An Investigation on IEEE 802.15.4 MAC Layer Attacks

Radosveta Sokullu*, Ilker Korkmaz†, Orhan Dagdeviren‡, Anelia Mitseva§, Neeli R.Prasad§
*Department of Electrical and Electronics Engineering, Ege University, Izmir, Turkey
e-mail: radosveta.sokullu@ege.edu.tr
†Department of Computer Engineering, Izmir University of Economics, Izmir, Turkey
e-mail: ilker.korkmaz@ieu.edu.tr
‡Department of Computer Engineering, Izmir Institute of Technology, Izmir, Turkey
e-mail: orhandagdeviren@iyte.edu.tr
§Center for TeleInfrastructure, Aalborg University, Aalborg, Denmark
e-mail: {mitseva,np}@kom.aau.dk

***Abstract*— IEEE 802.15.4 has been established as a dominant MAC layer protocol for wireless sensor networks (WSNs). Recently the security concepts of sensor networks have quickly gained more significance because of two major factors: widening the range and variety of possible applications and increased implementation rate. Because the nodes are very resource-constrained, the attacks on these networks and detection of the attacks must carefully be considered. This paper dissects the known attacks on wireless sensor networks and also identifies two new attacks: PANId conflict attack, and Guaranteed Time Slot (GTS) attack taking as a basis the IEEE 802.15.4 MAC protocol for WSN. The attack evaluations are analyzed from the perspectives of the attacker and the network. A detection mechanism for PANId conflict attack is presented, and the simulation results for this attack implementation on ns2 are given.**

***Keywords*— IEEE 802.15.4 MAC, attack, wireless sensor networks, PANId conflict attack, GTS attack.**

I. Introduction

WSN is the short range wireless communication network of a huge collection of tiny sensor devices operating for various specific applications. Since the nodes are generally embedded in unrestricted environments, WSNs are prone to attacks. The nodes are unattended; they can be physically destroyed or reprogrammed.

An attack on a network is a defective action on the efficient operations of the whole system or a malicious invasion on a specific part of the network. An attacker is an adversary within the network that attacks with the aim of damaging some nodes of the network or gaining more selfish benefits on the provided services than the other legitimate users. An attacker may exploit protocol weaknesses to obtain network resources to his own benefit by depriving others or simply to cause trouble to the network. Such attacks can be carried at any layer, for example non respecting MAC access rules, routing strategy, or transport layer congestion control algorithm. The basic feature of attack and misbehavior strategies is that they are entirely unpredictable [1]. Reliable and timely detection of deviation from legitimate protocol operation is recognized as a prerequisite for ensuring efficient use of resources and minimizing performance losses in WSNs.

This paper presents a literature survey of the attacks on wireless sensor networks designed on IEEE 802.15.4 MAC layer protocol, and proposes two new attack scenarios. Further, ns2 implementation results of one of the proposed attack scenarios and its countermeasures are detailed. The paper is organized as follows: Section II covers the related work on attacks, Section III defines the new attacks identified by us, Section IV evaluates all attacks, and Section V concludes the paper.

II. Related work

This section surveys the known attacks in IEEE 802.15.4 WSNs. Some of the attacks (radio jamming and link layer jamming) are common to all MAC layer definitions. Others like back-off manipulation may also occur in IEEE 802.11 wireless networks due to some common properties in the MAC layer implementations. The rest (same-nonce attack, replay-protection attack, ACK attack) are specific variants of some general attacks applied on IEEE 802.15.4 MAC layer security mechanisms defined in the IEEE 802.15.4 standard[2].

A. Radio jamming

Jamming is basically creating radio interference that causes a denial of service on receiver or transceiver nodes. Radio jamming is the type of attack that can be accomplished through emitting a radio signal targeted at jamming a specific channel. According to Xu et. al. [3], the adversaries vary with respect to their use of different radio jamming attack strategies: constant jammer, deceptive jammer, random jammer, reactive jammer. The attacker nodes or compromised nodes bypass the MAC protocol in order to defect the negotiated MAC protocol use of communication through the legitimate nodes. Hence, it may be seen as a misbehavior attack (an attack to acquire selfish use of protocol) or even a denial of service (DoS) attack for 802.15.4 MAC due to its dependence on physical layer communication rather than link layer.

B. Link layer jamming

Link layer jamming is a more complicated type among the jamming attacks. An intelligent adversary, who wisely uses the link layer protocol logics, can be as defective as a blind radio jammer but consuming less energy. The two objectives of a jamming attacker are first to survive as long as it can, secondly to misbehave in order to frustrate the legitimate neighbors from gaining the medium. The motivation of this DoS attack is to attack the MAC layer at specific times to improve energy efficiency of attacker[4].

C. Back-off manipulation

In a network where many nodes, that use IEEE 802.11 Distributed Coordination Function (DCF), are trying to access the same physical medium simultaneously, the data being transmitted could be corrupted. In the DCF protocol, a sender listens to the channel before transmitting its packet. If the channel is found busy the sender will defer its access by an amount of time which is called *"back-off period"*. DCF gives the recent channel access to the contending node with the smallest back-off value. This value is randomly chosen from the range of the contention window which is enlarged exponentially for a node that finds the channel busy each time. An adversary node can take the advantage for channel access over legitimate nodes by not applying the protocol rules and constantly choosing a small back-off interval [5]. Since the legitimate nodes select the rule-based back-off intervals, their chance of channel access would reduce exponentially. The back-off manipulation is not only applicable to IEEE 802.11 wireless networks but can occur in IEEE 802.15.4 sensor networks due to their similar CSMA based protocols.

D. Same-nonce attack

In 802.15.4 specification, devices operating in secured mode and providing access control service maintain an access control list (ACL) that identifies the nodes to receive data from [6]. ACL entry format consists of the destination address, secured mode options, related key, and the nonce contents [7]. An ACL list of a sender may include two entries with the same key and same nonce. If the sender uses same keys and same nonces within two different transmissions, an adversary who can obtain these two different ciphertexts may retrieve useful information without the need of the key [7]. When two different data are enciphered as c_1 and c_2 using the same key and same nonce values, of which c_1=[$data_1$ XOR E_{key}(nonce)] and c_2=[$data_2$ XOR E_{key}(nonce)], an eavesdropper can obtain [$data_1$ XOR $data_2$] through computing [c_1 XOR c_2].

E. Replay-protection attack

Replay protection mechanism is done by checking the counter of a recent message with the previous obtained counter. If the recent counter is equal to or less than the previous one, then the frame would be rejected. In the IEEE 802.15.4 specification, the replay protection mechanism is provided, but it is subjected to replay-protection attack which can be accomplished by an adversary via sending many frames containing large counters to a legitimate receiver [6]. When another legitimate sender transmits a frame with a lower counter, it will be rejected according to replay protection procedure.

F. ACK attack

In the middle of a transmission between two legitimate users, an eavesdropper can listen to the un-encrypted sequence numbers of the frames. When the eavesdropper wants to prevent the legitimate receiver from getting a frame, it corrupts the frame by interferencing at the receive time. Then, the eavesdropper sends a fake ACK frame with the related sequence number to the sender in order to fool the sender as if the ACK was coming from the receiver [6].

III. Identified new attack scenarios

In this section we identify and describe two new attacks for IEEE 802.15.4 MAC layer: Personal Area Network (PAN) identifier conflict attack and Guaranteed Time Slot (GTS) attack.

A. PANId conflict attack

In 802.15.4 wireless sensor networks, a PAN in a personal operating space (POS) includes one PAN coordinator and a group of nodes. The members of a PAN know the PAN coordinator's identifier (PANId). If there exists more than one PAN coordinator operating in same POS, a PANId conflict could occur [8]. If such a PANId conflict occurs, the PAN coordinator may detect the conflict through its received beacons or one of the member nodes can notify the PAN coordinator on receiving signal from two PAN coordinators with same PANId. On notification, the PAN coordinator performs the conflict resolution procedure. This mechanism mainly covers the channel scans and coordinator realignment procedure that includes choosing a new PANId and broadcasting it to all PAN nodes. After resynchronization with beacons, the network is ready to communicate in a stable way, which implies that the conflict resolution is completed [2].

We propose an attack scenario in which an adversary device can frequently send fake conflict notification messages to the coordinator and oblige the coordinator to perform the conflict resolution procedure. An intelligent attacker, which is capable of easily generating PANId conflict notification commands by setting the related field in the message frames, can use these fake messages to prevent or greatly delay communication between devices and the PAN coordinator.

B. GTS attack

According to IEEE 802.15.4 standard, GTS is the portion of the superframe reserved for a specific device which provides contention free communication between the device and the coordinator in beacon enabled mode [2].

A possible attack scenario using the GTS interval can be described as follows: assume that the adversary, an intelligent attacker device, has achieved syncronization with the coordinator by receiving beacon messages. The adversary can learn the GTS times of the coordinator through extracting the GTS descriptor within beacon frame. The GTS descriptor indicates the length and the start of the GTS in the superframe [8]. After obtaining the allocated GTS times, the adversary can create interference at any of these moments. This interference will cause collision and corruption of the data packets between the legitimate GTS node and the coordinator. The collision occurring during the GTS period can be considered as a kind of DoS paradigm since these slots are assumed to provide collision-free communication.

IV. Evaluation

In this section we evaluate the attacks represented in the paper with respect to the attacker properties and the network dynamics.

A. Radio jamming

A constant jamming attack is the easiest approach among radio jamming techniques. The jammer continuously emits a radio signal in order to corrupt the communication between the receiver and the sender. From the point of the attacker, this method is the simplest one to implement since there is no constraint on jamming. However, the adversary, which is also a battery-limited sensor node in the network, consumes its energy unwisely. From the point of the network, since a jam signal is always available, it would be easier to detect that a part of the communication area is invaded. By comparing statistical dynamics such as signal strength with a threshold value, the network can detect the jamming attack in a fast energy-efficient manner.

A deceptive jammer that consumes as much energy as a constant jammer continuously emits regular packets rather than a radio signal. So, the receiver in the network can not easily understand whether the coming packets are sent by a legitimate node or not. Another weakness on the network is that all neighbors around the attacker switch to receiver mode and can not send or forward any packets.

A random jammer sends regular packets or a constant radio signal at random times. The attacker saves energy by switching between its sleeping and jamming modes randomly. The network would be less defected than the continuous jamming attack types in a fixed period of time. Nevertheless, the network would detect the attack in a longer time by measuring not only the signal strength but also the carrier sensing time and packet delivery ratio [3].

As the most effective jamming approach, reactive jamming is based on sensing the network activity. A reactive jammer stays quiet when the channel is idle and jams when it senses an activity in the communication area [3]. This approach is the most energy-efficient method, because the adversary does not consume its energy in the idle times of the network. So the attack is done in a more utilized way from the point of the intelligent attacker. Due to the attacker not being the only sender in the network, it is harder to detect the jamming node than the other jamming cases. The network might consider more advanced techniques such as mapping jammed area [3] rather than just observing the statistical network dynamics in order to detect such wise jamming attacks.

B. Link layer jamming

Link layer jamming which uses MAC layer semantics is a more complicated type of reactive jamming attacks. A link layer jammer not only switches between the sleeping and active modes but also adjusts its operations to the MAC layer rules of the participants in the communication. So, the jammer uses its total energy in an efficient manner [4]. According to the network, detection time for this type of attack delays nearly the same as in reactive radio jamming.

C. Back-off manipulation

An adaptive intelligent adversary, who aims to gain a selfish advantage over the network by manipulating its back-off value, behaves like a legitimate node when the congestion is low, misbehaves like an attacker otherwise [5]. While misbehaving or not, the adversary does not consume extra energy. This type of attack targets all neighbors of the attacker. Due to the attacker's channel invasion at misbehaving intervals, the neighbors can not gain the medium access, they can not send or forward any packets, which leads to packet drop. This attack is one of the most practical ones to be implemented in the networks using CSMA based MAC protocols, as in IEEE 802.15.4 networks. Radosevac et. al. [5] uses sequential probability ratio test (SPRT) to analyze the optimal attack detection times. According to the network dynamics, it is hard to differentiate a misbehaving node from a legitimate one.

D. Same-nonce, replay-protection, and ACK attack

These three attacks are rooted in the security services supported in IEEE 802.15.4 security mechanisms [2]. Rather then evaluating their detection procedures, it is more meaningful to prevent these attacks by modifying the provided security service, or the frame header structure [6]. On the other hand, if these attacks occur, they would explicitly defect the communication. Hence, these attacks are the vulnerabilities of the security services that need to be proactively prevented.

E. PANId conflict attack

In order to detect an attacker node that forges the PAN coordinator with PANId conflict messages in our attack scenario described in Section III, we propose that the coordinator checks two parameters: the total number of conflicts for any node and the maximum number of conflicts in a deterministic time interval. After detecting the attacker, PAN coordinator shall simply ignore any packets from this node at the MAC layer.

We have simulated the proposed attack and the detection approach implementation on ns2.31 [9]. ns2.31 comes with IEEE 802.15.4 MAC layer protocol in which a PANId conflict case is commented but not implemented [10,11]. However, generating PANId conflict notification command messages in the simulator is as simple as generating standard messages.

After implementing a notification procedure for a device node, the PANId handle procedure is constructed for the PAN coordinator device. Handling mechanism is based on first checking whether the conflict message is sent by a pre-known attacker reserved in a misbehavior list or the message is a real conflict alarm coming from a legitimate node. If it is decided that the message is a fake one, then the attacker will be put into the misbehavior list in order to disallow communication with this node in the future. If it is decided that there is a real PANId conflict in the network, PAN coordinator will establish the proposed handling mechanism as provided in IEEE 802.15.4 standards [2].

In the simulations, we have constructed an IEEE 802.15.4 star network with 5 and 10 devices respectively, of which one node is determined as PAN coordinator and some nodes are chosen as the attackers. Initially, all devices in this star topology scan the communication channels in order to associate with the PAN coordinator. Then, the attacker node(s) sends fake PANId conflict notification commands at randomly chosen times. During the simulation, the PAN coordinator applies the proposed handling mechanism after receiving a conflict notification.

In the simulated misbehavior scenarios, the factors that can effect the detection and conflict solution times are the number of attackers, the coordinator parameters, and the total number of nodes. However, the total number of nodes is not thought to be a decisive factor to effect the detection times; it causes the total realignment time to be postponed for all nodes.

In the experiments, the attack times for the attacker nodes are selected at random. Nevertheless, at least two criterions are considered before the experiments: the initial start time of the first attack and the interval time between the detection of a conflict and the end of the realignment procedure of this conflict. The first attack time is chosen at the 15^{th} second since all synchronizations should be completed by that time. The latter parameter, interval time, is observed as nearly 3 seconds. Therefore, the difference between the attack times for any two attackers should not be in the same range of (3-ϵ, 3+ϵ) where ϵ refers to the process of realignment message transmission that takes approximately 5-10 milliseconds. If any attacker sends a fake conflict message in any (3-ϵ, 3+ϵ) time duration in which the coordinator is sending realignment messages, the attacker could not receive the realignment message and would be orphaned which means the device loses contact with its PAN coordinator. This is not allowed in the scenarios. Moreover, any attack in (ϵ, 3-ϵ) duration would not be received by the coordinator. Such an attack is declared as ignored one, and is not handled. This case is allowed in the scenarios, indeed it is observed in the experiments that this kind of attack is ignored at the MAC layer. The handled ones of the received messages are declared as successful attacks. For all cases, including both single attacker and multiple attacker scenarios, overlapping attacks (any attacks accomplished in (ϵ, 3-ϵ) duration) are not successful and it is seen that they are ignored.

The three parameters of the coordinator are p_1, p_2, p_3 where the first parameter is the maximum number of conflicts for an attacker, and the second is the maximum number of conflicts in a duration time which is defined with the last parameter.

Considering the above statements, the detection time of misbehavior in the single or multiple attacker cases can be identified with a function depending on the coordinator parameters. f(p_1) in (1) defines the detection time of an attack that exceeds the maximum number of conflicts parameter; f(p_2, p_3) in (2) defines the detection time of an attack that exceeds the maximum number of conflicts in an interval. The minimum of f(p_1) and f(p_2, p_3) gives the attack detection time, as in (3).

$$f(p_1) = successful\_(p_1+1)^{th}\_attack\_time + \epsilon_2 \quad (1)$$

$$f(p_2,p_3) = successful\_(p_2+1)^{th}\_attack\_time \_in\_the\_last\_p_3\_duration + \epsilon_2 \quad (2)$$

$$detection\_time = min(f(p_1), f(p_2,p_3)) \quad (3)$$

It is assumed in (1) and (2) that all first attacks are accomplished after the time that the coordinator is synchronized with all nodes. ϵ_2 in (1) and (2) refers to the running time of the misbehavior checking algorithm, which decides a conflict coming from a legitimate node or a misbehavior node.

Three types of scenarios are dissected: single-attacker, double-attacker and triple-attacker within a fixed size star topology with fixed coordinator parameters. The results are given in Fig. 1 and Fig. 2.

In Fig. 1, three different attacker scenarios with fixed coordinator

P_1=4 P_2=2 P_3=20	Attack Times(s)											Misbehavior Type	Attack Solution Time
Single Attacker	15	19	27	*31*	*35*	*100*						2	27+ ϵ_2
	16	23	39	44	63	*71*						1	63+ ϵ_2
Double Attacker	15	19	27	*31*	*35*	*100*						2	27+ ϵ_2
	16	23	39	44	63	71						1	71+ ϵ_2
Triple Attacker	15	19	27	*31*	35	*100*						2	27+ ϵ_2
	16	23	39	44	63	71	81	96				1	71+ ϵ_2
	17	21	33	40	50	56	67	73	*80*	*85*	*95*	2	67+ ϵ_2

Fig. 1. Attack times v.s number of attackers

Double Attacker	Attack Times(s)											Misbehavior Type	Attack Solution Time
P_1=2 P_2=2 P_3=20	15	19	27	*31*	*35*	*100*						3	27+ ϵ_2
	16	23	39	44	*63*	*71*						1	44+ ϵ_2
P_1=3 P_2=2 P_3=20	15	19	27	*31*	*35*	*100*						2	27+ ϵ_2
	16	23	39	44	63	*71*						1	63+ ϵ_2

Fig. 2. Attack times v.s coordinator detection parameters

detection parameters are shown. The misbehavior types define the detection approaches where type 1 depends on maximum allowed conflict number for a legitimate node (p_1), type 2 depends on maximum allowed conflict number in an interval of time (p_2 conflicts in p_3 duration), and type 3 refers to the detection of both types of misbehaviors at the same time. The green colored and underlined values represent the successful attacks, the red colored and italic values represent the received but dropped conflicts that were sent by known attackers which are already in the misbehavior list of the coordinator. The attacks, for which values are not colored, are the overlapping attacks.

For the single attacker scenario in Fig. 1, first attacker is detected at 27s with type 2. Other attacks are ignored and dropped after this detection time. The detection time for misbehavior type 1 is at 63s for the second attacker. For the double attacker scenario, the first misbehavior node is detected at 27s with type 2 and the second attacker is detected at 71s with type 1. The first attack of the second attacker which is at 16s is ignored due to its overlapping with first attacker. For the triple attacker case, the detection of all misbehaviors is delayed to the 71s. These detection times will change according to the scenarios. However the detection times will be delayed proportional to the number of the attackers.

For the double attacker scenario with varying coordinator parameters (p_1,p_2, and p_3) in Fig. 2, the first attacker is detected with a different type of misbehavior at the same time as in Fig. 1. Other attacker scenarios are detected with the same type of misbehavior but at different times. Thus, the coordinator parameters can both affect the misbehavior type and the detection time. If the values of the parameters are decremented, the misbehavior will be detected earlier as shown in Fig. 2, but the chances of a false alarm will be increased accordingly.

All of the experiments above are implemented with 5 nodes. A 10-node implementation has been tested for the double attacker scenario and it was observed that the results were nearly the same as in Fig. 1 and Fig. 2. Considering the same given attack scenarios of the same number of attackers, attack times, and coordinator parameters on a star topology of any n nodes, the results are not expected to vary much. However, it should be pointed out that when the node number increases the realignment interval (ϵ) will increase which leads to more overlapping chances and higher orphaning probability following that the detection times will be delayed.

F. GTS attack

This attack needs GTS request and GTS allocation procedures that are still not implemented in ns2.31. That is why, this attack has not been simulated in our experiments so far. This attack requires that the adversary should synchronize with the coordinator in a fine-grained manner. The attacker must track all the beacon frames sent by the coordinator and obtain the GTS times. As a disadvantage from the point of view of the attacker, this initial procedure may take time prior to the attack. After synchronization, the attacker can utilize its energy efficiently by adjusting its sleeping times to the coordinator. The strategy of the GTS attacker is to apply 802.15.4 MAC layer semantics in order to attack adaptively by sending corrupting packets at the corresponding times. Due to this, the GTS attack can be categorized as a special variant of link layer jamming.

From the point of view of the network, the attacker can easily be detected in one case. This is the case when the adversary can emit regular packets in the GTS interval to corrupt the communication, but can not attack at the precise moments in the CFP slots due to the lack of exact synchronization. So, the coordinator can detect the attacker's ID by extracting the source field in the received packets. In other cases, in which the adversary emits jamming signals instead of regular packets or emits regular packets at precise moments, GTS attack is considered very hard to detect.

V. Conclusions

This paper presents a detailed investigation of IEEE 802.15.4 MAC layer protocol attacks. Radio jamming, link layer jamming, back-off manipulation, same nonce, replay-protection, and ACK attacks are surveyed. Moreover, two new attack scenarios are described: PANId conflict, and GTS attacks. All attacks are evaluated with respect to attacker attributes and the network dynamics.

After defining PANId conflict misbehavior, a proper solution for this problem by exploring the IEEE 802.15.4 specification is designed. The implementation of the suggested approach with the sample scenarios is built for ns2.31. To study its effects on the detection times in various attacker cases, the instance solutions depending on the detection metrics, and the evaluation of the results is presented.

It was observed that the coordinator detection parameters can both affect the misbehavior type and the detection time. If the PAN coordinator behaves in an aggressive manner, which corresponds to the small parameter values, not only the misbehaviors but also some false alarms can be detected. Suggested solution for PANId conflict involves the determined PAN coordinator characteristics with fixed parameters.

It was discussed in the paper that the GTS attack requires a fine-grained synchronization. The GTS attack was evaluated as a special case of link layer jamming, and considered as a very hard one to detect.

Future work directions will focus on some probabilistic approaches to design a proactive detection method for PANId conflict attack. Also, the simulation of the suggested GTS attack scenario will be investigated.

Acknowledgements

This paper presents work performed in the framework of the IST-4-027738 NoE CRUISE, which is partly funded by the European Union.

References

[1] S. Radosavac, J.S. Baras and I. Koutsopoulos, "A framework for MAC layer misbehavior detection in wireless networks", in Proceedings of the 4^{th} ACM Workshop on Wireless security, 2005, pp.33-42.

[2] IEEE Std 802.15.4TM-2003, IEEE Standard for Information technology-Telecommuncations and information exchange between systems-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).

[3] W. Xu, K. Ma, W. Trappe and Y. Zhang, "Jamming sensor networks: attack and defense strategies", IEEE Network, vol.20, no.3, 2006, pp.41-47.
[4] Y.W. Law, P. Hartel, J. den Hartog and P. Havinga, "Link-layer jamming attacks on S-MAC", in Proceedings of IEEE WSN'05, 2005, pp.217-225.
[5] S. Radosavac, A. A. Crdenas, J. S. Baras and G. V. Moustakides, "Detecting IEEE 802.11 MAC Layer Misbehavior in Ad Hoc Networks: Robust strategies against individual and colluding attackers", Journal of Computer Security, special Issue on Security of Ad Hoc and Sensor Networks, vol.15, no.1, 2007, pp.103-128.
[6] Y. Xiao, S. Sethi, H.-H. Chen and B. Sun, "Security services and enhancements in the IEEE 802.15.4 wireless sensor networks", in Proceedings of IEEE GLOBECOM'05, vol.3, 2005.
[7] N. Sastry and D. Wagner, "Security Considerations for IEEE 802.15.4 Networks", in Proceedings of the 2004 ACM workshop on Wireless security, 2004, pp-32-42.
[8] S. C. Ergen, "ZigBee/ IEEE 802.15.4 Summary", Internal Report to Advanced Technology Lab of National Semiconductor, 2004.
[9] K. Fall and K. Varadhan, "The ns manual", `http://www.isi.edu.tr/nsnam/ns/doc/ns_doc.pdf`, 2007.
[10] I. Ramachandran, A. K. Das and S. Roy, "Analysis of the contention access period of IEEE 802.15.4 MAC", Journal of ACM Transactions on Sensor Networks, vol.3, no.1, 2007.
[11] J. Zheng and M. J. Lee, "A Comprehensive Performance Study of IEEE 802.15.4", IEEE Press, 2004.