CANTrack: Enhancing Automotive CAN Bus Security Using Intuitive Encryption Algorithms

Wael A. Farag

American University of the Middle East (AUM), Kuwait
Cairo University, Egypt
wael.farag@aum.edu.kw, wael.farag@cu.edu.eg

***Abstract* - In this paper, the proposed CANTrack solution is described and its implementation is thoroughly explained. CANTrack is a sophisticated Computer Aided Design (CAD) tool that supports the entire development process for automotive networked systems. CANTrack differentiates itself from other competitive tools; by not only supporting planning, development, testing and finally starting-up; but also incorporating the unique features of CAN bus security enhancement and tool customization upon customer needs. The Controller Area Network (CAN) bus security feature is implemented using an intuitive algorithm that encrypts the 8-byte payload data using a symmetric key that is being dynamically changed using synchronized key generators across all nodes. This algorithm makes the encrypted message unique at any instance of time to avoid replay attacks. The algorithm is tested thoroughly on an experimental setup using Vector Canoe; with the results of two use cases presented.**

Index Terms – CAD, CAN, Automotive, Security, Encryption.

I. INTRODUCTION

The security of vehicle networks is becoming an important issue [1]. When CAN was developed it was mimicking an ideal society of devices working in a democratic and trustworthy environment. The automotive systems [2] and CAN protocol were designed to take care of malfunctioning devices but a device with mal-intention can definitely wreak havoc with the system. Having so many systems relying on CAN, the security issue should be addressed definitely. The very important research papers from Koscher [3] and later Checkoway [4] showed that vehicles can be easy targets for malicious adversaries.

However, there are only few research results for assuring security on communication buses inside vehicles [1] or outside vehicles [5]. This is because the intra-vehicle communication is subject to constraints and specifications that are quite different from other well studied protocols. Most of the approaches advocate the use of secure gateways between different ECUs (Electronic Control Unit) or sub-networks and rely on basic building blocks from cryptography (encryptions, signatures, … etc.). However, none of these approaches is meant specifically for assuring broadcast authentication on CAN which is still the most common communication bus in automotive industry.

The more communications between vehicles and the surrounding infrastructures [5], the more risks on the security of car busses. Therefore, any presence of unauthentic information on the CAN bus of the car will expose the whole car security to risks and hacking.

In this respect, two main results in assuring CAN security can be found so far, one of them is based on the well-known TESLA protocol [6-7] and the other proposes a new paradigm which closely follows CAN specifications. Van Herrewege et al. [8] design a backward compatible message authentication protocol "CANAuth" from scratch and clearly noted that the constraints of CAN "eliminate all the authentication protocols published so far". We do agree with this conclusion in the sense that we believe that standard authentication approaches, may cover only some of the application areas for CAN; therefore, new approaches (even non-standard) are needed.

In Previous propositions, TESLA like protocols [6-7] proved to be highly effective in sensor networks and so far are the most efficient alternative for assuring broadcast authentication with efficient Message Authentication Codes (MAC). However, when it comes to CAN bus, this protocol family has one drawback that is critical for automotive: delays, which by the nature of TESLA are unavoidable [8]. Delays in the order of milliseconds or below, as shown to be achievable are satisfactory for many applications, but such delays do not appear to be small enough for intra-vehicle communication. There is no obvious way to improve on these delays further [8]. Of course one alternative is in using a bus with a higher throughput, more computational power and better electronic components (e.g., oscillators) but this will greatly increase the cost of components, nullifying in this way the cost effectiveness of CAN.

Hazem et al. [9] proposed and implemented a lightweight message source authentication protocol. According to the authors, it is only required to append a magic number to the message that can be verified by the receiver. This magic number can be only selected by the sender and verified by the receiver. The process of generating this magic number is based on the one-way hash function employed in TESLA protocol. The sender selects a random number then applies a transformation function multiple times. The result is used in reverse order. The last generated value of the chain is communicated initially to each receiver. Each receiver can verify the message by applying the transformation function on the current received value and compare it to the previous value. Keeping in mind that the payload of a CAN message is only 8 bytes, not much overhead should be added. The

978-1-5090-5454-1/17/$31.00 ©2017 IEEE

proposed length of the magic number is 2 bytes. The protocol does not require any hardware modifications to be done in the CAN network. Also, it does not add much overhead to the embedded software of the ECUs. Moreover, it tends to avoid any modifications from being done to the existing CAN message sets that are being exchanged between ECUs.

TABLE I CANTrack main features.

Feature	Supported in current version
General	
Bus Types	CAN
Bus analysing and monitoring	
Trace Window: Detail, Difference and Statistics views for displaying the time flow of events	YES
Data Window: Momentary display of bus signals, environment and system variables	YES
Graphic Window: Graphic display of signal responses	YES
Analysis Filter in Trace Window: Temporarily reduce the displayed data	YES
Offline Mode: Replay a logged measurement	No
Data Export: Use the logged data in other programs: *.txt, *.ascii,*.CSV	YES
Stimulation, Simulation, and Modeling	
Interactive Generator	YES
Replay: Replay a logged measurement in parallel to a running simulation	No
Define/access Environment Variables	YES
Execute Simulation Models	YES
CAPL	
CAPL programming/execution/debugging	YES
CAPL functions for bus access	No
Import CAPL code	YES
Panels	
Create/execute display panel	YES
Create/execute control panel	YES
Import panels	YES
Additional Options	
Supported HW devices	CANCaseXL VN16xx series

Udea et al. [10] proposed a monitoring system which uses Message Authentication Code (MAC) that is the generally effective against spoofing. The objective of the proposed security monitoring system is to prepare against spoofing attacks. In particular, a monitoring node authenticates each ECU and verifies the message authentication codes assigned to the CAN messages. However, in the proposed method, it is essential to install a special purpose CAN controller in the monitoring node. The special purpose CAN controller uses an error frame to overwrite spoofed messages on a real time basis. It could be considered an advantage of the proposed security monitoring system is that the only new hardware required is the monitoring node on the CAN bus. For other ECUs, only the software for node authentication and key exchange needs to be modified.

In this paper, our proposed simple and intuitive algorithm is based on using a dynamic key for encrypting CAN messages. The key is generated as function of the counter of the messages sent on the bus; and thus, messages are always unique at a given instance. Therefore, using this method will ensure that messages become unrecognizable and un-understandable by any receiver without the encryption key, as well as this method has the capability of preventing replay attacks [11].

II. CANTRACK

CANTrack is a Windows-based high-performance tool that supports the entire development process for automotive networked systems. It supports planning, development, testing and finally starting-up. Our main idea is to provide most of the features provided by our competitors' products while adding CAN bus security features as well as empowering the tool with the capability of customizing it upon customer needs.

CANTrack is developed to interface with different existing CAN hardware and represent the bus messages in a user friendly way that gives the user the ability to customize the look and feel of the window, and signals, in addition to importing and designing the user's own panels. CANTrack incorporates CAN bus security features, that are much needed in the industry today for in-vehicle security, as well as vehicle-vehicle communication. In addition, CANTrack provides flexible licensing options such as floating and standalone licenses, different versions of the software Basic and Pro versions according to the supported features. Moreover, developing a cloud service model is into perspective, and offering a "Pay As You Go" option will be provided as well.**Error! Reference source not found.** lists the features that are supported by CANTrack showing Bus analyzing and monitoring features; stimulation, simulation, modeling functions, CAPL support and various panels. Figure 1 depicts the architecture of the Solution. Moreover, Figures 2-6 shows samples of the intuitive windows provided by CANTrack to users with modern and simple look enabling straight forward usability and easy navigation.

978-1-5090-5454-1/17/$31.00 ©2017 IEEE

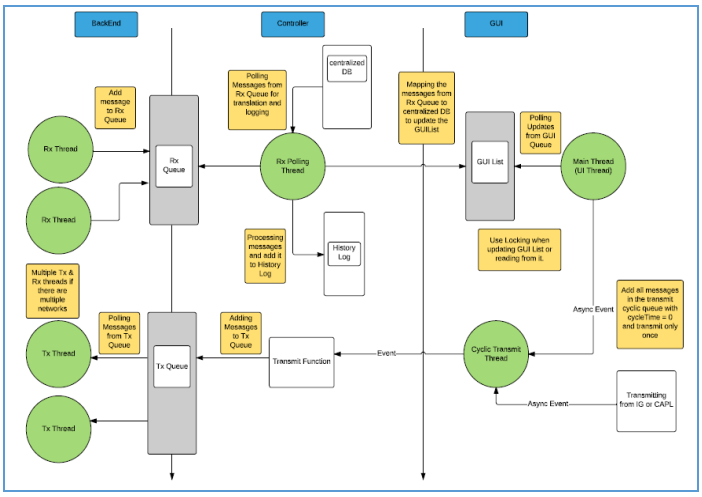

Fig. 1 CANTrack architecture.

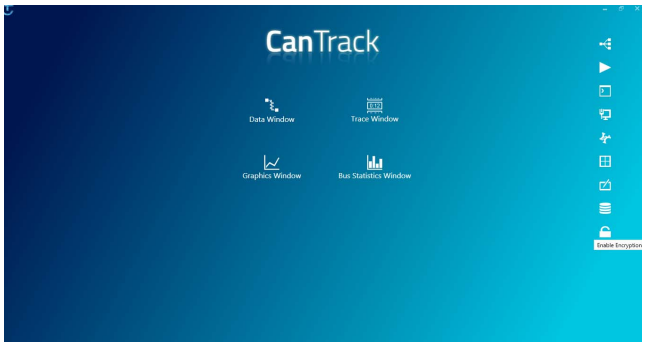

Fig. 2 CANTrack main window.

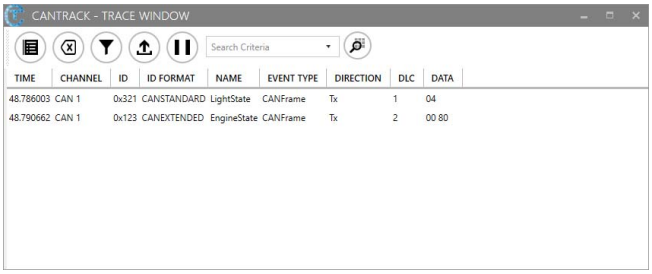

Fig. 3 CANTrack Trace window.

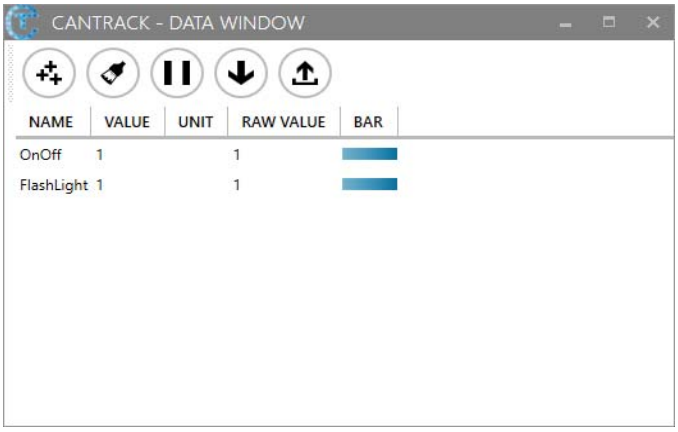

Fig. 4 CANTrack Data window.

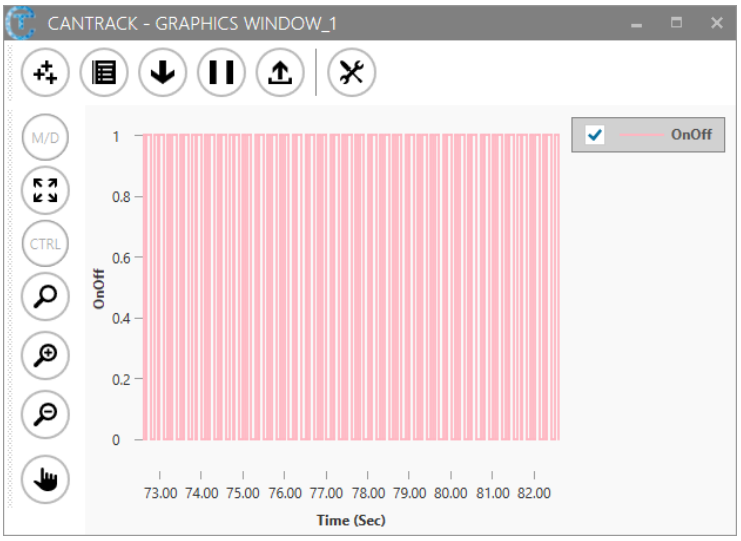

Fig. 5 CANTrack Graphics window.

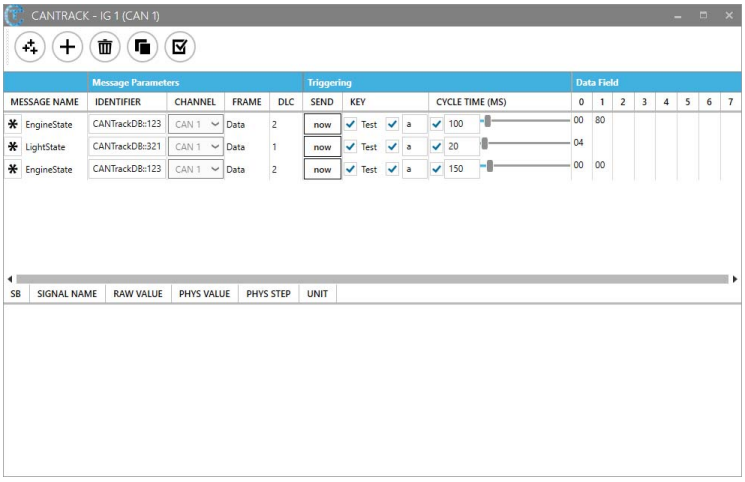

Fig. 6 CANTrack interactive generator.

III. Proposed Security Algorithm

It is well known that any physical presence on the bus for any untrusted element will expose payload data and messages IDs to be captured and understood. Messages sent on the bus doesn't include any info about the source of the messages, so messages sent by an intruder will not be ignored and will be treated as If they are from a trusted node.

Therefore, the required approach is to encrypt messages so they became unrecognized and non-understandable, while preventing replay attacks as well.

However, some limitations have to accommodated within the proposed algorithm as follows:

- We are using hardware APIs to send physical messages on the bus; so we can't edit the CAN message frame.
- The payload data can't be extended to include more data bytes.
- The messages IDs are used for setting the priorities of messages on the bus where for example a message of ID

978-1-5090-5454-1/17/$31.00 ©2017 IEEE

"0" is of highest priority; so we can't change or encrypt them.

Therefore, based on the above limitations, the following are the steps of the implementation methodology:

- The 8-byte payload data will be encrypted using a symmetric key.
- The encrypted message should be unique at any instance of time to avoid replay attacks.

Accordingly, synchronized key generators are used on each node. Keys must change dynamically without being shared over the bus, and this can be done in two steps:

- Add a counter for each incoming encrypted message for each ID and by this old sent messages will be ignored in case of replay attacks.
- Use timestamps in key generation (in case of the same timestamp on all nodes is guaranteed).

The current implementation for CANTRACK is based on the following points:

- Encryption of messages is optional, the user is allowed to select either to deal with encrypted or non-encrypted messages.
- Implementation is based on dynamic key for encrypting messages, the key is generated as function of the counter of the messages sent on the bus, and thus, messages are always unique at a time.
- Currently for just proving the Idea the dynamic key generated is XORed with the payload data of the message, more complexity could be used for encrypting messages using the generated dynamic key.

IV. Testing the Algorithm

The test methodology adopted here is based on using a third-party application "Vector CANoe" [12] which interacts with CAN bus and reads messages. Our solution CANTrack is used to send encrypted messages on the hardware connected to one CAN channel and Vector CANoe is used to receive these encrypted messages on another channel as shown in Figure 8. That is to prove that the data is continuously changing over time and the actual payload is not transparent to any intruder.

The test bench is set-up as follows:

1. Connect one channel of the CAN network to CANTrack.
2. Connect Vector Canoe to another channel.
3. Join both channels together (send from CANTrack and receive on Vector CANoe).

Several test cases have been developed to verify the functions this algorithm. The following are some samples:

1. Use Case #1: Start sending messages from channel 1 and receive them on channel 2 in CANTrack. Messages sent on channel 1 were received correctly on channel 2 and the payload data is decrypted as it should and appearing as transmitted.
2. Use Case #2: Start sending messages from channel 1 from CANTrack and receive them on channel 2 in Vector CANoe. Messages sent on channel 1 were received as random changeable data on channel 2 and the payload data is not decrypted in CANoe as shown in Figure 8.

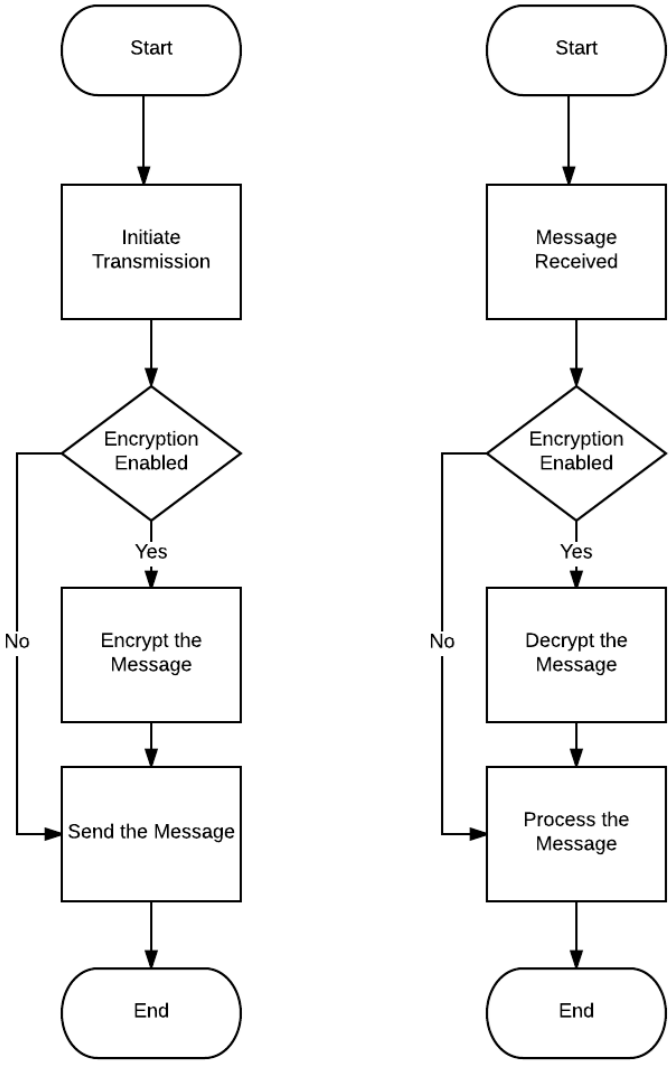

Fig. 7 CANTrack encryption flowcharts.

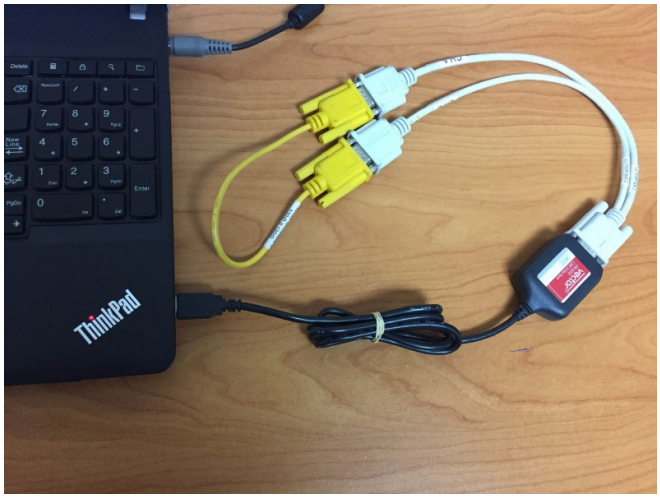

Fig. 8 Real experimental setup.

978-1-5090-5454-1/17/$31.00 ©2017 IEEE

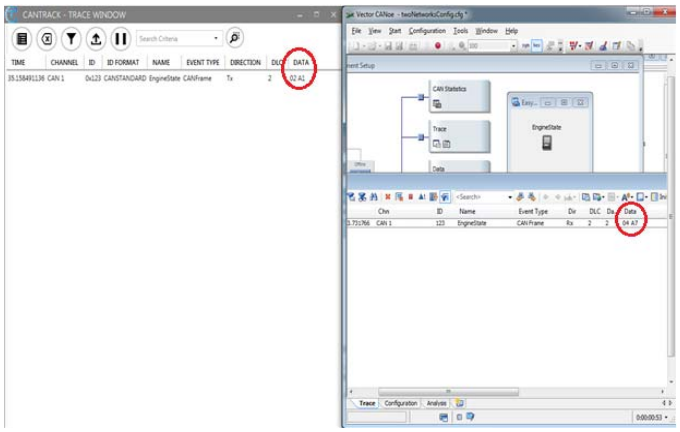

Fig. 9 CANTRACK sending encrypted message to CANoe and it couldn't be recognized.

V. Conclusion

The developed solution CANTrack is thoroughly described. CANTrack is a sophisticated CAD tool that supports the entire development process for automotive networked systems. CANTrack differentiates itself from other competitive tools; by incorporating the unique features of CAN bus security enhancement, which is implemented using an intuitive algorithm that encrypts the 8-byte payload data using a symmetric key that is being dynamically changed using synchronized key generators across all nodes. This algorithm makes the encrypted message unique at any instance of time to avoid replay attacks. The algorithm is tested thoroughly on an experimental setup using Vector Canoe; with the results of two use cases presented. The tests were done successfully and the messages became unrecognized and un-understandable to any 3rd party application or ECU and replay attacks are stopped by using changeable encryption key.

VI. Future Work

Several improvement proposals for CANTrack are taken into consideration as a future work. The following are a subset of them:-

- Adding the handshaking procedures when adding new node to the Network.
- Handling-out of Synchronized nodes.
- Increasing the complexity of the key generation function for encryption.
- Increasing the complexity of Encryption using the generated key.
- Implement the generation of key using timestamps (in case of time synchronized nodes) and compare the results with the message counters methodology.
- Using intelligent algorithms [13-16] in encoding and decoding CAN messages, as well as in key generation.

Acknowledgment

This work was supported by the Egyptian Information Technology Industry Development Agency (ITIDA), under ITAC Program CFP # 98.

References

[1] B. Groza et al, "LiBrA-CAN: a Lightweight Broadcast Authentication protocol for Controller Area Networks", Proc. 11th Inter. Conf. on Cryptology and Network Security (CANS'12), Springer-Verlag, LNCS, 2012.

[2] Mina Nagiub, Wael Farag, "Automatic selection of compiler options using genetic techniques for embedded software design", IEEE 14th Inter. Symposium on Comp. Intelligence and Informatics (CINTI), Budapest, Hungary, Nov. 19, 2013, ISBN: 978-1-4799-0194-4.

[3] K. Koscher, "Experimental security analysis of a modern automobile," in Security and Privacy (SP), 2010 IEEE Symp., Oakland, CA, USA, May 2010, pp. 447–462.

[4] S. Checkoway et al., "Comprehensive experimental analyses of automotive attack surfaces," 20th USENIX Conf. on Security, Berkeley, CA, USA, Aug 2011.

[5] K Mansour, W Farag, "AiroDiag: A Sophisticated Tool that Diagnoses and Updates Vehicles Software Over Air", 2012 IEEE Inter. Elec. Vehicle Conf. (IEVC), Greenville, SC, USA, March 2012, ISBN: 978-1-4673-1562-3.

[6] A. Perrig, R. Canetti, J. D. Tygar, and D. X. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," in IEEE Symposium on Security and Privacy, 2000, pp. 56–73.

[7] A. Perrig et al., "Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction", Network Working Group, The Internet Society (2005). Available at https://www.ietf.org/rfc/rfc4082.txt.

[8] Van Herrewege, D. Singelee, and I. Verbauwhede, "CANAuth - a simple, backward compatible broadcast authentication protocol for CAN bus", in 9-th Embedded Security in Cars Conference, 2011.

[9] A. Hazem, and H.A.H. Fahmy, "LCAP - A Lightweight CAN Authentication Protocol for Securing In-Vehicle Networks", 10th escar Embedded Security in Cars Conference, Berlin, Germany, 2012.

[10] H. Ueda, R. Kurachi, H. Takada, T. Mizutani, M. Inoue and S. Horihata, "Security Authentication System for In-Vehicle Network", SEI Technical Review, No. 81, Oct. 2015.

[11] Available at: https://en.wikipedia.org/wiki/Replay_attack.

[12] Available at: https://vector.com/vi_canoe_en.html

[13] WA Farag et al., "Genetic algorithms and back-propagation: a comparative study", IEEE Canadian Conf. on Elec. and Comp. Eng., 1998, 93-96.

[14] W Farag, "Synthesis of intelligent hybrid systems for modeling and control", University of Waterloo, 1998.

[15] WA Farag et al., "Neuro-Fuzzy Modeling of Complex Systems Using Genetic Algorithms", IEEE Inter. Conf. on Neural Networks (IEEE ICNN'97) 1, pp. 444-449.

[16] Wael A. Farag, "Digital Filters Design Using Artificial Neural Networks", 22nd Inter. Conf. on Comp. and Industrial Eng. (ICC & IE '97), pp. 68-71, Dec. 20-22, 1997, American University, Cairo, Egypt.

978-1-5090-5454-1/17/$31.00 ©2017 IEEE