Analysis of security approaches for vehicular ad-hoc networks

Alexandra Mihaita (Mocanu) *, Ciprian Dobre§, Bogdan Mocanu*, Florin Pop§, and Valentin Cristea§
University Politehnica of Bucharest
Bucharest, Romania
* E-mail:{alexandra.mihaita, bogdan.mocanu}@hpc.pub.ro
§ E-mail:{ciprian.dobre, florin.pop, valentin.cristea}@cs.pub.ro

***Abstract*—In the last years, the number of vehicles has increased up to a point where the road infrastructure cannot easily cope anymore, and congestion in cities becomes the norm rather then exception. Smart technologies are vastly employed to cope with advanced scheduling mechanisms – from intelligent traffic lights designed to control traffic, up to applications running inside the car to provide updated information to the driver, or simply keep him socially connected. The time for such smart technologies is right: the power of computation along with the memory size of microprocessors have increased, while price per computation, storage and networking power decreased. What few years ago might have sounded rather futuristic, like technologies designed to facilitate communication between cars and automate the exchange of data about traffic, accidents or congestion, is now becoming reality. But the implications of these ideas have only recently become relevant; in particular, security and trust-related implications are just now arising as critical topics for such new applications. The reason is that drivers face new challenges, from their personal data being stolen or applications being fed with false information about traffic conditions, to technology being exposed to all kind of hijacking attacks. A practitioner developing a smart traffic application is faced with an important problem: what security technology or algorithm to use to better cope with these challenges. In this paper, we first present an analysis of various cryptographic algorithms in the context of vehicular scenarios. Our scope is to analyze the designs and approaches for securing networks formed between vehicles. In particular, we are interested in the security layers able to provide strong cryptographic algorithms implementation that can guarantee high levels of trust and security for vehicular applications. The analysis exploits the realistic simulator being developed at the University Politehnica of Bucharest.**

I. Introduction

In the context of constant growth of the number of vehicles on the roads, the inefficiency of the road infrastructure and increasing traffic congestion are more and more obvious. This weak points have lead to the need of a new paradigm called simply intelligent traffic systems(ITS). Their use have various reasons starting from egoistic reasons like finding faster routes to improve environmental protection by decreasing nuisances. But each new field, needs time to grow and gather practical experience. To this respect, experiments have shown that an intelligent traffic system has very high perspectives when used properly. But if malicious intentions are taken into consideration when talking about automation of traffic systems, the risks become very high.
In order to prevent abusive behaviors, or worse, malicious ones security aspects need to be taken into consideration. The problem with growing fields is that there are a lot of new innovative ideas like different ciphers, each stating better security than the other, but none tested over long periods of time in order to reveal its true potential. Taking this fact into consideration along with the time constraints and the ad hoc nature of the inter vehicular communication it is very hard to implement a security mechanism.
This paper's main goal is to research the most reliable cryptographic symmetrical ciphers and to this respect we will test multiple ciphers comparatively over a simulator of real life conditionsin. The most reliable cryptographic algorithm has to provide high levels of trust and security for vehicular applications while stil making the message exchange possible. In the next chapters, related work in the field of ITS are presented, with their advantages and disadvantages. Then, a comparative analysis of various symmetrical ciphers has been made both in theoretical aspects and performance. The performances of the ciphers have been firstly observed in a independent application in order to determine the existence of a unique solution and, based on these first results, tests within a simulator of real time conditions have been made. The theoretical aspect have been supported by the test results in certain conditions, revealing that the application's design must be thoroughly analyzed and deeply taken into consideration in the implementation phase.

II. Related Work and an Analysis of Prior Work

Intelligent Transportation Systems (ITS) combine information and communication technologies in the field of road transport. They provide advanced applications and services that allow users to be better informed about the status of the roads, to improve the safety and efficiency on the streets, to relieve traffic congestion and reduce air pollution. ITS get information directly from traffic, from road sensors or other vehicles – they use data such as vehicle's location, driver's traffic experience and even other neighbors. Considering that each driver uses devices with limited resources, and they compete for the same road infrastructure (i.e., to go faster to destination), malicious actions can occur: drivers can willingly provide wrong information about location, or forge information about the current traffic status.

Attacker	Description
Insider vs. Outsider	The insider is an authenticated member of the network.
	The outsider is an intruder and his actions are therefor limited.
Malicious vs. Rational	The malicious does not seek personal retribution but to create damage to the network.
	The rational is more predictable since it seeks personal advantages.
Active vs. Passive	The active can generate messages or signals.
	The passive can not generate messages but only to eavesdropping.

TABLE I
CATEGORIES FOR ATTACKERS.

Raya and Hubaux [1] present a critical analysis of the evolution of vehicular security, from the early solutions designed to cope with tachometers, all the way to the use of GPS tracking devices and applications for smartphones.

Securing vehicular applications tend to be more complicated than is the case with more traditional applications, especially because data can be highly sensitive [1], and the time for communication and for taking preventive actions is quite limited. Shuo et al [3] describe the main principles for security in the case of vehicular communication (now a reference in the field). Among these principles, the authors allocate an important space to the management of trust (in data and traffic participants) and security of data transmission. Hubaux et al [4] have taken the security issues forward and discuss about privacy and position forgeries. They also introduced the concept of Electronic License Plate(ELP) as a unique identifier for vehicles in ITS. Gollan et al [5] propose one of the first ideas of securing the VANET with digital signatures, while Furgel and Lemke [6] propose a security architecture based on PKI for digital tachometers [2]

On a social side, Raya et al [7] discuss about the various mechanisms of an attacker (briefly presented in Table I), highlighting the scope of an attack based on roles. Authors conclude that attacks can be spitted, at a superficial view, into five categories:

- *Bogus information* – is sent by a malicious attacker in order to confuse the other users and create a distorted image of the network.
- *Cheating with positioning information* – is used in the case of running from responsibility in case of accidents.
- *ID disclosure* of one's neighbor – can be done in order to rebuild their traces.
- *Denial of service* attacks – are used in order to make unavailable the network or even cause accidents.
- *Masquerade* or impersonating attacks – are used to send bogus information into the network.

To address the problems, Raya et al [7] present the different types of attack specific for ITS, and propose multiple security methods and mechanisms. A comparison of several approaches was later made in [**?**], between: ARAN [2], ARIADNE [3], CONFIDANT [4], DCMD [5], SAODV [6], SEAD [7], SLSP [8], SPAAR [9], SOLSR [10] and WATCHDOG-PATHRATER [11]. A comparative summary can be seen in Table II.

The **ARAN**(Authenticated Routing for Ad hoc Networks) [2] approach is PKI-oriented, using a trusted certificate authority that is publicly known by all users of the ITS application. Each user has to get a certificate in order to be able to enter the network, which must be IP-based. The advantages of the approach are a better protection against malicious nodes by using authentication, message integrity and non-repudiation, protection against spoofing or even alteration of routes, elimination of the reply attacks by using timestamps and a good performance for route discovery and maintenance. The disadvantages of the approach are the fact that it is not scalable, it causes overhead in the network and latency in the communication.

ARIADNE [3] is a symmetric cryptography-based approach that presents three versions: shared secret between each pair of nodes, between communication nodes combined with broadcast authentication or digital signature. The advantages of the approach are a better protection against malicious nodes by using authentication and message integrity, protection against malicious node attacks, routing loops or reply. The main disadvantage of the approach is the fact that it increases the package length which in turn decreases the ratio of the package exchange between the users of the network.

CONFIDANT(Cooperation Of Nodes: Fairness In Dynamic Ad hoc NeTworks) [4] is a trust approach for security, that uses a monitor (an entity that is able to observe, objectively and trustfully, the traffic), a trust manager (the alarm generating entity), the reputation system (which manages the ranking of trustworthiness), and the path manager (the path-decision responsible entity). The advantages of the approach is the fair detection of malicious nodes by constantly monitoring the status of the messages in the network and the reports about the attacks. A disadvantage of the approach is lack of scalability, since for networks with large number of vehicles it has to manage increasingly larger trust lists, which directly proportional increases the computation overhead with the number of vehicles.

DCMD(Detecting and Correcting Malicious Data in VANET) [5] is rather an application-oriented approach than a routing protocol. It is based on the data collected from the sensors in order to determine the correctness of the information received, and therefore to spot malicious nodes. The advantage of the approach is that it is scalable and can be easily rendered mobile by using a typical reputation system where events are classified (rather than the user being in charge of this), which allows a better image of the network. The disadvantages are the fact that data from the sensors can be not integrity-secured and, therefore, by manipulating this data one can manipulate the network itself.

SAODV(Secure Ad hoc on demand Distance Vector) [6] is an asymmetric cryptography-oriented approach based on

[1]We recall the recent incident with Uber accidentally exposing personal data of over 50,000 drivers [2]

[2]The instrument measuring the rotation speed of the shaft or disk in the motor of the car (usually in RPM).

Approach	Objectives	Mechanism
ARAN	authentication, integrity and non-repudiation of signaling packets	certificate authority and timestamps
ARIADNE	authentication and integrity of signaling packets	symmetric cryptography, hash functions and timestamps
CONFIDANT	exclude misbehaviour	reputation system
DCMD	detect and correct malicious data	observation and plausibility of events
SAODV	authentication and integrity of signaling packets	digital signatures and hash chains
SEAD	authentication and integrity of signaling packets	hash chains and sequence numbers
SLSP	authentication, integrity and non-repudiation of signaling packets	certificate authority
SPAAR	authentication, integrity, non-repudiation and confidentiality of signaling packets	certificate authority and timestamps
SOLSR	authentication and integrity of signaling packets	MACs and timestamps
WATCHDOG - PATHRATER	excludes misbehaviors	observation and reputation

TABLE II
A COMPARISON OF SECURITY APPROACHES.

splitting messages into modifiable fields that are signed, and fixed fields that are transmitted through their hash. The advantages of the approach are the fact that it provides integrity for the modifiable fields, and that it proves to be secure efficient. The main disadvantages are the fact that it increases the total overhead of the network, and it is resource dependable, in the sense that the messages of a node with high computational power will be potentially interpreted as a DoS attack by a node with lower computational power.

SEAD(Secure Efficient Ad hoc Distance Vector) [7] is a distance-vector routing protocol in which asymmetric cryptography is replaced with one-way hash functions of the message in order to grant integrity. The advantages of this approach are good computational performances with limited resources, and the fact that it has more recent routing tables thus performing better in high mobility situations. The disadvantage of the approach is the fact that it needs an extra security step in order to prevent message forgeries.

The **SLSP**(Secure Link State routing Protocol) [8] uses hash functions and public key cryptography in order to secure message routing. The advantage of this method is the fact that it uses division of the vehicle based on areas which makes the approach scalable. Another advantage is the fact that it is easily adaptive to different topologies. The disadvantage is that it is resource consumptive.

The **SPAAR**(Secure Position Aided Ad hoc Routing) [9] is an asymmetrical cryptography-based approach that provides authentication, message integrity, non-repudiation of sent messages and confidentiality. The advantage of this approach is that it is secure efficient, but the disadvantage is that it takes twice the time to compute messages and therefor the message exchange ratio is split by half.

The **SOLSR**(Secure Optimized Link State Routing) [10] uses one way hash MACs in order to grant authentication and prevent reply attacks. The advantage of the approach is that it has low computational requirements whereas the main disadvantages are scalability issues and increased overhead.

The **WATCHDOG-PATHRATER** [11] is a two step approach based on a "watchdog" that monitors the network in order to detect nodes that misbehave, and a "pathrater" that needs to find alternative paths in order to avoid malicious nodes. The main advantage of the system is that it is low resource consumptive, while the main disadvantage is that it takes long to exchange messages which decreases the message exchange ratio.

III. COMPARATIVE ANALYSIS

A. Algorithm description

After we analyzed the most promising security mechanisms for ITS, we selected: for our comparison several symmetric encryption algorithms: AES [12], AES Fast [12], AES Light [12], Blowfish [13], Camellia [14], Camellia Light [14], Tea [15], and Twofish [16].

The **Advanced Encryption Standard (AES)** [12] is an encryption algorithm which has been established by the U.S. National Institute of Standards and Technology(NIST). The algorithm has three versions based on the key lengths of 128, 192 and 256 bits; the length, in turn, determines the number of encryption rounds (which can be 10, 12 and 14). The algorithm uses operations like substitution-permutation, which are fast both in hardware as in software implementation.

The **AES Fast** algorithm is an optimized version of the AES algorithm in the sense that it uses 8KB of static tables to store precomputed round calculation. Each table has 4256 word tables, which are used for encryption, and 4 word tables used for the decryption phase.

The **AES Light** algorithm is an optimized version of the AES algorithm in terms of footprint. It has no static tables, and therefore it is the slowest version of the AES algorithm. But the fact that it has the smallest footprint makes the algorithm attractive to hardware devices with little or limited memory.

Blowfish [13] is one of the first open-source encryption algorithms. The algorithm has 16 rounds, and uses block sizes of 64-bits and keys with variable length between 32 bits and 448 bits. It is considered to be a fast algorithm, except when the keys are changed, and has a rather small footprint. The advantage is that it can still be implemented on older devices, but the disadvantage is that it is not small enough to be implemented on smartcards for example.

Twofish [16] is one of Blowfish's successors. It has 16 rounds, and can support three possible key block sizes of 128, 192 and 256 bits, with data blocks of 128 bits. One

distinctive features of the algorithm is the use of pre-computed key-dependent S-boxes, and another one is the complex key schedule.

Camellia [14] is another symmetric algorithm made by Mitsubishi. It has 18 or 24 rounds, and three possible key dimensions of 128, 192 and 256 bits, with fixed data blocks of 128 bits. The security offered by the algorithm is comparable to that offered by the AES and there are no known attacks that can successfully weaken the cipher. The Light version of the Camellia cipher is optimized for size and therefore has a smaller implementation.

The **Tiny Encryption Algorithm (TEA)** [15] is one of the simplest in description. It has a variable number of rounds, although 64 rounds are recommended. It uses 64 bits block size and key sizes of 128 bits. The main disadvantage that the algorithm presents is the fact that a key has 3 equivalents, making it 4 times faster to break.

B. Performance results

In order to determine the better choice of a criptographic algorithm for ITS, we made several simulations using VNSim, a simulator developed at the University Politehnica of Bucharest [3].

The simulator uses a model for 802.11b Wireless MAC layer, an UDP transport layer, whose routing and addressing schemes have been changed to depend on geographical position.

The input of the simulator consists of vehicle mobility models according to which the vehicles are positioned on the map. Their trace is updated periodically in order to keep a realistic view of the grid. An interesting fact is that it takes into account traffic rules and multiple types of driver behaviors.

The UPB VANET Simulator's basic entities are vehicle and servers along with central unit called an Engines. Each vehicle has two event handlers for the message exchange: Send and Receive Handler. The engine is the entity that transforms each Send event of a vehicle into a Receive event on the destination vehicle. The GPS data of a vehicle is updates regularly according to a scheduler. The input data of the simulator is given by raw datasets corrections and traces generation and it has Node, Way and Location entity.

The cryptographic library collection that has been added to the Bouncy Castle which represents a collection of the most common known cryptographic algorithms. Its architecture has two basic components in order to support the cryptographic capabilities and these are the low level application programming interface(API) and the java cryptography extension (JCE) provider.

The library collection gives the user a set of symmetric and asymmetric algorithms with one can implement and test comparatively according to its conditions. In the present paper, a series of encryption and decryption have been made for various data block sizes: 1908 bytes, 19080 bytes,248040 bytes and 2480400 bytes.

[3]VNSim is accessible online at http://cipsm.hpc.pub.ro/vanet/vnsim.html.

These individual tests have revealed that there is no perfect cipher to perform the best in any circumstances, and that the conditions from the actual implementation are the most relevant when choosing a cipher.

The sizes of the data blocks have been chosen randomly, in order to have coverage of various data lengths. Based on the medium length of the packets sent in the simulator, an optimal algorithm can be deduced.

For small packets of data, the Blowfish algorithm proves to be the fastest, whereas the largest amount of data to be encrypted has revealed AES as being the fastest.

These results are somewhat expectable since Blowfish is known to be a fast block cipher for small amount of data since it does not need to change the keys so often. The change of keys is the more time consuming in the cipher and when encrypting large amount of data the change of keys brings delays.

The AES algorithm is known to have been optimized in hardware and in software for best performance, so the bigger the amount of data to be encrypted, the more time saved. The AES LIGHT cipher has a small footprint and therefore brings an advantage when used on devices with small amounts of memory. The AES Fast cipher has the advantage of loading precomputed temporary tables into memory, but that is noticeble only for small amounts of data.

The decryption of the packets for small amount of data has been Camellia whereas on the long term AES performed the best.

The Camellia cipher is composed of two parts: the "key scheduling part" and the "data randomizing part". The key scheduling part splits the key into two and then computes the key for each round. The data randomization implies 18 rounds. The bigger number of rounds as well as the bigger number of operations implied makes a great difference with large amount of data.

The Camellia Light cipher has not performed as well as the initial cipher in terms of time. A reason may be the fact that the cipher has been optimized for litter footprint.

Given the results from an independent application, further investigation has been made in order to determine the best cipher for a VANET network.

The simulation ran on the UPB's simulator have had the goal of monitoring the numbers of messages exchanges between the cars with each of the ciphers. The average packet size of the messages exchanged between cars is 220 bytes.

The result of the simulations has revealed a much larger number of messages exchanges between vehicle when using the TEA cipher. The simulation using this cipher has had the maximum number of messages exchanged at a certain point almost double that the least efficient cipher Camellia Light.

This shows that even though in an independent application the Blowfish cipher produced better time results, in the application the TEA cipher is more useful.

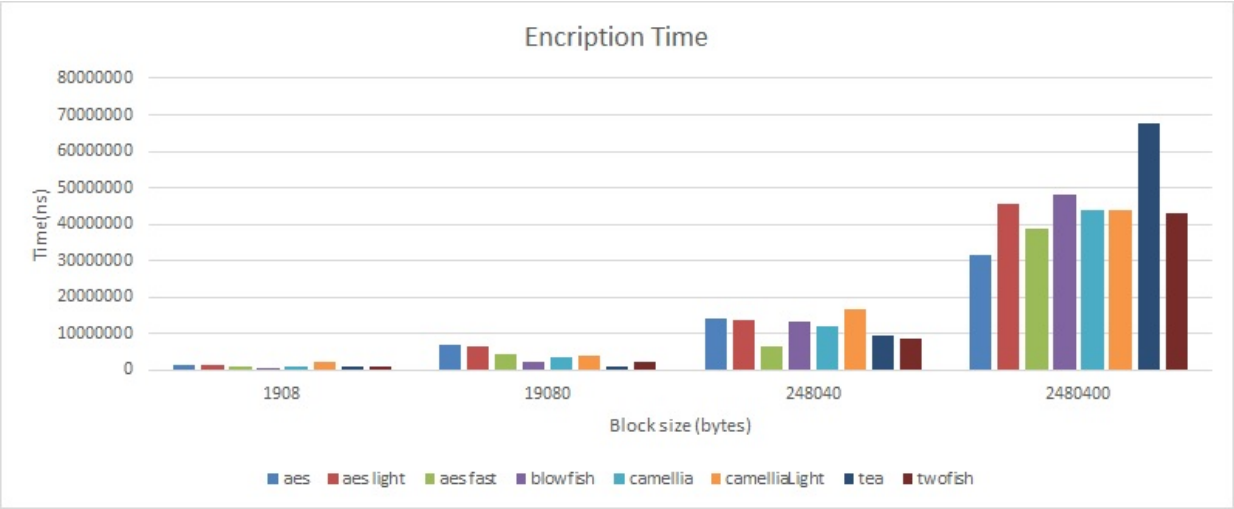

Fig. 1. Comparison for encription time between algorithms.

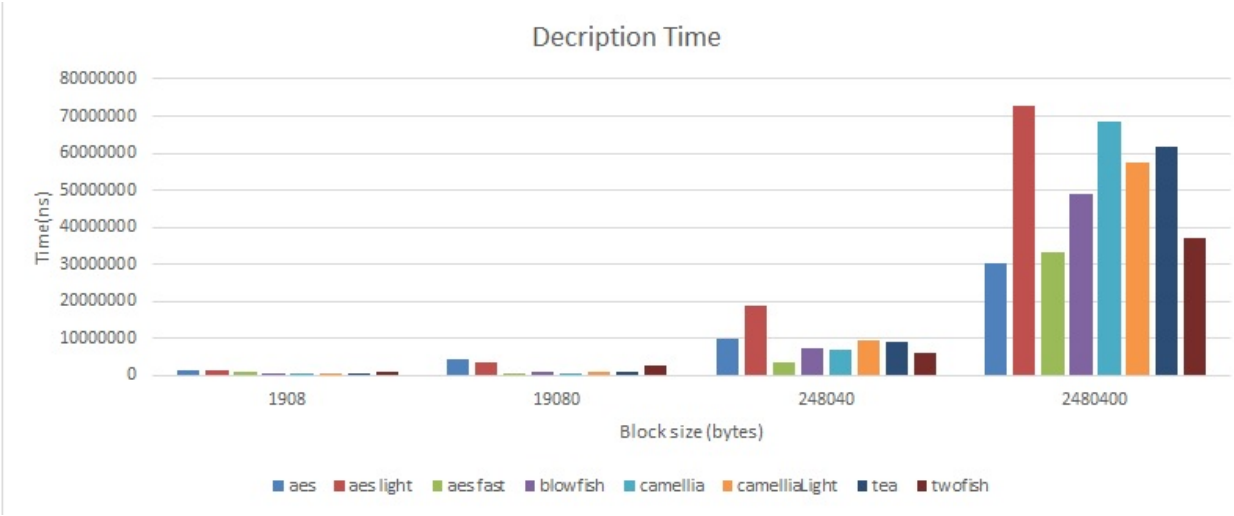

Fig. 2. Comparison for decryption time between algorithms.

IV. Conclusion

This paper's main goal has been to research the most reliable cryptographic symmetrical ciphers and to test them comparatively over a simulator of real life conditions. in order to do so, the Bouncy Castle collection of libraries has been studied and several algorithms like AES, AES Light, AES Fast, Blowfish, Camellia, Camellia Light, TEA and Twofish have been implemented.

The performances of the ciphers previously mentioned have been firstly observed in an independent application where, for the same key size, various clear text lengths have been chosen. The purpose of this test was to see if the performance of one algorithm is always better than the others performances. As expected, there has not been an unique algorithm to perform the best with the various clear text lengths, thus supporting the need of close analysis of each application's design.

The following test have been with the UPB's simulator in order to better take into considerations the application design. To this respect, the results have been surprising in the sense that a rather medium cipher in terms of performance when making the independent tests has had the best performance. The performance basic parameter in the application motorization has been the number of packets exchanged in a fixed amount of time of about 30 minutes. In this sense, ciphers with medium performances in the independent tests have been deeply separated in the application tests, one almost doubling the number of packets exchanged than the other.

The theoretical aspect have been supported by the test results in certain conditions, revealing that the application's design must be thoroughly analyzed and deeply taken into consideration in the implementation phase. These needs of analysis are even more supported after the tests performed with the UPB's simulator, differentiating two ciphers with almost the same results in independent tests at opposite sides in terms of

packets exchanged.

ACKNOWLEDGMENT

The work has been funded by the Sectoral Operational Programme Human Resources Development 2007-2013 of the Ministry of European Funds through the Financial Agreement POSDRU/187/1.5/S/155536, and national project MobiWay, Project PN-II-PT-PCCA-2013-4-0321.

REFERENCES

[1] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*. ACM, 2005, pp. 11–21.

[2] Z. Miners, "Personal data on 50,000 uber drivers exposed in breach," http://www.networkworld.com/article/2890473/personal-data-on-50000-uber-drivers-exposed-in-breach.html, accessed: 2015-08-01.

[3] S. Ma, O. Wolfson, and J. Lin, "A survey on trust management for intelligent transportation system," in *Proceedings of the 4th ACM SIGSPATIAL International Workshop on Computational Transportation Science*. ACM, 2011, pp. 18–23.

[4] J.-P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy*, no. 3, pp. 49–55, 2004.

[5] L. Gollan, I. L. Gollan, and C. Meinel, "Digital signatures for automobiles?!" in *in Systemics, Cybernetics and Informatics (SCI*. Citeseer, 2002.

[6] I. Furgel and K. Lemke, "A review of the digital tachograph system," in *Embedded Security in Cars*. Springer, 2006, pp. 69–94.

[7] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications*, vol. 13, no. LCA-ARTICLE-2006-015, pp. 8–15, 2006.

REFERENCES

[1] Fonseca, Emanuel, and Andreas Festag. "A survey of existing approaches for secure ad hoc routing and their applicability to VANETS." NEC network laboratories 28 (2006): 1-28.

[2] K.Sanzgiri et al. - "A Secure Routing Protocol for Ad-Hoc Networks"

[3] Y.-C. Hu et al. - " ARIADNE: A Secure-On-Demand Routing Protocol for Ad-Hoc Networks"

[4] S.Buchegger and J.-Y. LeBoudec - " Performance Analysis of the CONFIDANT Protocol"

[5] P. Golle, D. Greene, andJ. Staddon - " Detecting and Correcting Malicious Data in VANETs"

[6] G. M. Zapata - " Secure Ad hoc On-Demand Distance Vector Routing"

[7] Y.-C. Hu, D. B. Johnson, and A. Perrig - "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks"

[8] P. Papadimitratos and Z. J. Haas - "Secure Link State Routing for Mobile Ad Hoc Networks"

[9] S.Carterand A.Yasinsac - " Secure Position Aided Ad hoc Routing Protocol"

[10] T. Clausen, C. Adjih, P. Jacquet, A. Laouiti, A. Muhlethaler, and D. Raffo - "Securing the OLSR Protocol"

[11] S. Marti, T. J. Giuli, K. Lai, and M. Baker - "Mitigating Routing Misbhavior in Mobile Ad Hoc Networks"

[12] J.Daemen, V.Rijmen - "AES Proposal: Rijndael" http://www.cryptosoft.de/docs/Rijndael.pdf

[13] Schneier, Bruce. "Description of a new variable-length key, 64-bit block cipher (Blowfish)." Fast Software Encryption. Springer Berlin Heidelberg, 1994.

[14] Kato, Akihiro, Shiho Moriai, and Masayuki Kanda. "The Camellia cipher algorithm and its use with IPSec." (2005).

[15] Andrews, Benjamin, Scott Chapman, and Steven Dearstyne. "Tiny Encryption Algorithm (TEA) Cryptography 4005.705. 01 Graduate Team ACD Final Report".

[16] Schneier, Bruce, et al. The Twofish encryption algorithm a 128-bit block cipher. John Wiley & Sons, Inc., 1999.