Trust-Based Defence Model Against MAC Unfairness Attacks for IoT

Nabil DJEDJIG
Research Center on Scientific and Technical Information
Abderrahamane MIRA University
ALGIERS, ALGERIA
djedjig_nabil@cerist.dz

Djamel TANDJAOUI
Research Center on Scientific and Technical Information
ALGIERS, ALGERIA
dtandjaoui@cerist.dz

Imed ROMDHANI
Edinburgh Napier University, School of Computing
Edinburgh, UK
I.Romdhani@napier.ac.uk

Faiza MEDJEK
Research Center on Scientific and Technical Information
Abderrahamane MIRA University
ALGIERS, ALGERIA
medjek-f@dtri.cerist.dz

***Abstract*—The vulnerability of Internet of Things (IoT) networks makes channel access security a serious problem. The IEEE 802.15.4 Media Access Control (MAC) layer faces the risk of attacks from malicious nodes which attempts to get a dominating position and hold unfair advantages over the other nodes. In this paper, we address MAC unfairness attacks where attackers attempt to bypass the MAC priority. We propose a MAC-trust-based model to handle unfairness attacks while maintaining channel access to all participating nodes. In our scheme, a Pan Coordinator Manager (PCM) cooperates with PANs and Coordinators to detect malicious behavior, calculate trust values for participating nodes, and maintain a blacklist of malicious nodes. Our model modifies Guaranteed Time Slots (GTS) allocation policies according to nodes' trust values.**

Keywords-Trust; IEEE 802.15.4; Internet of Things; Security; unfairness attack; GTS.

I. INTRODUCTION

The Internet of Things (IoT) is collectively formed of emergent embedded objects, such as smart-phones, tablets, smart watches/glasses, intelligent building devices, and even smart vehicles [1]. These objects are addressable, and have low-power and low-processing capacities. They are interconnected to transfer sensing data to the Internet using compatible and heterogonous radio communications. In such heterogeneous environment, security is among the key issue to overcome.

The research community considers the IEEE 802.15.4 standard as one of enabling technologies for short range, low rate, wireless communications that is most suitable for IoT, which makes it the de-facto standard to define physical and MAC (Media Access Control) layer for IoT networks [2]. Although researches in IoT security have focussed on all security aspects for the different OSI layers, most security solutions are being specifically designed for network and application layers [3]-[6]. Given that, the MAC layer is the basis of interconnecting IoT nodes, it is therefore targeted by several attackers [7]. Yasmin et al. surveyed IEEE 802.15.4 attacks [8]. In this paper, we focus on MAC unfairness attacks, especially Guaranteed Time Slots (GTS) related attacks. In these attacks, malicious node cheats to obtain higher priority than legitimate nodes to maximize the channel access utilization [9]. Most of MAC security solutions proposed in the literature are based on cryptography mechanism to deal with confidentiality and authentication issues. Nevertheless, these solutions cannot handle MAC unfairness attacks. Indeed, embedding minor changes in the IEEE 802.15.4 standard itself will make it more secure against this type of attacks.

In this paper, we introduce a new MAC-trust-based model to solve MAC unfairness attacks. In this model PANs and Coordinators collaborate with a centralized PAN Coordinator Manager to evaluate trust values of participating nodes. Indeed, the allocation of the GTS is based on the evaluated trust values. Each time the trust decreases, the number of slots allocated to the node decreases too until no priority is assigned to the node.

The rest of this paper is structured as follows. Section II presents a background of IEEE 802.15.4 GTS MAC process and related attacks. Section III introduces our proposed model. Finally, Section IV concludes the paper.

II. IEEE 802.15.4 PROTOCOL

A. GTS MAC Background

IEEE 802.15.4 networks can operate on beacon or non-beacon enabled modes. In this paper, we focus on beacon enabled mode. In this mode, a superframe is delimited by two beacons, and is divided into 16 time slots. Each of periodic superframe is divided into a Contention Access Period (CAP) and a Contention Free Period (CFP). Slotted CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is used in the CAP, whilst, GTS is used in CFP [10]. The superframe is fully defined using a beacon interval (BI) and a superframe duration (SD). BI refers to the time between two consecutive beacons and is constituted by an active portion and an optional inactive portion, as shown in Figure 1. During the inactive portion, the coordinator enters a low-power mode to conserve its power resources. The active period corresponds to the SD and is divided into 16 time slots, as shown in Figure 2.

 ISBN: 978-1-61208-572-2

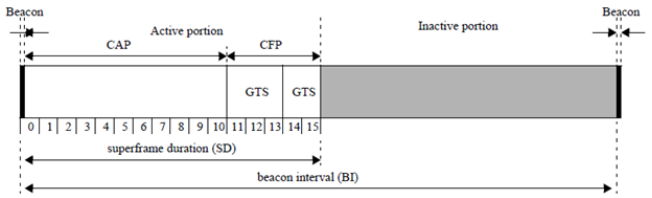

Figure 1. IEEE 802.15.4 superframe structure.

The PAN coordinator reserves GTS within the CFP of each superframe duration in order to provide real-time guaranteed channel access to in-network nodes for delay-sensitive applications. The PAN coordinator allocates and de-allocates GTS on a First-come, First-serve basis [10], as depicted in Figure 3. Indeed, it may allocate up to 7 GTS at the one time. A node requests GTS from the coordinator, by sending a GTS request frame during the CAP. The node waits for the response of the coordinator in the next beacon. The coordinator either accepts or rejects the request based on the current resource capacity available in the superframe. Once a GTS request from a node is granted, the coordinator reserves the GTS for the node during the CFP. Upon receiving beacon transmitted by the PAN coordinator, each node tries to transmit its packet using the superframe. Nodes that do not succeed in accessing the channel discard the packet, and at the next superframe, they generate a new packet.

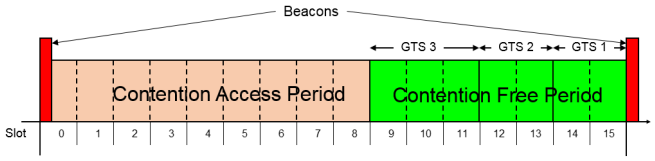

Figure 2. Structure of the active periods with GTSs.

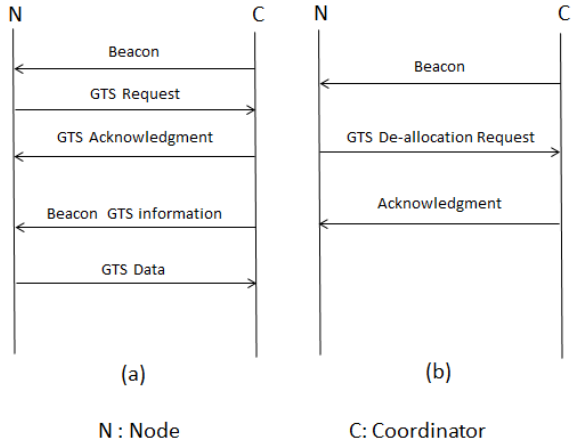

Figure 3. (a) GTS allocation process, (b) GTS de-allocation processes.

B. GTS MAC Attacks

The GTS MAC channel sharing mechanisms are vulnerable to malicious nodes that misbehave and break the standard communication rules to capture the channel with higher priority utilization. Indeed, malicious nodes extract slots information from the beacon sent by the PAN/Coordinators to trigger different MAC attacks.

There exist several GTS related attacks that have been defined in the literature. Among them the following:

- Malicious nodes can keep sending several GTS allocation request frames, and thus can allocate a maximum number of GTS and keep the channel busy, omitting legitimate nodes from allocating GTS and transferring data [8] [11] [12].
- A malicious node can spoof unallocated legitimate node identities and send GTS allocation requests on their behalf [13]. The malicious node can then inject false data. Also, the malicious node can use its proper identity or fabricated identities to send GTS allocation requests [14].
- A malicious node can spoof identities of legitimate nodes with allocated GTS. It can then send GTS de-allocation requests on their behalf, which leads to terminate their channel access rights [13].
- One or two attackers can create interference during the GTS allocated to legitimate nodes. This leads to corrupt ongoing transmissions [13] [12].

III. THE PROPOSED MODEL

To enhance MAC security, we propose two algorithms. The first algorithm aims to verify the association process. The second one to allocate GTS dynamically for real time applications based on nodes trustworthiness. The GTS period in the IEEE 802.15.4 is adjustable by beacon parameters (BeaconOrder-BO and SuperframeOrder-RO) [10]. In our model, the GTS period is initially set using BO and RO. After the first GTS request, the GTS period is recalculated and reallocated based on nodes trust values. In the following, we present our model and how to calculate trust values.

Three entities (actors) participate in the proposed model: A Pan Coordinator Manager denoted PCM, at least one PAN Coordinator and Coordinators denoted C_i, and nodes denoted N_j. Coordinators and PANs are full function devices (FFDs), whilst the nodes can be FFDs or reduced function devices (RFDs). The PCM keeps in its table (database) a list of all coordinators and PANs, and a list of all nodes within the network. Indeed, for each Coordinator C_i, PCM maintains the list of nodes associated with it, the trust value, denoted T_{Nj}, of each node N_j, and the number of GTS request frames, denoted NB_{Nj}, for each node N_j. In our model, the PCM monitors GTS across the entire network by keeping the history of all nodes stationary and mobile.

For security consideration, we assume each node N_j is associated to only one C_i at time t.

A. Controlled Association MAC

As already said, each node is allowed to be associated to only one PAN/Coordinator at one time t. Thus, each time a node sends an association request to a PAN or a Coordinator, this later sends an association control request to the PCM. The PCM checks in its database the state of the node. Two

cases rise: 1) The node does not exist in the database, which means it is not associated to any PAN/Coordinator. 2) The node is already associated to one PAN/Coordinator. In the first case, the PCM sends an Association Control Acknowledgment, and the PAN/Coordinator can associate this node. In the second case, the PCM sends a Request status to the PAN/Coordinator associating the node. Two cases can occur: 1) The node is associated correctly to the PAN/Coordinator. 2) The node became orphan because it lost the connexion with the PAN/Coordinator. In the first case, the PCM blacklists the node and sends an association control notification to all PAN/Coordinators. In the second case, the PCM sends an association control acknowledgment and updates its database. Algorithm 1 (Figure 4) and Figure 5 summarise the controlled association process.

Algorithm 1 Trust-Based Association Algorithm

Input: One PCM; a number of coordinators M; a number of nodes N; each node Nj is associated to only one coordinator $C_i \in M$;
Nj sends Association Request to C_i;
C_i sends Association Control Request (N_j,C_i) to PCM
PCM checks if $N_j \in C_h$ ($h \neq i$)
If $N_j \in C_h$ ($h \neq i$) **do**
  PCM sends Request status to C_h ($h \neq i$)
  If N_j is associated **do**
    $N_j = 0$;
    Blacklists T_{Nj};
    sends Association Control notification (N_j) to C_i;
    sends Disassociation notification (N_j) to C_h;
    C_i sends Disassociation notification to N_j;
  Else If N_j is orphan **do**
    PCM sends Association Control Acknowledgment (N_j) to C_i;
    C_i sends Association Acknowledgment to N_j;
  END If
Else If $N_j \notin C_h$ **do**
  PCM sends Association Control Acknowledgment (N_j) to C_i;
  Ci sends Association Acknowledgment to N_j;
END If

Figure 4. Trust-Based Association Algorithm.

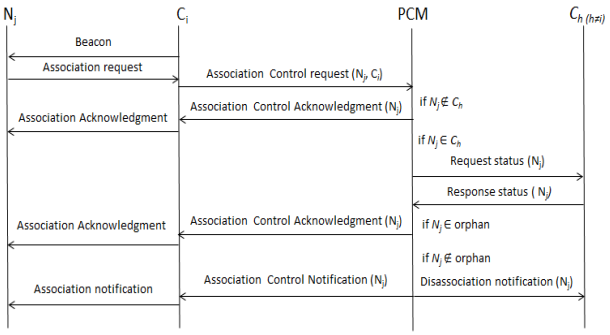

Figure 5. Controlled Association process.

B. *Adaptive Allocation GTS MAC*

Algorithm 2 (Figure 7) and Figure 6 summarise the proposed Adaptive Allocation GTS process.

Initially, at the first association, all nodes are fully trusted, which means trust values of all nodes are set to 1 (i.e. T_{Nj}=1). In addition, the number of GTS request frames for each node is set to 0 (i.e. NB_{Nj}=0). The maximum number of GTS request frames allowed within a period T for each node is set as threshold, denoted TH.

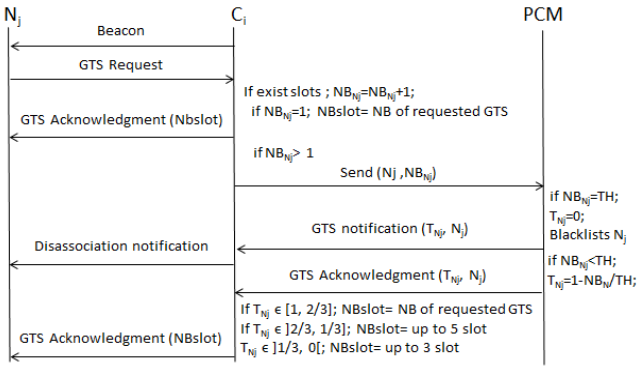

Figure 6. Trust-Based GTS Allocation process.

Algorithm 2 Trust-based GTS Allocation Algorithm

Input: One PCM; a number of coordinators M; a number of nodes N; each node N_j is associated to only one coordinator $C_i \in M$; the trust value of each node $_{Nj} \in N$ is set to $T_{Nj} = 1$; the number of request to GTS from each node Nj is set to $NB_{Nj} = 0$; TH= Threshold;(TH : a maximum number of requests to GTS);
While (T) **do**
  N_j sends GTS Request to C_i;
  C_i calculates $NB_{Nj} = NB_{Nj} + 1$;
  If $NB_{Nj} = 1$ **do**
    NBslots= NB.GTS.Req;
    Sends GTS Acknowledgment (NBslots);
  END If
  If $NB_{Nj} > 1$ **do**
    sends (N_j, NB_{Nj}) to PCM;
    If NB_{Nj}= TH **do**
      T_{Nj}=0;
      Blacklists N_j;
      Sends GTS notification (T_{Nj}, N_j) to C_i;
      C_i sends Disassociation notification to N_j;
    END If
    If $NB_{Nj} < TH$ **do**
      T_{Nj}=1- NB_{Nj}/TH;
      Sends GTS Acknowledgment (T_{Nj},N_j) to C_i;
      If $T_{Nj} \in [1, 2/3]$ **do** NBslots=NB.GTS.Req;
      If $T_{Nj} \in]2/3, 1/3]$ **do** NBslots = up to 5 slot of NB.GTS.Req;
      If $T_{Nj} \in]1/3, 0]$ **do** NBslots= up to 3 slot of NB.GTS.Req;
      Sends GTS Acknowledgment (NBslots);
    END If
  END If
END While

Figure 7. Trust-based GTS Allocation Algorithm.

After successfully associated with the PAN/coordinator, nodes send GTS request frames through which they ask the PAN/coordinator to assign them a number of GTS (according to BO and RO). Once the PAN/Coordinator receives the request, it increments NB_{Nj} (i.e. NB_{Nj}= NB_{Nj}+1) and sends N_j and NB_{Nj} to the PCM. Upon receiving N_j and NB_{Nj}, the PCM checks if $NB_{Nj} \leq TH$. If NB_{Nj}=TH, the PCM sets T_{Nj} to 0, blacklists N_j and sends GTS notification to all PAN/Coordinators. If $NB_{Nj} < TH$, the PCM calculates the new trust value T_{Nj} according to equation 1, and sends GTS Acknowledgment with the node identifier N_j, the number of

GTS request frames NB_{Nj}, and the new trust value T_{Nj} for this node to the PAN/Coordinator.

$$T_{Nj} = 1 - NB_{Nj} / TH \quad (1)$$

For the first GTS request, the PAN/Coordinator acknowledges the nodes and allocates them a number of GTS equal to the number of requested GTS. After that, the allocation is done according to nodes trust value as follow.

We split GTS to three sub-GTS: GTS1 (2 slots), GTS2 (2 slots) and GTS3 (3 slots) [10]. We split the trust interval onto three sub-intervals: [1, 2/3],]2/3, 1/3], and]1/3, 0[.

- If the new calculated trust value $T_{Nj} \in [1, 2/3]$, the PAN/Coordinator allocates the node a number of GTS equal to the number of requested GTS (Up to 7 slots).
- If $T_{Nj} \in]2/3, 1/3]$, the PAN/Coordinator allocates the node a number of GTS up to 5 slots (GTS3+GTS2). Hence, if the number of requested GTS is greater than 5, the node will be assigned a maximum of 5 slots.
- If $T_{Nj} \in]1/3, 0[$,the PAN/Coordinator allocates the node a number of GTS up to 3 slots (GTS3). Hence, if the number of requested GTS is greater than 3, the node will be assigned a maximum of 3 GTS.

If the PAN/Coordinator receives GTS request from two or more nodes at the same time, instead of allocating GTS on a First-come, First-serve basis, the PAN/Coordinator allocates GTS on trust basis. Which means, the first served is the node with the greatest trust value.

The allocation process is repeated while T not expired. Once T expired, PAN/Coordinators and PCM reset NB_{Nj} to 0 and T_{Nj} to 1.

IV. CONCLUSION

A trust-based defence and dynamic GTS allocation method is introduced in this paper to prevent and detect some MAC unfairness attacks in beacon-enabled IoT 802.15.4 networks. We introduced a new central entity to IEEE 802.15.4 topology to act as a global neighbor discovery proxy. This new entity (PCM), caches the new identity of all nodes and monitor local GTS allocation based on nodes' behavior. This new approach can handle easily mobile nodes.

REFERENCES

[1] C. Shen, H. Choi, S. Chakraborty, and M. Srivastava, "Towards a rich sensing stack for iot devices," in Computer-Aided Design (ICCAD), 2014 IEEE/ACM International Conference on. IEEE, 2014, pp. 424–427.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, "New trust metric for the rpl routing protocol," in Information and Communication Systems (ICICS), 2017 8th International Conference on. IEEE, 2017, pp. 328–335.

[4] F. Medjek, D. Tandjaoui, I. Romdhani, and N. Djedjig, "New trust metric for the rpl routing protocoll," in The 10th IEEE International Conference on Internet of Things (iThings-2017). IEEE. IEEE, 2017, in press.

[5] J. Guo, R. Chen, and J. J. Tsai, "A survey of trust computation models for service management in the internet of things systems," Computer Communications, vol. 97, pp. 1–14, 2017.

[6] B. B. Zarpelˆao, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in i nternet of things," Journal of Network and Computer Applications, 2017, pp 25–37.

[7] S. M. Sajjad and M. Yousaf, "Security analysis of ieee 802.15. 4 mac in the context of internet of things (iot)," in Information Assurance and Cyber Security (CIACS), 2014 Conference on. IEEE, 2014, pp. 9–14.

[8] Y. M. Amin and A. T. Abdel-Hamid, "A comprehensive taxonomy and analysis of ieee 802.15. 4 attacks," Journal of Electrical and Computer Engineering, vol. 2016, p. 4, 2016.

[9] C. Balarengadurai and S. Saraswathi, "Comparative analysis of detection of ddos attacks in ieee 802.15. 4 low rate wireless personal area network," Procedia Engineering, vol. 38, pp. 3855–3863, 2012.

[10] IEEE, "Local and metropolitan area networksspecific requirementspart 15.4: wireless medium access control (mac) and physical layer (phy) specifications for low rate wireless personal area networks (wpans)," IEEE Standard for Information Technology, 2006.

[11] B. M. David and T. de Sousa Jr, "A bayesian trust model for the mac layer in ieee 802.15. 4 networks," in I2TS 2010-9th International Information and Telecommunication Technologies Symposium, 2010.

[12] S. Saleem, S. Ullah, and K. S. Kwak, "A study of ieee 802.15.4 security framework for wireless body area networks," Sensors, vol. 11, no. 2, pp. 1383–1395, 2011.

[13] R. Sokullu, O. Dagdeviren, and I. Korkmaz, "On the ieee 802.15.4 mac layer attacks: Gts attack," in Sensor Technologies and Applications, 2008. SENSORCOMM'08. Second International Conference on. IEEE, 2008, pp. 673–678.

[14] C. P. O'Flynn, "Message denial and alteration on ieee 802.15.4 low-power radio networks," in New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on. IEEE, 2011, pp. 1–5.

 ISBN: 978-1-61208-572-2