Design and Implementation of an RFID-GSM based Vehicle Identification System on Highways

Fatemeh Nafar and Hossein Shamsi

***Abstract*—In this paper, a real-time RFID-GSM based vehicle identification system compatible with IEEE802.15.4 is designed and implemented at 2.4GHz which provides a full automation of highway scanning far away from the monitoring station. Once RFID reader broadcasts "Auto-Highway-Scanning" RF signal, each tagged-vehicle within the RF-field of 80m from the reader runs a collision-avoidance scheme involving two strategies. Firstly, the unique tag's CC2530F256 SoC MAC address is used to generate a fixed waiting-time. The second strategy utilizes tag's CC2530F256 pseudorandom number generator to add a random value to the first strategy output. This strategy makes the proposed scheme dynamic and secure because it prevents the attackers from accessing to the tag ID by estimating fixed waiting-time of the first strategy. Such a collision-avoidance scheme overcomes the conventional methods constraints such as tag population estimation latency in Aloha-based methods and time-consuming lengthy queries in Tree-based protocols. Simulation results show that the collision is avoided by using the carrier sensing capability and the identification efficiency of 63% is achieved by the proposed scheme, which is more efficient than conventional tag anti-collision schemes such as ISO/IEC 18000-7, CSMA non persistent, CSMA p-persistent, QT, CT and QWT. Besides, experimental results prove above scheme works properly.**

***Index Terms*—active RFID, collision avoidance, ISM band, GSM, random number generation, MAC address**

I. Introduction

Radio Frequency Identification (RFID) is a contact-less non line-of-sight auto-identification technology using RF communications to identify tagged objects. RFID is one of the core technologies of the Internet of Things (IoT) which supports a wide range of tracking and monitoring applications such as barcode replacement, toll collection, supply-chain management, anti-theft immobilizers, automatic vehicle identification (AVI) systems and etc. Tagged-objects play network nodes role in the hybrid infrastructures formed by combination of RFID and middleware, back-end database, internet and etc [1]-[5]. RFID tags could be either active, passive, or semi-passive [2]. Both passive and semi-active tags use backscatter modulation to send information back to the reader [6]. Passive tags are preferred when low cost and long lifetime are sought, but provide less coverage [7]. Since passive tags have no batteries and ICs to perform any on-tag computation, they are cost-effective for the short-range communications. The reader has to continuously radiate energy to power the passive tags. Tag-to-tag coordination and data relaying are challenging in typical passive tags [8]. A near-far problem [9], in the passive RFID system is very common so that a tag that is close will transmit a much stronger signal than one that is far away. Passive/semi-passive tags cannot sense the channel and detect collisions [10]. Active tags have their own power source to transmit RF signals to the reader actively. So, they are more expensive than passive tags. The energy consumption from a battery is one of the disadvantages of an active tag. The activity of an active tag is independent of the electromagnetic waves transmission by the reader. Therefore, active tags can enable longer RF communication range, more computation capabilities, more data storage capacity and extra-functionalities such as carrier sensing. Active RFID systems which utilize active RFID tags, are being applied in vehicle identification and tracking applications [11]-[15].

Tag-to-reader collision occurs when multiple tags transmit their IDs to the reader through a shared wireless channel simultaneously. In a practical environment, tags may conflict with each other's signals and consequently data loss makes the reader incapable of decoding the tag IDs [16]-[17]. Collided tags must retransmit their IDs, which results in performance degradation and wastage of time, energy and bandwidth [11], [18]-[20]. Therefore, an anti-collision mechanism is essential to handle the multipoint-to-point communication in an efficient RFID system.

In this paper, a real-time high efficient RFID-GSM based highway scanning system utilizing a novel collision-avoidance scheme is designed and implemented to perform "Auto-Highway-Scanning" operation at 2.4GHz. As shown in Fig. 1, the proposed system consists of three main infrastructures to provide full automation. The first one (active RFID subsystem) contains a roadside RFID reader and multiple active tags attached to the moving vehicles on highways. The second one (GSM subsystem) contains GSM SIM900 modems and interface boards responsible for long range communication. The third one (monitoring station) contains a developed user interface software on a host PC/Laptop.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2018.2855410, IEEE Sensors Journal

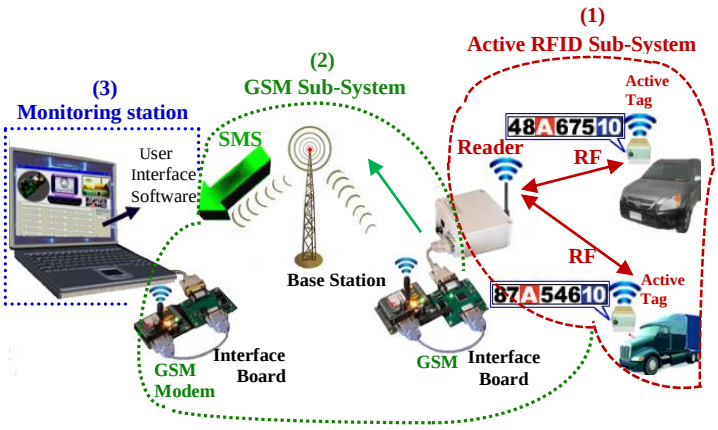

Fig. 1. The overall architecture of the proposed RFID-GSM based vehicle identification system.

The rest of this paper is organized as follows. Section II reviews conventional tag anti-collision schemes. Section III introduces the proposed hybrid system. Section IV describes the proposed collision-avoidance scheme and discusses simulation results. Section V presents the system implementation that covers the RFID subsystem hardware implementation and relevant practical experiments, interface board and GSM modem structure description and user interface software development. Finally, section VI concludes the paper.

II. Conventional Tag Anti-Collision Schemes

Traditional TDMA-based tag anti-collision schemes are classified into Tree-based and Aloha-based methods [1], [18], [20]-[23]. Reading process of a Tree-based algorithm can be modeled by a tree. It splits colliding tags into subsets iteratively, so the performance is sensitive to the tree height (ID length) [21]-[22]. Binary tree algorithm adopts random binary numbers to split the tag set [22]. It uses splitting probability of 0.5 to resolve collided groups [7]. Tree-based algorithms are computationally complex and time-consuming lengthy queries issued by the reader increases the power consumption of the reader and tags. Besides, some bits of tag identifier must be stored at the reader-side (stack or queue) during the identification process. In a deterministic Query Tree method, reader broadcasts a binary string; each tag compares the prefix of its ID with this string and replies to the reader's inquiry if they match [21]. Enhanced Query Tree (EQT) protocol can dynamically adjust the length of prefix code to avoid unnecessary reader's inquiry [24]. The Collision Tree (CT) protocol adopts Manchester encoding to encode tag signals so that the reader can detect collided bits [25]. The QT queries tag's ID directly whereas the CT queries tag's collided bit and splits tags into subsets according to the first collided bit [21], [24]. Although Collision Tracking Tree Algorithm (CTTA), Enhanced Anti-collision Algorithm (EAA) and New Enhanced Anti-collision Algorithm (NEAA) [19] all adopt bit tracking technology based on Manchester code that allows the reader to detect the locations of collided bits in a collision slot [11], but still face collision occurrence at the start of identification and cannot avoid the idle cycle [22]. In consequence, their overall identification efficiency is smaller than 50% [18], [23]-[26]. Compared with an ALOHA-based algorithm, tree-based algorithms do not suffer from tag starvation, but still generate many collision slots in the face of long tag IDs [27].

In Aloha-based algorithms the reader broadcasts a frame length (F) and each tag randomly picks one time-slot between 1 and F [2], [28]-[29]. The most important issue in Aloha-based systems is to predict and adjust the frame length exactly. Such algorithms suffer from tag starvation problem in which a tag may never be identified because its responses always collide with others. Besides, each tag needs a random number generator and a synchronization circuit. If the number of tags becomes large or dynamic, the identification performance will be declined [23]. Frame Slotted Aloha (FSA) is a static probabilistic algorithm which needs to know the frame size. When the difference between the number of the tags and the frame size is large, the throughput of FSA becomes low [28]-[29]. Dynamic frame slotted ALOHA (DFSA) has been adopted by some RFID standards, including ISO 14443–3, ISO 18000–6C, and EPCglobal UHF Class-1 Generation-2 [30]. DFSA initially estimates the number of tags in the interrogation area, and then calculates the optimal frame size for the next reading cycle [31].

Two bodies are responsible for RFID air interface standards: International organization for standardization (ISO) and EPCglobal. Electronic Product Code (EPC) is a global automated universal identification system service. ISO/IEC 18000 consists of several standards that define the air interface for RFID devices. Part 7 of ISO/IEC 18000 (ISO/IEC 18000-7) is an international anti-collision standard based on Frame Slotted Aloha (FSA) for active RFID systems at 433MHz band [10]. In ISO/IEC 18000-7, Reader broadcasts wake up signal and collects data from all the tags within its coverage area through multiple collection rounds. Three steps of each collection round include collection command, listen period, and acknowledgement period. Frame Slotted ALOHA arbitration protocol adopted for the ISO/IEC 18000-7 standard results in a system throughput of about 0.328. The deference of 0.04 from the theoretical value of 0.368 is mainly due to the estimation error in the tag population [32]. ISO/IEC 18000-7 does not have enough capability to retrieve data from a massive number of tags in a timely manner [33]. Besides it has drawbacks of poor performance and slot synchronization overhead. ISO/IEC 18000-7 can use only one channel which has 433.92MHz as its center frequency [10]. EPCglobal develops industry-driven RFID air interface standards such as EPC C0/1 for read-only passive tags, EPC C2 for passive tags with additional functionalities, EPC C3 for semi-passive tags, EPC C4 for active tags with broad-band peer-to-peer communications, EPC C5 for readers which can power class 1, 2 and 3 tags and communicate with classes 4 and 5. EPC Class 1 Generation 2 (EPC C1 G2) is in use by passive Ultra-High Frequency (UHF) RFID tags in supply chain management, industrial RFID systems, inventory checking, driver's license and access control applications [30]. EPC C1 G2 provides the physical layer and MAC layer specifications for passive UHF RFID tags at 860–960 MHz frequency with 30m communication range [15], [34-37]. It takes advantage of Q-algorithm to determine the number of time slots required at each query. Q-algorithm is a frame slotted aloha-based algorithm which randomizes access time of tags to reduce collisions. Frame size (L) is dynamically updated

by means of the parameter named Q (L = 2Q) [38]. The identification process in EPC C1 G2 includes several commands: Select, Query, Query Adjust, Query Repeat, and Ack [31]. In Q-algorithm, not only the hidden tags but also the tags collided in a previous frame will enter the next frame.

Pseudorandom Generation (PRNG) and Cyclic Redundancy Code (CRC) are the only supported functions by passive UHF RFID tags in EPC C1 G2. PRNG and CRC functions cannot be used instead of cryptographic algorithms. Also there is no RFID authentication technique in EPC C1 G2. So, tags are vulnerable to simple counterfeiting and man-in-the-middle attacks.

EPC C1 G2 standard, under ideal conditions, theoretically adds 10% overhead in terms of delay to the basic FSA protocol [39].

IEEE802.15.4 devices like CC2530 can listen to the channel and CCA is one of CC2530F256 Radio capabilities in CC2530-based active RFID tags [12]-[13]. CSMA have been used in some RFID systems [12], [13], [20], [31], [40]-[43]. The basic idea in CSMA is to decide to transmit or back off the packets according to the channel conditions [24]. If the channel is busy, the node will wait for a randomly chosen period of time, and then will check the channel again. This period of time is called the backoff factor and is counted down by a counter. If the channel is clear when the backoff counter reaches zero, the node will transmit the packet, otherwise the backoff factor is set again. The European standard ETSI EN 302 208 for RFID readers uses a CSMA based protocol called "Listen Before Talk (LBT)" to reduce the reader collision problem [31], [42]. The reader first listens on the data channel for any on-going communication for a specified minimum time. If the channel is idle for that time, it starts reading the tags. If the channel is not idle, it chooses a random backoff.

Passive tags are not able to sense the channel and utilize CSMA. In RCSMA [20], the reader notifies the tags channel condition. According to different sensing results of reader's notifications, the tags take corresponding actions, e.g., random backoff. Carrier sense medium access data communication protocol that dynamically adjusts its back-off algorithm [43] is an instance of carrier sensing in an active RFID protocol. CSMA-based MAC protocols still suffer from traditional backoff scheme and face hidden and exposed terminals problem.

Due to limited presence time of mobile tags passing through the reader's RF-field in the mobile RFID systems, there are burst and dynamic variations in the number of tags and arriving tags may collide with staying tags [44]. Thus a dynamic mechanism flexible to the number of tags or a novel technique independent of the RFID network density would be applicable as an efficient anti-collision method.

III. Proposed System

Communication model of the RFID subsystem is Reader Talks First (RTF). Implemented reader and tags are low-power radio nodes. In order to retrieve presented number plates on a highway, RFID reader broadcasts "Auto-Highway-Scanning" RF signal at 2.4GHz periodically. All of the tags within the RF-field of 80m from RFID reader, transmit their ID over the same RF channel by using a novel collision avoidance scheme. CRC and checksum computation beside data transmission is performed. Number plates of tagged-vehicles are sent through SMS (text mode) on digital cellular network. Fig. 2 illustrates the layered architecture of the suggested RFID-GSM based vehicle tracking system. Table I and II summarize the system specifications [44]-[46].

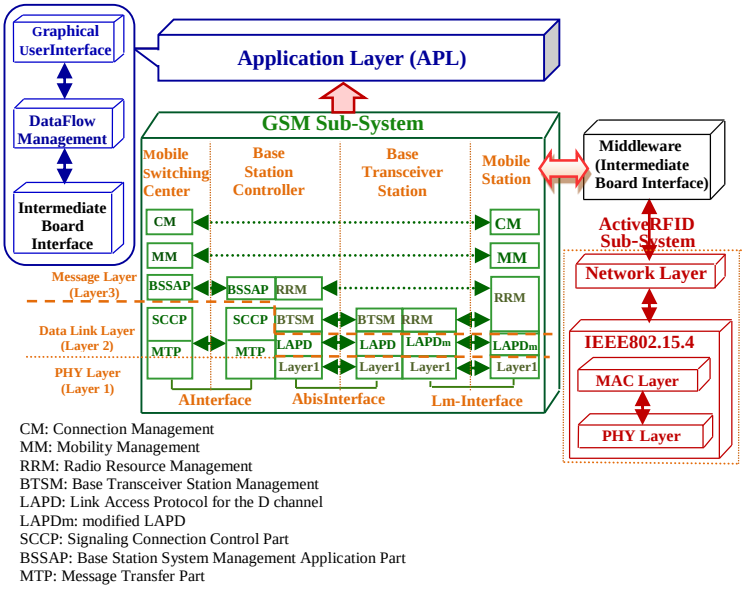

Fig. 2. The hierarchical layered structure of the system.

TABLE I
RFID SUBSYSTEM SPECIFICATIONS [45]-[46].

Subsystem	Reader/ Tag Parameters	Value	Unit
Active RFID Subsystem	RF frequency range	2.394~2.507	GHz
	Tag power consumption(Sleep Mode)	2.64	μW
	Reader power consumption	95.7	mW
	Tag power consumption(Active Mode)	68.64	mW
	RFID subsystem coverage range	80	m
	8-bitMCU+RFModule	CC2530F256	-
	Reader/Tag Software Stacks (CC2530F256)	Z-Stack TIMAC SimpliciTI RemoTI RF4CE	
	In-System Programmable Flash Memory	256	kB
	RAM	8	kB
	Core Frequency	32	MHz
	Number of channels	16 Channel 11~26	-
	Modulation	O-QPSK	-
	Pulse Shaping Filter	Half -Sine	-
	PHY/MAC Layers Standard	IEEE802.15.4	-
	Link Budget	101.5	dB
	Radio Bit Rate	250	kbps
	Symbol Rate	62.5	ksymb/s
	Radio Chip Rate	2	Mchip/s
	Channel Space	5	MHz
	Bandwidth	2	MHz
	Receiver Sensitivity	-97~ -88	dBm
	ReaderDipole Antenna Gain	5	dBi
	Tag Stub Antenna Gain	1	dBi
	Transmitter Output Power	-28~ +4.5	dBm
	Reader Board Dimensions	58×54	mm^2
	Tag Board Dimensions	51×48	mm^2

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2018.2855410, IEEE Sensors Journal

TABLE II
GSM SUBSYSTEM SPECIFICATIONS [44].

Subsystem	Parameters	Value	Unit
GSM Subsystem	Dual-band GSM/GPRS Module	SIMCom-SIM900	-
	Frequencies	EGSM900/ DCS1800 2/2+Class 4(2W- 900) 2/2+Class 1(1W-1900)	MHz
	Channel Number	1-124	-
	Channel Space	200	kHz
	Module Current Consumption	1.5 (Sleep mode)	mA
	Antenna Frequency range	824-960 /1710-1990	MHz
	Antenna Gain	2	dBi
	Specifications for SMS	Point to point MO and MT SMS cell broadcast (Text /PDU mode)	-
	Flash Version	64	MB
	GSM Modem Voltage Range	6~12	V
	GSM Modem Current Consumption	580	mA
	Baud Rate(Serial)	9600	bps

IV. PROPOSED COLLISION-AVOIDANCE SCHEME

The proposed RFID-GSM based vehicle identification system utilizes a novel collision avoidance protocol utilizing unique identifier and pseudorandom number generator of CC2530F256 SoC. The main chip of the RFID reader/tag hardware structure is TI's CC2530F256 which supports the ZigBee, ZigBee PRO and RF4CE standards and mainly is used in sensor networks and ZigBee PRO mesh networks [45]-[46]. There are four software stacks available for the CC2530F256: The Zigbee protocol stack Z-Stack, the IEEE802.15.4 MAC stack TIMAC, TI's proprietary SimpliciTI stack, and the RemoTI RF4CE stack. All active RFID tags will keep sleeping until an external interrupt wakes them up and make them leave the sleep mode. RFID reader broadcasts "Auto-Highway-Scanning" RF signal in a multi-vehicle highway periodically. Upon broadcasting "Auto-Highway-Scanning" command, RFID reader switches to the receive mode and stays in this mode during the scanning period. Once Start-of-Frame Delimiter (SFD) in "Auto-Highway-Scanning" frame is received by each tagged-vehicle within the RF-field of 80m from the reader, the SFD flag will be raised to trigger SFD interrupt and frame reception starts with SFD detection. So, all active RFID tags receive scanning command at the same time and run the proposed collision-avoidance scheme so that the response times of different active RFID tags differ from one another. Such different response times are generated based on the IEEE-defined 64-bit Extended Unique Identifier (EUI-64) of CC2530F256SoC which is used to address hardware interfaces within existing IEEE802 or IEEE802-like networking applications. EUI-64 has been located in CC2530F256 flash memory information page [45]-[46].

Fig. 3 illustrates a schematic view of the IEEE802.15.4 frame format at the RFID subsystem.

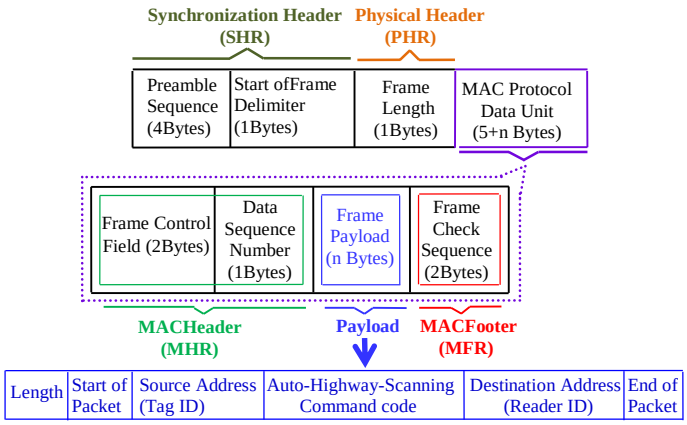

Fig. 3. Schematic view of the IEEE 802.15.4 frame format.

$$Frame\text{-}time=(SHR+PHR+MHR+payload+MFR)/Radiobit\ rate \quad (1)$$
$$Frame\text{-}time=(5_{Bytes}+1_{Bytes}+3_{Bytes}+18_{Bytes}+2_{Bytes})\ /250_{kbps}=0.906ms$$

$$Propagation\ delay = \frac{distance}{c} = \frac{80m}{3\times10^8 m/s}=0.266\mu sec \quad (2)$$

where c is the speed of light in vacuum. According to the CC2530F256 SoC data sheet [46]:

$$T_{RX/TX\ turnaround} = 192\mu sec$$

T_{slot} represents the minimum time required for a tag to introduce itself to the reader in the single tag coverage area as follows:

$$T_{slot}=T_{RX/TXturnaround}+Frame\text{-}time+Propagation\ delay=1.098ms \quad (3)$$

A. The First Strategy Description

The IEEE-defined 64bit Extended Unique Identifier (EUI-64) of CC2530F256 SoC in each tag is formed as a concatenation of a 24 bit Organizationally Unique Identifier (OUI) value assigned by the IEEE Registration Authority (IEEE RA) and a 40bit extension identifier assigned by the organization. Considering 64bit EUI as the base of unique waiting-time for each tag leads to a long waiting-time and prolonged highway scanning operation. So, 24bit OUI between $(00\ 00\ 01)_{Hex}$ and $(FF\ FF\ FE)_{Hex}$ in each tag's CC2530F256 flash memory information page is passed into $log_2^{(OUI)}$ function. $log_2^{(OUI)}$ is an injective function (one-to-one) by which a wide domain of all CC2530F256s Organizationally Unique Identifiers (OUI) are mapped into a restricted range of unique outputs with low dispersion. The unique waiting-time for each tag is based on the unique output of this function. The time complexity of this function is *O(log n)* which means time goes up linearly while the size of the input goes up exponentially. In terms of time complexity, this function is better than Query Tree (QT), Bitwise Arbitration (BTA), and Tree Splitting (TS) methods whose time complexities are O(n), $O(2^k)$, and O(n) respectively where n denotes the number of tags and k represents the length of tag's ID [47]. Inequality (4) represents a time complexity comparison of the functions which are commonly encountered when analyzing algorithms. "*c*" is an arbitrary constant.

$$O(1)<O(log(n))<O(n)<O(n\times log(n))<O(n^2)<O(n^c)<O(c^n)<O(n!) \quad (4)$$

Fig. 4 illustrates $log_2^{(OUI)}$ function which is used by the first strategy.

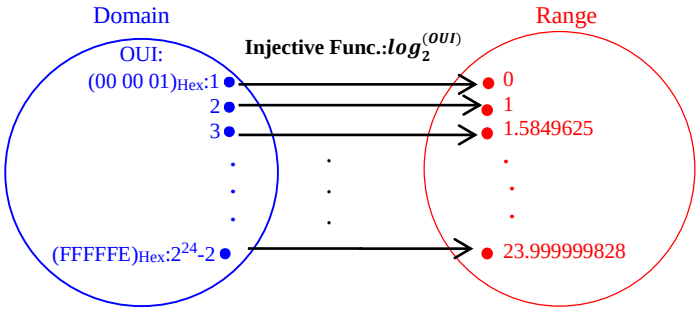

Fig. 4. The first strategy injective function.

By defining such a function in the tag's firmware, there is no need to deploy a central management, which is aware of all tags unique identifiers and therefore the implementation complexity is reduced.

In order to avoid tag-tag collision, it is imperative that the waiting-time of each tag becomes an integer multiple of T_{slot}. According to equation (5), T_{W1} denotes the output of the first strategy. Utilizing the bracket function in equation (5) causes T_{W1} to be an integer multiple of T_{slot}:

$$T_{W1}=[a\ log_2^{(OUI)}]\times T_{slot} \quad (5)$$

B. The Second Strategy

The second strategy has two main advantages: reducing the collision probability and making the proposed scheme more secure. The output of the first strategy is a fixed waiting-time for each tag in every scan. This waiting-time can be considered as a security bottleneck. Because in addition to the conventional security threats on tag's ID, such as jamming, blocking, cloning, eavesdropping, and non-invasive side channel attacks [49], attackers can access to the tag ID by estimating the fixed waiting-time. Pseudorandom number generator which is supported by CC2530F256, is a 16-bit linear-feedback shift register with polynomial $x^{16} + x^{15} + x^2 + 1$ which is routinely utilized to generate random security keys. So, there is no need to add a random number generator hardware structure in our work. A seed for the LFSR is formed by sampling the IF_ADC random value in the RF receive path. In order to use this seeding method, the radio is placed in the infinite RX state to avoid possible sync detect in the RX state. The random seed values are read from the RF register called RFRND. The RSSI value is the result of averaging the received power over eight symbol periods as specified by IEEE802.15.4 [46]. The RSSI-VALID status signal can be used to verify that Clear Channel Assessment (CCA) signal becomes valid [45]-[46]. CCA is one of CC2530F256 Radio capabilities in each active tag. The CCA is based on Received Signal Strength Indicator (RSSI) value and has programmable threshold value in dBm. Radio detects a busy channel when the RSSI value is greater than the threshold and an idle channel when the RSSI value is less than the threshold [45]-[46].

According to equation (6), *Rand* represents the random value between 0 ~ *Randmax* which is produced by the pseudorandom number generator in the second strategy.

$$T_{W2}=[Rand]\times T_{slot} \quad (6)$$

where *Rand* ϵ [0, *Randmax*]

Finally, the overall waiting time T_W is obtained as follows:

$$T_W = T_{W1}+T_{W2} =\left([a\ log_2^{(OUI)}]+[Rand]\right)\times T_{slot} \quad (7)$$

Utilizing the bracket function in equation (7) causes T_W to be an integer multiple of T_{slot}.

Upon receiving "Auto-Highway-Scanning" command from the reader, each tag runs two strategies of the proposed collision-avoidance scheme. Each tag upon spending the overall waiting time generated by two strategies, uses CCA to sense the channel before transmitting its ID. In this way it ensures that the channel is idle. In busy channel condition, the tag retries to transmit its ID for a limited number of times and Retry_counter holds the number of times that tag retries to transmit its ID. Retry_counter counts up until reaching the maximum value (n). Upon receiving a tag ID, RFID reader acknowledges it by issuing an ACK frame to the relevant tag. Once it is acknowledged, the tag ensures that there are no tag-tag collisions. So when the ACK is not received within a timeout interval, that tag will increase its Retry_counter value by 1. The tag will retransmit its ID if its Retry_counter is less than n. The tag will switch to the sleep mode when it receives ACK from the reader or its Retry_counter becomes n. The flowcharts of Active RFID Tag and RFID Reader are illustrated in Fig. 5(a) and 5(b) respectively.

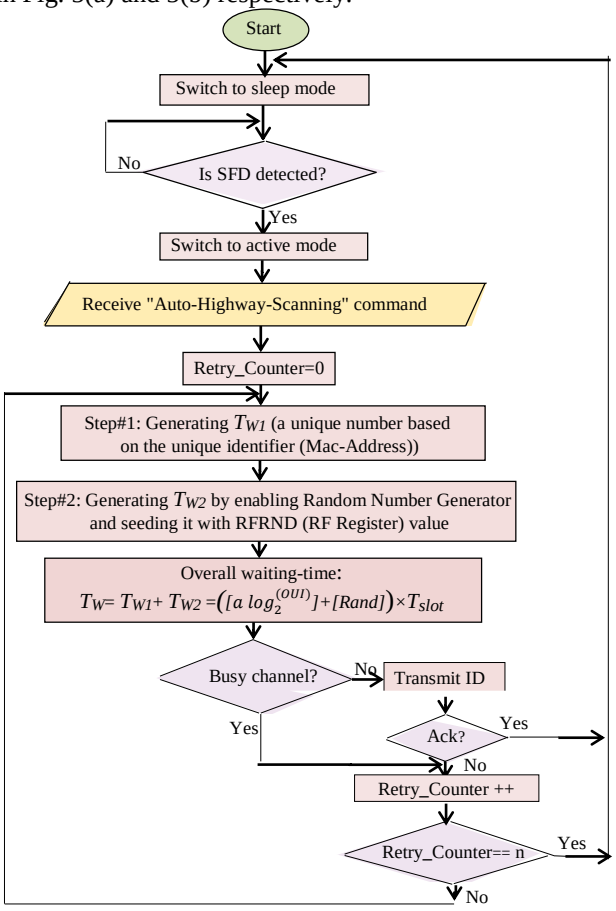

Fig. 5(a). Active RFID Tag flowchart.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2018.2855410, IEEE Sensors Journal

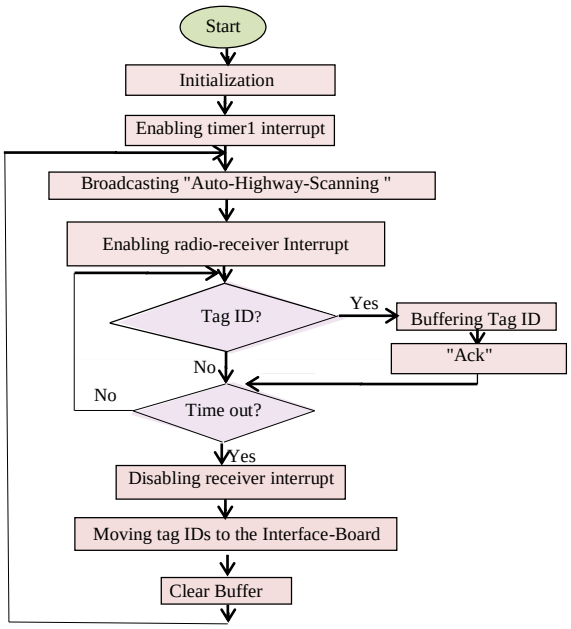

Fig. 5(b). RFID Reader flowchart.

"Identification efficiency", η denotes the ratio between "the number of identified tags" to "the total number of tags passing through the reader's RF-field", which is calculated as follows.

$$\eta = 1 - \left(\frac{D-R}{D} \times \frac{M}{R}\right) \quad (8)$$

where D is the number of unique inputs based on the tag's OUI. M is the average number of tagged-vehicles in the reader's reader's RF-field. R is the number of the T_W function outputs (range).

For an injective function (one-to-one), we have: $R=D$ and $\eta=1$. Obviously, in this work T_W is not an injective function because its range is more limited than its domain to avoid an extremely long waiting-time/scanning.

$$D=((2^{24}-2) - 1)+1=16777214$$

In order to achieve the highest possible value for the identification efficiency (η) and lowest value for the average waiting-time ($\overline{T_W}$), the optimum values must be assigned to "*a*" and "*Randmax*" which are considered as the design parameters of the proposed function in equation (7). "*a*" represents the *log* coefficient and "*Randmax*" denotes the maximum allowed value for T_{W2}. As shown in Fig. 6, by sweeping "*Randmax*" between $3\times T_{slot}$ and $36\times T_{slot}$ properly, two diagrams including *"Identification efficiency* (in %)" and "*Average waiting-time* (in Tslot)" both versus "*a*" are plotted.

As shown in Fig.6, selecting optimum values for "*a*" and "*Randmax*" requires a trade-off between the identification efficiency (η) *and* average waiting-time ($\overline{T_W}$).

Selecting $a=3$ & $Randmax=9$ results in T_W to be an integer multiple of T_{slot} between 0 and $80\times T_{slot}$.

The maximum output of $80\times T_{slot}$ is obtained when *OUI* has the maximum value of $(FF\ FF\ FE)_{Hex}$.

$$T_{wmax}=[3\times log_2^{(14+(15\times16)+(15\times16^2)+(15\times16^3)+(15\times16^4)+(15\times16^5))}]+9)\times T_{slot}$$
$$=([3\times log_2^{(16777214)}]+9)\times T_{slot}=80\times T_{slot}$$

So,

$$R=(T_{wmax} - 0)+1=(80 - 0)+1=81$$

The identification efficiency with the average number of 30 tagged-vehicles in the range of 80m from the reader is calculated as follows:

$$\eta = 1 - \left(\frac{16777214-81}{16777214} \times \frac{30}{81}\right)=63\ \%$$

$$\overline{T_W} = \overline{T_{W1}} + \overline{T_{W2}}=39\times T_{slot}$$

$$\frac{\overline{T_{W1}}}{\overline{T_{W2}}}=8.75$$

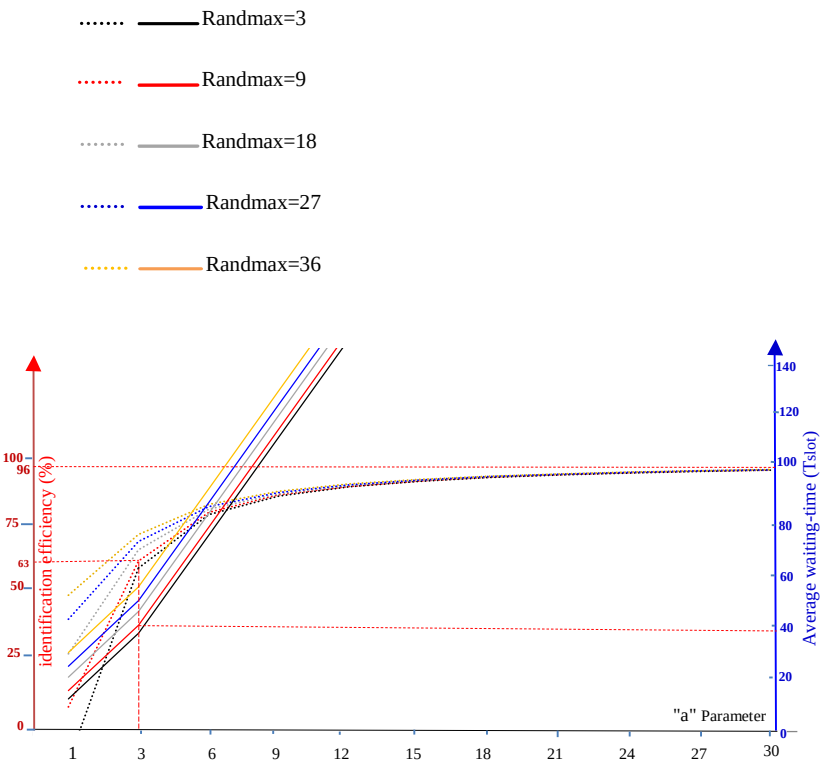

Fig. 6. The identification efficiency and average waiting time both versus "*a*" parameter.

Fig. 6 and above results are obtained for a system with 30 tagged vehicles. If the number of tags varies, the above design methodology should be repeated similarly. Making use of MATLAB simulation, the optimum values for "*a*" and "*Randmax*" parameters are reported in Table III.

TABLE III
THE OPTIMUM VALUES FOR "a" AND "Randmax"

Num of Tags	100	200	300	400	500	600	700	800	900	1000
Optimum "Randmax"	6	12	18	24	30	36	42	48	54	60
Optimum "a"	11	22	33	44	55	66	77	88	99	110
Efficiency	63%	63%	63%	63%	63%	63%	63%	63%	63%	63%
$\overline{T_W}$ *(Tslot)*	134 Tslot	269 Tslot	404 Tslot	539 Tslot	674 Tslot	809 Tslot	944 Tslot	1079 Tslot	1214 Tslot	1349 Tslot
$\overline{T_W}$ *(ms)*	147 *(ms)*	295 (ms)	443 (ms)	591 (ms)	740 (ms)	888 (ms)	1036 (ms)	1184 (ms)	1332 (ms)	1481 (ms)

Assuming 63% identification efficiency, in Fig. 7(a), the average total number of Tslots, which is required for identification, versus the number of tags are depicted. It is obvious that by increasing the number of tags, more time slots are needed.

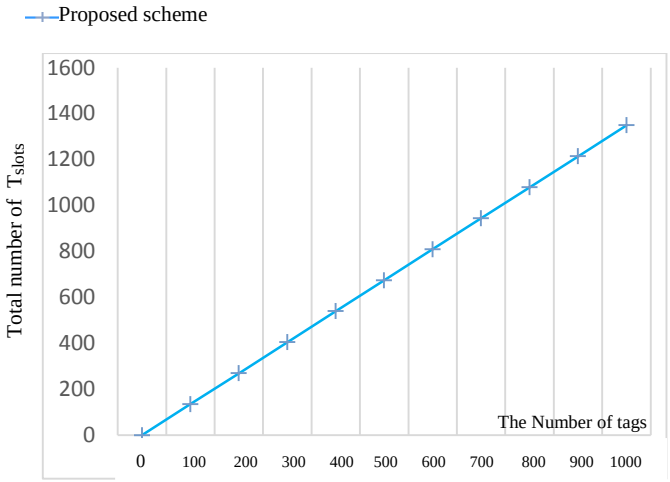

Fig. 7(a). Required T_{slots} for identification versus the number of tags.

In Fig. 7(b), tag density is the simulation parameter that increases from 0 to 100. Fig. 7(b) depicts the identification time in milliseconds versus the number of tags, in which the tag density increases from 0 to 100. As shown in Fig. 7(b), the proposed scheme requires less time than the conventional anti-collision protocols for active RFID systems such as ISO/IEC 18000-7 (k=64), CSMA non persistent (k=8) and CSMA p-persistent (k=8) [32].

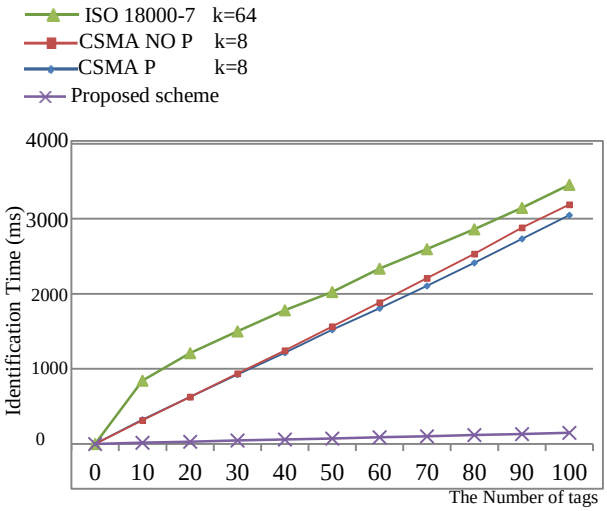

Fig. 7(b). Identification time versus the number of tags.

Fig. 7(c) also depicts the identification time in milliseconds versus the number of tags. As a drawback the identification time of the proposed scheme is not better than CT, OQTT and CWT [7]. In order to improve the identification time of the proposed scheme in comparison with OQTT and CWT, as a tradeoff we can scarify the efficiency by appropriate selection of parameters "*a*" and "*Randmax*".

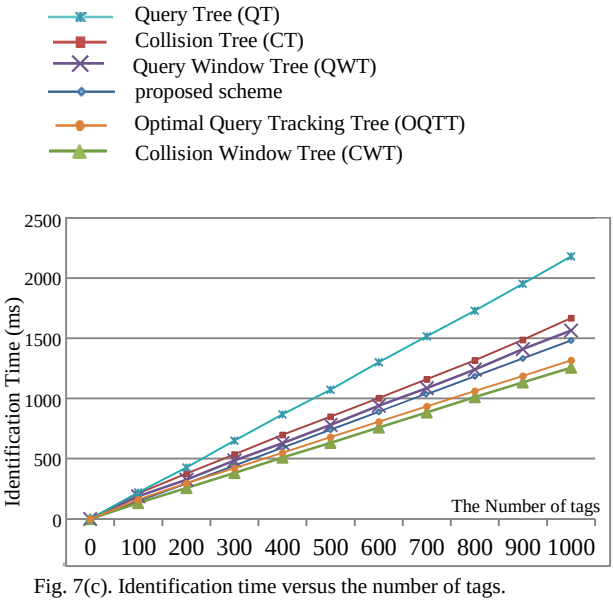

Fig. 7(c). Identification time versus the number of tags.

Fig. 7(d) illustrates the identification efficiency versus the number of tags, which depends on the system hardware design and physical implementation parameters. As a result of the carrier sensing capability of active tags and hardware implementation with 250kbps data rate, the collision is avoided and the identification efficiency of 63% is achieved. Remaining a tag unidentified during the scanning process is the only challenge of the proposed scheme. Such a problem has been handled by choosing the optimum values for "*a*" and "*Randmax*" parameters. The proposed system is more efficient than [7], [16] and [32], which have the data rate of 80kbps, 160kbps and 10kbps respectively. According to Fig. 7(d) and table IV, the suggested scheme identification efficiency is about 63%, which is better than QT, FSA, DFSA, CT, EQT, OQTT and CWT [50].

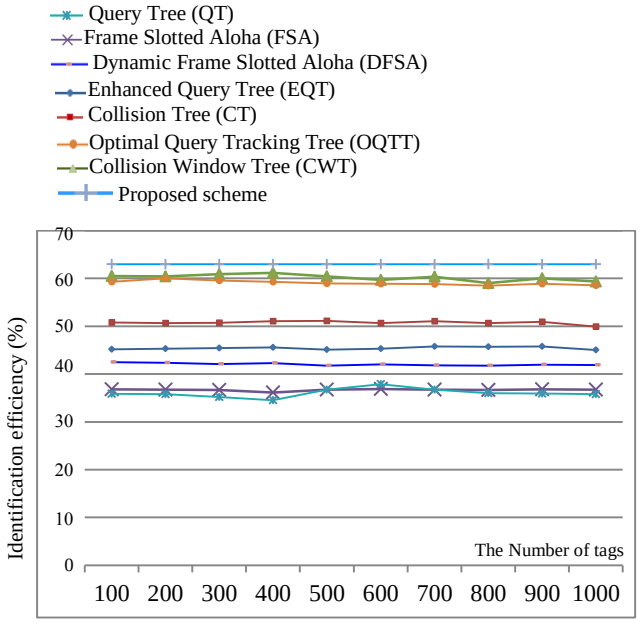

Fig. 7(d). Identification efficiency versus the number of tags.

TABLE IV
COMPARISON OF THE ANTI-COLLISION PROTOCOLS IDENTIFICATION EFFICIENCY. [3], [10], [11], [23], [24], [31], [51], [52]

Anti-collision Protocols	Identification Efficiency (%)
ISO/IEC 18000-7	32.8
Pure Aloha (PA)	18.4
Frame Slotted Aloha (FSA)	36.8
Dynamic Frame Slotted Aloha (DFSA)	42.6
Query Tree (QT)	35
EPCglobal UHF Class-1 Generation-2	36.1
Enhanced Query Tree (EQT)	45
Collision Tree (CT)	50
EPCglobal UHF Class-1 Generation-2	36.1
Optimal Query Tracking Tree (OQTT)	59
Collision Window Tree (CWT)	60.4
Proposed hybrid scheme	63

The key improvements obtained by the proposed collision-avoidance scheme, are as follows: There is no need to estimate tag population during scan process within the reader's RF-field. The performance of Aloha-based algorithms is significantly affected by the initial frame size, furthermore because of the tag population estimation latency, reading of mobile tags before leaving the reader's scope is missed. The first strategy in our scheme, eliminates the risk of random access.

Compared with the Tree-based protocols, described scheme not only eliminates the latency bottleneck caused by lengthy queries and prefix matching, but also avoids any on-reader computation and reader memory usage during scanning, so total number of exchanged packets, communication overheads, energy consumption and computational cost/complexity at the reader-side are declined.

In comparison with CSMA/CA, the problem of waiting for a pure random period of time in the busy channel condition is solved.

Furthermore, in comparison with traditional RFID-based vehicle tracking systems, GSM subsystem utilization has extended the coverage area. In this way, the real-time vehicle tracking on a road/highway far away from the monitoring station becomes possible.

V. SYSTEM IMPLEMENTATION

Cost effective hardware design, implementation and test of the RFID reader, active RFID tag and interface board are carried out in this work. Single-chip designing, in which MCU, 2.4GHz IEEE802.15.4 compliant RF transceiver and pseudorandom number generator are integrated in a CC2530F256 SoC, not only avoids the need of costly extra hardware and minimizes hardware dimensions, but also prevents circuit complexity and high frequency noises.

A. RFID Reader

The key task of the roadside RFID reader is to detect the passing tagged-vehicles in the range of 80m and transfer the collected IDs to the GSM subsystem. The hardware of the reader includes a microprocessor and a 2.4GHz IEEE802.15.4 compliant RF transceiver integrated in a low-power single chip, a bi-directional 2.4GHz antenna, and a peripheral serial interface to perform monitoring. Power consumption of the RFID reader is 95.7mW. Fig. 8(a), 8(b), and 8(c) illustrate the implemented hardware, structure diagram and power consumption pie diagram of the RFID reader respectively.

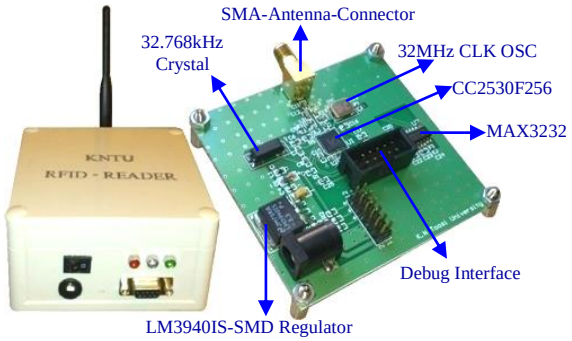

Fig. 8(a). Implemented RFID Reader hardware.

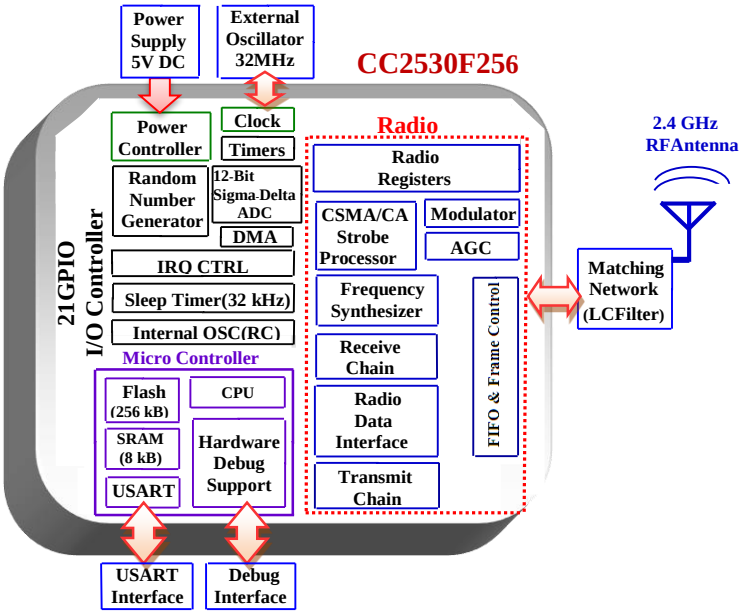

Fig. 8(b). RFID reader structure diagram.

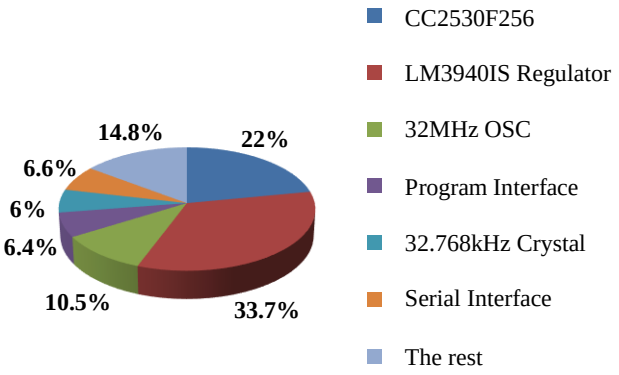

Fig. 8(c). RFID reader power consumption pie diagram.

B. Active RFID Tag

An active rewritable RFID tag capable of channel sensing and collision detecting is designed and implemented at 2.4GHz. It saves a lot of space in the hardware and does not need SPI or I^2C interfaces between RF and MCU modules. Each tag is attached to a vehicle and powered by the 12V DC vehicle battery to reduce the overall cost. Switching to the sleep-mode by using the CC2530F256 ultra-low power sleep timer in each tag is an energy-efficient solution to reduce the tag power consumption while waiting for an incoming interrogation

signal. At the sleep-mode, the digital voltage regulator, 16MHz RCOSC and 32MHz crystal oscillator are disabled; SRAM and internal registers retain their contents and 32.768kHz XOSC, POR, and sleep timer are active. On this basis, the designed active tag only consumes 2.64μW in the sleep-mode, meanwhile 68mWpower consumption is achieved in the active mode [45]-[46]. The implemented hardware and power consumption pie diagram of the active RFID tag are shown in Fig. 9(a) and 9(b) respectively.

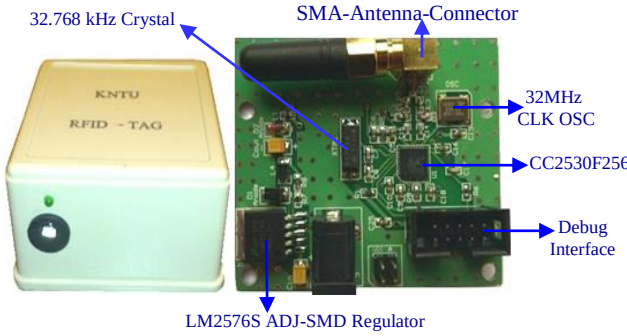

Fig. 9(a). Implemented active RFID tag hardware.

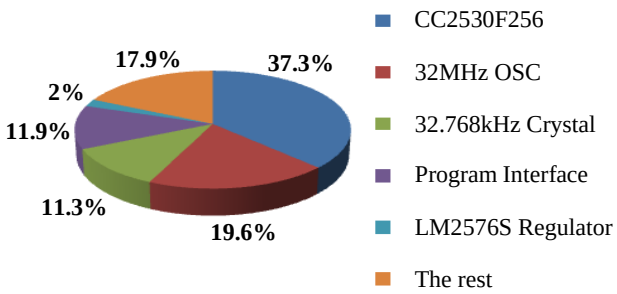

Fig. 9(b). Active RFID tag power consumption pie diagram.

C. RFID Subsystem Practical Tests

IEEE802.15.4 specifies the PHY/MAC layers of the proposed RFID subsystem by using DSSS (O-QPSK) modulation with half sine wave pulse shaping at 2.4GHz unlicensed ISM band. CC2530 has a 2.4GHz IEEE802.15.4 compliant RF transceiver. So, low-power wireless communication with the transmission rate of 250kbps is supported by CC2530-based RFID reader and tags as wireless nodes of the RFID subsystem [45]-[46].

LOS radiation, reflections, diffractions and scattering from static obstacles and moving vehicles lead to multipath fading and shadowing on highways. Rayleight and Rician multi-path fading are dependent on Doppler shift [51]. Ignorable Doppler shift of DSSS (O-QPSK) at 2.4GHz in the developed system results in precise identification while tagged-vehicles are moving at high speed relative to the fixed roadside RFID reader. According to Fig. 10(a), the RSSI level is higher than the receiver sensitivity threshold for distances smaller than 80m between the reader and tag. As shown in Fig.10(b), the Packet Error Rate (PER) is increased with increasing the distance. Making use of Texas Instruments SmartRF Studio 7 software [52], these experiments performed for two different TX output powers to ensure the proper operation of the RFID subsystem.

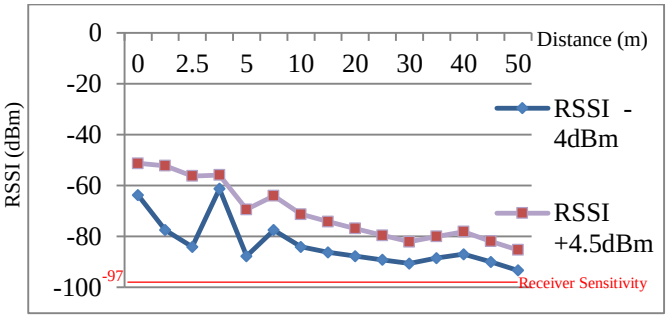

Fig. 10(a). RSSI versus distance.

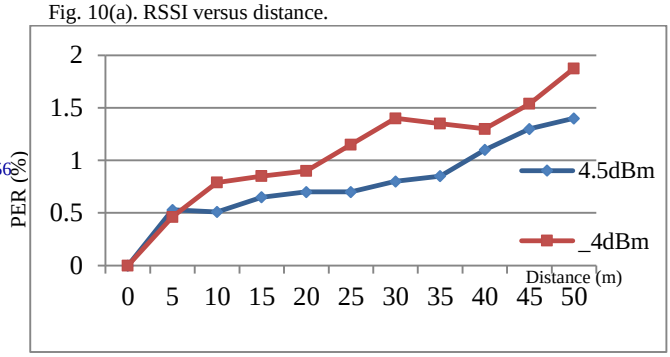

Fig. 10(b). PER versus distance.

D. Practical Experiments

Suppose that *"q"* is the number of tagged-vehicles passing the reader coverage area per minute, *"v"* is the velocity of each tagged-vehicle passing through the reader's RF-field at the moment of scanning, *"T"* is the period of "Auto-Highway-Scanning" operation, and "*r*" is the detection range. T_W for each tag has been measured by 16-bit timer of CC2530F256.

Test1. Peak-hour traffic congestion

The proposed system has been tested with the test condition of q=37 $\frac{vehicle}{min}$, *Tx-Power=4.5dBm*, *T=3500ms* and *r=80m* at Tehran-Qom highway on March 23, 2017. Since 53000 vehicles within 24-hour was reported for the above-mentioned highway on that day, all 9 tagged-vehicles were stopped at the reader's RF-field *(v=0km/h)* because of peak-hour traffic congestion as can be seen in Fig. 11. Table V illustrates "Auto-Highway-Scanning" operation log-file in test 1.

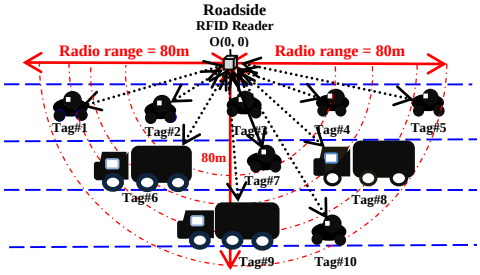

Fig. 11. The proposed system testing in peak-hour traffic congestion.

TABLE V
PEAK-HOUR TRAFFIC CONGESTION LOG FILE

Detection Date/Time Stamp	Detected Tag 64-bit EUI	Detected Tag 24-bit OUI	T_{W1} (T_{slot})	T_{W2} (T_{slot})	T_W (T_{slot})
Mar 23, 2017 - 05:23:11 P.M.	(**011673**01004B1200)$_{Hex}$	(011673)$_{Hex}$	309	30	339
Mar 23, 2017 - 05:23:11P.M.	(**201673**01004B1200)$_{Hex}$	(201673)$_{Hex}$	403	3	406
Mar 23, 2017 - 05:23:11P.M.	(**147301**01004B1200)$_{Hex}$	(147301)$_{Hex}$	390	21	411

Mar 23, 2017 - 05:23:11P.M.	(**2A78F1**01004B1200)$_{Hex}$	(2A78F1)$_{Hex}$	411	26	437
Mar 23, 2017 - 05:23:11P.M.	(**3B77F1**01004B1200)$_{Hex}$	(3B77F1)$_{Hex}$	420	19	439
Mar 23, 2017 - 05:23:11P.M.	(**5E78F1**01004B1200)$_{Hex}$	(5E78F1)$_{Hex}$	433	10	443
Mar 23, 2017 - 05:23:11P.M.	(**4878F1**01004B1200)$_{Hex}$	(4878F1)$_{Hex}$	425	28	453
Mar 23, 2017 - 05:23:11P.M.	(**B11473**01004B1200)$_{Hex}$	(B11473)$_{Hex}$	450	9	459
Mar 23, 2017 - 05:23:11P.M.	(**D4DA0B**01004B1200)$_{Hex}$	(D4DA0B)$_{Hex}$	455	37	492

Test2. Low-density traffic condition

The proposed system has been tested with the test condition of $q=9\frac{vehicle}{min}$, *Tx-Power=4.5dBm*, *T=3500ms*, *r=80m* and$v\epsilon[33$ *km/h*, *90 km/h*$]$at Tehran-Qom highway on Sep 29, 2017. Since 13200 vehicles within 24-hour was reported for the above-mentioned highway on that day, there was free-flow of traffic. Table VI illustrates "Auto-Highway-Scanning" operations log-file in test 2.

TABLE VI
LOW-DENSITY TRAFFIC CONDITION LOG FILE

Detection Date /Time Stamp	Detected Tag 24-bit OUI	V (km/h)	T_{W1} (T_{slot})	T_{W2} (T_{slot})	T_W (T_{slot})
Sep 29, 2017 - 10:30:54 A.M.	(011673)$_{Hex}$	70	309	7	316
Sep 29, 2017 - 10:30:54 A.M.	(D4DA0B)$_{Hex}$	80	390	31	421
Sep 29, 2017 - 10:30:54 A.M.	(3B77F1)$_{Hex}$	65	420	2	422
Sep 29, 2017 - 10:30:54 A.M.	(201673)$_{Hex}$	33	403	30	433
Sep 29, 2017 - 10:30:54 A.M.	(4878F1)$_{Hex}$	36	425	13	438
Sep 29, 2017 - 10:30:54 A.M.	(2A78F1)$_{Hex}$	90	411	40	451
Sep 29, 2017 - 10:30:54 A.M.	(5E78F1)$_{Hex}$	75	433	22	455
Sep 29, 2017 - 10:30:54 A.M.	(D4DA0B)$_{Hex}$	60	455	7	462
Sep 29, 2017 - 10:30:54 A.M.	(B11473)$_{Hex}$	65	450	15	465

As shown in tables V and VI, there was no tag-tag collision by using the proposed system.

In order to study the effect of variations in *v* on the sequence of tags responses, test 1 and 2 has been performed only by the first strategy. Variations in *v* had no effect on the sequence of tags responses because of ignorable Doppler shift of DSSS (O-QPSK) at 2.4GHz.

E. GSM Subsystem Key Elements

GSM is an open, digital cellular underlying technology in which digital encoding is used for mobile voice communication and TDMA methods provide an efficient data rate for data services. The long range communication between the roadside unit and monitoring station is supported by the SIM900-based GSM modems connected to the ATmega64-based interface boards. SIM900A is managed by a AMR926EJ-Sprocessor which has a Harvard cached architecture and supports the 32-bit ARM and 16-bit Thumb instruction sets. ATmega64-the interface board core chip is an 8-bit CMOS microcontroller based on the AVR enhanced RISC architecture which has dual programmable serial USARTs. The roadside interface board gets the collected IDs from the RFID reader and transfers them to the roadside GSM modem. These IDs are sent on the digital cellular network over SMS(text-mode). Text-based data via SMS provides a low-cost solution with an extensive coverage of mobile phone networks [44]. Once the SMS is received by the monitoring station GSM modem, the second interface board extracts IDs from the SMS content and transfers them to the PC/Laptop serial port. Fig. 12(a) and 12(b) illustrate the implemented hardware and structure diagram of the GSM modem and interface board respectively.

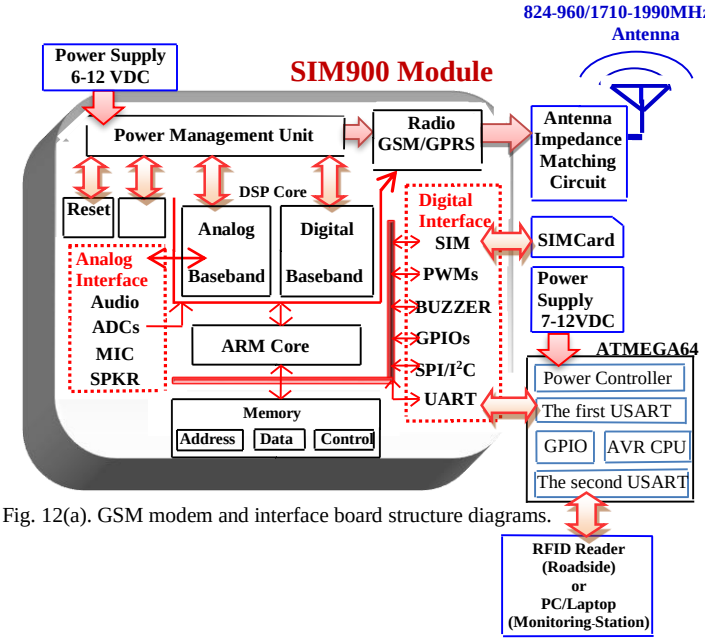

Fig. 12(a). GSM modem and interface board structure diagrams.

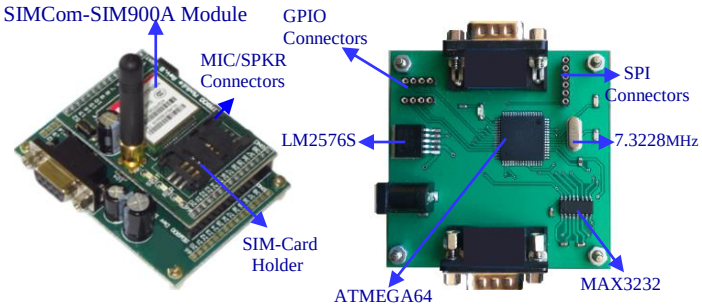

Fig.12(b). Implemented GSM modem and interface board hardware.

F. User Interface Software

In the suggested remote tracking and monitoring system, a User Interface (UI) is an effective tool for an operator to remotely access received IDs from the tagged-vehicles and scanning time stamp on a real-time basis. Therefore, "Auto-Highway-Scanning" operation results are displayed by a developed high-level multi-layer user interface software. Table VII summarizes developed user interface software specifications.

TABLE VII
DEVELOPED USER INTERFACE SOFTWARE SPECIFICATIONS.

User Interface Software Parameters	Value
Application Type	Real-Time Remote Monitoring
Application platform	Windows-Based
Architectural Style	Layered Architecture
UML software design tool	IBM Rational Rose
Development methodology	MFC Dialog Based
Programming Language	Microsoft Visual C++
IDE(Integrated Development Environment)	Microsoft Visual Studio

The developed user interface software is organized with layered architecture style by dividing tasks between three reusable logical layers. Layered architecture is a call and return style

which represents hierarchical organization and supports extensibility, reusability, code readability, high abstraction level and portability. Each layer provides services to the layer above and consumes services from the layer below. Complexity and tangling become more manageable by less code per layer in layering [53]-[55]. Fig. 13 illustrates three-layer architecture of the proposed user interface.

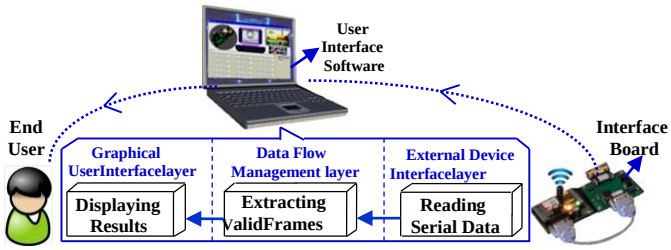

Fig. 13. Three-layer architecture of the proposed user interface software.

"GUI" layer is responsible for Human-Computer-Interaction (HCI) and graphically displaying "Auto-Highway-Scanning" results. "Data-flow-management" layer is responsible for extracting valid frames and error-handling. "External Device Interface" layer is responsible for setting up the serial port and data exchanging between the PC/Laptop serial port and the interface board which is connected to the GSM modem to extract effective data from SMS.

The user interface software development is performed by Microsoft Visual C++ through Microsoft Foundation Classes (MFC) dialog based methodology in Microsoft Visual Studio. Fig. 14 illustrates the main dialog of the developed user interface during "Auto-Highway-Scanning" process.

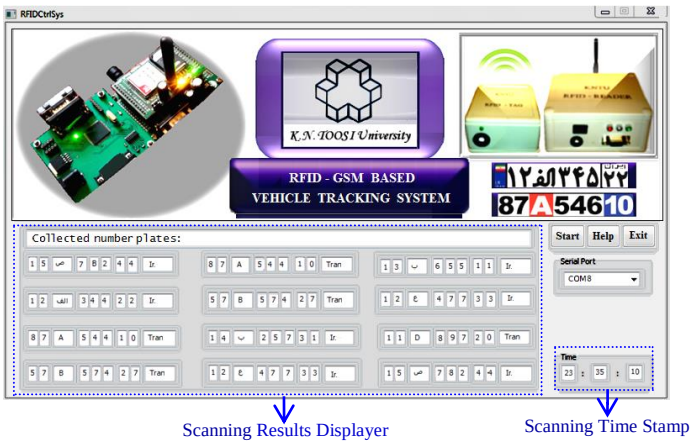

Fig. 14. Developed user interface main dialog during real-time monitoring.

According to Fig. 15, UML (Unified Modeling Language) class diagram of the three-layer suggested user interface software is designed by means of IBM Rational Rose software design tool. There are two boundary classes and one control class. This structural model is based on tight cohesion in each class and loosely coupling between classes and represents a static view of the software system.

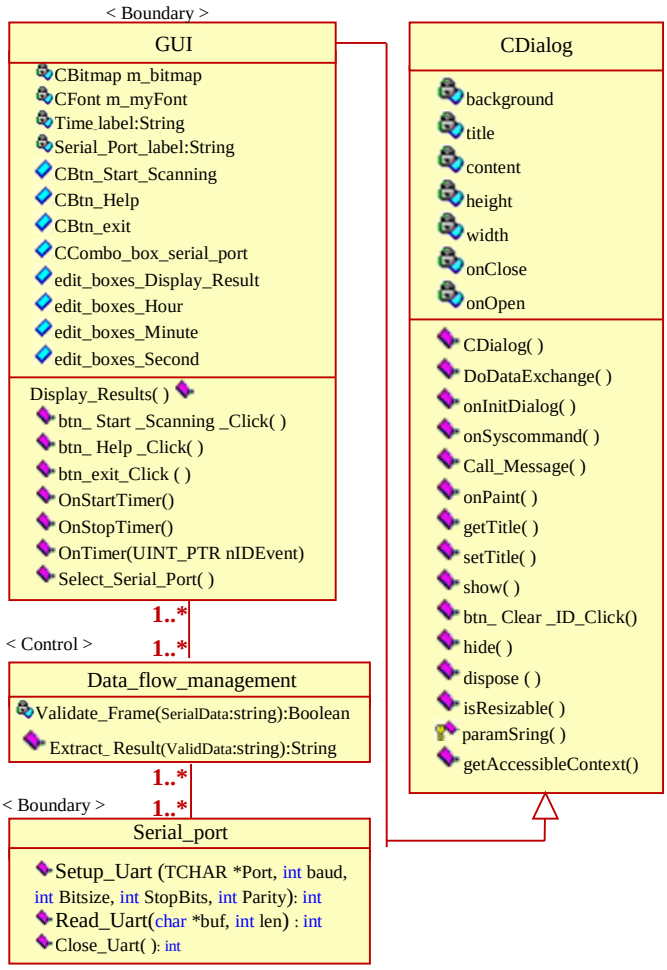

Fig. 15. UML representation of the suggested user interface classes.

VI. Conclusion

In this paper, a real-time high efficient RFID-GSM based vehicle identification system is designed and implemented at 2.4GHz. Integration of GSM and active RFID technologies has resulted in full automation of periodic highway scanning far away from the monitoring station. The proposed collision-avoidance scheme involving two strategies will be run in the tag's firmware. In order to generate a unique waiting-time for each tag in the first strategy, CC2530F256 SoC unique identifier is passed into an injective logarithmic function with low time complexity. The second strategy utilizes tag's CC2530F256 pseudorandom number generator to add a restricted random value to the first strategy output. The second strategy is responsible for reducing the collision probability and making the proposed scheme more secure.

The proposed scheme overcomes the conventional methods limitations such as tag population estimation latency in Aloha-based methods; time-consuming lengthy queries in Tree-based protocols and network resources utilization by RTS-CTS mechanism in CSMA-based protocols. Monte-Carlo simulation results show that the proposed scheme is more efficient than the conventional tag anti-collision schemes such as ISO/IEC 18000-7, CSMA non persistent, CSMA p-persistent, QT, CT and QWT.

Another highlight of this work is the single-chip hardware

realization of the reader and tag which has minimized hardware dimensions and prevented the circuit complexity and high frequency noises. Moreover, a high-level multi-layer user interface software is developed to remotely display "Auto-Highway-Scanning" results on a real-time basis.

ACKNOWLEDGMENT

The authors would like to appreciate Mr. Mahdi Karimi Ahmadabadi. He was responsible for implementing the interface board.

REFERENCES

[1] W. K. Sze, Y. Deng, W. C. Lau, M. Kodialam, T. Nandagopal and O. Yue, "Channel-Oblivious Counting Algorithms for Large-Scale RFID Systems," IEEE Transactions on Parallel and Distributed Systems, Vol. 26, No. 12, pp. 3303–3316, 2015.

[2] C. Boyer and S. Roy, "Backscatter Communication and RFID: Coding, Energy, and MIMO Analysis," IEEE Transactions on communications, Vol. 62, No. 03, pp. 770–785, 2014.

[3] D. G. Zhang and W. B. Li, "A Novel ID-based anti-collision approach for RFID," Enterprise Information Systems, Taylor & Francis, Vol. 10, No. 07, pp. 771–789, 2016.

[4] H. Guo, Ch. He., N. Wang and M. Bolic, "PSR: A Novel High-Efficiency and Easy-to-Implement Parallel Algorithm for Anticollision in RFID Systems," IEEE Transactions on Industrial Informatics, Vol. 12, No. 03, pp. 1134–1145, 2016.

[5] W. Su, N. Alchazidis and T. T. Ha, "Multiple RFID Tags Access Algorithm," IEEE Transactions on Mobile Computing, Vol. 09, No. 02, pp. 174-187, 2010.

[6] M. V. Bueno-Delgado, R. Ferrero, F. Gandino, P. Pavon-Marino and M. Rebaudengo, "A Geometric Distribution Reader Anti-Collision Protocol for RFID Dense Reader Environments," IEEE transactions on Automation Science and Engineering, Vol.10, No.02, pp.296-306, 2013.

[7] H. Landaluce, A. Perallos, E. Onieva, A. Laura and L. Bengtsson, "An Energy and Identification Time Decreasing Procedure for Memoryless RFID Tag Anti-Collision Protocols," IEEE Transactions on Wireless Communications, Vol. 15, No. 06, pp. 4234-4247, 2016.

[8] A. Alma'aitah, H. S. Hassanein and M. Ibnkahla, "Tag Modulation Silencing: Design and Application in RFID Anti-Collision Protocols," IEEE Transactions on Communications, Vol. 62, No. 11, pp. 4068–4079, 2014.

[9] H. Wu and Y. Zeng, "Passive RFID Tag Anticollision Algorithm for Capture Effect," IEEE Sensors Journal, Vol. 15, No. 01, pp. 218–226, 2015.

[10] H. Wang, Ch. Pei and B. Su, "Collision-Free Arbitration Protocol for Active RFID Systems," IEEE Journal of Communications and Networks, Vol. 14, No. 01, pp. 34-39, 2012.

[11] Y. C. Lai, L. Y. Hsiao and B. Sh. Lin, "Optimal Slot Assignment for Binary Tracking Tree Protocol in RFID Tag Identification," IEEE/ACM Transactions on Networking, Vol. 23, No. 01, pp. 255-268, 2015.

[12] F. Nafar and H. Shamsi, "On the Design of a User Interface for an RFID-Based Vehicle Tracking System," International Journal of Wireless Information Networks, Vol. 24, No. 01, pp. 56–61, 2017.

[13] D. Moeinfar and H. Shamsi, "A Low-Collision CSMA-Based Active RFID for Tracking Applications," Wireless Personal Communications, Vol. 71, No. 04, pp. 2827–2847, 2013.

[14] D. Moeinfar, H. Shamsi and F.Nafar, "Design and implementation of a low-power active RFID for container tracking at 2.4 GHz frequency," Advances in Internet of Things, Vol. 02, No. 02, pp. 13–22, 2012.

[15] F. Hessar and S. Roy, "Energy Based Performance Evaluation of Passive EPC Gen 2 Class 1 RFID Systems," IEEE Transactions on Communications, Vol. 61, No. 04, pp. 1337-1348, 2013.

[16] W. T. Chen, "Optimal Frame Length Analysis and an Efficient Anti-Collision Algorithm with Early Adjustment of Frame Length for RFID Systems," IEEE Transactions on Vehicular Technology, Vol. 65, No. 05, pp. 3342-3348, 2016.

[17] T. Lindgren, B. Kvarnstorm and J. Ekman, "Monte Carlo simulation of an radio frequency identification system with moving transponders using the partial element equivalent circuit method," IET Microwaves, Antennas & Propagation, Vol. 04, No. 12, pp. 2069-2076, 2010.

[18] F. Li, Y. Wei, Y. Chen and X. Zhang, "System Design of Online Monitoring and Controlling System Based on Zigbee in Greenhouse," Computer and Computing Technologies in Agriculture VIII, Vol. 452, pp. 702-713, 2015.

[19] J. Su, G. Wen, D. Hong, "A New RFID Anti-collision Algorihm Based on the Q-Aray Search Scheme," Chinese Journal of Electronics, Vol. 24, No. 04, pp. 679-683, 2015.

[20] L. Kang, J. Zhang, K. Wu, D. Zhang and L. Ni, "RCSMA: Receiver-Based Carrier Sense Multiple Access in UHF RFID Systems," IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 04, pp. 735-743, 2012.

[21] H. Safa, W. El-Hajj and Ch. Meguerditchian, "A distributed multi-channel reader algorithm for RFID environments," Computer Communications, Vol. 64, pp.44–56, 2015.

[22] Y. Ch. Lai, L. Y. Hsiao, H. J. Chen, Ch. N. Lai and J. W. Lin, "A Novel Query Tree Protocol with Bit Tracking in RFID Tag Identification," IEEE Transactions on Mobile Computing, Vol. 12, No. 10, pp. 2063-2075, 2013.

[23] Y. He and X. Wang, "An ALOHA-based improved anti-collision algorithm for RFID systems," IEEE Wireless Communications, Vol. 20, No. 5, pp. 152-158, 2013.

[24] D. Zhang, G. Li, Zh. Pan, and Y. Liang, "A new anti-collision algorithm for RFID tag," International Journal of Communication Systems, John Wiley & Sons Vol. 27, No. 11, 2014.

[25] X. Jia, Q. Feng and L. Yu, "Stability Analysis of an Efficient Anti-Collision Protocol for RFID Tag Identification," IEEE Transactions on Communications, Vol. 60, No. 08, pp. 2285-2294, 2012.

[26] Y. Cui and Y. Zhao, "Performance evaluation of multi-branch tree algorithm in RFID," IEEE Transactions on Communications, Vol. 58, No. 05, pp. 1356-1364, 2010.

[27] J. Su, G. Wen and D. Hong, "A New RFID Anti-collision Algorithm Based on the Q-Ary Search Scheme," Chinese Journal of Electronics, Vol. 24, No. 04, pp. 679-683, 2015.

[28] X. Liu, Z. Qian, Y. Zhao and Y. Guo, "An adaptive tag anti-collision protocol in RFID wireless systemes," China Communications, Vol. 11, No. 07, pp. 117-127, 2014.

[29] Y. Du and Z. Chi, "A slot-controlling method for anti-collision in active RFID system," 6th International Congress on Image and Signal Processing (CISP), Vol. 03, pp. 1489-1493, 2013.

[30] W. T. Chen, "A Feasible and Easy-to-Implement Anticollision Algorithm for the EPCglobal UHF Class-1 Generation-2 RFID Protocol," IEEE Transactions on Automation Science and Engineering, Vol. 11, No. 02, pp. 485-491, 2014.

[31] K. Nishide, H. Kubo and R. Shinkuma, T. Takahashi, "Detecting Hidden and Exposed Terminal Problems in Densely Deployed Wireless Networks," IEEE Transactions on Wireless Communications, Vol. 11, No. 11, pp. 3841-3849, 2012.

[32] D. Leonardo, M. Sanchez, M. Victor, and R. Ramos "p-Persistent CSMA as a collision resolution protocol for active RFID environments," Eighth International Conference on Wireless and Optical Communications Networks, pp. 1-5, 2011.

[33] W. J. Yoon, S. H. Chang, "ISS-TCA: An Identified Slot Scan-Based Tag Collection Algorithm for Performance Improvement in Active RFID Systems," IEEE Transactions on Industrial Electronics, Vol. 59, No. 3, pp. 1662-1672, 2012.

[34] Y. H. Chen, Sh. J. Horng, R. Sh. Run, J. L. Lai, R. J. Chen, W. Ch. Chen, Y. Pan and T. Takao, "A Novel Anti-Collision Algorithm in RFID Systems for Identifying Passive Tags," IEEE Transactions on Industrial Informatics, Vol. 06, No. 01, pp. 105-121, 2010.

[35] E. Vahedi, R. K. Ward and I. F. Blake, "Analytical modeling of RFID Generation-2 protocol using absorbing Markov chain theorem," IEEE Global Communications Conference (GLOBECOM), pp. 385-390, 2012.

[36] X. Tan, M. Dong, Ch. Wu, K. Ota, J. Wang and D. W. Engels, "An Energy-Efficient ECC Processor of UHF RFID Tag for Banknote Anti-Counterfeiting," IEEE Access, Vol. 05, pp. 3044-3054, 2017.

[37] I. Bratuž, A. Vodopivec and A. Trost, "Resolving Collision in EPCglobal Class-1 Gen-2 System by Utilizing the Preamble," IEEE Transactions on Wireless Communications, Vol.13, No.10, pp. 5330-5339, 2014.

[38] V. Namboodiri, M. DeSilva, K. Deegala and S. Ramamoorthy "An extensive study of slotted Aloha-based RFID anti-collision protocols," Computer Networks, Vol. 35, No. 16, pp. 1955 - 1966, 2012

[39] I. Amadou and N. Mitton "Revisiting Backoff algorithms in CSMA/CA based MAC for channel reservation in RFID reader Networks through broadcasting," IEEE 9th International Conference on Wireless and

Mobile Computing, Networking and Communications (WiMob), pp. 452-457, 2013.
[40] B. Nilsson, L. Bengtsson and B. Svensson "Selecting back off algorithm in active RFID CSMA/CA based medium-access protocols," International Symposium on Industrial Embedded Systems, pp. 265-270, 2008.
[41] R. Alesii, P. D. Marco, F. Santucci, P. Savazzi, R. Valentini and A. Vizziello, "Backscattering UWB/UHF hybrid solutions for multi-reader multi-tag passive RFID systems," EURASIP Journal on Embedded Systems, pp.1-19, 2016.
[42] B. Nilsson, L. Bengtsson and B. Svensson, "An Energy and Application Scenario Aware Active RFID Protocol," EURASIP Journal on Wireless Communications and Networking, 2010.
[43] W. Zhu, J. Cao, H. C. B. Chan, X. Liu and V. Raychoudhury, "Mobile RFID with a High Identification Rate," IEEE Transactions on Computers, Vol. 63, No. 7, pp. 1778-1792, 2014.
[44] SIMCOM Wireless Solutions Ltd. SIM900A Hardware Design, V1.01, pp.12-23, 2010.
[45] Texas Instruments Inc., "CC2530 User's Guide,"SWRU191D, 2013.
[46] Texas Instruments Inc., "CC2530 Datasheet,"SWRS081B, 2011.
[47] D. K. Klair, K. W. Chin and R. Raad, "A Survey and Tutorial of RFID Anti-Collision Protocols," IEEE Communications Survey & Tutorials, Vol. 12, No. 3, pp. 400-421, 2010.
[48] A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," IEEE Transactions on Emerging Topics in Computing, Vol. 05, No. 04, pp. 586 - 602, 2017.
[49] V. Namboodiri and L. Gao, "Energy-Aware Tag Anticollision Protocols for RFID Systems," IEEE Transactions on Mobile Computing, Vol. 9, No. 1, pp. 44-59, 2010.
[50] D. Zhang, X. Wang, X. Song, D. Zhao, "A Novel Approach to Mapped Correlation of ID for RFID Anti-Collision," IEEE Transactions on Service Computing, Vol. 07, No. 04, pp. 741-748, 2014.
[51] [42] M. Bharadwaj Mantri, P. Velagapudi, B. Ch. Eravatri, M. VV, "Performance analysis of 2.4GHz IEEE 802.15.4 PHY under various fading channels," International Conference on Emerging Trends in Communication, Control, Signal Processing & Computing Applications (C2SPCA), pp. 1-4, 2013.
[52] Texas Instruments, SmartRF™ Studio 7 Overview, (2009).
[53] M. Galster, A. Eberlein, M. Moussavi, "Systematic selection of software architecture styles," IET Software, Vol. 04, No. 05, pp. 349-360, 2010.
[54] A. Kumar, "Software Architecture Styles a Survey," International Journal of Computer Applications, Vol. 87, No. 09, 2014.
[55] L. Dobrica and E. Niemela, "A Survey on Software Architecture Analysis Methods," IEEE Transactions on Software Engineering, Vol. 28, No. 07, pp. 638-653, 2002.

F. Nafar received the M.Sc. degree in Information and Communications Technology (ICT) from Iran University of Science and Technology (IUST) in 2016. She received two B.Sc degrees in Electrical Engineering-Electronics and Computer Software Engineering from IAU South Tehran Branch and K. N. Toosi University of Technology in 2009 and 2011 respectively. She has worked as major engineer in three research projects under the supervision of Dr. Hossein Shamsi at the Faculty of Electrical Engineering, K. N. Toosi University of Technology between Feb 2011-Sep 2015. These research projects include "Design and Implementation of an RFID reader at 2.4GHz ", "Design and Implementation of an acticve RFID tag at 2.4GHz" and "Design, implementation and user interface development of a vehicle tracking system on highways". Her research interests include RFID Systems and Cryptanalysis.

H. Shamsi received the B.Sc., M.Sc. and Ph.D. degrees in Electronics Engineering from the University of Tehran in 2000, 2002 and 2006 respectively. She has been working as assistant professor with the Faculty of Electrical Engineering, K. N. Toosi University of Technology since 2007. His current research activities include Integrated Circuits, Data Converters, RFIC, and RFID systems.