On the IEEE 802.15.4 MAC Layer Attacks: GTS Attack

Radosveta Sokullu[1], Orhan Dagdeviren[2], Ilker Korkmaz[3],
[1]*Department of Electrical and Electronics Engineering, Ege University, Izmir, Turkey*
radosveta.sokullu@ege.edu.tr
[2]*Department of Computer Engineering, Izmir Institute of Technology, Izmir, Turkey*
orhandagdeviren@iyte.edu.tr
[3]*Department of Computer Engineering, Izmir University of Economics, Izmir, Turkey*
ilker.korkmaz@ieu.edu.tr

Abstract

In the last several years IEEE 802.15.4 [1] has been accepted as a major MAC layer protocol for wireless sensor networks (WSNs) and has attracted the interest of the research community involved in security issues as the increased range of application scenarios bring out new possibilities for misuse and taking improper advantage of sensor nodes and their operation. As these nodes are very resource restrained such possible attacks and their early detection must be carefully considered. This paper surveys the known attacks on wireless sensor networks, identifies and investigates a new attack, Guaranteed Time Slot (GTS) attack, taking as a basis the IEEE 802.15.4 MAC protocol for WSN. The GTS Attack is simulated with different scenarios using ns-2 and the results are evaluated both from the point of view of the attacked and the attacker.

1. Introduction

Wireless Sensor Networks (WSNs) have many potential applications. In the ubiquitous environment enhanced with actuator capabilities they can materialize the interface between people and the environment by establishing a context for a great variety of applications ranging from environmental monitoring to assisted living and emergency measures and transport. In many of these scenarios, WSNs are of interest to adversaries and are easily prone to attacks as they are usually deployed in open and unrestricted environments. In many cases single nodes might be unattended and can be even physically destroyed or reprogrammed.

An attack on a WSN in general is defined as a defective action on the efficient operations of the whole system or a malicious invasion on a specific part of the network [2]. The attacker can be an adversary within the network that attacks with the aim of damaging some nodes of the WSN or gaining more selfish benefits on the provided services than the other legitimate users. On the other hand the attacker may exploit protocol weaknesses to obtain network resources to his own benefit by depriving others or simply to cause disrupt in the operation of the network. The basic feature of attacks and misbehavior strategies is that they are entirely unpredictable [3]. Early definition and investigation of possible attacks and misbehavior patterns can provide valuable insight into reliable and timely detection which is a main prerequisite for ensuring proper operation and minimization of performance losses in WSNs.

In this paper a new type of MAC layer attack is defined, called the Guaranteed Time Slot (GTS) attack, which is based on the inherent properties of the IEEE 802.15.4 superframe organization in beacon-enabled operational mode for WSNs. The sequence of communication for realizing a GTS attack is presented, four different possible attack scenarios are defined and their ns-2 implementation results are presented and evaluated. From here on the paper is organized as follows: Section 2 covers the related work on attacks in WSN and their definitions, Section 3 identifies the new attack and presents the evaluation from the point of view of the attacker and the attacked taking into consideration both incurred damage and related energy consumption and finally Section 4 concludes the paper.

2. Related work

The known attacks in IEEE 802.15.4 WSNs can be classified into different categories according to different taxonomical representations. In this section the attacks for wireless sensor networks are categorized with regards to the different OSI layers whose operation and functions are attacked, destroyed or damaged, such as physical layer, MAC layer attacks, or routing layer attacks [4].

Physical layer attacks cover mainly the radio jamming or signal jamming modifications aiming to corrupt the communication within the channel due to frequency interferences. If jamming is handled as just emitting signals instead of sending packets, it is called radio jamming at the physical layer.

MAC layer attacks have attracted a lot of interest and there are a number of studies in this respect [2, 3, 5, 6]. MAC layer attacks are mainly targeted at the IEEE 802.15.4 data link layer specifications to achieve denial of service (DoS). Attackers generally aim to disrupt the channel using IEEE 802.15.4 procedures or to consume the channel resources unfairly through modifying the IEEE 802.15.4 protocol definitions in a selfish and malicious manner. In the following we present a brief description of some various IEEE 802.15.4 MAC layer attack types.

Jamming attack is basically constructing radio interference to cause a DoS on transmitting or receiving nodes. Xu et. al. [7] classified the jammers as constant, deceptive, random, and reactive according to their radio jamming strategies. Link layer jamming is fundamentally creating collision at the link layer by jamming packets rather than signals. An intelligent jammer that knows the link layer protocol logics misbehaves in the channel to deprive the legitimate users from gaining access to the medium. Rather than a blind jammer that emits signals or useless packets randomly without knowing the protocol logics, an intelligent jammer, from the point of the energy usage, aims to attack at specific times to preserve its energy [8]. Back-off manipulation is defined as selfishly and constantly choosing a small back-off interval in IEEE 802.11 Distributed Coordination Function (DCF) rather than applying the rules of the protocol for choosing a random back-off period [6]. Back-off manipulation is applicable to both IEEE 802.11 wireless networks and IEEE 802.15.4 wireless sensor networks due to their similar CSMA-CA based protocols. Same-nonce attack is related to the access control lists (ACL) identifying the nodes that data can be received from [9]. In order to be used in an encrypted transmission, ACL entry includes the destination address, the key, the nonce and option fields. If the sender uses the same key and nonce pairs within two transmissions, an adversary obtaining those ciphertexts may retrieve useful information [10]. Replay-protection attack targets the replay protection mechanism provided in IEEE 802.15.4 specification. This mechanism is used to accept a frame by checking whether the counter of the recent message is larger than the previous one. If an adversary sends many frames with large counters to a legitimate node, the legitimate user using the replay protection mechanism will reject the legitimate frames with small counters from other nodes [9]. ACK attack [9] can be accomplished by eavesdropping the channel. An eavesdropper, firstly, may block the receiver node from taking the transmitted packet, then, can mislead the sender node by sending a fake ACK that it comes from the receiver. PANId conflict attack [2] creates a fake conflict within a Personal Area Network (PAN). The members of a PAN know the PAN coordinator's identifier (PANId). If there exist more than one PAN coordinator operating in same Personal Operating System (POS), a PANId conflict occurs [1]. An adversary may send fake PANId conflict notification messages to PAN coordinator in order to make PAN coordinator execute conflict resolution procedure, which delays the communication between the PAN coordinator and the legitimate nodes [2].

Routing layer attacks are usually designed to hinder the route selection mechanism or routing strategy. A routing layer attacker possibly attacks the operation at the network layer at route discovery time, or at route selection time, or after the establishment of the routes [5]. For a wireless sensor network, an example for the routing layer attack on route discovery process is the fake route information attack providing incorrect routing data to the network [11]. Some attacks on routing selection processes are i.) HELLO flood attacks [12] to convince the receiving nodes that the attacker is within one-hop transmission range indeed the attacker has a high-power transmission and is far away, ii.) sinkhole attacks [12] to attract the neighboring nodes of an attacker to forward their packets through the attacker, iii.) wormhole attacks [13], by at least two negotiated attackers supporting tunneling the packets within the low-delay path established between each other, to fool the legitimate users for relaying the packets earlier, iv.) sybil attacks [14] providing more than one different identifications to the network to make the attacker be more possibly selected on many routes. An example for the attacks on established routes is blackhole attack [15] causing the node to drop all or selectively some received packets. More details about routing layer attack types can be found in [11].

3. GTS attack

3.1. Definition of Guaranteed Time Slots and their assignment

In the IEEE 802.15.4 standards [1], GTS slots are defined as part of the superframe for collision free transmission. Each slot is exclusively dedicated to a single device. A device must track beacons in order to request and allocate a GTS slot. The PAN coordinator decides whether to accept a GTS allocation of a device and may give more than one slot if there are available slots. There are 7 slots provided for GTS transmission in the contension free period (CFP) of the superframe. The GTS allocation policy is first-come-first serve and GTS slots are located after the contension access period(CAP). Figure 1 shows the usual communication sequence of a GTS slot allocation scenario.

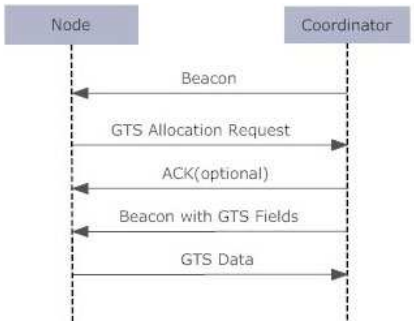

Figure 1. Communication sequence in GTS allocation.

First of all, the node must receive the beacon successfully in order to synchronize with the coordinator. After receiving the beacon, the node can communicate with the coordinator in CAP. Secondly, the node sends a GTS Allocation request to PAN coordinator. The GTS request message includes the length and direction. The GTS direction can be defined as either transmit or receive. On receipt of this command, the PAN coordinator may send an ACK to indicate the successful reception of GTS request. Then, the PAN coordinator checks for available slots in the current superframe within *aGTSDescPersistenceTime* superframes time. If there are available slots, new GTS information is included in the following beacon. The GTS requesting node receives the beacon and extracts the GTS transmission time if it is inserted by the PAN coordinator. In this case, the GTS transmission is successfully achieved as seen in Figure 1. If no GTS descriptor is found in the superframe, the node notifies the next upper layer of failure. The device can deallocate its GTS Slot in the same way as seen in Figure 2.

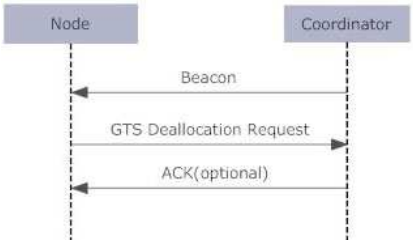

Figure 2. Communication sequence in GTS deallocation.

The above mentioned GTS management including request, allocation and deallocation is based on IEEE 802.15.4 explicit standards [1]. In addition to this procedure, some modified GTS allocation schemes have also been proposed. Ji et. al. [16] proposed an efficient GTS allocation algorithm for IEEE 802.15.4 that is capable of traffic analysis. Their GTS allocation scheme is based on packet arrival rate and number of devices in the network. When devices are transmitting, the ones with the higher packet transmission rate can cause more collisions and longer delay compared to ones with the lower rate. So, their scheme allocates the GTS slots to devices with the higher packet rates. The proposed GTS algorithm also uses the number of nodes due to at most 7 GTS slots being ready for allocation. Ji et. al. [16] constructed a 17-node IEEE 802.15.4 star topology in order to compare their proposed GTS allocation machanism with the standard one. By tracing the packet delivery rates, it is shown that their proposed scheme achieves 16% higher throughput than the standard one. Additionally, the amount of dropped packets caused by collisions is decreased significantly. By tuning the algorithm's parameters, they reach a 18% improvement on average throughput.

One of the basic disadvantage of the standard GTS management scheme is that the number of nodes having GTS slots is limited by 7. So, the GTS slots can be quickly consumed by a few number of nodes and devices with low data rates can cause the underutilization of the GTS resources. To overcome these problems, Koubaa et. al. [17, 18] proposed a GTS allocation approach, which is based on the idea that a slot can be used by more than one node. By considering the arrangement of GTS request arrivals with traffic specifications and the delay parameters, their algorithm makes a decision about the slot sharing policy among the nodes sending requests. They provide a kind of round-robin scheduling mechanism to prevent starvation, however they indicate that some modified scheduling schemes can be used. They implemented the proposed GTS algorithm with nesC on micaZ platforms. Their experimental test bed includes 1 PAN coordinator and 7 motes which are located under the transmission range of the PAN coordinator. The experiment results show that this implicit GTS management mechanism, i-GAME, is more efficient in bandwidth utilization than the explicit one defined in IEEE 802.15.4 standard.

3.2. Identified GTS attack

GTS slots create a vulnerable point which can allow an attacker to disrupt the communication between a device and its PAN coordinator. A possible attack scenario using the GTS interval is illustrated in Figure 3. Assume that all the nodes as well as the adversary, which is an intelligent attacker device, have achieved synchronization with the coordinator by receiving beacon messages. A legitimate node may request a GTS slot by sending a GTS request command to the PAN coordinator including the GTS descriptor. The PAN coordinator may respond with an optional ACK for

this GTS request. Meanwhile the coordinator handles the GTS request. The coordinator may accept the GTS request and allocate demanded GTS slot(s) or may reject it. The accepted requests are announced in the following beacon message broadcasted to all nodes. The adversary can learn the GTS slot times through extracting the GTS descriptor(s) from the beacon frame. 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.

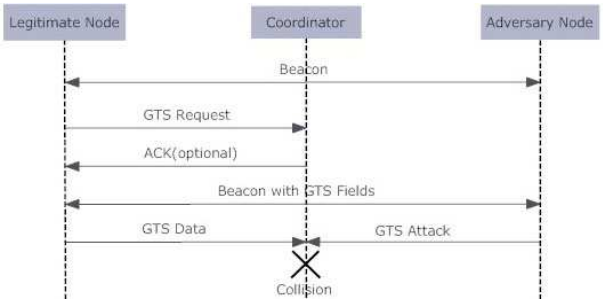

Figure 3. Communication sequence in GTS attack scenario.

3.3. Evaluation

We have simulated the proposed GTS attack implementation on ns2.31 [19]. ns2.31 comes with IEEE 802.15.4 MAC layer protocol in which GTS data structures are defined but GTS management methods are not implemented [20, 21]. In the simulations, we have implemented and used the explicit GTS management mechanism defined in IEEE 802.15.4 MAC layer standard [1].

Two types of attackers are defined in the simulations: intelligent attacker and random attacker. An intelligent attacker aims at corrupting the communication in the GTS slot with maximum length in the CFP, whereas a random attacker randomly chooses a GTS slot to be attacked. Attacking to a slot, which is allocated for communication between the PAN coordinator and a legitimate user, can be achieved by creating a collision through jamming or sending messages within that slot. In our simulations, both attackers corrupt the communication by sending a message to the coordinator at the starting time of the selected GTS slots.

A star network with ten nodes has been simulated, of which at most two attackers are on duty. Four types of scenarios are defined: "one intelligent attacker" (OIA), "one random attacker" (ORA), "two intelligent attackers" (TIA), and "two random attackers" (TRA). It is expected that, for the ORA scenario, the adversary attacks the allocated slot of an average length communication. In the case of TRA scenario, two attackers may attack two different communications or may attack the same communication, in which case the energy of the attackers is consumed to unconsciously corrupt the same node communication. In contrast to this, an intelligent attacker can use its energy in an efficient manner by attacking the first slot of the communication that has the maximum length in slots. For the TIA scenario, the adversaries can cooperatively attack the nodes as one of them attacking the maximum length communication (with the maximum number of slots allocated) and the other attacking the communication with the second maximum length. For this last scenario, the common goal of the attackers is to cause maximum possible decrease in bandwidth utilization within the CFP period.

Table 1. GTS request schedule.

NodeID	*Request Length(slots)*	*Request Time(s)*
7	3	25
8	5	28
6	2	31
4	1	35
5	1	40

The predetermined GTS request schedule of the nodes used in the simulations is given in Table 1. All of these requests except the request of node 8 are accepted by the PAN coordinator, and it is observed that the accepted requests are announced in the GTS field attribute of the following beacons. Nodes 1 and 2 are selected as intelligent attackers, nodes 3 and 9 are selected as random attackers. The simulation results are gathered for 60s where the beacon interval is set to 0.98304s. The number of total attack messages sent, and corrupted slots for four different scenarios of OIA, ORA, TIA and TRA respectively are given in Table 2.

In the first scenario, node 1 corrupts 35 different communications each with 3 slot length of node 7 causing 105 slot corruptions. It means that, 105 out of 208 slot-time data communication is prevented by the attack. Assuming all other parameters equal, this prevention leads to 105/208 (50.48%) decrease in bandwidth utilization of CFP period. Node 3 corrupts 35 different communications with random slot lengths leading to 69 slot corruptions in the second scenario. So, the utilization decrease in the second case is 33.17%. In the third case, two attackers totally broadcast 64 attack messages that result in 163 corruptions leading

Table 2. The number of attack messages and corrupted slots.

Scenario No	*Attack Messages*	*Corrupted Slots*
1	35	105
2	35	69
3	64	163
4	70	92

to a 78.36% decrease in utilization. The two random attackers in the fourth scenario totally corrupt 92 slots using 70 attack messages and decrease the utilization by 44.23%. Depending on the corrupted slots per attack messages, the best scenario is the first one, the worst scenario is the fourth one. Depending on the corrupted slots per unit time, the best scenario is the third one, the worst scenario is the second one. Consequently, the intelligent attack method causes more damage to the sensor network communication than the random attack, and cooperating attackers decrease bandwidth utilization in CFP period more than a single attacker.

The attackers are also compared for their energy consumptions in the attacks. ns-2 supports the simulation of the energy use of the sensor nodes, therefore the energies of the attackers have been traced within the simulations. Using the scenarios in Table 1, the energy consumptions of one intelligent attacker, one random attacker, two intelligent attackers, and two random attackers during their 60-second attack period is plotted in Figure 4. Figure 4 includes the consumed energies of the attackers for corrupting the communication slots. The energy exhaustion for each corrupted communication is calculated and recorded at the attacker nodes by subtracting the current traced energy levels from their previous values after each attack. As seen in Figure 4, the slopes of the intelligent attackers' energy consumption curves are lower than the ones of the random attackers'. Therefore, intelligent attackers consume less energy per corrupted slot than random attackers.

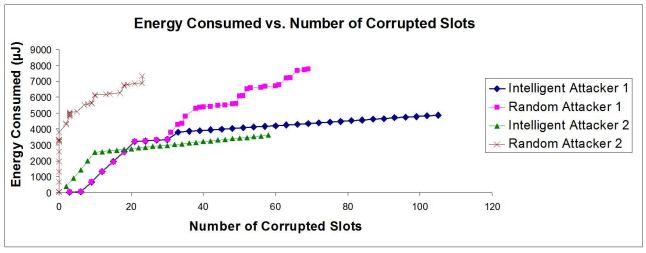

Figure 4. Energy consumed vs number of corrupted slots.

Neither the intelligent attacker nor the random attacker can be easily detected in GTS attack cases. Since the attackers are synchronized with the PAN coordinator in a fine-grained manner, the attack messages, which reveal collisions in the channel, cannot be received by the coordinator. Therefore, the coordinator can not perceive the ID of the attacker. However, if the synchronization between the attacker and the PAN coordinator is not fine-grained but still allowing to communicate with a small drift in the attacker's clock, 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. So, the coordinator may be able to 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.

4. Conclusions

This paper investigates WSN attacks including a brief survey of physical layer, MAC layer, and routing layer attacks. Furthermore, a new IEEE 802.15.4 MAC layer attack, the GTS attack, is defined and evaluated with respect to intelligent and random attacker behavior scenarios.

Based on the definition of the GTS attack, a sample communication sequence of this attack, exploring the IEEE 802.15.4 specification, is designed. It is shown that a GTS attack is possible. The implementation of the suggested approach with different scenarios is built using ns-2.31. To study their effects on the communication process during the CFP periods, the number of total corrupted slots and the number of total collisions are analyzed in various attacker cases, and the bandwidth utilization and energy consumption evaluations of the results are presented.

It is observed that the intelligent attacker can achieve an important decrease up to 75% in bandwidth utilization during the CFP period communication. Also, from the viewpoint of the attacker, an intelligent GTS attacker uses the energy much more efficiently than a random GTS attacker. Moreover, the intelligent attack method causes more damage to the sensor network communication compared to the random attack method.

Future work directions will focus on tunning different parameters in the GTS attack scenarios. The detection probability will be investigated when there is a lack of fine-grained time synchronization between the PAN coordinator and the GTS attacker. Additionally, a GTS-based application will be simulated and analyzed under GTS attack conditions.

References

[1] 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).

[2] R. Sokullu, I. Korkmaz, O. Dagdeviren, A. Mitseva, and N.R. Prasad, "An Investigation on IEEE 802.15.4 MAC Layer Attacks", *in Proc. of WPMC*, 2007.

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

[4] H. Chan and A. Perrig, "Security and privacy in sensor networks", *IEEE Computer*, IEEE, vol. 36, no. 10, 2003, pp. 103-105.

[5] V.B. Misic, J. Fung, and J. Misic, "MAC Layer Attacks in 802.15.4 Sensor Networks", *Security in Sensor Networks*, Auerbach Publications, Taylor & Francis Group, 2007, pp. 27-44.

[6] 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.

[7] 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.

[8] Y.W. Law, P. Hartel, J. den Hartog, and P. Havinga, "Link-layer jamming attacks on S-MAC", *in Proc. of IEEE WSN*, 2005, pp. 217-225.

[9] Y. Xiao, S. Sethi, H.H. Chen, and B. Sun, "Security services and enhancements in the IEEE 802.15.4 wireless sensor networks", *in Proc. of IEEE GLOBECOM*, vol.3, 2005.

[10] N. Sastry and D. Wagner, "Security Considerations for IEEE 802.15.4 Networks", *in Proc. of the ACM Workshop on Wireless Security*, 2004, pp. 32-42.

[11] Y.C. Wang and Y.C. Tseng, "Attacks and Defenses of Routing Mechanisms in Ad Hoc and Sensor Networks", *Security in Sensor Networks*, Auerbach Publications, Taylor & Francis Group, 2007, pp. 3-25.

[12] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", *IEEE SNPA*, vol. 1, 2003, pp. 113-127.

[13] Y.C. Hu, A. Perrig, and D.B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks", *in Proc. of IEEE INFOCOM*, vol. 1, 2003, pp. 1976-1986.

[14] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: analysis & defenses", *in Proc. of IPSN*, vol. 1, 2004, pp. 259-268.

[15] H. Deng, W. Li, and D.P.Agrawal, "Routing security in wireless ad hoc networks", *IEEE Communications Magazine*, IEEE, vol. 40, no. 10, 2002, pp. 70-75.

[16] Y. Ji, W. Park, S. Kim, and S. An, "Efficient GTS Allocation Algorithm for IEEE 802.15.4", *in Proc. of ICCS*, 2007, pp. 869-872.

[17] A. Koubaa, M. Alves, and E. Tovar, "i-GAME: an implicit GTS allocation mechanism in IEEE 802.15.4 for time-sensitive wireless sensor networks", *in Proc. of ECRTS*, 2006.

[18] A. Koubaa, M. Alves, and E. Tovar, "Time Sensitive IEEE 802.15.4 Protocol", *Sensor Networks and Configuration*, Springer, 2007, pp. 19-49.

[19] K. Fall and K. Varadhan, "The ns manual", `http://www.isi.edu/nsnam/ns/doc`, 2007.

[20] J. Zheng and M.J. Lee, "A Comprehensive Performance Study of IEEE 802.15.4", *Sensor Network Operations*, IEEE Press, Wiley Interscience, 2006, pp. 218-237.

[21] I. Ramachandran, A.K. Das, and S. Roy, "Analysis of the contention access period of IEEE 802.15.4 MAC", *ACM Transactions on Sensor Networks*, vol.3, no.1, 2007.