Open Archive Toulouse Archive Ouverte

OATAO is an open access repository that collects the work of Toulouse researchers and makes it freely available over the web where possible

This is an author's version published in:
http://oatao.univ-toulouse.fr/22031

Official URL
https://doi.org/10.1109/SSIC.2016.7571807

To cite this version: Khalid, Ahmad Shahrafidz Bin and Conchon, Emmanuel and Peyrard, Fabrice *Evaluation of RAIN RFID authentication schemes.* (2016) In: International Conference on Security of Smart cities, Industrial Control System and Communications (SSIC 2016), 18 July 2016 - 19 July 2016 (Paris, France).

Any correspondence concerning this service should be sent to the repository administrator: tech-oatao@listes-diff.inp-toulouse.fr

Evaluation of RAIN RFID authentication schemes

Ahmad Shahrafidz Khalid*, Emmanuel Conchon†, Fabrice Peyrard*
*University of Toulouse; INP; IRIT 2 rue Charles Camichel, Toulouse, France.
Email: {ahmad.khalid, fabrice.peyrard}@enseeiht.fr
†University of Limoges, XLIM, UMR CNRS 6172, 123 avenue Albert Thomas, 87060 Limoges, France.
Email: {emmanuel.conchon}@unilim.fr

***Abstract*—In this paper, we present different authentication schemes of Radio Frequency Identification (RFID) Generation 2 version 2 (Gen2V2) in UHF mode. We model the anti-collision management and evaluate it by simulation with OMNeT++. We evaluate the overall performance of RFID Gen2v2 network in terms of measurement of collisions and association time. We present four main cryptographic suites of the Gen2V2 standard, namely XOR, AES128, PRESENT80 and CryptoGPS. After their modelling and simulation, the obtained results allow us to put forward the necessary time for each authentication algorithms. The objective of this work is to show the impact of the cryptographic suites used to ensure the authentication of connected objects in the Internet of Things.**

***Index Terms*—IoT, Gen2v2, passive RFID.**

1. Introduction

Nowadays, the use of Radio Frequency IDentification (RFID) system is widespread in various application such as stock inventories and system automations. It is also applied to logistics, access control, smart environment, and healthcare. With the new paradigm of the Internet of Things (IoT) the number of RFID system is increasing very quickly.

Indeed, RFID, especially Low Frequency (LF) and High Frequency (HF), is a well known technology that has been in use for at least 20 years.

Since October 2013, GS1 (Global Standards) has ratified EPC Gen2v2, a new version of the widely used Gen2 Ultra high frequency (UHF) RFID standard. Gen2v2 is backwards compatible with Gen2 but adds new features mainly for authenticating tags and readers as well as consumer privacy. These new features ease the adoption of RFID especially in application areas where the tag carries more information than only its identity. UHF is now an established technology, solutions can be reliably deployed for long read range, passive, and cheap. This new generation of tags is supported by an alliance of manufacturers called RAIN (RAdio-frequency IdentificatioN) [1].

The RAIN RFID Alliance is a non-profit organization that promotes awareness, education, and initiatives to accelerate the adoption of passive UHF RFID standards developed by GS1 (EPC Gen2) and incorporated by ISO/IEC (18000-63) [2] in business and consumer applications worldwide.

But, this technology presents several security weaknesses that can be of concern for the IoT. The main concern is the security of the data collected by this system. This information could be used against the owner if it is not well protected. Most information's leaks happen through passive eavesdropping that could bring toward a man-in-the-middle attack or a replay attack. An access to the physical tags could also leads to RFID tags cloning.

Moreover, as RFID Tag can be widespread in the environment, the information they provide is critical in regards to the user privacy. Therefore, authentication mechanisms have to be provided to prevent an unauthorized reader to collect this information. This authentication process has to be performed both by tags as well as by readers. In tag authentication, a reader asks a tag to encrypt a message using its stored secret key. If the reader is able to decrypt the tag response, the tag is genuine. This approach can be used to detect unauthorized or spy tags. Similarly, in reader authentication, access to a tag is limited to legitimate readers.

Gen2v2 does not define a single authentication method in the standard. Instead, the standard Gen2v2 propose nine authentication schemes based on cryptographic suites defined in the ISO/IEC 29167 standard family [3], [4], [5], [6], [7], [8], [9], [10], [11], [12]. The scheme to use depends on the system under use. Some schemes target low power consumption and quick authentication whereas others may enforce more secure authentication.

In this paper four cryptographic suites among the nine have been selected to measure the additional time induces by the authentication mechanism during the tag association process. We chose XOR[4] for its simplicity that is suitable for low cost passive tags. AES-128[5] was chosen because it is a cryptographic suite widely used by other well-known technologies for embedded connected devices like Bluetooth, Zigbee and LoRa [13]. Present-80[6] was also selected because it is a lightweight algorithms that can be used by devices with low computation resources. Finally CryptoGPS [7] proposed by the French provider Orange has been chosen because it offers a highly secure authentication process.

Based on OMNeT++ [14] simulations, an evaluation of

the four above cryptographic suites has been performed to identify how this additional security component may affect the overall association process between a single reader and tags.

The paper is organized as follows: Section 2 discusses on the basic concept and the current standard; Section 3 introduces the different cryptographic suites that are available in Gen2v2 standard to perform an authentication; Section 4 presents the performance evaluation of these cryptographic suite based on OMNet++ simulation. Finally, Section 5 concludes the paper with a discussion and open issues.

2. Background

2.1. RAIN RFID Model

RFID Gen2v2 is the current standard for passive UHF RFID tags. It defines every aspects of signalling, collision management and up to the enhancement of security features.

The collision arbitration protocol implemented in the standard is based on the Frame Slotted Aloha (FSA). In Aloha, any device is free to send data whenever it is required to do so. If collision happens, the device waits for a random time and retransmits the data. Collisions could occur at any time during the transmission. As a consequence, a 99% completed data transmission could be corrupted by a collision. This will require a retransmission of the whole data. Slotted Aloha solves this issue by fixing a time frame where a device can transmit its message. A device can only start to relay the message at the beginning of the predefine time slot. Therefore the collision can only happen at the beginning of each slot reducing the unproductive transmission. The frame slotted Aloha protocol gathers slots into a frame.

Problem exists when more than one tag are within the reach of the reader and when they decide to backscatter the signal simultaneously. This could results in unproductive situations, where the signal collides and becomes unreadable and the association process duration will increase.

2.2. Method Used for Collision Management

The collision management of Gen2v2 is similar to the Gen2 standard. No modification has been made by this new version. The Gen2 standard [15] introduces a Q parameter and a slot number to improve the collision management.To begin a frame, the reader choose a total number of available slots for the whole frame. This total is defined as 2^Q with a maximum value of 15 for Q. The reader sets the Q value for all tags within its reach. When a tag receives Q, it will randomly choose a number of slots within the frame. In the following, this number will be known as the 'slot counter'.

Figure 1 represents the RAIN RFID collision management process that has been implemented in our simulation model.

To deal with collisions, the standard [15] defines that the reader should first send a value between 0 and 15 called Q to all tags. Q defines the number of slots available to all

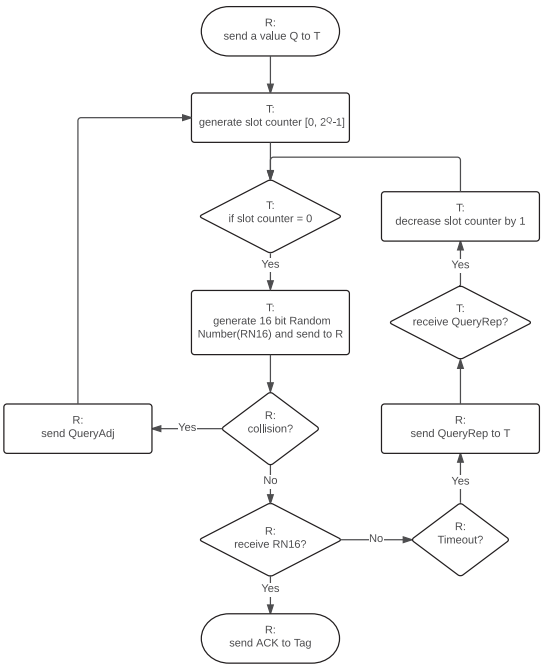

Figure 1. Gen2V2 Collision Management

tags. Upon receiving Q, the tag generates a random number between 0 and $2^Q - 1$. This random number is used as a slot counter. The slot counter determines the moment when the tag should send back its reply. In order to go through the given slot, the reader sends a *QueryRep* request so that the tag has to decrease its slot counter by 1. The reader runs through the tag at least $2^Q - 1$ iteration of the *QueryRep* request. It is important to note that a tag only starts to transmit when the slot counter is 0. However, if any collision occurs during the respond backscattered, the reader will send a *QueryAdjust* request to reset and restart the counter slot from 0, and start to go through all the slot in the frame once again.

Based on this protocol, the maximum number of iterations depends on the number of collisions and on the value of Q as presented as in Equation 1

$$Maximum\ iteration = collision\ number \times 2^Q \quad (1)$$

Therefore, a high number of collisions will increase the association time for all tags and then reduce the system efficiency.

2.3. Efficiency

Studies such as Chen and Zhang in [16], Namboodiri et al. in [17], Su-Ryun et al. in [18], and Harald in [19] addressed the evaluation of Framed Slotted Aloha to manage the anti-collision in RFID from a theoretical standpoint relying on different mathematical models. In this paper, we

chose to model the frame slotted Aloha protocol and to compare the theoretical efficiency found in these studies with the simulated results that we have obtained. This comparison will help to validate our implementation of frame slotted Aloha so that it can be used as the underlying communication protocol in order to evaluate the different authentication mechanisms provided by the Gen2V2 standard.

The Framed Slotted Aloha model has a maximum theoretical efficiency of 36%. The equation (2) represents the efficiency of the system, where n is the number of tags and N is the value of 2^Q.

$$S = \frac{n(1-\frac{1}{N})^{(n-1)}}{N} \tag{2}$$

Collisions happen although the slot number is big enough. Indeed, a high Q value does not guarantee a collision free environment. However, the higher the slot number, the higher the total duration required to associate all tags. Figure 2 represents the efficiency differences between theoretical and simulation values. In both cases, for 20 and 100 tags, the Q value is shifted to the right by 1. For the group of 20 tags the best efficiency is reached at a maximum value of Q=5 instead of Q=4 for the theoretical value. For 100 tags density, the best practical efficiency is obtained with Q=8 while the optimum theoretical value is with Q=7. This theoretical value depicted in Equation 2 does not take into account the use of *QueryAdjust* which restarts a new frame when a collision occurs. Indeed, during simulations we integrate the collision management by calculating N (refered as N_{sim}) according to Equation 3.

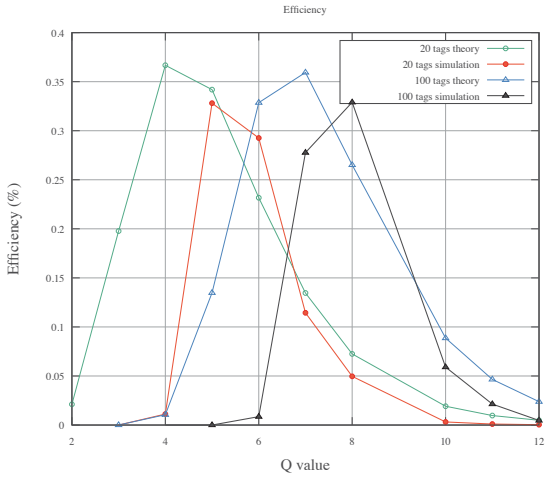

Figure 2. Efficiency for 20 tags and 100 tags

$$N_{sim} = \frac{total\ slot\ offered}{total\ collision\ occurred} \tag{3}$$

The current standard does not define the utilisation of Q in a specific manner. The Q value could remain static, incrementing or decrementing. It is interesting to be able to vary Q in a context where the number of tags rapidly evolved over time. Indeed, this is particularly true when the Q value is small and the number of tags increases. If the process does not dynamically adjusts the Q value then appear numerous collisions during the association. In our evaluation context, we performed several simulation runs with a fixed number of tags for each run, so a fixed value of Q in the same run.

The current Gen2v2 standard enhances the Gen2 standard with the introduction of security functionalities as described as in [3] among which is authentication.

3. Authentication Cryptographic Suites

Several cryptographic suite is introduced to the existing protocol. It applies several lightweight cryptographic such as XOR [4], AES-128 [5], PRESENT-80 [6], CryptoGPS [7], ECC-DH [8], Grain-128A [9], AES-OFB [10], ECDSA-ECDH [11] and RAMON [12].

These cryptographic suites relates to the capabilities of the passive tags to deal with security. This could prevent unauthorized communication between the reader and the tag. In the remaining of the paper, we choose to focus only on the fourth first cryptographic suites as Elyptic curves are not available on most RFID Tags currently available.

3.1. XOR

This authentication algorithm depicted in Figure 3 uses the logical operation called the exclusive OR (XOR). In this algorithm, the reader and all related tags share the same pre-shared key (*PSK*) and a constant O_n. Verification is based on the exchange value passed between the reader and tags. The values come from an operation between the random number(RN), the constant O_n and the *PSK*.

The reader starts the authentication process by sending *SRNi* computed according to Equation 4 where *RNi* is a 64bit random number generated by the reader and O_n is a constant of value 5555 5555 5555 5555h.

$$SRNi = (RNi + O_n) \oplus PSK \tag{4}$$

When a tag successfully receives *SRNi*, it retrieves *RNi* according to Equation 5. As a reminder, O_n and *PSK* are shared by the reader and tags.

$$RNi = SRNi \oplus PSK - O_n \tag{5}$$

Once *RNi* is known, tag calculates the total iteration of '1' in the binary value of *RNi*. By using the total iteration value, it performs a bit-wise rotation to the left on *RNi* and PSK in order to get both *RNi'* and *PSK'*.

The tag finally computes *SORNi* according to Equation 6 and sends it back to the reader.

$$SORNi = (PSK' + O_n) \oplus RNi' \tag{6}$$

In order to verify the authentication process, the reader computes *RNi'* and *PSK'* and performs both operations depicted in Equation 7 and in Equation 8.

$$SORNi \oplus RNi' \tag{7}$$

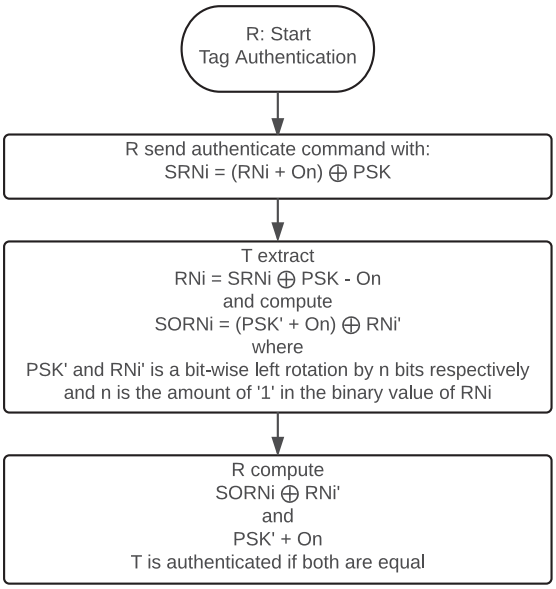

Figure 3. Tag authentication using XOR

$$PSK' + O_n \tag{8}$$

The reader compares results from Equation 7 and Equation 8. As a consequence, the tag is authenticated if results are identical.

3.2. AES-128

AES128 [5] is a variant of a symmetric block cipher called Advanced Encryption Standard (AES) standardized in ISO/IEC 18033-3 [20]. It performs a series of substitutions and permutations. It is designed for very limited resources environment and can be used as a basis for authentication protocols. In Gen2v2, AES128-based tag authentication relies on a challenge/response scheme.

Figure 4 depicts the authentication process. The authentication starts with the reader (R) generating a 80bit random number challenge. The reader broadcasts the challenge along with a key identification (*KeyId*) to be used. When a tag (T) receives the challenge, it encrypts the challenge with the given *KeyId*. A 16bit constant '*C*' and a 32bit random number are then concatenate to the encrypted result (*IChallenge*). The tag finally sends the response to the reader. Based on this response, the reader decrypts the response and retrieves both '*C*' and *IChallenge*. The tag authentication is considered successful if both values are identical.

3.3. PRESENT-80

PRESENT80 [21] is a symmetric block cipher using 64 bits data block with a 80 bits pre-shared key standardized

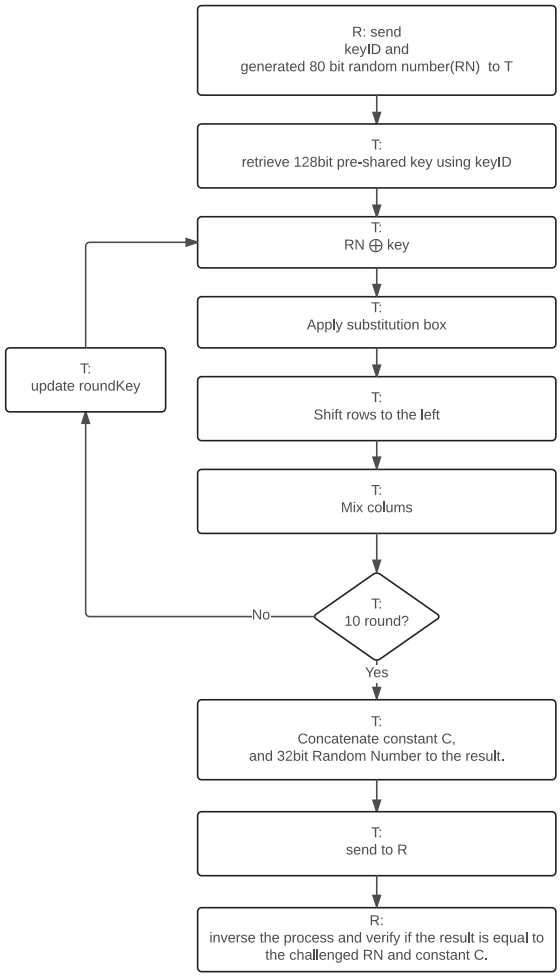

Figure 4. Tag authentication using AES128

in ISO/IEC 29192-2:2011 [22]. Gen2v2 uses this standardized proposition as a cryptographic suite for authentication purposes.

The overall authentication algorithm is a challenge/response protocol similar to the one used in 3.2.

Figure 5 illustrates the overall process. In total, it performs 31 rounds of substitution and permutation. In every single round, tag performs an exclusive OR (XOR) of a 64 bits round key with the challenge (42 bits) sent by *R*. The round key value changed for each round. The first round key is the 64 most significant bits of the 80 bits pre-shared key. To get the next round key, a 61 bit shift to the left is applied to the current round key to get the new round key as presented as in Equation 9.

$$roundKey_1 = key_{79}key_{78}key_{77}...key_{16} \tag{9}$$

The outcome is then passed through a substitution box (S-box) and a bit permutation box (P-Box). Finally, the result is then sent back to the reader in order to be verified.

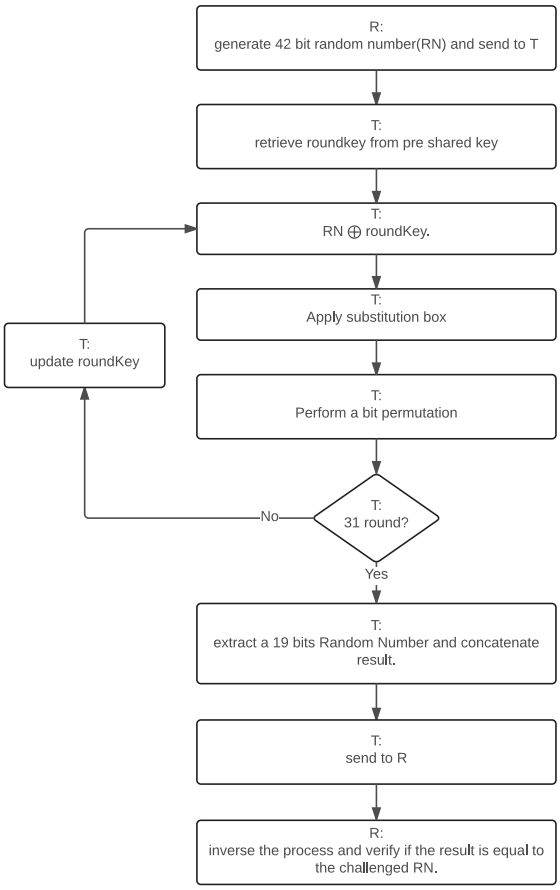

Figure 5. Tag authentication using PRESENT80

3.4. CryptoGPS

CryptoGPS [7] is a lightweight asymmetric identification scheme based on pre-computed coupons from an elliptic curve discrete logarithm problem (ECDLP) based on Equation 10.

$$y^2 = x^3 + ax + b \tag{10}$$

Both reader and tags refer to the same elliptic curve *E* with a field size of *q*, a base point *P* and a multiplier *s*. Any random point *V* on *E* is equal to the multiple of base point *P* as presented as in Equation 11.

$$V = -[s]P = (x_v, y_v) \tag{11}$$

V is the public key and *s* is the private key. Due to the complexity of the CryptoGPS calculation, tags uses coupons, a set of (r_i, X_i), with a precomputed data with the size of ρ-bit string. The coupon must be used only once. Figure 6 highlights the authentication process. To start with, the reader sends an authentication command to the tag. If a tag receives the command, it retrieves a coupon X_i of *x* bytes length and sends it to the reader.

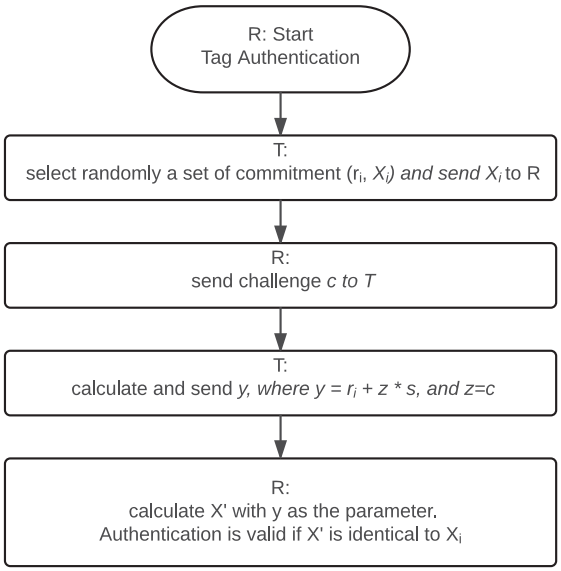

Figure 6. CryptoGPS Commitment Challenge Response (CCR)

When the reader receives X_i, it retrieves randomly c from its list of challenge named S_c and sends it to the tag.

Tag checks if the challenge is an element of S_c. If c is valid, it then computes y according to Equation 12 and sends it to the reader.

$$y = r_i + z * s \tag{12}$$

Upon reception of *y*, the reader can deduce the r'_i value according to Equation 13 where z=c.

$$r'_i = y - z * s \tag{13}$$

With r'_i; the reader can then find X'_i and compare it to X_i. If they are identical, the tag is then authenticated.

4. Model Evaluations

Previous simulation studies in RFID is done by Marino et al. [23] using OPNET, and by Mota and Batista [24] using jRFIDsim that is based on JAVA and R language. Both studies concentrated on looking at different implementation of RFID MAC layer. These contributions howedo not integrate authentication algorithms of Gen2V2 standard.

In our study, we decided to evaluate the impact of *Q* on the authentication process and on the different cryptographic suites presented in section3. To proceed with this, we choose the OMNeT++[14] discrete event simulator. The first step has been to implement a Frame Slotted Aloha and to compare it to the theoretical analysis to enforce the validity of results obtained during the authentication evaluation. This validation has been presented in section 2.

To enforce the confidence in the simulation results, we perform every simulation 30 times. In the remaining of the section, the mean results as well as confidence intervals are provided. Finally, to ensure that every cryptographic is

evaluated under the same conditions, the same seed is used by random generators for every algorithms to evaluate. More specifically as there are 30 runs, the same 30 seeds are used for every algorithm. This control is needed to ensure that collisions will occur on the same time slot for all algorithms and therefore that they encounter the same conditions.

As a reminder, it must be noted that collisions occur when several tags try to transmit during the same time slot. In this case, the standard offers 3 different solutions:

1) The reader ignores the data received and recaps with the rest of the slot.
2) The reader sends a command to the tag to re-generate slot counters and restarts counting.
3) The reader restarts the communication with new parameters.

In this paper, we choose to re-generate the slot counter when a collision occur. The objective is to minimize the total number of slots offered.

The communication scenario that has been used is rather simple: A reader try to perform an association with every tag within its communication range. When the association is carried out, the reader try to authenticate every tag using one of the cryptographic suites.

In the remaining of the section, we will first present the overall performances of the scenario before focussing on the impact of authentication.

4.1. Overall performances

The choice of the Q should depend on the number of tags. A small Q offers a limited number of slots. But, when this number is too low, the number of collisions will increase leading to more retransmissions, hence the additional time to accomplish the task. As an example, for 20 tags when $Q = 2$ only 4 slots are offered. As a result, the lowest number of retransmission occurs when slot 1, 2, and 3 succeed to associate a tag and the remaining is in slot 4. Even with the best scenario, we need at least 6 retransmissions. Thus, the same number of tags with a Q value of 1 will requires a huge number of retransmissions.

Our first result represents the number of tag collisions for different Q values. As depicted in Figure 7, the value of Q has a direct impact on the number of collision a tag may encounter. It reflects our expectation. The collision number is decreasing over the value of Q. While the number of tag is fixed, and the number of slots offered increased, we should have a figure similar to $\frac{1}{x}$. Indeed, each group of tags requires a minimum value of Q to prevent it from having a high collision number. As an example, 20 tags with a Q value of 1 will have difficulties avoiding collisions as every tag's slot counter can only be 0 or 1. Minimizing the collision number requires that the number of slots is larger than the number of tags. As an example, the smallest Q value to accommodate 20 tags is 5.

Therefore, any value between 5 and 15 is suitable to accommodate 20 tags. Of course, the efficiency will be better with a small value of Q as depicted as in section 2.

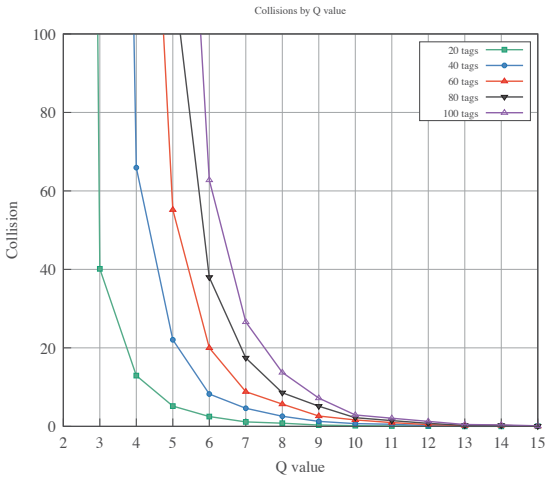

Figure 7. Simulated Gen2V2 collision by Q value

Figure 8 enforces this affirmation showing that the duration to associate the group of tags increases when Q increases. Hence, the negative effect of minimizing collision is the increase of the total duration to associate all tags. But, a small number of collision is better than a zero collision that will reduce the performance of the overall authentication.

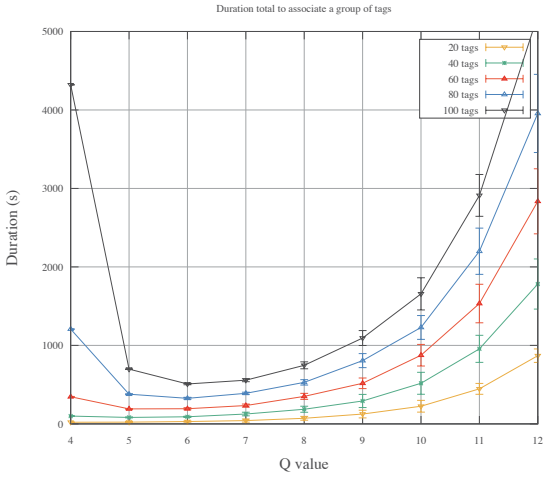

Figure 8. Gen2V2 total duration of association

It is interesting to note in Figure 9 the correlation between the number of collisions and the time required for association. It must be understood that the more the value of Q, the more the duration. This phenomenon is due to the Q values that are greater than 7 leading to a number of time slots greater than 128. This means that on the same frame, the times slots are vacant and that the association process should continue until the end of the frame.

The compromise Duration/Collision for 100 tags is a Q value between 8 and 9. The compromise for 20 tags is the

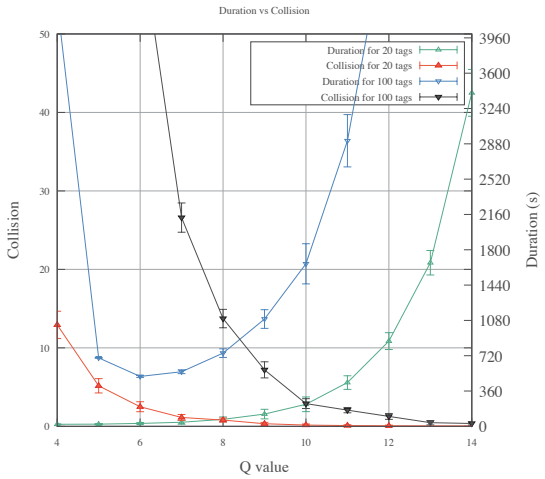

Figure 9. Duration vs Collision for 20 and 100 tags

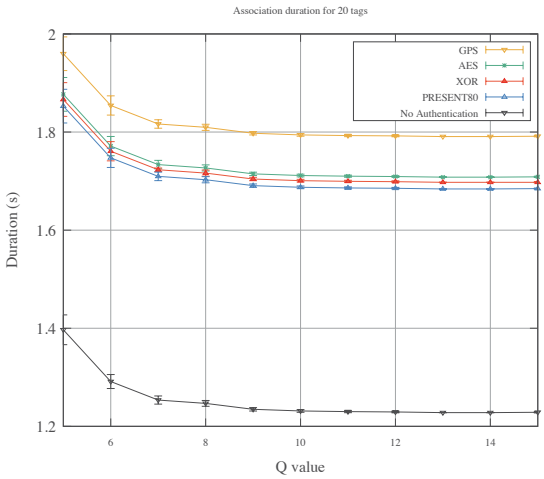

Figure 10. Total duration for 20 tags including authentication

Q value equals to 8. The value of $Q = 8$, with 256 time slots, allows both the 20 and 100 tags' association without degradation of the overall network performances in terms of collisions and useless waiting time.

4.2. Authentication performances

The objective of these simulations is to evaluate whether tag authentication has in impact to the time performance of a Gen2V2 tag system. We choose 4 different algorithms to investigate the total duration to associate a group of tags. The chosen algorithms are XOR, AES128, PRESENT-80 and cryptoGPS. A baseline is set by performing the tag association without any authentication. Then, the algorithms are tested based on the standard given in ISO/IEC 29167 variations. The duration to perform the authentication for each algorithm is then compared to the baseline.

The simulation focusses on a group of 20 and 100 tags. For 20 tags, we choose a Q value of 5 whereas for 100 tags a Q value of 8 will be used. Both of these Q values are based on the figure 2 and depict the highest degree of efficiency.

Figures 10 and 11 show the time induced by authentication schemes after the association phase.

The curves in Figure 10 for 20 tags illustrate the average time needed to perform the association of every tags. It takes about 1.2s to associate 20 tags without authentication while an additional 0.5s is necessary for the authentication with cryptographic suites. For the authentication based on CryptoGPS, we managed to distinguish an additional time that is linked to the mutual authentication between the reader and the tag as presented as in section 3.4. Figure 11 illustrates the results obtained for 100 tags. The shape of the curves is identical to the 20 tags' curves with a scale factor of 5 that is proportional to the evolution of tags numbers (i.e from 20 to 100).

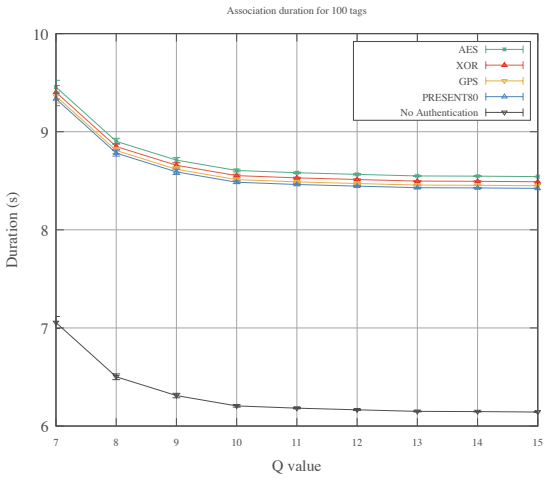

Figure 11. Total duration for 100 tags including authentication

5. Conclusion

In this paper, we presented results of the evaluation of a RFID tags network based on Gen2v2 RAIN RFID standard. This network has a star topology with a single reader and several UHF RFID Tags disseminated within a radius of a hundred meters. In addition to the traditional identification of a tag by a reader, standard version 2 provides authentication mechanisms of both reader and tags to improve network security. Fake or spy tags and readers can no longer connect to this type of RAIN RFID network. In this work, a performance evaluation of several cryptographic suites is performed to evaluate the impact of this additional security feature that is authentication. Due to the lack of RFID Gen2v2 stack simulation models in well-known simulators, we have first modellized the collision management protocol based on Framed Slotted Aloha (FSA)

on OMNeT++. Simulation results of the efficiency have enabled us to validate this basic model measuring the impact of collisions and of execution time with regards to the size of the frames (and thus the number of slots). Four patterns of authentications among the 9 standard were presented, then modelled and simulated with OMNeT++. We wanted to highlight the necessary time to the authentication phase of cryptographic suites XOR, AES, PRESENT and CryptoGPS. These evaluations have helped to show the impact of time required for the authentication process to be considered for secure applications conformed to RFID RAIN standard. The evaluations were considered in an environment with a variable number of tags but with a single reader. Our short-term prospects aim to consider several readers and a dynamic use of the frame size to deal with the number of tags variability. The inclusion of these parameters aims to integrate a tag location information and ensure privacy when tags will worn by people.

References

[1] "RAIN RFID." [Online]. Available: http://rainrfid.org/

[2] "ISO/IEC 18000-63 Information technology - Radio frequency identification for item management - Part 63: Parameters for air interface communications at 860 MHz to 960 MHz type C."

[3] "ISO/IEC FDIS 29167-1:2013(e) information technology automatic identification and data capture techniques part 1: Security services for rfid air interfaces."

[4] "ISO/IEC CD 29167-15 information technology automatic identification and data capture techniques part 15: Air interface for security services crypto suite xor."

[5] "ISO/IEC FDIS 29167-10:2014(e) Information technology Automatic identification and data capture techniques Part 10: Crypto suite AES-128 security services for air interface communications."

[6] "ISO/IEC FDIS 29167-11:2014(e) Information technology Automatic identification and data capture techniques Part 11: Air interface for security services crypto suite PRESENT-80."

[7] "ISO/IEC 29167-17 Information technology Automatic identification and data capture techniques - Part 17: Crypto suite cryptogps security services for air interface communications," 2011.

[8] "ISO/IEC FDIS 29167-12:2014(e) Information technology Automatic identification and data capture techniques Part 12: Crypto suite ECC-DH for air interface communications."

[9] "ISO/IEC FDIS 29167-13 Information technology Automatic identification and data capture techniques Part 13: Air interface for security services crypto suite grain-128A."

[10] "ISO/IEC CD 29167-14 Information technology Automatic identification and data capture techniques Part 14: Air interface for security services crypto suite AES OFB."

[11] "ISO/IEC DIS 29167-16 Information technology Automatic identification and data capture techniques Part 16: Air interface for security services crypto suite ECDSA-ECDH."

[12] "ISO/IEC DIS 29167-19 Information technology Automatic identification and data capture techniques Part 16: Air interface for security services crypto suite RAMON."

[13] "LoRa Alliance." [Online]. Available: https://www.lora-alliance.org/

[14] "OMNeT++, Discrete Event Simulator." [Online]. Available: https://omnetpp.org/

[15] "EPC TM Radio-Frequency Identity Protocols Generation-2 UHF RFID Specification for RFID Air Interface." 2013.

[16] Y. Chen and F. h. Zhang, "Study on anti-collision Q algorithm for UHF RFID," in *Communications and Mobile Computing (CMC), 2010 International Conference*, vol. volume 3, 2010, pp. 168–170.

[17] V. Namboodiri, M. Desilva, K. Deegala, and S. Ramamoorthy, "An extensive study of slotted aloha-based rfid anti-collision protocols," *Comput. Commun.*, vol. 35, no. 16, pp. 1955–1966, Sep. 2012. [Online]. Available: http://dx.doi.org/10.1016/j.comcom.2012.05.015

[18] C.-W. L. Su-Ryun, Sung-Don Joo, "An enhanced dynamic framed slotted ALOHA algorithm for RFID tag identification," ser. MobiQuitous 2005, 2005.

[19] H. Vogt, "Efficient Object identification with passive RFID tags," in *Proc. Int. Conf. on Pervasive Computing, Zurich*, vol. 2414, 2002, pp. 98–113.

[20] "ISO/IEC 18033-3 Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers."

[21] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, *Cryptographic Hardware and Embedded Systems - CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, ch. PRESENT: An Ultra-Lightweight Block Cipher, pp. 450–466. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-74735-2_31

[22] "ISO/IEC 29192-2 Information technology - Security techniques - lightweight cryptography - Part 2: Block ciphers."

[23] F. Marino, G. Massei, and L. Paura, "Modeling and performance simulation of epc gen2 rfid on opnet," in *Measurements and Networking Proceedings (M N), 2013 IEEE International Workshop on*, Oct 2013, pp. 83–88.

[24] R. P. B. Mota and D. M. Batista, "Simulator and benchmark for rfid anti-collision evaluation," in *Application of Information and Communication Technologies (AICT), 2015 9th International Conference on*, Oct 2015, pp. 614–618.

View publication stats