Routine Scrutiny of an RFID Key Management Scheme for Vehicular Networks

SUJEETH T.
Dept. of Computer Science &Engineering
Sri Venkateswara University,Tirupati
Andhra Pradesh, India

KIRAN KUMAR REDDY D.
Dept of computer Science &Engineering
Sree Venkatesa Perumal College of Engineering & Technology
Andhra Pradesh, India

Abstract:
In this paper we analyze the performance of an RFID Key Management scheme to be applied in VANETs. As often being considered as a precondition for the realization of the Internet of Things (IoT), RFID can be utilized in the vehicles, so as to make the vehicles identifiable and inventoriable by computers as long as they are fitted out with radio tags. One of the public concerns is likely to focus on a certain large number of security and privacy issues. Various light symmetric key management schemes will be proposed for different RFID scenarios. In order to perform a reliable and trusted authentication, one prerequisite is to ensure the credibility of RFIDs by means of digital certificate validation. We propose a certificate revocation status validation scheme called EKA2, using the concept of clustering from data mining to evaluate the trustiness of digital certificates.

Keywords: *Routine security, RFID, RFID Key Management, VANETs*

1. Introduction

As a living entity, the Internet is always evolving. Recently a novel paradigm: the Internet of Things (IoT) is swiftly gaining ground in the scenario of contemporary wireless telecommunications industry. The Internet of Things is driven by the pervasive presence around individuals of a variety of things or items, e.g., Radio-Frequency Identification (RFID) tags, mobile phones, sensors, etc. Those objects are capable of interacting with each other, so as to cooperate with their neighbors to achieve shared goals.

In vehicular communication environments, RFID is typically used in such a scenario, where the tag is resided on the vehicle and the tag reader is located on the road. Usually, tags are read statically, due to the reasons that the vehicles will slow down or stop over the reader. The advantage of this arrangement is that tags do not require a power source, reducing the cost of maintenance and thus the cost of globalizing the system. In fact, before mass society generally accepted the concept of RFID techniques and their implementation in VANETs, academia still needs to tackle down several challenges and develop telecommunication technologies for linking thousands of items as social nodes. Those challenges include a full interoperability of potentially interconnected entities; a higher degree of intelligence should be embedded with those entities so as to improve their capability of adaptation in unexpected situations. Furthermore, the trustworthiness and privacy should be secured. At the same time, RFID techniques also pose a threat to many new issues in the telecommunication industry.

In general, the main framework of Io T is composed of several entities such as RFID Tag, RFID Reader, RFID Middleware, and digital certificates authentication of RFID Tag. A brief illustration of RFID tags from [1] is shown in Figure 1. Usually, the authentication in a certificate-based system will be conducted by verifying the digital certificates that were received by an entity. In order to so, the receiver needs to check the revocation status of these certificates in the latest issued CRLs. This ensures that this certificate is not listed in any CRL, and can therefore be considered as sent by a trustworthy entity. Traditional cryptographic methodologies cannot be applied to the IoT directly since they usually consume large amount of resources such as energy and network bandwidth. Thus, many lightweight symmetric key cryptographic mechanisms have been proposed for either RFID scenarios [4] or sensor network scenarios [5].

Because the number of RFID tags could be unpredictably large, the authentication process followed by the receiving entity could be quite overwhelming. In addition, due to the high number of certificates issued and revoked, as well as the fact that CRLs will keep all revoked certificates as well as new ones until they expire, CRLs could be large in size, rendering the search for a revoked certificate in the CRL even more troublesome. The main objective is to design and implement an authentication scheme for vehicular communication that is able to provide fast response to peer vehicles authentication by integrating clustering techniques from data mining with certificate revocation status verifying; besides, two goals are set: taking certificate's reputation into account, and improving the clustering techniques we employed. The rest of the paper is organized as follows. Section II discusses digital certificates and CRL; Section III describes the EKA2 scheme for RFID authentication; Section IV illustrates the effectiveness of our proposed technique via a few simulation results; Finally, Section V provides a future research plan and draws the conclusion of the work.

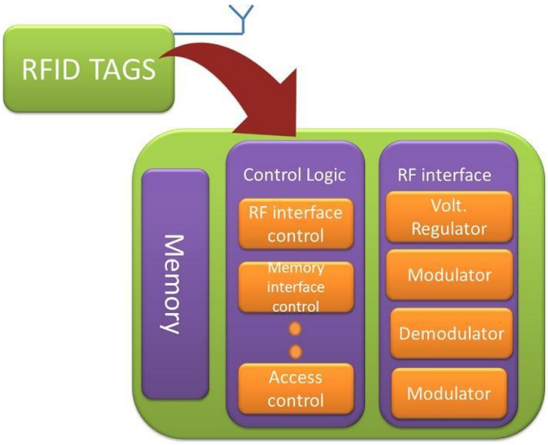

Fig. 1. An brief illustration of RFID tags.

2. Digital Certificates and CRL

In order to establish a reliable RFID communication environment, the guarantee of a RFID's credibility is required. Usually, authentication and digital certificates act as the major tools by which to validate the identification of each communicating entity. An entity's certificate can be validated by checking its digital certificates. However, the promptness of validation is more important for VANETs when compared to conventional networks, because it is not unusual for one RFID tags reader to scan products in large bulks in a short amount of time. Thus, it is necessary to find an efficient scheme by which to expedite the certificate validation process.

Certain new solutions are compulsory for assisting the addressing of RFID tags into IPv6 networks. Recently, embedding RFID tags into IPv6 networks has been investigated. At the same time, few approaches have been proposed that aim at incorporating RFID identifiers and IPv6 addresses [2] [3]. In addition, a complete altered methodology is demonstrated in [1], where the RFID message and headers are encompassed into the IPv6 packet payload. An instance is shown in Table I. Using the same principles of data mining (i.e., retrieving informative patterns from large of data), we integrate the clustering method from data mining into the process of checking the certificate revocation status in CRLs. In order to achieve this, the k-Means clustering algorithm is used. In the following section, further details regarding digital certificates and CRLs will be presented.

2.1 The Structure of Digital Certificates

The well-known X.509 standard specifies all necessary information that consists in X.509 certificate and defines their data pattern. In addition to a digital signature from the CA, X.509 certificates consist of contents which are specified by the Internet Engineering Task Force (IETF). CAs are essential in implementing PKI solutions for security purposes. The CA’s primary responsibilities relating to public key certificates could be listed as following: certificate generation, certificate distribution, certificate renewal and certificate revocation. As we just mentioned, certificate revocation is a critical responsibility that are taken on by CAs. CRLs are issued to all nodes in networks in order to maintain the list of revoked certificates. Digital certificates may be revoked Key Compromising, Change of Affiliation or Termination of Operation.

In a situation where the CA is absent, an authentication mechanism will be necessary between newly-joined mobile users and inexperienced domains. Chang and Tsai in [6] suggested a novel self-verified authentication scheme which involves *Elliptic Curve Cryptography* in order to achieve security goals. Recently, researchers’ efforts have been put on using physical layer information to improve wireless securitizing *et al.* in [7] conducted a survey of several non-cryptographic methods that use physical layer information in both static and mobile wireless networks. Wen *et al.* in [8] introduced a message authentication framework which uses physical layer data to perform cryptography.

3. EKA2 for Rfid Authentication

In the previous section, we discussed the prerequisites for certificate-based authentication. In this section, we pro-pose a fast certificate revocation status validation scheme for RFID authentication in VANETs. It was built based on our previous proposed authentication scheme, i.e., EKA in [10]. The acceleration in EKA2 is achieved by using newly introduced elements in the CRL and adopting a *k*-Means clustering algorithm with enhanced cancroids selection. In virtue of the acceleration procedure, a successful validation could be potentially achieved.

3.1 Enhanced K-Means Authentications 2

The Effective *k*-Means Authentication 2 (EKA2) is a scheme proposed in this section. And we have made an improvement based on EKA. Before vehicles and terminals initialize a conversation with each other, four phases need to be performed during the revocation validation.

3.1.1 Clustering

In this phase, CAs pre-process the latest CRL file using the two newly added attributes, issued date and credibility, combined with both the *k*-Means clustering algorithm and the enhanced initial cancroids selection scheme in order to efficiently cluster the revocation certificates entries. A sample illustration of the clustering results is shown in Figure 2. After the CRL processing is completed, the CAs distributes the processing results along with the CRL files themselves.

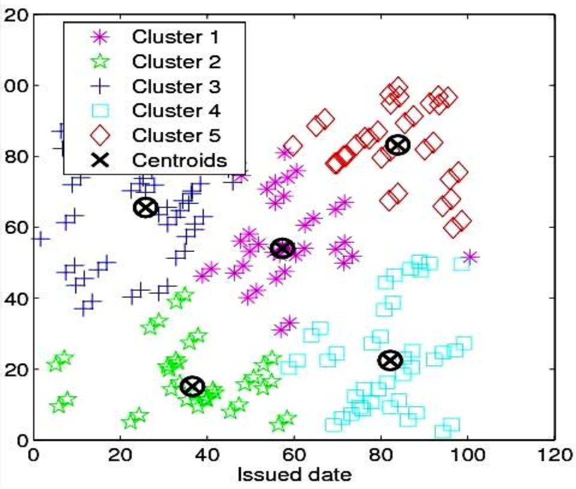

Fig. 2. An example of clustering results using all entries in a CRL file, where *n* = 100, *k* = 5.

3.1.2 Retrieving

Upon receiving a connection set up request RFID message from other vehicles, receivers will check the certificates contained in that message and extract all relevant information included in that certificate i.e. serial number, issue time, and credibility.

Table 1. Encapsulation of RFID message into an ipv6 packet

Version	Traffic Class			Flow Label		
	Pay Load Length			Next Header	Hop Limit	*IPv6 packet*
		Source Address (128 bits)				*fixed headers*
	Destination Address (128 bits)					
Next Header	Header Length		Option Type	Option Length		
RFID type	Message Type			Reserved		*IPv6 packet*
		RFID Code (96 bits)				*extension*
		Message Data				*headers*

3.1.3 Localizing

Using the credibility and issued date, the receiver can calculate the Euclidean Distance between the data point (i.e., new certificate) and all cancroids in order to locate the closest cluster to join.

3.1.4 Verifying

In this phase, the new data points that join will check all neighboring data points in the recently joined cluster for a match in terms of credibility and issue date. If a match is found, this indicates that its certificate has been revoked. Otherwise, this data point is not in the CRL and can therefore be trusted.

4. Performance Evaluations

Our simulations are performed on the network simulator-2 with SUMO [12]. Three node authentication algorithms are evaluated in this section. This first searches through the CRLs linearly; that is, its authentication scheme would go through the CRL file in a linear fashion and search for a match; The second, EKA, which was presented in our previous publication; And the third one follows the one proposed in EKA2. The elapsed time for each authentication process is recorded for comparison purposes. A comparison of the three CRL verification methods is illustrated in Table II.

Approaches	linear	EKA1	EKA2
CA decentralized verification	√	√	√
Targeted for ad hoc networks		√	√
Reputation feature considerd		√	√
Digital certificates feature extraction		√	√
Redundant CRL pre-process		√	
Dense communications network considered			√
Can extract multi centificates features			√
Robustness to malicious attacks			√
Response time at dynamics topology	Slow	Fast	Very Fast

4.1 Scenarios

In this section, we briefly demonstrate the scenarios we used to perform extensive sets of simulation experiments. After describing the scenarios, we will present the metrics and simulation results.

TABLE III. SIMULATION PARAMETERS

Parameter	Value
Number of nodes(n)	100, 200, 300, 400, 500
Size of CRL(s)	1000, 3000, 5000, 7000
Number of clusters(k)	5, 7, 10, 13, 15

4.1.1 Authentication Process

During the simulation, the RFID tags nodes transmission messages which contained their own serial number, credibility, and issued date to RFID tags reader. Once other readers come into communication range, they would receive the messages and extract all the information in order to conduct an authentication by verifying the CRL file using two searching schemes: linear searching and EKA2. The linear searching scheme was represented as *l-searching* in, whereas the searching phase in both EKA and EKA2 is denoted as *k-searching*. Furthermore, the time that is needed to conduct clustering by both algorithms EKA and EKA2 is also recorded. Which is denoted as *EKA1* and *EKA2* respectively.

4.1.2 Simulation Parameters

Table III shows the detailed parameter settings for the implemented simulations. Three searching schemes (linear searching, EKA1 and EKA2) were evaluated for the purpose of comparing performance. The EKA2 was modified to perform authentication and five sets of simulations were implemented for evaluation. All of these evaluations were performed within the environment defined in the previous section. The five sets of experiments performed were done using the following varying values:

Number of RFID tags nodes and terminal nodes (*n*): The evaluation compared the elapsed time between a different number of nodes. The number of nodes varied from 100 to 500 with increments of 100. *Size of CRL* (*s*): The evaluation was performed in order to analyze the effect of the size of the CRL on the performance of the two searching schemes being evaluated. The size (*s*) was varied from 1000 to 7000 with increments of 2000.

Number of clusters in k-Means clustering (*k*): In this set of experiments, the number of clusters was varied from 5 to 15. This was undertaken with the aim to elucidate the effects of increasing the number of clusters on the authentication process in order to better select a suitable number of clusters.

4.2 Metrics

Two metrics were utilized to assess the performance of our authentication mechanism.

1) *CRL Verification Latency*: the total needed time for all nodes to complete the CRL verification.
2) *Communication Overhead*: the average number of messages broadcasted by all terminals and vehicles nodes during execution time.

4.2 Simulation Results

4.3.1 Impact of simulation running time:

Table IV compares search execution time for the linear searching scheme and EKA with varying simulation runtimes. As is illustrated at Figure 3, extending the simulation run time can increase the execution time of both searching schemes. However, the execution time of *k-searching* and *k-full* remained under 10s in all five simulations. On the contrary, the execution time increased dramatically with the linear searching scheme.

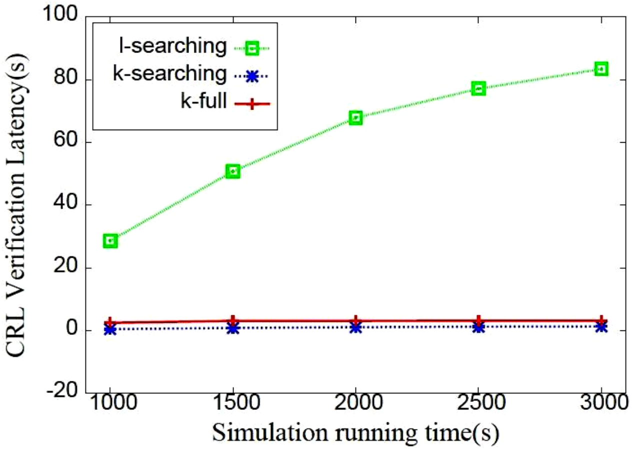

Fig. 3. Average Verification Latency and simulation running time

The time of the authentication latency was prolonged because both searching schemes needed to process additional messages for the purpose of authentication. Because the node overhead is related to the execution time, setting a higher threshold also introduced an increase numbers of messages. Based on the above results, it is obvious that EKA2 would be more advantageous rather then EKA1 when the number of vehicles and terminal nodes grows, since the CAs take the workload of the CRLs pre-processing rather than leaving it to each nodes.

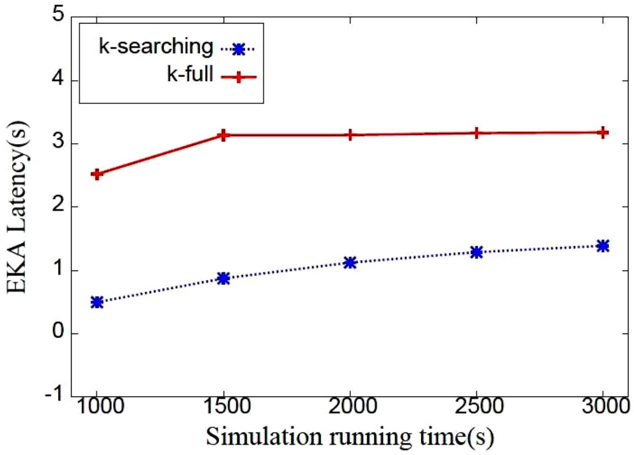

Fig. 4. Average Verification Latency for *k-searching*

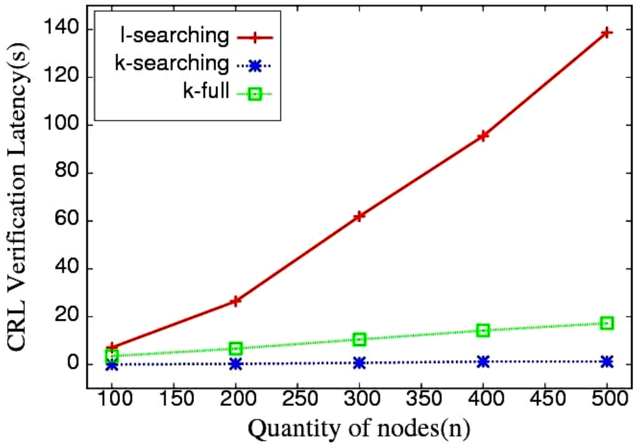

Fig. 5. Impact of different quantity of nodes

4.3.2 Impact of CRL Size

Both the authentication latency and communication overhead increased with a larger CRL size. The reason for this is that with a larger CRL size, the linear searching scheme needed to verify more entries in the CRL file, thus the nodes thus spent more time on the verifying process; this also applies to the EKA1 and EKA2. The needed authentication overhead for either two EKA scheme was also enlarged in order to deal with more entries and clustering due to the increasing CRL size. Therefore the authentication latency was prolonged. But still, compared to EKA1, EKA2 is still stay in a lower level of running time.

4.3.3 Impact of the Quantity of Cluster

The Average Verification Latency for *l-searching* and *k-searching* were little affected by different numbers of clusters; However, unlike the others, increasing the number of clusters helped to increase the latency. The reason for this is that an increase in clusters cause nodes to take more time to find out which cluster centroid is closer to them.

5. Conclusion and Future Works

In this paper, an efficient certificate revocation status validation scheme, i.e., EKA2, which built on the basis of EKA1, has been presented to provide reliable, secure and rapid certificate-based authentication over RFID tags in VANETs. In terms of future work, we intend to develop an offline cryptographic scheme that will be able to exclude specific nodes from participation when transmitting and receiving messages. This ideal scheme can be designed as an “elimination” scheme, in order to only allow all legitimate nodes to form a secure and trusted group.

TABLE IV. IMPACT OF SIMULATION RUNNING TIME TO AVERAGE VERIFICATION LATENCY

Simulation running time(t)	Communication Overhead	Average Verification Latency (s)			Ratio Comparison (*l-searching* to *k-full*)
		l-searching	*k-searching*	*k-full*	
1000	119204	28.67	0.50	2.52	11.38
1500	178932	50.80	0.88	3.14	16.17
2000	240198	67.85	1.13	3.15	21.53
2500	305368	77.12	1.29	3.17	24.32
3000	366120	83.44	1.39	3.18	26.24
where n = 100, k = 3, s = 1000, l = 1000m.					

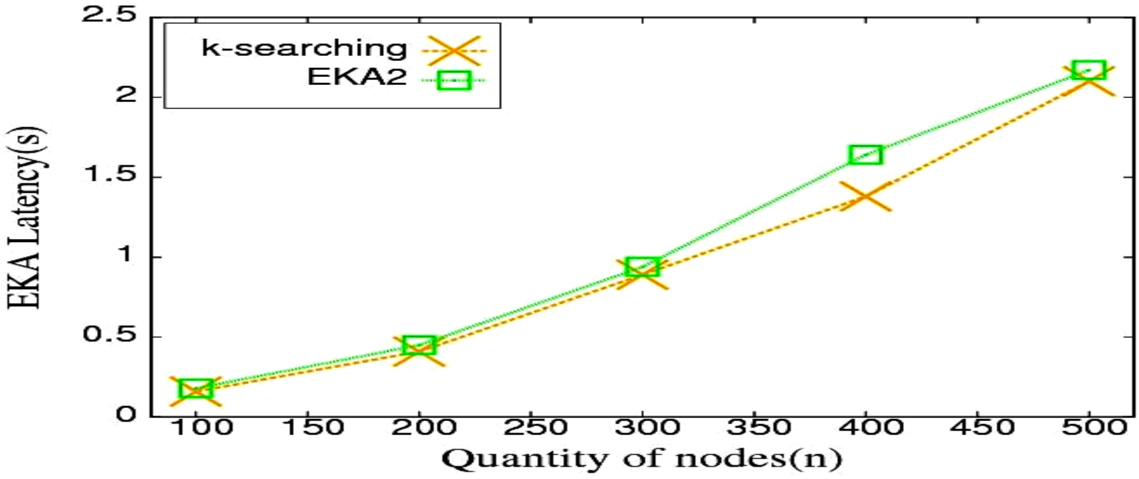

Fig. 6. Average CVL for EKA1 and EKA2 in the case of various quantities of nodes

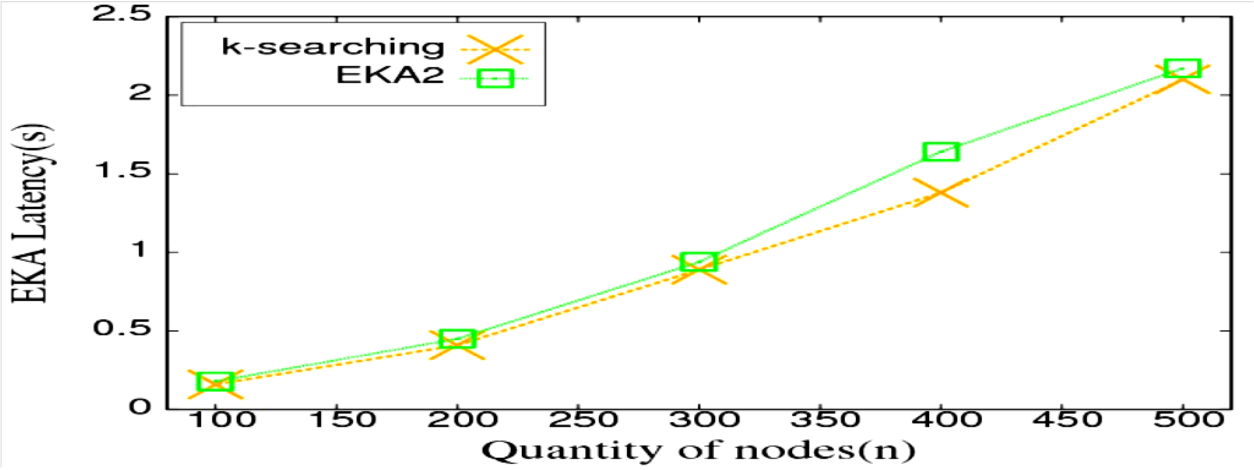

Fig. 7. Average CVL for EKA2 only in the case of various quantities of nodes

References

1. Almulla, M. Q. Zhang, A. Boukerche, and Y. Ren, (2012).“An efficient k-means authentication scheme for digital certificates revocation validation in vehicular ad hoc networks,” *Wireless Communications and Mobile Computing*, pp. n/a–n/a.
2. Chang, C. and H. Tsai, (2010).“An anonymous and Self-Verified mobile authentication with authenticated key agreement for Large-Scale wireless networks,” *Wireless Communications, IEEE Transactions on*, vol. 9. 3346–3353, Nov.
3. Eschenauer L. and V. D. Gligor, (2002).“A key-management scheme for distributed sensor networks,” in *Proceedings of the 9th ACM conference on Computer and communications security*, CCS ’02, (New York, NY, USA), pp. 41–47, ACM.
4. Feldhofer, M. S. Dominikus, and J. Wolkerstorfer, (2004). “Strong Authentication for RFID Systems Using the AES Algorithm,” pp. 357–370.
5. Lakshmi Tech, “Using RFID & IPv6.” http://ipv6.com/articles/applications/Using-RFID-and-IPv6.htm.
6. Lee, S.-D. M.-K. Shin, and H.-J. Kim, (2007).“Epc vs. ipv6 mapping mechanism,” in *Advanced Communication Technology, The 9th International Conference on*, vol. 2, pp. 1243 –1245, feb.
7. Ma, Y.-W. C.-F. Lai, Y.-M. Huang, and J.-L.(2009). Chen, “Mobile rfid with ipv6 for phone services,” in *Consumer Electronics, 2009. ISCE ’09. IEEE 13th International Symposium on*, pp. 169 –170, may.
8. Ren, Y. and A. Boukerche, “An efficient trust-based reputation protocol
9. Wen, H. P. Ho, C. Qi, and G. Gong, (2010). “Physical layer assisted authentication for distributed ad hoc wireless sensor networks,” *Information Security, IET*, vol. 4, pp. 390–396, Dec.
10. Zeng, K. K. Govindan, and P. Mohapatra, (2010). “Non-cryptographic authentication and identification in wireless networks [Security and privacy in emerging wireless networks],” *Wireless Communications, IEEE*, vol. 17, 56–62, Oct.