GTS Attack: An IEEE 802.15.4 MAC Layer Attack in Wireless Sensor Networks

Radosveta Sokullu
Dept. of Electrical and Electronics Eng.
Ege University
Izmir, Turkey
radosveta.sokullu@ege.edu.tr

Ilker Korkmaz
Dept. of Computer Eng.
Izmir University of Economics
Izmir, Turkey
ilker.korkmaz@ieu.edu.tr

Orhan Dagdeviren
Dept. of Computer Eng.
Izmir Institute of Technology
Izmir, Turkey
orhandagdeviren@iyte.edu.tr

***Abstract*—In the last several years IEEE 802.15.4 has been accepted as the major MAC layer protocol for wireless sensor networks (WSNs). It has attracted the interest of the research community involved in security issues because the increased range of application scenarios brings 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.**

Keywords—IEEE 802.15.4 MAC; *wireless sensor network attacks*; *Guaranteed Time Slot*; *GTS attack*

I. Introduction

Through the developments on micro electro-mechanical systems (MEMS) to be used as sensor devices [2], many ad-hoc network researchers have been focusing on Wireless Sensor Networks (WSNs). WSNs have many potential applications [3]–[7]. In the ubiquitous environment, WSNs enhanced with actuator capabilities 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. 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 to work in a way different than their usual operations.

An attack on a WSN in general is defined as a defective action on the efficient operation of the whole system or a malicious invasion on a specific part of the network [11]. The attacker, as Wood et. al. [8] adapted from the National Information Systems Security Glossary [9], is mainly the originator of an attack and is used synonymously with the term adversary. The attacker can be an adversary within the network that attacks with the aim of damaging some nodes or gaining more selfish benefits on the provided services than the other legitimate users of the WSN. On the other hand the attacker may exploit protocol weaknesses to obtain network resources to his own benefit by depriving others or may simply try to cause disrupt in the operation of the network. The basic feature of attacks and misbehavior strategies is that they are entirely unpredictable [12]. 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. These issues motivated us to research on WSN attacks. Our goals are to survey the important WSN attacks categorized according to their target layers and to identify possible new attack types.

This paper extends the work in [1] and dissects the Guaranteed Time Slot (GTS) attack. 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 II covers the related work on attacks in WSN and their definitions, Section III discusses the IEEE 802.15.4 MAC layer security issues and Section IV 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. Finally Section V concludes the paper.

II. 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. Chan et. al. [13] made this categorization mainly based on physical layer attacks, MAC layer attacks, and routing layer attacks; in addition to this, Raymond et. al. [14] has surveyed the denial-of-service attacks based on all protocol layers including transport and application layers.

A. Physical Layer Attacks

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 carried out by emitting just signals instead of

sending packets, it is called radio jamming at the physical layer.

Another physical layer attack is *node tampering* [8], [14], [15]. An attacker, who has a physical direct access to the nodes, may tamper with the nodes. In this way, the attacker can interrogate a node's memory, can capture private information including the cryptographic data, can compromise the node's function, or can totally destruct the hardware [8], [14], [15].

Regarding the physical security concerns including physical accesses to sensor nodes or other network resources, wireless sensor networks are very vulnerable. Since sensor nodes are generally distributed in a wide area or are used in great numbers to realize a fault tolerant application, destructive physical accessibility to some single sensors, due to its perceivability, is not considered as very harmful for the whole network operation.

B. MAC Layer Attacks

MAC layer attacks have attracted a lot of interest and there are a number of studies in this respect [11], [12], [17], [29]. IEEE 802.15.4 MAC layer attacks target the data link layer specifications to achieve mainly denial of service (DoS). Attackers generally aim to disrupt the specified IEEE 802.15.4 procedures for channel use 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 IEEE 802.15.4 MAC layer attack types.

Jamming is basically constructing radio interference to cause a DoS on transmitting or receiving nodes. Xu et. al. [18] 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 intentionally misinterprets the channel use rules 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 [19]. *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 [17]. 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 [20]. 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 [21]. *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 [20]. *ACK attack* [20] 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* [11] 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 [10]. 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 [11].

C. Routing Layer Attacks

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 [29]. For a wireless sensor network, an example of a routing layer attack on the route discovery process is the *fake route information attack*, which provides incorrect routing data to the network [22]. Some attacks on routing selection processes are i.) *HELLO flood attack* [23] in which the receiving node is convinced that the attacker is within one-hop transmission range when in fact the attacker is carrying out high-power transmission and is far away, ii.) *sinkhole attack* [23]that convinces the attacker's neighboring nodes to forward their packets through the attacker, iii.) *wormhole attack* [24], realized by at least two negotiating attackers using tunneling the packets through a low-delay path established between them to fool the legitimate users for relaying the packets earlier, iv.) *sybil attack* [25] in which the attacker provides more than one different identifications to the network in order to increase his probability of being selected on many routes. An example of the attacks on established routes is *blackhole attack* [26] causing the node to drop all or selectively some received packets. More details about routing layer attack types can be found in [22].

D. Transport Layer Attacks

According to the OSI protocol functions, transport layer provides the data transfer through the management of end-to-end connections. In this manner, Wood et. al. [8] describe the flooding and the desynchronization approaches as two important denial of service attacks.

Based on the classical *TCP SYN flood* [27] approach, an attacker may send many connection requests to a legitimate node.The node's resources, mainly its memory, shall be con-

sumed to maintain those unnecessary connections unless there is a defense mechanism specified in the protocol.

An active connection established between two legitimate nodes can be deteriorated by the *desynchronization attack* [8]. An attacker listening to the connection between two end points can forge messages to either of them in order to make the receiver node request retransmission of related messages from the sender. If the attacker can attack the messages carrying connection specific control data at proper times, the synchronization between the two end points might be lost.

E. Application Layer Attacks

An interesting case for the application specific sensor networks are the attacks targeting the application itself, including the application data as well as the privacy concerns of the nodes/devices participating in the application. The wireless sensor network attacks targeted at the application layer may be viewed in many and various aspects as the sensor applications constitute a very large variety, from environmental monitoring to medical, military and target tracking applications. Among those attacks, Raymond et. al. [14] discussed the *overwhelming attack* and the *path-based DoS attack*, which aim denial of service.

The overwhelming attack is related to event-based monitoring applications, such as motion detection, in which sensors trigger an action upon detection of an event. An attacker or a group of attackers may try to overwhelm the sensor nodes, which will cause the network to forward a huge amount of traffic to the sink [14].

A path-based DoS attack [28] feeds some replayed packets into the network at the leaf nodes. Through the forwarding of these packets to the sink node, valuable network resources, mainly the bandwidth, would be consumed. The attacker may also decrease the lifetime of the network by making the nodes consume energy via forwarding irrelevant relayed packets.

Furthermore, other attacks can also be constructed within application specific sensor network scenarios. Therefore, various attack types can be modified and specialized to the network application area. In relation to this issue, Misic et. al. [29], for example, analyzed some possible security attacks on healthcare related WSNs, whose sensors are usually deployed on the patients' body.

Figure 1 summarizes above mentioned sensor network attacks with their target protocol layers.

Target Protocol Layer	Attack Type
Physical	radio jamming
	tampering nodes
MAC	link layer jamming
	back-off manipulation
	same-nonce attack
	replay-protection attack
	ACK attack
	PANId conflict attack
Routing	fake route information attack
	HELLO flood attack
	sinkhole attack
	wormhole attack
	sybil attack
	blackhole attack
Transport	SYN flood attack
	desynchronization attack
Application	overwhelming the nodes
	path-based DoS attack
	application specific attacks

Fig. 1. Sensor network attacks and target layers.

III. IEEE 802.15.4 SECURITY

In this section some details on security requirements and security modes of IEEE 802.15.4 MAC layer are presented.

A. Requirements

Access control, *confidentiality*, *frame integrity*, *sequential freshness* are the four security requirements specified for IEEE 802.15.4 [20]. Definitions and additional explanations are briefly presented below:

- *Access Control*: Legitimate nodes must be protected from frames of unauthorized nodes. This security requirement is achieved by maintaining an ACL of valid devices [20].
- *Frame Confidentiality*: To make information confidential, only the legitimate nodes must share the secret information [21]. This is done by encryption. Only the legitimate devices that share the secret key can decrypt frames for communication.
- *Frame Integrity*: The frames generated by legitimate nodes must not be manipulated by adversary nodes. The frame integrity is provided by message authentication code (MAC).
- *Sequential Freshness*: Legitimate nodes must not accept old messages (previously replayed). A simple message counter is provided to ensure sequential freshness.

More details on these definitions and requirements can be found in [20], [21].

B. Modes

There are three security modes to cover the security requirements of different types of application [20]. An ACL includes multiple entries. Each entry is composed of an address (source, destination), a security suit, a shared key, a last initial vector, and a replay counter. The last initial vector is used by the source, while the replay counter is used by the destination for sequential freshness. The modes are listed as follows:

- *Unsecured Mode*: In this mode, no security service is provided. It is used for low cost applications that do not require any security.
- *ACL Mode*: In ACL mode, each node maintains its ACL. In this mode, devices only receive message from those devices in its ACL. No other cryptographic protection is provided.
- *Secured Mode*: All the security requirements (access control, frame confidentiality, frame integrity and sequential freshness) are provided in this mode according to defined security suits. It uses all the fields in the ACL entry format. According to [20], [21], the security suits are summarized in Figure 2.

		Security Services			
Security Suit Name	**Description**	**Access Control**	**Frame Confidientiality**	**Frame Integrity**	**Sequential Freshness**
Null	No Security				
AES-CTR	Encryption only, CTR Mode	X	X		X
AES-CBC-MAC-128	128 bit MAC	X		X	
AES-CBC-MAC-64	64 bit MAC	X		X	
AES-CBC-MAC-32	32 bit MAC	X		X	
AES-CCM-128	Encryption & 128 bit MAC	X	X	X	X
AES-CCM-64	Encryption & 64 bit MAC	X	X	X	X
AES-CCM-32	Encryption & 32 bit MAC	X	X	X	X

Fig. 2. Security suits.

IV. GTS ATTACK

This section explains the use of Guaranteed Time Slots in WSN communication. After introducing the communication sequences of GTS allocation and deallocation schemes, the section identifies GTS attack through illustrating various scenarios. Besides the attacks stated in Section II, our GTS attack scenarios contribute WSN attack literature as categorized in MAC layer attack type.

A. Guaranteed Time Slots of IEEE 802.15.4 MAC Layer

In IEEE 802.15.4 MAC Standards, a superframe structure is allowed to manage the services with and without contention. The superframe is managed by the PAN coordinator. The IEEE 802.15.4 generic superframe structure is shown in Figure 3 [10]. The PAN coordinator sends *BEACON* messages at the beginning of each superframe thus the superframe interval is also called the *beacon interval*. Each *BEACON* message includes the network identifier, beacon periodicity and superframe structure in order to help other network devices to synchronize. The superframe is divided into 16 slots as shown in Figure 3. The network devices communicate with the PAN coordinator in the superframe interval. This duration is called contention access period (CAP) for the generic superframe shown in the figure.

The structure of the superframe can be configured by the PAN coordinator to meet the needs of various applications. For nodes running applications with relaxed latency requirements, the superframe can be partitioned into active and inactive portions as shown in Figure 4. The nodes sleep in the inactive portion. The length of the active and inactive portions are determined in accordance with the application's requirements. The inactive portion of the superfame prevents idle listening thus helps preserving the energy of the battery constrained nodes.

According to the IEEE 802.15.4 standards the PAN coordinator can assign dedicated slots to one or more separate network devices [10]. A slot assigned by the coordinator for communication only with a given device is defined as a Guaranteed Time Slot (GTS). GTSs support applications with particular bandwidth requirements or ones with relax latency requirements. Each GTS can contain a single or an integer multiple of time slots each one being equal to 1/16 of the beacon interval. The superframe structure with the contention free period (CFP), which includes GTSs is shown in Figure 5. There are 7 slots provided for GTS transmission in CFP of the superframe. GTSs are located after the CAP.

A device must track beacons in order to request and get an allocation for a GTS. The PAN coordinator decides whether to accept a GTS allocation request of a device and may give more than one slot if there are available slots. The GTS allocation policy is first-come-first serve. Figure 6 shows the usual communication sequence of a GTS slot allocation procedure.

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 the PAN coordinator. The GTS request message includes the length and the 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 the 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 6. If no GTS descriptor is found in the superframe, the node notifies the next upper layer of failure. The device can deallocate its GTS in the same way as shown in Figure 7.

The above mentioned GTS management including request, allocation and deallocation is based on the IEEE 802.15.4 explicit procedure/algorithm [10]. In addition to this procedure, some modified GTS allocation schemes have also been proposed. Ji et. al. [30] 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 the ones with the lower rate. So, their scheme allocates the GTS slots to devices with the higher packet rates. The proposed GTS algorithm also takes into consideration the number of nodes because there are at the most 7 GTS slots available for allocation. Ji et. al. [30] constructed a 17-node IEEE 802.15.4 star topology in order to compare their proposed GTS allocation mechanism with the standard one.

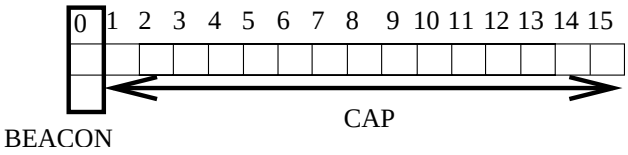


Fig. 3. IEEE 802.15.4 generic superframe structure.

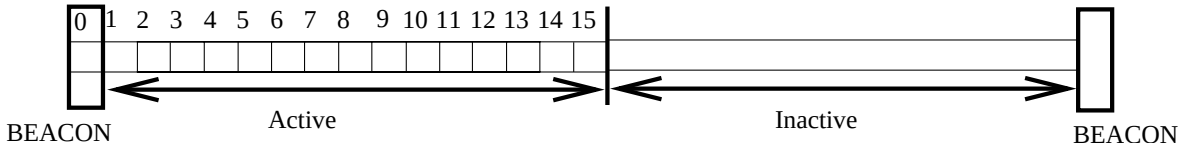


Fig. 4. IEEE 802.15.4 Superframe structure with active and inactive portions.

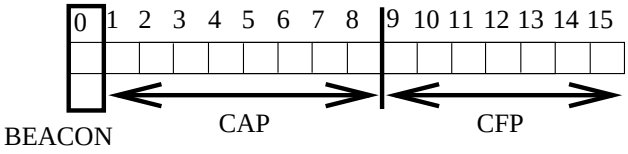


Fig. 5. IEEE 802.15.4 superframe structure with GTS.

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 to 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. [31], [32] 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 within 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.

B. Identified GTS attack

As described in [1], GTS attack is based on the inherent properties of the IEEE 802.15.4 superframe organization in beacon-enabled operational mode for WSNs. 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 8. 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 by 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.

C. Evaluation

We have simulated the proposed GTS attack implementation on ns-2.31 [33]. ns-2.31 comes with IEEE 802.15.4 MAC layer protocol in which GTS data structures are defined but GTS management methods are not implemented [34], [35]. In the simulations, we have implemented and used the explicit GTS management mechanism defined in IEEE 802.15.4 MAC layer standard [10].

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

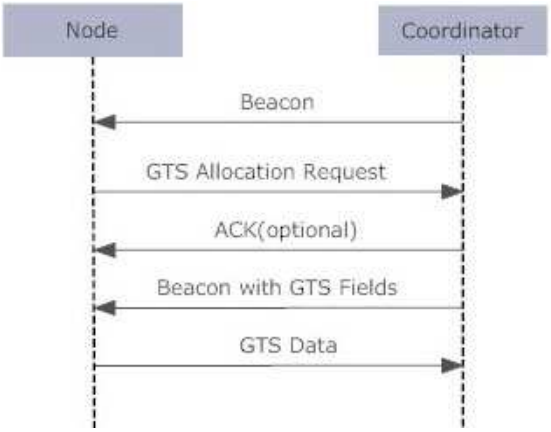


Fig. 6. Communication sequence in GTS allocation.

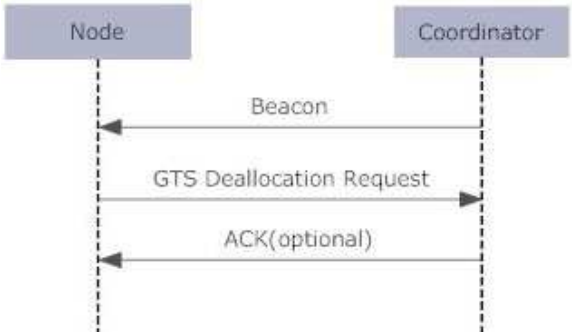


Fig. 7. Communication sequence in GTS deallocation.

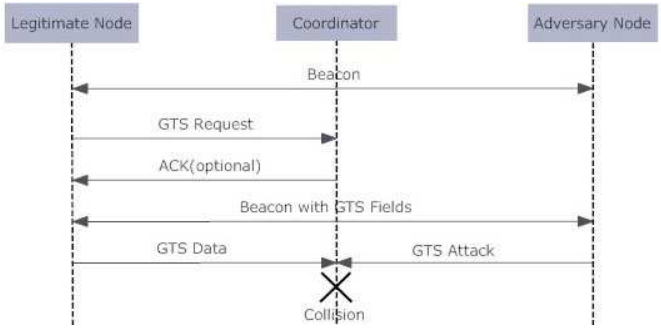


Fig. 8. Communication sequence in GTS attack scenario.

maximum length in the CFP, whereas a random attacker randomly chooses a GTS slot to be attacked. Attacking 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 in 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 ineffectively to corrupt the same node communication. In contrast to this, an intelligent attacker can use its energy in a more efficient manner. It can attack the first slot of the communication with maximum slot length thus destroying the whole communication. For the TIA scenario, the adversaries can cooperatively attack the nodes with 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 slot 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 I summarizes the definitions of the attack scenarios used in simulations.

TABLE I
ATTACK SCENARIOS

No	*Name*	*Definition*
1	OIA	One Intelligent Attacker
2	ORA	One Random Attacker
3	TIA	Two Intelligent Attackers
4	TRA	Two Random Attackers

In the simulations we have used the predetermined GTS request schedule of the nodes presented in Table II. According to this, the request of node 8, which is for 5 slots in length, can not be granted due to the remaining capacity of 4 out of 7 CFP slots after the reservation of 3 slots for node 7. The requests of node 6, node 4, and node 5 are granted for the communication within the remaining free slots sequentially. It is observed that the accepted requests are announced in the GTS field attribute of the following beacons as shown in Figure 9.

TABLE II
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

In the attack scenario experiments, node 0 is the PAN coordinator, nodes 1 and 2 are selected as intelligent attackers, nodes 3 and 9 are selected as random attackers, and the rest are the ordinary nodes. The simulation results are gathered for 60 s where the beacon interval is set to 0.98304 s. The number of total attack messages sent, and corrupted slots for the four different scenarios OIA, ORA, TIA and TRA respectively are given in Table III.

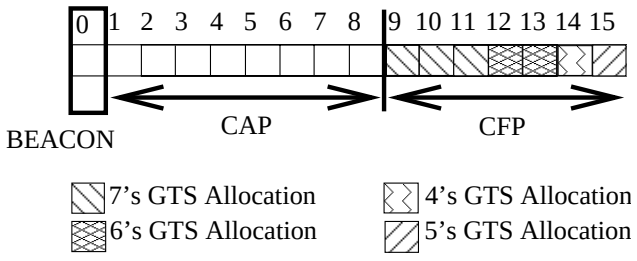


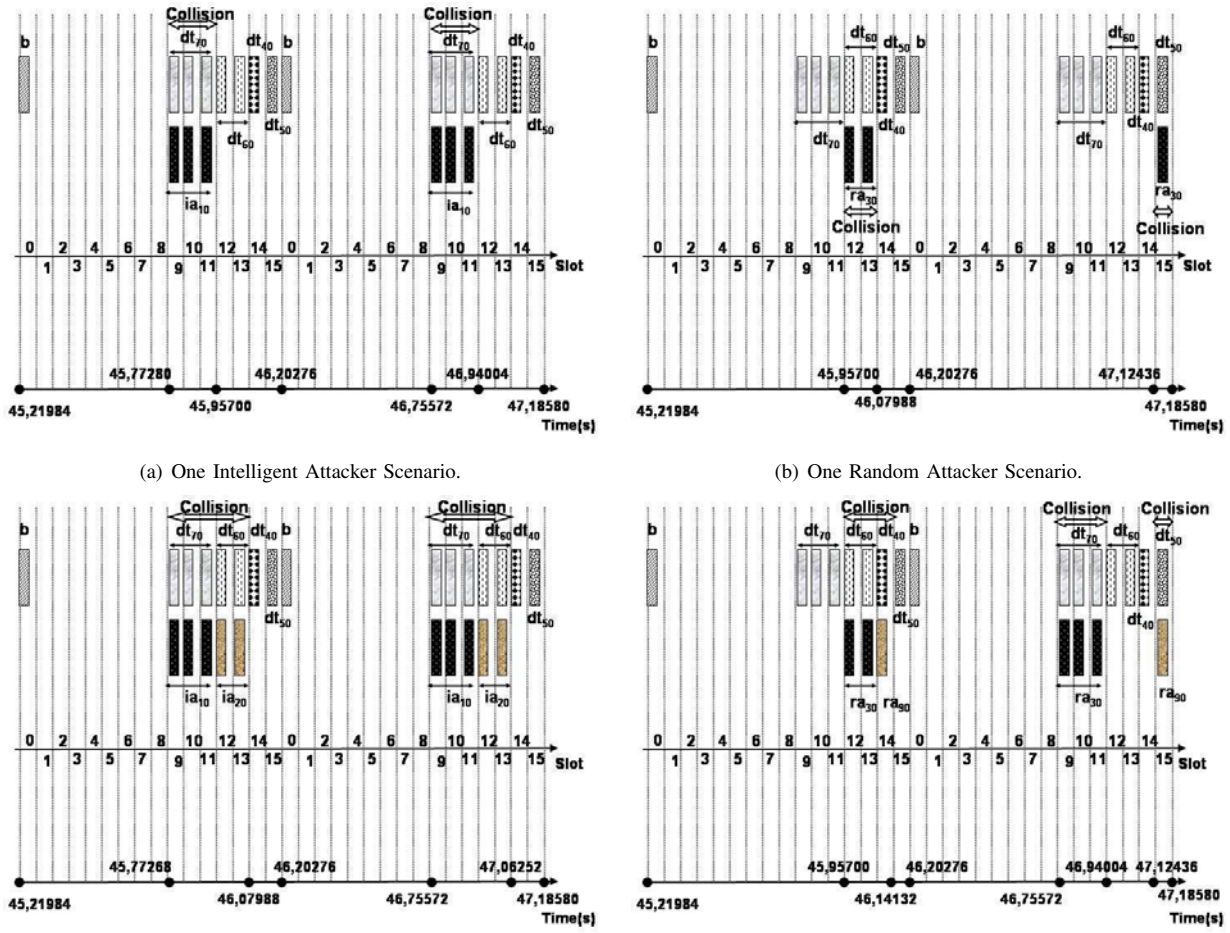
Fig. 9. Granted GTS allocation.

TABLE III
THE NUMBER OF ATTACK MESSAGES AND CORRUPTED SLOTS

Scenario Name	*Attack Messages*	*Corrupted Slots*
OIA	35	105
ORA	35	69
TIA	64	163
TRA	70	92

Figure 10 illustrates the collisions on the related communication between legitimate nodes and the PAN coordinator for the relevant scenarios. The figures indicate the details of the transfers of 2 sequential superframe structures on given times measured in simulation experiments. In all subfigures, the first frame transfer starts at 45,21984 s, which is the 46th beacon transmission time in the experiments. According to our simulation settings in Figure 9, the last GTS request is made at 40 s, which corresponds to the 41st ($\lceil 40/0.98304 \rceil$) beacon transmission. It is clear from the relation between the data presented in Table II and Figure 9 that all sequential frames transmitted after the 42nd beacon shall include the same communication pattern. As an example, the 46th beacon at 45,21984 s in the figures is chosen to be the beacon *b* of the first frame. The slots between 9 and 15 correspond to the slots of the CFP periods for the related superframes. The data transfer, *dt*, in those slots corresponds to the guaranteed amount of data communication between the nodes that have been granted the requested GTS. For example, dt_{70} refers to the data communication from node 7 to the PAN coordinator (node 0). The attack messages sent by the attacker are shown as *ia* for the intelligent attacker(s), and *ra* for the random attacker(s). For example, ia_{10} refers to the attack message sent from the intelligent attacker node 1 to the PAN coordinator. When an attacker sends its attack messages concurrently with the data communication between a node and the PAN coordinator, a collision occurs. In the OIA scenario given in Figure 10.a, the communication of node 7, shown as dt_{70}, is corrupted by node 1, shown as ia_{10}, in between 9th and 10th time slots. In the ORA scenario given in Figure 10.b, TIA in Figure 10.c, and TRA in Figure 10.d, the same notation is used to demonstrate the relevant collisions.

In the OIA scenario, node 1 corrupts 35 different data transfers each of 3 slot length belonging to node 7 causing all together 105 slots to be corrupted. It means that, the data of 105 slots out of 208 slots is affected by the attack. Assuming all other parameters equal, this attack results in 105/208 (50.48 %) decrease in bandwidth utilization during the CFP period. Node 3 corrupts 35 different data transfers with random slot lengths leading to 69 slot corruptions in the ORA 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 to a 78.37 % 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 %. In order to numerically evaluate



(a) One Intelligent Attacker Scenario.

(b) One Random Attacker Scenario.

(c) Two Intelligent Attackers Scenario.

(d) Two Random Attackers Scenario.

Fig. 10. The collisions on different attacker scenarios

the damaging effects of the attacker and compare the different scenarios in the following we introduce two new variables. The first one, related to the attacker's behavior, is called *corruption strength* and is defined as the ratio of the number of damaged slots to the total number of slots of data. The *transmission strength* on the other hand describes the node's behavior and is defined as the ratio of the number of slots with successfully completed transmission to the total number of slots. The corruption strength and the transmission strength are visualized in Figure 11. Depending on the corrupted slots per unit time, the best scenario from the attacker's point of view is the TIA, the worst scenario is ORA as seen in Figure 12. 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.

To evaluate the effectiveness of the atttacks we introduce another parameter - the energy consumed by the attacker for achieving a certain degree of damage. ns-2 supports the simulation of energy use of the sensor nodes, therefore the energies of the attackers have been traced within the simulations. Using the scenarios in Table II, 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 13. Figure 13 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 node by subtracting the current traced energy level from their previous values after each attack. As seen in Figure 13, 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.

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.

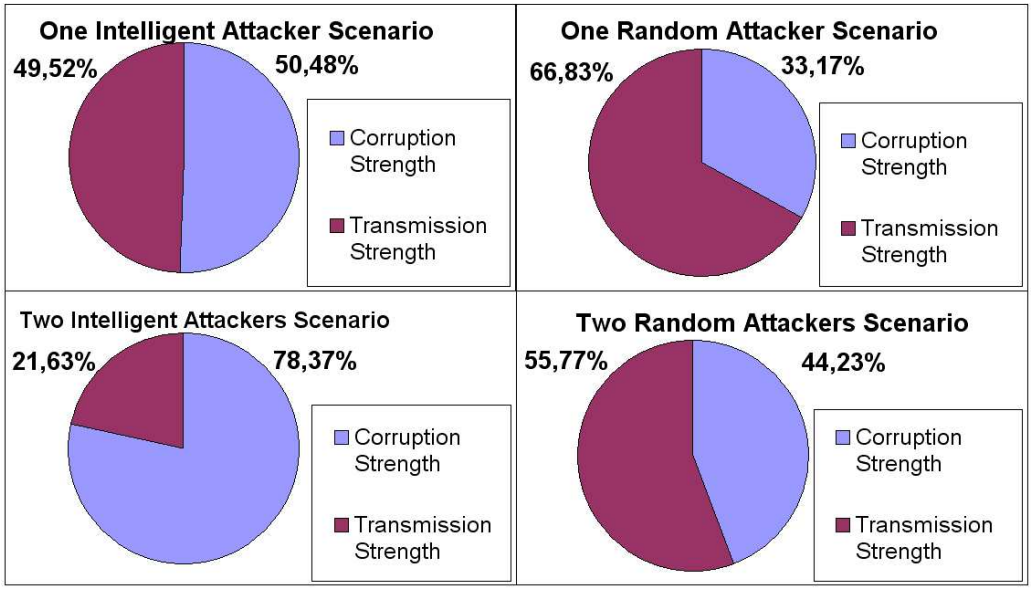


Fig. 11. Transmission and corruption strength.

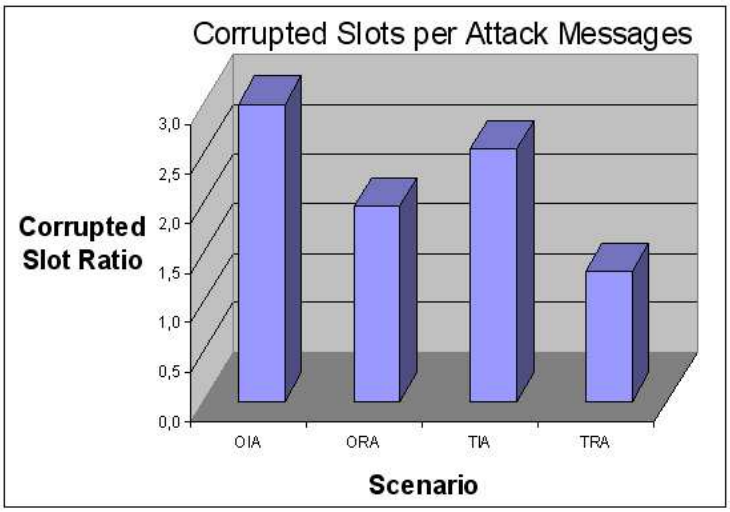


Fig. 12. Corrupted slots per attack messages.

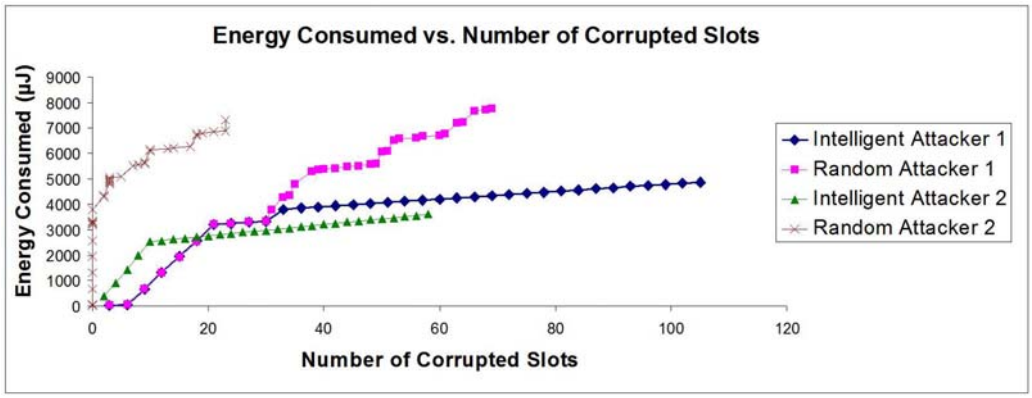


Fig. 13. Energy consumed vs number of corrupted slots.

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 is not able to synchronize precisely with the CFP slots. This allows the coordinator to detect the attack and extract his *ID* by from the source field of the received packets. In other cases, in which the adversary emits jamming signals instead of regular packets or emits regular packets with precise synchronization, GTS attack is considered very hard to detect.

V. Conclusions

This paper investigates WSN attacks including a brief survey of physical layer, MAC layer, routing layer, transport layer, and application layer attacks. Furthermore, a new IEEE 802.15.4 MAC layer attack, the GTS attack [1], 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 has been shown that a GTS attack is quite possible to realize. 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.

In order to numerically evaluate the effects of the different attack scenarios two new variables, the corruption strength and the transmission strength are introduced. It is observed that the intelligent attacker can achieve a corruption strength of up to 78.37 % which actually means that only one quarter of the available bandwidth is actually used for the communication during the CFP period.

Another aspect that has been evaluated is the energy consumption from the point of view of the attacker. An intelligent GTS attacker uses the energy much more efficiently than a random GTS attacker. On the whole, the intelligent attack method causes more damage to the sensor network communication requiring less energy from the attacker node as 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] R. Sokullu, O. Dagdeviren, and I. Korkmaz, "On the IEEE 802.15.4 MAC Layer Attacks: GTS Attack", *in Proc. of SENSORCOMM08*, 2008, pp. 673-678.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks", *IEEE Communications Magazine*, vol.40, no.8, 2002, pp. 102-114.

[3] M. Kuorilehto, M. Hannikainen, and T. D. Hamalainen, "A Survey of Application Distribution in Wireless Sensor Networks", *EURASIP Journal on Wireless Communications and Networking*, vol.5, no.5, 2005, pp. 774-788.

[4] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, "Wireless Sensor Networks for Habitat Monitoring", *in Proc. of ACM International Workshop on Wireless Sensor Networks and Applications*, 2002, pp. 88-97.

[5] E. Biagioni and K. Bridges, "The Application of Remote Sensor Technology to Assist the Recovery of Rare and Endangered Species", *in Special issue on Distributed Sensor Networks for the International Journal of High Performance Computing Applications*, vol.16, no.3, 2002, pp. 315-324.

[6] L. Schwiebert, S. K. S. Gupta, and J. Weinmann, "Research Challenges in Wireless Networks of Biomedical Sensors", *in Proc. of Mobile Computing and Networking*, 2001, pp. 151-165.

[7] M. B. Srivastava, R. R. Muntz, and M. Potkonjak, "Smart Kindergarten: Sensorbased Wireless Networks for Smart Developmental Problem-Solving Enviroments", *in Proc. of Mobile Computing and Networking*, 2001, pp. 132-138.

[8] A. D. Wood and J. A. Stankovic, "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks", *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, CRC Press, 2004.

[9] Committee on National Security Systems (CNSS), *National Information Assurance Glossary*, NSTISSI no.4009, 2003.

[10] 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).

[11] 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.

[12] 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.

[13] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks", *IEEE Computer*, IEEE, vol.36, no.10, 2003, pp. 103-105.

[14] D. R. Raymond and S. F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses", *IEEE Pervasive Computing*, vol.7, no.1, 2008, pp. 74-81.

[15] A. Wood and J. A. Stankovic, "Denial of Service in Sensor Networks", *IEEE Computer*, vol.35, no.10, 2002, pp. 54-62.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", *in Proc. of IEEE SNPA*, vol.1, 2003, pp. 113-127.

[24] 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.

[25] 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.

[26] H. Deng, W. Li, and D.P.Agrawal, "Routing Security in Wireless Ad Hoc Networks", *IEEE Communications Magazine*, vol.40, no.10, 2002, pp. 70-75.

[27] C.L. Schuba, I.V. Krsul, M.G. Kuhn, E.H. Spafford, A. Sundaram, and D. Zamboni, "Analysis of a Denial of Service Attack on TCP", *in Proc. of IEEE Symp. Security and Privacy*, 1997, pp. 208-223.

[28] J. Deng, R. Han, and S. Mishra, "Defending against Path-Based DoS Attacks in Wireless Sensor Networks", *in Proc. of 3rd ACM Workshop Security of Ad Hoc and Sensor Networks*, 2005, pp. 89-96.

[29] J. Misic, F. Amini, and M. Khan, "On Security Attacks in Healthcare WSNs Implemented on 802.15.4 Beacon Enabled Clusters", *in Proc. of IEEE Consumer Communications and Networking Conference*, 2007, pp. 741-745.

[30] 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.

[31] 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, pp. 183-192.

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

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

[34] 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.

[35] 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.

SFN Gain Simulations in Non-Interfered and Interfered SFN Network

Jyrki T.J. Penttinen
Member, IEEE
jyrki.penttinen@nsn.com

Abstract

The DVB-H (Digital Video Broadcasting, Hand-held) coverage area depends mainly on the area type, i.e. on the radio path attenuation, as well as on the transmitter power level, antenna height and radio parameters. The latter set has effect also on the audio / video capacity. In the detailed network planning, not only the coverage itself is important but the quality of service level should be dimensioned accordingly.

This paper describes the SFN gain related items as a part of the detailed radio DVB-H network planning. The emphasis is put to the effect of DVB-H parameter settings on the error levels caused by the over-sized Single Frequency Network (SFN) area. In this case, part of the transmitting sites converts to interfering sources if the safety distance margin of the radio path is exceeded. A respective method is presented for the estimation of the SFN interference levels. The functionality of the method was tested by programming a simulator and analyzing the variations of carrier per interference distribution. The results show that the theoretical SFN limits can be exceeded e.g. by selecting the antenna height in optimal way and accepting certain increase of the error level that is called SFN error rate (SER) in this paper. Furthermore, by selecting the relevant parameters in correct way, the balance between SFN gain and SER can be planned in controlled way.

Index Terms—*Mobile broadcast, single frequency network, radio planning, performance evaluation.*

1. Introduction

The DVB-H is an extended version of the terrestrial television system, DVB-T. Both are defined in the ETSI standards along with the satellite and cable versions of the DVB.

The mobile version of DVB suits especially for the moving environment as it has been optimized for the fast variations of the field strength and different terminal speeds. Furthermore, DVB-H is suitable for the delivery of various audio / video channels in a single bandwidth, and the small terminal screen shows adequately the lower resolution streams compared to the full scale DVB-T.

As DVB-H is meant for the mobile environment, the respective terminals are often used on a street level for the reception. This creates a significant difference in the received power level compared to DVB-T which uses fixed and directional rooftop antenna types. Furthermore, the DVB-H terminal has normally only small, in-built panel antenna, which is challenging for the reception of the radio signals.

The DVB-H service can be designed using either Single Frequency Network (SFN) or Multi Frequency Network (MFN) mode. In the former case, the transmitters can be added within the SFN area without co-channel interferences even if the cells of the same frequency overlap. In fact, the multi-propagated SFN signals increases the performance of the network by producing SFN gain.

Especially in the Single Frequency Network, the coverage planning is straightforward as long as the maximum distance of the sites does not exceed the allowed value defined by the guard interval (GI). The guard interval takes care of the safe reception of the multi-path propagated signals originated from various sites or due to the reflected radio waves. If the GI and FFT dependent geographical SFN boundary is ex-ceeded, part of the sites starts to act as interferers instead of providing useful carrier.

The maximum size of the non-interfered Single Frequency Network of DVB-H depends on the guard interval and FFT mode. The distance limitation between the extreme transmitter sites is thus possible to calculate in ideal conditions. Nevertheless, there might be need to extend the theoretical SFN areas e.g. due to the lack of frequencies.

Sites that are located within the SFN area minimises the effect of the inter-symbol-interferences as the guard interval protects the OFDM signals of DVB-H,