IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 6, Ver. IV (Nov - Dec. 2014), PP 44-50
www.iosrjournals.org

An Efficient Authentication Scheme for Rfid in Vanet By Using Ikev2

Ms.T.Durga[1], Mr.V.Vijayakumar[2]
(Communication Systems, Dhanalakshmi Srinivasan Engineering College/ Anna University, India)
[2](Assistant Professor, Department of ECE, Dhanalakshmi srinivasan Engineering college/ Anna University, India)

Abstract: *The aim of Vehicular Adhoc networks($VANET_S$) is to control the road traffic. This paper address an improved authentication scheme for Radio Frequency Identification (RFID) applied in $VANET_s$. In earlier the authors used symmetric key cryptography with EKA2,for that authentication delay will occur. To overcome this we proposed an group based authentication asymmetric key cryptography with IKEV2 key management. This improves the authentication of RFID and provide the better computation efficiency in $VANET_s$ and reduced the complexity of symmetric key management system.*

Keywords: *RFID, VANETs, key management, Authentication*

I. Introduction

Road user applications. In order to perform the trusted vehicular communications, we need to ensure peer vehicle Vehicular adhoc network plays an important role in credibility by means of IKEV2 authentication scheme. Due to the high mobility rate of VANETs, the unsuccessful delivery of information between the vehicles. To overcome this loss of information by speeding up the process of certificate validation In previous approach they are capable of utilizing the single key for both the prover and verifier. Due to this single key usage, the symmetric key approach could not hide the RF channel between the prover and verifier and also the verifier can do the lot of trails to select the decrypted key from the key database. Hence the authentication delay gets increased for symmetric key cryptography. So as to overcome this challenges include the authentication delay and security issues, we propose the novel RFID authentication protocol based on ELLIPTIC CURVE CRYPTOSYSTEM with asymmetric key cryptography. In this approach the certificate authority for authentication scheme is namely IKEV2.Besides two goals are set: to overcome the authentication delay and improving the security issue The rest of the paper is organized as follows. section II describes the overview of VANETs section III describes the privacy issues in RFID systems; section IV describes the concept of symmetric key management; section V describes the group based management section VI describes the performance analysis;

II. Review Of Vehicular Ad Hoc Networks

The following description of Vehicular Ad Hoc Networks and their security and privacy properties. The interested reader can get a broader view and deeper understanding on VANETs by reading the cited papers instead of only relying on this short introduction The main motivation to use VANETs is to enhance traffic safety, traffic efficiency, give assistance to drivers, and the possibility of infotainment applications. A VANET consist of vehicles equipped with On Board Units (OBUs) and wireless communication equipment, Road Side Units (RSUs), and backend infrastructure. The vehicles exchange messages regularly with each other and with the infrastructure using wireless communication to achieve the main goals such as safer roads. sample illustration of general structure of the VANETs is shown in Figure. 1 The main vulnerabilities in VANETs come from the wireless nature of the communication, and Figure1.An example of general structure of VANETs. the sensitive information, such as location of users, used by the network. One major vulnerability comes from the wireless nature of the system: the communication can be jammed easily, the messages can be forged. Another problem related to the wireless communication is that while the nodes are relaying messages, they can modify them. This is called In-Transit Traffic Tampering. Another kind of problem, that the vehicles can impersonate other vehicles with higher privileges such as emergency vehicles to gain extra privileges.

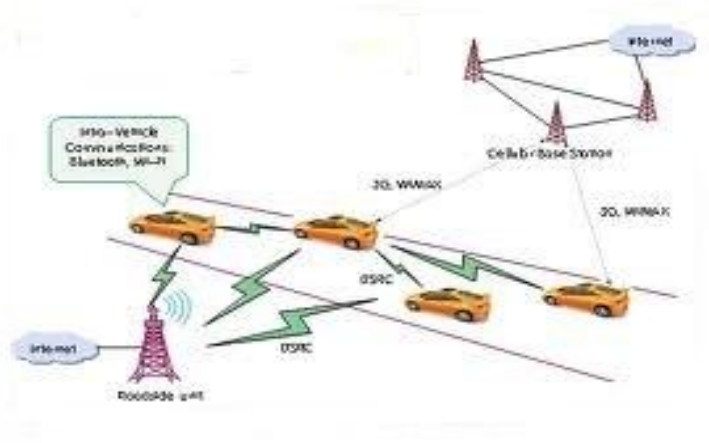


Figure.1 general structure of the VANETs

The most relevant problem to this dissertation is that the privacy of the drivers of the vehicles can be violated. This vulnerability is analyzed in general an attacker can achieve her goals by tampering the OBU, an RSU, sensor readings, or the wireless channel. Traditional mechanisms cannot deal with the vulnerabilities discussed above because of the new challenges in VANETs. Such challenge is the high network volatility caused by the highly mobile very large scale network. Another challenge is that the network must offer liability and privacy at the same time in an efficient way, as the applications are delay sensitive. To make things even worse, the network is very heterogeneous, different vehicles can have different equipment and abilities, so no unique solution can solve every problem When defining the key vulnerabilities and challenges of vehicular ad hoc networks, it is crucial to first define and characterize the possible attackers. In many papers the attacker can be characterized as follows:

Insider vs. Outsider

The key difference between an insider and an outsider attacker is that an insider poses legitimate and valid cryptographic credentials, while an outsider does not have any valid credentials. It is obvious that an insider attacker can mount stronger attacks, then an outsider.

Malicious vs. Rational

The main goal of a malicious attacker is to disrupt the normal operation

Active vs. Passive

A passive attacker only eavesdrops the messages of the vehicles, while an active attacker can send, modify, or delete messages.

Local vs. Global

A local attacker mounts his attack on a small area (or on some non continuous small areas), while a global attacker has influence on broader areas.

III. Privacy issues in RFID systems

The following description of RFID systems and its security and privacy problems is based on the key management. An RFID system consists of simple Tags, Readers, and Backend servers. The tags carry unique identifiers. These unique identifiers are read by nearby Readers by radio communication. The Readers send the obtained identifiers to Backend Servers. The goal of an RFID system is the unique identification of the holders of the Tags. Example applications of RFID systems include smart appliances, shopping, interactive objects or medication compliance. This list can be expanded to hundreds of scenarios.The main threats to privacy in RFID systems are tracking and inventorying. A tracking attacker can eavesdrop message exchanges in different parts of the network. If the system is not defended against such attacks, the attacker can link different message exchanges of the same user, hence can track the user. This is a very important concern in RFID systems (the problem of tracking is actually not unique to RFID systems, namely in vehicular networks).Inventorying is a specific attack against RFID systems. It relies on the assumption that in the near future, most of our objects will be tagged with distant readable RFID tags. An attacker carrying out an inventorying attack can get know exactly what a user wears, has in her pockets or bag without the consent of the user. Two private authentication methods are given, which make it difficult for an attacker to carry out tracking and inventorying attacks. Another important field of security problems regarding RFID is the authenticity of the tags. In short, the privacy problem is related to malicious readers, while the authenticity problem is related to malicious tags. The main problem is that illegitimate tags can be counterfeited to obtain the same rights as the legitimate tag holds. In the following assume the presence of malicious readers, but no malicious tags are considered. When considering the RFID

tags capabilities, the tags on the market can be classified into two main categories: basic tags with no real cryptographic capabilities and advanced tags with some symmetric key cryptography capabilities.

Basic tags

Basic RFID tags lack the resources to perform true cryptographic operations. The lack of cryptography in basic RFID tags is a big impediment to security design; cryptography, after all, is the main building block of data security. The main approaches to provide privacy to basic tags are the following: killing, sleeping, renaming, proxying, distance measurement, blocking, and legislation. Killing and sleeping are very similar approaches. The basic idea is that an authenticated command can reversibly or permanently switch off the tag. The authentication of basic tags is as hard as providing privacy to them. There are some work, how the kill PIN can be used to authenticate the tags.

Advanced tags

Advanced tags are capable of simple symmetric key operations. However weak cryptographic algorithms are targets of successful attacks.Another attack type against cryptographically enabled tags are the man-in-the-middle attacks. In a MiM attack the attacker is relaying messages between the tag and the reader and by doing so, he can modify, delete, and inject messages in their communication. This can also be done if the tag and the reader are not in vicinity.In short, the problem is that the tag is not allowed to send its identifier in order to avoid tracking, therefore the reader needs a lot of trials to find the right decryption key. The computational burden on the reader can be partly alleviated with key-trees, synchronization , or time-memory tradeoffs. However, all known mitigation techniques lead to degradation of privacy or efficiency.

IV. Symmetric Key Management

The problem of using symmetric key encryption to hide the identity of the prover is that the verifier does not know which symmetric key it should use to decrypt the encrypted identity, because the appropriate key cannot be retrieved without the identity. The verifier may try all possible keys in its key database until one of them properly decrypts the encrypted identity1, but this would increase the authentication delay if the number of potential provers is large. Long authentication delays are usually not desirable, moreover, in some cases, they may not even be Some years ago, Molnar and Wagner proposed an elegant approach to privacy protecting authentication that is based on symmetric key cryptography while still ensuring short authentication delays. More precisely, the complexity of the authentication procedure in the Molnar-Wagner scheme is logarithmic in the number of potential provers, in contrast with the linear complexity of the negative key search approach. The main idea of Molnar and Wagner is to use key-trees in proposed architecture of VANETS).Key-tree is a tree where a unique key is assigned to each edge. The leaves of the tree represent the potential provers, which is called members in the sequel

Each member possesses the keys assigned to the edges of the path starting from the root and ending in the leaf that corresponds to the given member. The verifier knows all keys in the tree. In order to authenticate itself, a member uses all of its keys, one after the other, starting from the first level of the tree and proceeding towards lower levels. The verifier first determines which first level key has been used. For this, it needs to search through the first level keys only. Once the first key is identified, the verifier continues by determining which second level key has been used. However, for this, it needs to search through those second level keys only that reside below the already identified first level key in the tree. This process is continued until all keys are identified, which at the end, identify the authenticating member. The key point is that the verifier can reduce the search space considerably each time a key is identified, because it should consider only the sub tree below the recently identified key. Acceptable. As an example, let us consider again contactless smart card based electronic tickets in public transportation: the number of smart cards in the system (i.e., the number of potential provers) may be very large in big cities, while the time needed to authenticate a card should be short in order to ensure a high throughput of passengers and avoid long queues at entry points. There is a unique key assigned to each edge. Each leaf represents a member of the system that possesses the keys assigned to the edges of the path starting from the root and ending in the given leaf. For instance, the member that belongs to the leftmost leaf in the figure possesses the keys k1, k11, and k111. The problem of the above described tree-based approach is that upper level keys in the tree are used by many members, and therefore, if a member is compromised and its keys become known to the adversary, then the adversary gains partial knowledge of the key of other members too This obviously reduces the privacy provided by the system to its members, since by observing the authentication of an uncompromised member, the adversary can recognize the usage of some compromised keys, and therefore its uncertainty regarding the identity of the authenticating member is reduced (it may be able to determine which sub tree the member belongs to). One interesting observation is that the na¨ıve, linear key search approach can be viewed as a special case of the key-tree based approach, where the key-tree has a single level and each member has a single key. Regarding the above described problem of compromised members, the nagative

approach is in fact optimal, because compromising a member does not reveal any key information of other members. At the same time, as described above, the authentication delay is the worst in this case. On the other hand, in case of a binary key-tree, it can be observed that the compromise of a single member strongly2 affects the privacy of the other members, while at the same time; the binary tree is very advantageous in terms of authentication delay. Thus, there seems to be a trade-off between the level of privacy provided by the system and the authentication delay, which depends on the parameters of the key-tree, but it is far from obvious to see how the optimal key-tree should look like. After finding the optimal key-tree, I go further and I present a novel symmetric key private authentication scheme that provides a higher level of privacy and achieves better efficiency than the key-tree based approach. This approach is called the group based approach. More precisely, the complexity of the group based scheme for the reader can be set to be O(logN) (i.e., the same as in the key-tree based approach), while the complexity for the tags is always a constant (in contrast to O(logN) of the key-tree based approach). Hence, the group based scheme is better than the key-tree based scheme both in terms of privacy and efficiency, and therefore, it is a serious alternative to the key-tree based scheme to be considered by the RFID community.

V. Group Based Key Management System

In the group based authentication scheme, the set of all tags is divided into groups of equal size, and all tags of a given group share a common group key. Since the group keys do not enable the reader to identify the tags uniquely, every tag also stores a unique identifier. Keys are secret, but identifiers can be public. To avoid impersonation of a tag from the same group, every tag has a unique secret key as well. This key is only shared between the tag and the reader. To reduce the storage demands on the reader side, the pair wise key can be generated from a master key using the identifier of the tag. In order to authenticate a tag, the reader sends a single challenge to the tag. The answer of the tag has two parts. In the first part, the tag answers to the reader by encrypting with the group key the reader's challenge concatenated with a nonce picked by the tag, and the tag's identifier. In the second part, the tag encrypts the challenge concatenated with the nonce using its own secret key. Encrypting the identifier is needed since the key used for encryption does not identify uniquely the tag. Upon reception of the answer, the reader identifies the tag by trying all the group keys until the decryption succeeds. Then it checks the second part, that it was encrypted by the same tag. Without the second part, every tag could impersonate every other tag in the same group. The complexity of the group-based scheme for the reader depends on the number of the groups. In particular, if there are γ groups, then, in the worst case, the reader must try γ keys. Therefore, if the upper bound on the worst case complexity is given as a design parameter, then γ is easily determined. For example, to get the same complexity as in the key-tree based scheme with constant branching factor, one may choose $\gamma = (b \log_b N) - 1$, where N is the total number of tags and b is the branching factor of the key-tree. The minus one indicates the decryption of the second part of the message. An immediate advantage of the group-based scheme with respect to the key-tree based approach is that the tags need to store only two keys and an identifier. In contrast to this, in the key-tree based scheme, the number of keys stored by the tags depends on the depth of the tree. For instance, in the case of the Molnar-Wagner scheme, the tags must store $\log_b N$ keys. Moreover, by using only two keys, this scheme also has a smaller complexity for the tag in terms of computation and communication. Besides its advantages with respect to complexity, the group-based scheme provides a higher level of privacy than the key-tree based scheme when some of the tags are compromised.

VI. Proposed System

Internet Key Exchange Protocol Version2.

Dynamically establishes and maintains a shared state between the end-points of an IP datagram.IKEV2 performs mutual authentication between two parties and establishes the IKEV2 security association (SA).The IKE-SA uses shared secret information that it stores to-do two different functions. one is to establish CHILD-SAs for encapsulated security protocol(ESP) or authentication header protocol(AHP).Another is to defines the cryptographic algorithms to be used by the SA's. In this the Figure 2 illustrates an example of sample IKE exchange.IKEV2 is a request/response pair protocol. These pairs are refered to as exchanges. The requester bears the burden of ensuring reliability.If a response is not received the requester can either retransmits or abonden the connection IKEV2 has four types of exchanges.1.IKEV2-SA-INIT 2.IKE-AUTH 3.CREATE-CHILD-SA 4.INFORMATIONAL Once the first two mandatory exchanges have completed in their order, all subsequent exchanges can happen in any order.IKEV2 employs a number of cryptographic protocols to accomplish all the security requirements of key management.IKEV2 is based on the DIFFIE-HELLMAN KEY management protocol.IKE has four transform types that are mandatory to implement;

- Encryption algorithms
- pseudo-random functions

- integrity algorithms
- diffie-hellman groups

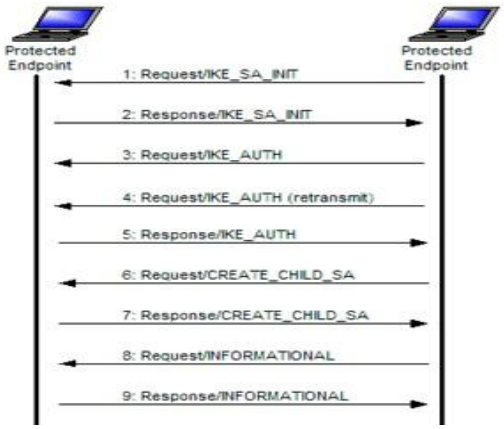


Figure 2 IKEV2 is a request/response pair protocol.

A Novel Rfid Authentication Protocol Based On Elliptic Curve Cryptosystem (ECC)

Recently, many researchers have proposed RFID authentication Protocols. They is mainly consists of two types: symmetric key based and asymmetric key based. The symmetric key based systems usually have some weaknesses such as suffering brute force, de synchronization, impersonation, and tracing attacks. In addition, the asymmetric key based systems usually suffer from impersonation, Man-in-the-middle, physical, and tracing attacks. To get rid of those weaknesses and reduce the system workload, we adopt elliptic curve cryptosystem (ECC) to construct an asymmetric key based RFID authentication system. Our scheme needs only two passes and can resist various kinds of attacks. It not only outperforms the other RFID schemes having the same security level but also is the most efficient. In general the bit size of the public key believed to be needed for ECDSA (elliptic curve digital signature algorithm) is about twice the size of the security level in bits. If the applications of RFID systems violate privacy principle, like the personal information leakage or illegal tracing by a malicious person, it will keep us from applying them. To prevent this situation, a secure RFID protocol is usually embedded with authentication functions to protect the communication from an intentional adversary. To safely authenticate a tag's identity the proposed protocols using symmetric key cryptography although cost less but usually cannot achieve the demanding security requirements of a RFID system. In PKC, elliptic curve cryptosystem (ECC) can provide the same security level with shorter keys. This makes ECC a suitable public key cryptosystem to be applied in RFID systems which has less powerful device such as tags. Hence in this paper, we will base on ECC to propose a novel RFID authentication protocol. In 1985 and 1987, Victor S. Miller and Neal Koblitz independently proposed the concepts of ECC [23]. Below, we roughly introduce ECC and Elliptic Curve Discrete Logarithm Problem [23, 25].In contrast public key involves the use of a public key and private key pair.

ECC (Elliptic Curve Cryptography): Suppose a and b are two field elements that define the curve of the equation y2=x3+ ax + b. All points (x, y) satisfying the elliptic curve equation along with an infinite point O and an addition operation form a group G. The elliptic curve has the following properties:

✧ suppose P = (x, y), then define –P = (x, -y).

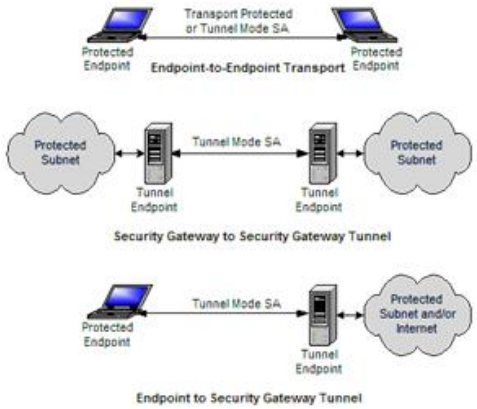


Figure 3 Elliptic Curve Cryptosystem

Some IKEv2 based elliptic curve cryptosystem examples are shown in Figure 3: IKEv2 scenario examples.In 2006, Tuyls et al. proposed Schnorr identification RFID protocol based on ECDLP. We depict their Schnorr identification protocol and describe the interactions between the Prover-Tag and Verifier-Reader as follows:

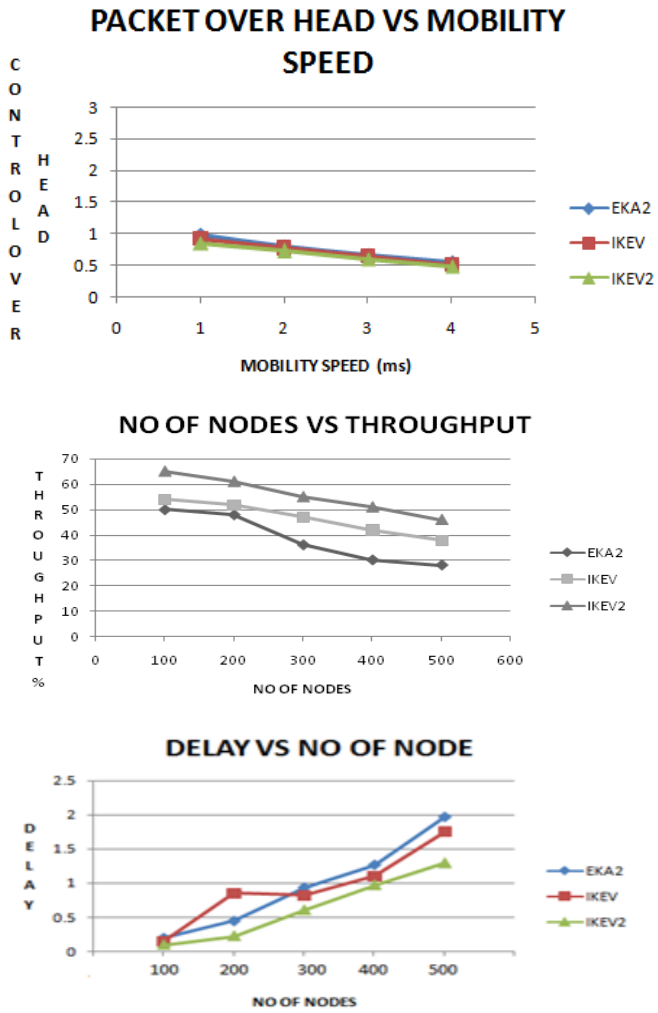
✧ **Commitment by a Prover-Tag**: The tag picks a random number r and sends X=rP to the reader.

✧ **Challenge from a Verifier-Reader**: After receiving X, the reader picks a Random number e and sends it to the tag.

✧ **Response from a Tag**: After receiving e, the tag computes y = ae + r and sends y to the reader. Upon receiving y, the reader computes yP+eZ and checks if it is equal to X. If it is, the reader accepts.

VII. Performance Analysis

Our simulators are performed on the network simulator-2 tool.



VIII. Conclusion

In this paper an efficient authentication of RFID is provided by introducing IKV2 protocol. Compared to the EKA2,the certificate validation process is efficient in IKV2 by producing group based key management process. In this process the control overhead is reduced for 0.07ms also the authentication delay gets reduced in 0.05ms. In future work we can allow only the genuine forwarder based on the secure overhead analysis of all the users in this the CRL validation process is done by the contention window (CW) concept for speed up the certificate revocation status.

References

[1] L. Eschenauer and V. D. Gligor, "A key-management scheme fo rdistributed sensor networks," in Proceedings of the 9th ACMconference on Computer and communications security, CCS '02, (NewYork, NY, USA), pp. 41–47, ACM, 2002.

[2] B. Parno, and A. Perrig "Challenges in securing vehicular networks," In Proc. of the Int.Workshop on Hot Topics in Networks (HotNets-IV), 2005XI Y., SHA K., SHI W., SCHWIEBERT L., ZHAN

[3] G. Calandriello, P. Papadimitratos, A. Lioy, and J.-P. Hubaux, "Efficient and robust pseudonymous authentication in vanet," in ACM International Workshop on VehiculAr Inter-NETworking (VANET), 2007.
[4] LO N., TSA H.: 'Illusion attack on VANET K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [Security and privacy in emerging wireless networks]," Wireless Communications, IEEE, vol. 17, pp. 56–62, Oct. 2010.
[5] L. Zhang, Q. Wu, A. Solanas, and J. Domingo- Ferrer, "A scalable robustauthentication protocol for secure vehicular communications," IEEE Trans. Veh. Technol., vol. 59, no. 4, pp. 1606–1617, May 2010.
[6] W. B. Jaballah, M. Mosbah, and H. Youssef,"Performance evaluation of key disclosure delay based schemes in wireless sensor networks," in Proc.IEEE PERCOM/PERSENS, Mar. 2013, pp. 566–571.