Classification and Analysis of IEEE 802.15.4 MAC Layer Attacks

Yasmin M. Amin, Amr T. Abdel-Hamid, *Senior Member*, IEEE
Department of Networks Engineering
German University in Cairo
Cairo, Egypt
{yasmin.amin, amr.talaat}@guc.edu.eg

Abstract — **IEEE 802.15.4 Wireless Sensor Networks (WSNs) possess additional vulnerabilities in comparison with traditional wired and wireless networks, such as broadcast nature of wireless medium, dynamic network topology, resource-constrained nodes, lack of physical safeguards in nodes, and immense network scale. These inherent vulnerabilities present opportunities for attackers to launch novel and more complicated attacks against such networks. For this reason, a thorough investigation of the attacks which can be launched against WSNs is required. This paper provides a single unified survey that dissects all IEEE 802.15.4 MAC layer attacks known to date. While the majority of existing references investigate the motive and behavior of each attack separately, this survey addresses the interrelationships and differences between the attacks following their classification. The survey defines two main classifications for the attacks by combining and refining existing classifications of the attacks obtained from external references. The defined classifications are further extended by including additional attacks, which have been left out by other references, within the classifications. The authors' opinions and comments regarding the placement of the attacks within the defined classifications are also provided. A comparative analysis between the classified attacks is then performed with respect to a set of evaluation criteria defined within the paper.**

Keywords — IEEE 802.15.4, MAC layer attacks, wireless sensor networks, denial of service, link layer jamming, back-off manipulation, same-nonce attack, replay-protection attack, ACK attack, MITM attack, GTS attack, steganography attack

I. INTRODUCTION

Many applications involving WSNs are security-sensitive, and possess zero tolerance for error and latency. While error and latency can occur due to network failure and congestion, they can also be triggered by malicious behavior. The IEEE 802.15.4 standard [2] has become the dominant enabling technology for WSNs. WSNs are networks of a large number of tiny sensor devices which target applications in a diverse set of fields, particularly military, healthcare, residential, transport and industrial fields to name a few. Such applications require very low data rates and relaxed Quality of Service (QoS) requirements over short ranges for wireless devices with very small sizes [3].

While attacks can be launched on both the PHY and MAC layers of 802.15.4 networks, the primary focus of this paper is on providing a comprehensive classification of the attacks which can be launched on the IEEE 802.15.4 MAC layer. This classification is used as the basis for performing a comparative analysis between the attacks. To the best of the authors' knowledge, this survey is the first to provide a single reference consolidating all IEEE 802.15.4 MAC layer attacks known to date. The paper is organized as follows: In Section II, we describe the operation and purpose of each attack and its variants. We also identify a new variant of the *GTS Attack*. In Section III, we present two significant classifications of MAC layer attacks, collectively obtained from external references, along with our own additions to these existing classifications. In Section IV, evaluation of the differences between the discussed attacks is performed based on a set of defined evaluation criteria. Section V concludes the paper.

II. ATTACKS ON IEEE 802.15.4 MAC LAYER

This section explains the purpose and operation of the attacks which can be launched by a malicious adversary against the MAC layer of an IEEE 802.15.4-based network. We refer to the different methods of launching the same attack as the attack's *variants*, and we discuss how an attack's variants can be conducted. We assign names for attacks which have not previously been named in existing literature.

A. Link Layer Jamming

Similar to *Radio Jamming* at the PHY layer, *Link Layer Jamming* is a MAC layer attack which is launched with the intent of creating a Denial of Service (DoS) against the network by disrupting the exchange of messages between transmitting and receiving network nodes. While *Radio Jamming* achieves its purpose by creating radio interference through the emission of radio signals, *Link Layer Jamming* involves the emission of packets rather than signals [8]. Two variants of *Link Layer Jamming* can be defined, both of which cause degradation and reduction of network performance and throughput [5]. These two variants differ with respect to the recurrence of packet transmission by the malicious adversary.

1) Random Jamming (also known as *Blind Jamming* [8])*:* In this variant, a malicious adversary emits packets of useless content at random time intervals, and for no specific purpose. While this variant can be considered as a stand-alone attack, it is also the basis for the *One Random Attacker (ORA)* and *Two*

978-1-4673-8511-4/15 $31.00 ©2015 IEEE

Random Attackers (TRA) scenarios of the *Interference During CFP* variant of the *GTS Attack*, which are explained later.

2) Intelligent Jamming: An intelligent jammer emits packets of useless content at specific times for specific purposes [8]. In addition to acting as a stand-alone attack, this variant can also be used as the basis for launching more powerful and complicated types of attacks, such as *Acknowledgment (ACK) Attack*, *Man-In-The-Middle (MITM) Attack*, and the *One Intelligent Attacker (OIA)* and *Two Intelligent Attackers (TIA)* scenarios of the *Interference During CFP* variant of the *GTS Attack*, as explained later.

B. Node-Specific Flooding

Misic *et al.* [5] describes an attack which involves the transmission of unnecessary packets whose destination addresses are set to the addresses of destination nodes targeted by malicious adversaries. The targeted nodes' power sources are eventually depleted due to excessive packet reception from the adversaries.

C. Back-off Manipulation

The Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) [2] channel access mechanism is used to govern the rules for medium contention among network nodes in IEEE 802.15.4 networks. For beacon-less networks, unslotted CSMA-CA is used. For beacon-enabled networks, slotted CSMA-CA is used during the Contention Access Period (CAP) of each superframe duration. A malicious adversary can manipulate CSMA-CA rules in such a way that the adversary constantly uses a short back-off period instead of selecting a random back-off period from its contention window. In doing so, the adversary hijacks channel access by ensuring that it is always granted higher priority to access the channel than legitimate nodes, which use larger back-off periods [6]. This attack increases both waiting time of legitimate nodes during channel access and power consumption of nodes during the reception of adversary data [5].

Misic *et al.* [5] mentions two variants of *Back-off Manipulation*, the difference between both variants being with respect to the methods they use to accomplish the common objective explained above.

1) Battery Life Extension (BLE) Pretense: BLE mode ensures the conservation of power for nodes operating on battery power. A malicious adversary can take advantage of this CSMA-CA feature by falsely pretending to run in BLE mode in order to acquire a smaller initial contention window size than the other legitimate nodes. This reduces the range of values from which the adversary can select its back-off period and ensures that its probability of accessing the medium is much higher than legitimate nodes.

2) Constant Back-off Exponent (BE): A malicious adversary can choose not to increment its BE after a failed transmission attempt. Maintaining a constant BE prevents contention window size from being increased, thus increasing probability of channel access.

3) Random Number Generator (RNG) Tampering: Another way of increasing the odds of channel access is for a malicious adversary to modify its RNG in such a way that ensures that the back-off periods selected by the adversary are much smaller than those selected by legitimate nodes.

4) Back-off Countdown Omission: Misic *et al.* [5] describes an attack which involves the complete omission of the random back-off countdown by a malicious adversary. We consider this omission to be the same as the complete omission of the entire CSMA-CA protocol. The effect of this would be the ability of the adversary to transmit its packets more frequently than legitimate network nodes, thus causing collisions between the adversary's packets and legitimate network packets, resulting in the same DoS outcome as *Link Layer Jamming*.

D. Clear Channel Assessment (CCA) Manipulation

Misic *et al.* [5] describes two attacks which can be launched against the CCA procedure of the CSMA-CA protocol. CCA is the process of initiating packet transmission if the channel is sensed idle for 2 successive back-off periods. Two variants of the CCA manipulation attack can be defined as follows.

1) Clear Channel Assessment (CCA) Reduction: In this attack variant, if the adversary senses that the channel is idle for only 1 back-off period (not 2), it initiates packet transmission, giving channel access more quickly and frequently to adversaries than to legitimate network nodes.

2) Clear Channel Assessment (CCA) Omission: Rather than reduce the number of back-off periods during which CCA is performed, an adversary may choose to omit the CCA procedure altogether in order to immediately start transmitting whenever the random back-off countdown is over. This could potentially cause collisions if the channel is not idle, leading to a DoS effect as in *Link Layer Jamming*.

E. Same-Nonce Attack

Consider a node providing the access control service in secured operating mode. In this case, if two entries within this node's Access Control List (ACL) possess the same key and nonce, a malicious adversary obtaining the cipher texts pertaining to these two entries will be able to infer useful information about the transmitted data, as explained in [6].

F. Replay-Protection Attack

Replay-protection is an IEEE 802.15.4 mechanism which causes a node to drop a frame if its sequence number is equal to or less than the sequence number of a preceding frame received by that same node. An adversary can send frames with large sequence numbers to targeted legitimate nodes, causing frames with smaller sequence numbers from other legitimate nodes to be dropped [6].

G. Acknowledgment (ACK) Attacks

In IEEE 802.15.4 as well as in other types of networks, ACK frames are sent between network nodes in order to confirm successful frame transmission. For some types of

frames, an *Acknowledgment Request* field is present, which is set to 1 if an acknowledgment is required upon frame receipt, or 0 if no acknowledgment is required [2].

In this subsection, we explain two variants of the *ACK Attack*.

1) ACK Spoofing: An adversary can perform *Intelligent Link Layer Jamming*, as described in Subsection A.2, in order to prevent legitimate data from correctly being received by the receiver. The adversary then sends back a forged ACK on the receiver's behalf with the correct expected sequence number to the sender, thus preventing data retransmission by tricking the sender into thinking that the frame has successfully reached the receiver [7].

2) ACK Dropping: In this variant, although the transmitted data is correctly received by the receiver, *ACK dropping* uses *Intelligent Link Layer Jamming* to jam the true ACK that is sent back by the receiver to the sender. Unlike *ACK Spoofing*, the malicious adversary sends no forged ACK in place of the jammed ACK. As such, the sender and receiver nodes' power and bandwidth are wasted during retransmissions up to a maximum number of retransmissions [5].

H. Man-In-The-Middle (MITM) Attack

This attack is an extension of the *ACK Spoofing* variant of the *ACK Attack* described in Subsection G.1. Following the transmission of the forged ACK by the adversary to the sender node, the adversary also transmits an altered version of the original data frame to the receiver and receives a true ACK frame from the receiver by pretending to be the original sender. *ACK* and *MITM Attacks* are also referred to as *Interception Attacks* [10].

I. Guaranteed Time Slot (GTS) Attacks

In beacon-enabled networks, the PAN coordinator reserves Guaranteed Time Slots (GTS) within the Contention Free Period (CFP) of each superframe duration in order to guarantee channel access for network nodes running time-critical applications with real-time delivery, low latency, or specific bandwidth requirements. A maximum of 7 GTS slots can be assigned at any one time, with each GTS slot possibly occupying more than one superframe slot within the superframe's CFP. Allocation and deallocation of GTS slots are performed by the PAN coordinator on a first-come-first-serve basis [2]. *GTS Attacks* are launched against the network by misusing the GTS management scheme [8].

Since there is no method of verifying of sensor nodes' identifiers (IDs), Jung *et al.* [9] defines two categories of variants of the IEEE 802.15.4 *GTS Attack* as follows.

1) Existing Identities in the PAN: In this category, a *GTS Attack* is launched when malicious adversaries spoof the IDs of existing legitimate nodes in the PAN. Two variants for this category are defined in [9] as follows.

a) DoS Against Data Transmissions During CFP: This variant requires the adversary to passively eavesdrop on network traffic in order to collect information about the IDs of legitimate nodes and their allocated GTS slots. The adversary can then use this collected data to spoof the IDs of the legitimate nodes and to send GTS deallocation requests on their behalf to the PAN coordinator. This leads to the termination of channel access rights previously granted to the legitimate nodes during their previously assigned GTS slots.

b) False Data Injection: While the *DoS During CFP* variant collects information about the IDs of nodes that have already been allocated GTS slots by the PAN coordinator, *False Data Injection* collects information about the IDs of legitimate PAN nodes that have not yet been allocated any GTS slots during the superframe's CFP. Using the collected information, the adversary pretends to be one of the unallocated nodes by spoofing its ID and sends a GTS allocation request on its behalf to the PAN coordinator. Finally, the adversary injects false traffic into the network during its falsely assigned GTS slot.

2) Non-Existing Identities in the PAN: Rather than spoofing the IDs of legitimate nodes within the PAN, a malicious adversary can use its own or other non-existing IDs to conduct either of the two attack variants contained within this category [10].

a) DoS Against GTS Requests: For this variant, a malicious adversary collects information about the GTS list, which contains both allocated and free GTS slots. Following this, the adversary keeps sending GTS allocation requests to the PAN coordinator until all 7 slots in the GTS list are filled up. Contrary to the *False Data Injection* variant, no ID spoofing is involved, as the adversary sends allocation requests using its own or other non-existing IDs to the PAN coordinator.

b) Stealing Network Bandwidth: This attack variant is identical to the previous *DoS against GTS Requests* variant with the addition that the adversary also injects false data into the network during the assigned GTS slots. This variant is harder to detect that the previous *DoS against GTS Requests* variant because the PAN coordinator recognizes that the allocated slots are indeed being used for transmitting data, and thus, does not drop the allocated slots.

Sokullu *et al.* [8] identifies four additional variants of the *GTS Attack*. We include these additional variants within a category of our choosing, which we call *Interference During CFP*.

3) Interference During CFP: In this type of *GTS Attack*, a malicious adversary collects information about the beginnings and ends of GTS slots which have been assigned to legitimate network nodes by the PAN coordinator. The adversary then creates interference by using *Link Layer Jamming* during these assigned slots with the intent of corrupting ongoing transmissions. The four variants defined in [8], which fall into this category, are as follows.

a) One Intelligent Attacker (OIA): In the *OIA* scenario, a malicious adversary corrupts the communication with the maximum GTS slot length, either by corrupting only the GTS slot's first superframe slot, or by corrupting all of the superframe slots contained within the GTS slot.

b) One Random Attacker (ORA): In this scenario, a malicious adversary attacks the GTS slot of a randomly selected communication.

c) Two Intelligent Attackers (TIA): This attack variant is considered as an extension to the *OIA* attack variant, with one malicious adversary attacking the communication with the largest GTS slot length, and a second adversary attacking the communication with the second largest GTS slot length. This requires collaboration between the two adversaries.

d) Two Random Attackers (TRA): As an extension to the *ORA* scenario, two malicious adversaries can attack the GTS slots of two randomly selected communications. Due to the random nature of this attack, it is possible for both adversaries to target the same communication.

4) DoS Against CAP Maintenance: CAP maintenance involves the use of a number of preventative actions in order to ensure that the length of the CAP period of each superframe does not fall below a predefined threshold known as *aMinCAPLength* [2]. An adversary can launch an attack against CAP maintenance by constantly sending GTS requests, even when the superframe has no available capacity and/or the length of the CAP is about to fall below *aMinCapLength*. This causes the length of the CAP to momentarily fall below *aMinCAPLength*, thus reducing the amount of time which member nodes have in order to contend for channel access [2]. While this variant of the *GTS Attack* has not been previously mentioned in any references, its discovery is inspired by the brief statement made by Jung *et al.* [9] that preventative actions of CAP maintenance are ineffective if a malicious node constantly sends either GTS requests or data at the assigned GTS slots during the CFP.

J. PANId Conflict Attack

IEEE 802.15.4 defines a conflict resolution procedure, which is initiated when two PAN coordinators residing within the same Personal Operating Space (POS) have the same coordinator ID, also referred to as *PANId* [2]. A malicious adversary can abuse the conflict resolution procedure by transmitting fake *PANId* conflict notifications to the targeted PAN coordinator in order to initiate conflict resolution, thus momentarily delaying or even preventing communication between member nodes and the PAN coordinator [6].

K. Ping-Pong Effect

The *Ping-Pong Effect* is an attack which is launched with the aim of causing packet loss and service interruption, reducing node performance, and increasing energy consumption and network load. As per its name, this attack causes fast, repeated and undue handovers of nodes between the coordinators of different PANs.

Balarengadurai *et al.* [11] explains that a *Ping-Pong Effect* can be launched via the manipulation of one or both of the following two network parameters.

1) Membership Degree: A node switches to a new PAN coordinator if the membership degree to the new PAN coordinator is greater than its membership degree to its current PAN coordinator.

2) Election Possibility: A new node is elected as the PAN coordinator if its election possibility is higher than the election possibility of the current coordinator. Election possibility is determined with respect to factors such as mobility and remaining battery capacity.

L. Bootstrapping Attack

O'Flynn *et al.* [10] explains an attack which forces a targeted network node to become unassociated with its PAN at a time of the adversary's choosing by launching any of the PHY or MAC layer attacks aimed at causing DoS. The next time that the legitimate node wants to rejoin the network, the adversary either passively eavesdrops on the association process in order to collect valuable bootstrapping information that it can use to perform its own association with the PAN, or the adversary can perform a *MITM Attack* in order to intervene with and thus prevent the association of the legitimate node with the PAN.

M. Steganography Attack

Steganography Attacks create a hidden channel between collaborating adversaries in the network. This hidden channel can be used by adversaries to exchange information regarding the execution of new attacks against the network, or to monitor the network and thus warn other adversaries when launched attacks within the network are detected. The latter enables adversaries to stop executing their attacks just in time to remove suspicions and prevent detection by the network. Martins *et al.* [12] explains how *Steganography Attacks* can be launched by hiding information within the PHY and/or MAC frame fields of the 802.15.4 protocol.

III. Classification of IEEE 802.15.4 MAC Layer Attacks

The explained attacks cannot be classified using one single deterministic classification. Therefore, we present two classifications which include some of the most important methods of classifying IEEE 802.15.4 MAC layer attacks obtained from external references. Novel extensions to these classifications are also presented. Figure 1 illustrates both classification methods, including our proposed extensions, as well as the interrelationships between related attacks, which denote the attacks used to facilitate the launching of other attacks.

A. Classification A

Sokullu *et al.* [6] classifies IEEE 802.15.4 MAC layer attacks into the following three main classes.

1) Common to All MAC Layer Definitions: Link Layer Jamming can be launched against all MAC layer definitions of all existing standards. We extend this class of attacks by adding *Node-Specific Flooding*.

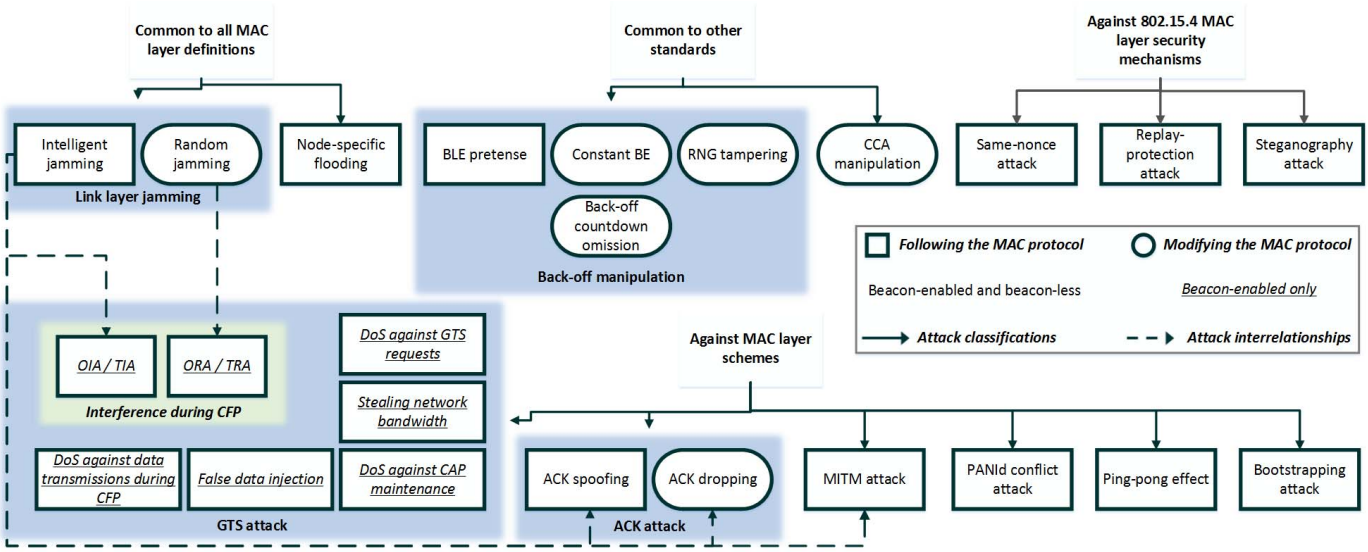

Fig.1. Classification of IEEE 802.15.4 MAC Layer Attacks

2) Common to Other Standards: Back-off Manipulation and *CCA Manipulation* attacks can be launched against both IEEE 802.15.4 Wireless Personal Area Networks (WPANs) and IEEE 802.11 Wireless Local Area Networks (WLANs) due to their similar CSMA-CA and Distributed Coordination Function (DCF) channel access protocols respectively.

3) Against 802.15.4 MAC Layer Security Mechanisms: This class contains specific variants of some general attacks applied against IEEE 802.15.4 MAC layer security mechanisms. *Same-Nonce* attack targets the access control service, and *Replay-Protection Attack* targets the replay protection mechanism. *Steganography Attacks* are also included.

In addition to the above three classes of attacks, we extend this classification by including the following additional class of attacks.

4) Against 802.15.4 MAC Layer Schemes: This class refers to attacks applied against IEEE 802.15.4 MAC layer schemes. Contrary to Sokullu *et al.* [6], we argue that acknowledgments are considered to be an implemented MAC layer scheme, and not a security mechanism. As such, we include *ACK* and *MITM Attacks* here. We also include the following additional attacks; *PANId Conflict Attack* targets the PANId conflict resolution procedure, *GTS Attacks* target the GTS management scheme, and *Ping-Pong Effect* and *Bootstrapping Attack* target PAN association.

B. Classification B

In this classification, we classify attacks with respect to conformance to MAC protocol rules and mode of network operation.

1) Conformance to MAC Protocol: Misic *et al.* [5] classifies attacks into those which either follow the MAC protocol to the letter, or modify its rules.

2) Mode of Network Operation: All MAC layer attacks can be launched against both beacon-less and beacon-enabled networks except for all *GTS Attack* variants, as GTS slots are only present during the CFP of each superframe in beacon -enabled networks.

IV. Comparative Analysis of IEEE 802.15.4 MAC Layer Attacks

In this section, we perform a detailed comparison between the attacks with respect to the following evaluation criteria.

A. Evaluation Criteria

1) DoS Intent: The primary intent of most MAC layer attacks is to cause a DoS against a specific part of or the entire network [8].

a) Exhaustion Attacks: One form of DoS involves the depletion of the already-constrained power, bandwidth, memory and/or storage resources of legitimate network nodes [11].

b) Collision Attacks: An adversary can corrupt legitimate packets by initiating transmission during ongoing legitimate packet transmissions [11].

c) Unfairness Attacks (also known as *Misbehavior Attacks* [6]): This attack ensures that an adversary is granted the same priority as or higher priority than legitimate nodes with respect to utilization of network resources, such as bandwidth and channel access. The latter causes starvation of legitimate nodes from network resources [11].

d) Sleep Attacks: A *Sleep Attack* manipulates a targeted node's duty cycle (the percentage of time during which the node remains in active state). If the attack causes the targeted node's duty cycle to increase above average, it is also referred to as a *Battery Exhaustion Attack* [13].

2) Security goal violation: Security goals are used to assess a WPAN's level of security.

B. Comparison Between IEEE 802.15.4 MAC Layer Attacks

Table I illustrates the comparison between IEEE 802.15.4 MAC layer attacks with respect to both DoS intent and primary security goal violation. We analyze each of the MAC layer attacks and their variants from a *Cause* and *Effect*

perspective. The *cause* (blue) of an attack is the primary intent with which the attack is launched, whereas the *effect* (black) of an attack refers to an unplanned repercussion of launching the attack in question.

Kumar *et al.* [4] defines two classes of security goals; primary and secondary. This paper only focuses on primary security goals, as no secondary goals are violated by any of the discussed attacks.

a) Data Confidentiality: Same-Nonce Attack is the only attack considered to violate data confidentiality, as it enables an adversary to decrypt ciphered network transmissions.

b) Data Integrity: We consider attacks that corrupt only the payload field of the frame, while preserving the value of the original frame's Frame Check Sequence (FCS) field, to violate data integrity. As such, *Steganography Attacks* are not considered to violate the integrity of network transmissions.

c) Data Authenticity: Attacks which involve the spoofing of legitimate node IDs violate authenticity.

d) Network Availability: Any attack variant which has at least one DoS intent as its *cause*, as illustrated in Table I, is considered to violate network availability.

V. CONCLUSION

This work constitutes a detailed survey on IEEE 802.15.4 MAC layer attacks. The purpose and operation of each attack and its *variants* were explained. A novel variant of the *GTS Attack*, *DoS against CAP Maintenance*, was proposed. Two classifications of the MAC layer attacks were presented. *Classification A* divided the attacks into four classes; common to all MAC layer definitions of all existing network standards, common to only a subset of other standards, launched against 802.15.4 MAC security mechanisms, and launched against implemented 802.15.4 MAC schemes. *Classification B* classified MAC attacks based on their conformance to MAC layer protocol rules and network mode of operation. Finally, a comparative analysis between all MAC layer attacks, as well as their multiple techniques and variants, was performed with respect to DoS intent and primary security goal violation.

REFERENCES

[1] Y. M. Amin, and A. T. Abdel-Hamid (2015). *Intrusion Detection in IEEE 802.15.4 Networks*. German University in Cairo: Cairo (Egypt). 2015:1.

[2] IEEE, *802.15.4-2006 – IEEE Standard for Information technology – Local and metropolitan area networks—Specific requirements—Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs)*, pp. 1-320, September 2006.

[3] S. C. Ergen, *ZigBee/IEEE 802.15.4 Summary*, September 2004, Retrieved April, 2015, from users.ece.utexas.edu/~valvano/EE345L/Labs/Fall2011/Zigbeeinfo.pdf.

[4] J. V. Kumar, A. Jain, and P. N. Barwal, *Wireless Sensor Networks: Security Issues, Challenges and Solutions*, International Journal of Information and Computation Technology (IJICT), vol. 4, no. 8, pp. 859–868, 2014.

[5] V. B. Misic, J. Fung, and J. Misic, *MAC Layer Security of 802.15.4-Compliant Networks*, IEEE International Conference on Mobile Adhoc and Sensor Systems, 2005.

[6] R. Sokullu, I. Korkmaz, O. Dagdeviren, A. Mitseva, and N. R. Prasad, *An Investigation of IEEE 802.15.4 MAC Layer Attacks*, n.d., Retrieved April 2015, from ube.ege.edu.tr/~dagdeviren/source/publications/wpmc07.pdf.

[7] P. Jokar, H. Nicanfar, and V. C. M. Leung, *Specification-based Intrusion Detection for Home Area Networks in Smart Grids*, IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 208-213, October 2011.

[8] R. Sokullu, O. Dagdeviren, and I. Korkmaz, *On the IEEE 802.15.4 MAC Layer Attacks: GTS Attack*, IEEE Second International Conference on Sensor Technologies and Applications (SENSORCOMM '08), pp. 673-678, August 2008.

[9] S. S. Jung, M. Valero, A. Bourgeois, and R. Beyah, *Attacking Beacon-Enabled 802.15.4 Networks*, Security and Privacy in Communication Networks, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 50, pp. 253-271, 2010.

[10] C. P. O'Flynn, *Message Denial and Alteration on IEEE 802.15.4 Low-Power Radio Networks*, 4th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pp. 1-5, February 2011.

[11] C. Balarengadurai, and Dr. S. Saraswathi, *Comparative Analysis of Detection of DDoS Attacks in IEEE 802.15.4 Low Rate Wireless Personal Area Network*, International Conference on Modelling Optimization and Computing, vol. 38, pp. 3855-3863, 2012.

[12] D. Martins and H. Guyennet, *Attacks with Steganography in PHY and MAC Layers of 802.15.4 Protocol*, 5th International Conference on Systems and Networks Communications (ICSNC), pp. 31-36, August 2010.

[13] F. Amini, Dr. J. Misic, and Dr. R. Eskicioglu (2008). *Simulation and Evaluation of Security and Intrusion Detection in IEEE 802.15.4 Network.* University of Manitoba: Winnipeg, Manitoba (Canada).

TABLE I. COMPARATIVE ANALYSIS OF IEEE 802.15.4 MAC LAYER ATTACKS

Attack	DoS Intent				Primary Security Goals			
	Exhaustion	Collision	Unfairness	Sleep	Confidentiality	Integrity	Authenticity	Availability
Link layer jamming	√	√	√	×	×	×	√	√
Node-specific flooding	×	√	√	×	×	×	√	√
BLE pretense, Constant BE, RNG tampering, CCA reduction	×	√ [11]	×	×	×	×	√	×
Back-off countdown omission, CCA omission	√	√ [11]	×	×	×	×	√	×
Same-nonce attack	×	×	×	√	×	×	×	×
Replay-protection attack	×	√	√	×	×	×	√	√
ACK spoofing attack	×	√	×	×	×	√	√	×
ACK dropping attack	×	√	√	×	×	×	√	√
MITM attack	×	√	×	×	√	√	√	×
PANId conflict attack	×	√	√	×	×	×	√	√
DoS against data transmissions during CFP	×	√	×	×	×	√	√	×
DoS against GTS requests	×	√	×	×	×	×	√	√
False data injection	×	√	×	×	√	√	√	√
Stealing network bandwidth	×	√	×	×	√	×	√	√
DoS against CAP maintenance	×	√	×	×	×	×	√	√
Interference during CFP	√	√	√	×	×	×	√	√
Ping-pong effect	×	√	√	×	×	×	√	√
Bootstrapping attack	×	√	×	×	×	×	√	√
Steganography attack	×	√	×	×	×	×	×	×