format proposal.

8 Conclusion

Ensuring that the IEEE 802.15.4 Standard is maintained to a level that ensures the safety of the network and the confidentiality of the information and data being transferred across it is imperative for the long-term reliability and security of the network. Weaknesses in the network should be determined and subsequently strengthened to prevent the likelihood of a successful attack against the network. Utilizing a simulation method can help with the identification of areas of weakness in this regard. Moreover, using tools like Castalia can provide a reliable simulation for attacking nodes and provide insight into how these attacking nodes infiltrate a system and alter its information.

This research was carried out with the main aim of ensuring that the security of the IEEE 802.15.4 Standard is as strong as possible. Measures such as these will help prevent future weaknesses from being exploited in networks such as the Standard, which provides MAC and PHY layer provisions for LR-WPAN connections.

This study concluded that the IEEE 802.15.4 Standard faces a potential new form of attack due to existing weaknesses in the system, and, as a result, hackers and those with malicious intentions could utilize attacker nodes to hack into the network and cause damage or put data anonymity at risk. This could be carried out due to the weaknesses presented in the disassociation process; therefore, attempts should be made to find a means of strengthening the relationship between the PAN coordinator and the associated nodes to prevent such weaknesses from causing potential privacy and security risks.

The threats faced by the IEEE 802.15.4 Standard can be minimized by adding an additional layer of protection to the system in the form of a disassociation nonce. The disassociation nonce will allow participants to check the value against the

expected session value, thereby providing an additional layer of security and helping to prevent disassociation attacks from occurring.

References

[1] Alabdulatif, A. A. (2020). Analyse Security of the Disassociation Procedure in the IEEE 802.15. 4 Standard. *International Journal of Computer Science and Information Security (IJCSIS)*, 18(5).

[2] Alabdulatif, A. A. (2019). Security Attacks in IEEE 802.15. 4: A Review Disassociation Procedure. In *International Conference of Reliable Information and Communication Technology* (pp. 477-485). Springer, Cham.

[3] I. C. S. L. M. S. Committee et al., "Wireless lan medium access control (mac) and physical layer (phy) specifications," *ANSI/IEEE Std. 802.11- 1999*, 2003.

[4] ——, ".: Ieee std 802. 15. 4-2015 (revision of ieee std 802. 15. 4-2011), ieee standard for low-rate wireless personal area networks (lr-wpans)," *IEEE Computer Society*, 2015.

[5] Rashid, A., Pecorella, T., & Chiti, F. (2020). Toward Resilient Wireless Sensor Networks: A Virtualized Perspective. *Sensors*, 20(14).

[6] Bayou, L. (2018). *Assessment and enforcement of wireless sensor network-based SCADA systems security* (Doctoral dissertation, Ecole nationale supérieure Mines-Télécom Atlantique Bretagne Pays de la Loire).

[7] Elijah, O., Rahman, T. A., Orikumhi, I., Leow, C. Y., & Hindia, M. N. (2018). An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. *IEEE Internet of Things Journal*, 5(5), 3758-3773.

[8] Hussain, I., Negi, M. C., & Pandey, N. (2019). Security in ZIGBEE using steganography for IoT communications. In *System Performance and Management Analytics* (pp. 217-227). Springer, Singapore.

[9] Cheema, R., Bansal, D., & Sofat, S. (2011). Deauthentication/disassociation attack: Implementation and security in wireless mesh networks. *International Journal of Computer Applications*, 23(7), 7-15.

[10] Hosenkhan, M. R., & Pattanayak, B. K. (2020). Security issues in internet of things (IoT): a comprehensive review. *New Paradigm in Decision Science and Management*, 359-369.

[11] Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2017). Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of things journal*, 5(4), 2483-2495.

[12] Amoozadeh, M. (2018). *Towards Robust and Secure Collaborative Driving and Interactive Traffic Intersections*. University of California, Davis.

[13] Amin, Y. M., & Abdel-Hamid, A. T. (2018). A Simulation Model of IEEE 802.15. 4 GTS Mechanism and GTS Attacks in OMNeT++/MiXiM+ NETA. *Comput. Inf. Sci.*, 11(1), 78-89.

[14] Nzabahimana, J. P. (2018). Analysis of security and privacy challenges in Internet of Things. In *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 175-178). IEEE.

[15] Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal*, 4(5), 1250-1258.
[16] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer networks*, 76, 146-164.
[17] Frustaci, M., Pace, P., & Aloi, G. (2017). Securing the IoT world: Issues and perspectives. In 2017 *IEEE Conference on Standards for Communications and Networking (CSCN)* (pp. 246-251). IEEE.
[18] Perlman, R., Kaufman, C., & Speciner, M. (2016). *Network security: private communication in a public world*. Pearson Education India.

Notes on contributors

Abdullah Alabdulatif is Assistant Professor of Computer Department, College of Sciences and Arts, Qassim University. He graduated from Qassim University, Saudi Arabia in 2004. He received a bachelor of computer Science degree. Then entered Newcastle University, UK and received a Master of Computer Security and Resilience degree in 2009 and PhD in Information Security from Nottingham Trent University in 2014. He has 6 research papers in refereed international journals and conferences. He is interesting research in Academic & Research includes Wireless security, IoT security, Blockchain Security. Email: A.Alabdulatif@qu.edu.sa