**Arūnas ANDZIULIS, Mindaugas KURMIS, Jonas VAUPŠAS, Sergej JAKOVLEV, Valdemaras PAREIGIS**

Klaipeda University, Department of Informatics Engineering

# Trust based authentication scheme for latency reduction in vehicular ad-hoc networks (VANETs)

***Abstract.*** *Vehicular Ad-Hoc Networks (VANETs) are getting more and more commercial relevance, because it offers a new level of vehicle communication services. One of the main problems of the analyzed communication system is the security assurance of transmitted data because security mechanisms common in wireless LANs are not suitable for VANETs and handoff latency is crucial. In this paper, VANET authentication schemes are analyzed and a new trust based authentication scheme is proposed which significantly can reduce the handoff latency time.*

***Streszczenie.*** *Samochodowe sieci Ad-Hoc (VANETs) mają coraz większe znaczenie komercyjne, ponieważ oferują nowy poziom usług komunikacji pojazdu. Jednym z głównych problemów analizowanego systemu komunikacji jest zapewnienie bezpieczeństwa przesyłanych danych, ponieważ mechanizmy bezpieczeństwa powszechne w bezprzewodowych sieciach LAN nie nadają się do sieci typu VANET, a wartość opóźnienia ma kluczowe znaczenie. W niniejszej pracy przeanalizowano metody uwierzytelniania systemów VANET i zaproponowano nowy system bezpieczeństwa oparty na uwierzytelnianiu, co może znacznie zmniejszyć czasy opóźnień. (**Nowe systemy uwierzytelniania jako metoda redukcji opóźnień w samochodowych sieciach ad-hoc (VANET)**)*

**Keywords:** VANET, authentication, vehicular networks, handoff.
**Słowa kluczowe:** VANET, uwierzytelnianie, sieci samochodowe, opóźnienie.

## Introduction

Vehicular ad hoc networks (VANETs) with interconnected vehicles and numerous services promise superb integration of digital infrastructure into many aspects of our lives, from vehicle-to-vehicle, roadside devices, base stations, traffic lights, and so forth. A network of a huge number of mobile and high-speed vehicles through wireless communication connections has become electronically and technically feasible and been developed for extending traditional traffic controls to brand new traffic services that offer large traffic-related applications. Applications of vehicular ad hoc networks range from rapid transportation development to civil life-support operations such as electronic toll systems, vehicle-collision avoidance, and collection of traffic information, vehicle diagnostics, cooperative driving, and entertainment-related applications [1].

In a vehicular network, wireless terminals can be divided into two groups, roadside units and vehicles. Roadside units can be access points which provide wireless connections and they are usually stationary. These roadside units can also connect with each others to construct the backbone infrastructure through either wires or wireless connections. Vehicles are equipped with wireless antennas and they can communicate with other vehicles and roadside units through wireless connections. Consequently, in a vehicular network, there are two types of communications, vehicle to infrastructure (V2I) and vehicle to vehicle (V2V). Using the vehicle to infrastructure communication, vehicles can access Internet through the access points to communicate with their correspondent nodes. Conversely, using the vehicle to vehicle communication, urgent messages can be transmitted among vehicles to support intelligent transport systems. [2].

As a difference from typical MANETs (Mobile Ad hoc Net works), in the VANET the Wired Internet infrastructure is omnipresent and readily accessible via IEEE 802.11p, WiFi, DSRC, WiMAX, 3G, LTE, etc. [3].

## Related works

There are proposed some improvements to 802.11i authentication scheme for VANETs in recent years. Mishra et. al proposed, a neighbor graph structure is introduced to extract the relationship among access points. Several candidate access points are determined before the handoff occurs. In addition, a PMK tree structure is used to generate new PMKs. Using this proactive key distribution, the authentication latency is shortened by waving the communication between the authentication server and the new access point. However, similar to other schemes, this protocol introduces communication and computing overhead to candidate access points and the resource is waste for the access points which are not the new access points of the suppliant [4].

Pazzi et al. has introduced a MAC layer handoff protocol designed to reduce the handoff latency. To enable fast handoff, an advertisement message is introduced to indicate the relationship between APs which can be used to predict the next AP by mobile nodes in the neighborhood. If the candidate AP can be used as the new AP, the probe delay in handoff process can be waived and the handoff latency can be minimized. The simulation results illustrate that the proposed scheme can reduce the MAC layer handoff latency to less than 50 ms [5].

Xu et al. has done a survey of large-scale dense-AP 802.11 networks to evaluate the general performance of handoff under complicated and chaotic wireless environment. They show that collection of AP responses in large AP-dense 802.11 networks is a very time-consuming process. The unique features of AP scan in this kind of environment were exposed. It was proposed an improved AP scan, D-Scan, where eavesdropping and shortened active probing cooperate to achieve an efficient AP pre-scan which meets the requirement of 10 ms/channel. Experiments showed that D-Scan works and helps to realize a faster and smoother handoff [6].

In [2] a lightweight authentication scheme is introduced to balance the security requirements and the handoff performance for 802.11p vehicular networks. The access points are divided into different trust groups and the group session key is introduced to generate the PTK. When the vehicle switches its access point in the same group, the new PTK can be generated based on the group session key without completing the whole authentication. For intergroup handoffs, the temporal session key is adopted to enable the vehicle to resume the communication with its correspondent nodes before the complete authentication is finished, and this operation will not introduce security hazard. The simulation results demonstrate that proposed authentication scheme is suitable for 802.11p networks in terms of authentication latency, packet loss ratio and traffic overhead.

**Proposed security scheme**

In this section, our proposed trust based middleware authentication scheme for reducing handoff latency time in 802.11p based vehicular networks is analyzed. The essence of the proposed system is that authentication process is based on trust mechanism and authentication process is initiated only when connected to a new AP or vehicle.

All vehicles and access points are divided into different trust groups. Every vehicle has calculated and assigned trust value and identification number, which is exchanged with all authentication servers. In a trust group, the AP or vehicle thinks that vehicles within this trust group are trustable and it can be exchanged secret data and security related frames between nodes in a trust group. When the vehicle wants to join the new VANET, it must complete a whole authentication procedure defined in 802.11i standard and the group session key is generated for the vehicle. The vehicle and AP record the group session key [2].

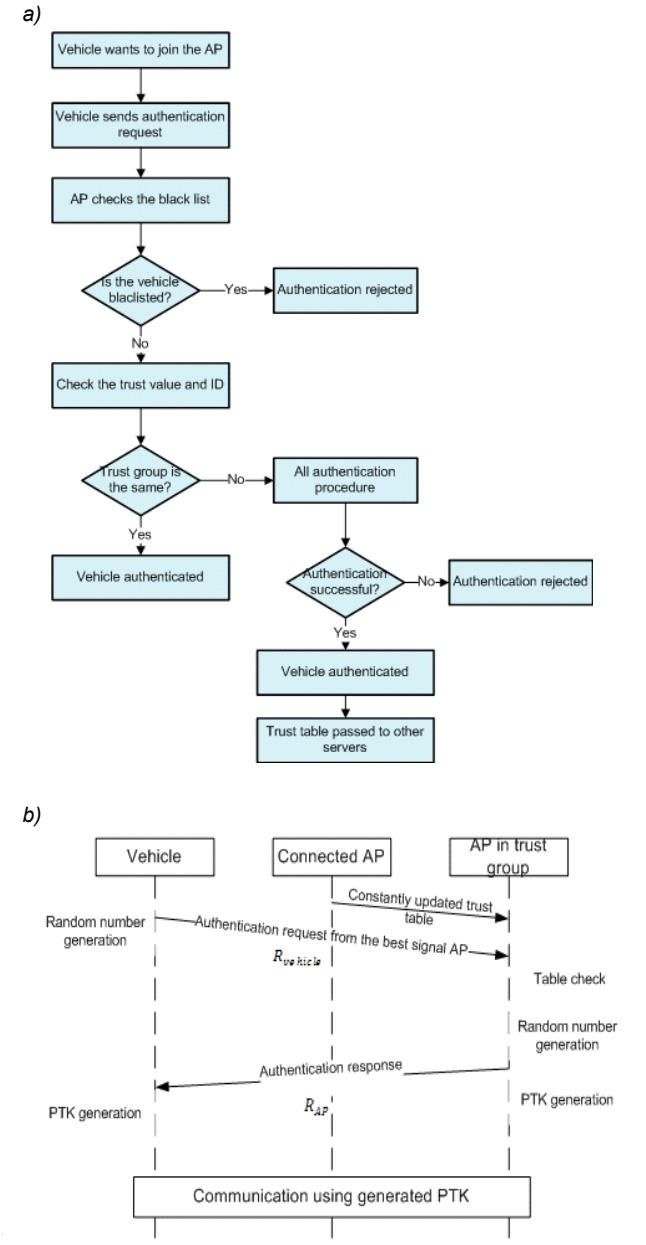


Fig.1. Vehicle authentication in the same trust group and in the other trust group algorithm *(a)* and PTK generation *(b)*

The authentication servers constantly passes thru a regularly updated table with connected nodes trust values, nodes IDs and information about successfully authenticated and blacklisted nodes. When the vehicle connects to other AP which has previous forwarded information about connecting vehicle it can use the group session key and information to generate PTK. With this scheme it is not necessary to perform all the procedure described in 802.11i standard. Using the proposed authentication scheme it is significantly reduced time needed for handoff procedure. In Fig. 2 it is showed the sample scenario for the proposed trust based authentication scheme.

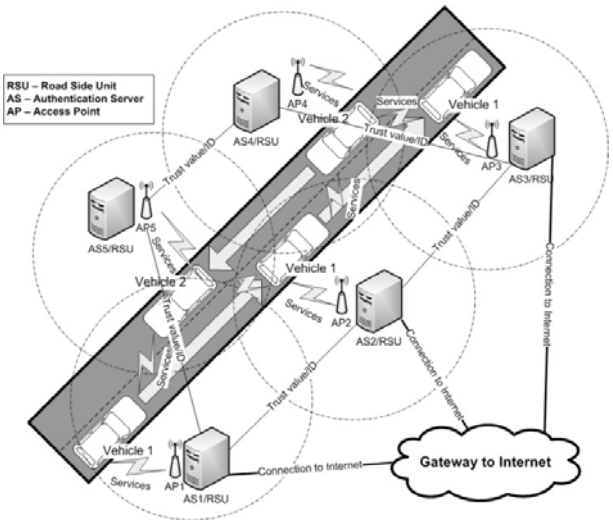


Fig.2. Sample vehicular network scenario for the proposed trust based security scheme

There are two types of authentication: authentication in the same trust group and authentication in other trust group (Fig. 1). In an IEEE 802.11i authentication process, there are three kinds of terminals participated, suppliants, authenticators and authentication servers [7]. For a vehicular network, supplicants are vehicles which are equipped with 802.11p wireless chips. These vehicles can communicate with each others directly using the ad hoc mode. Authenticators are access points which provide wireless connections for vehicles [2]. Vehicles can communicate with each others and with the APs to get different services and applications: connecting to the internet, multiplayer games, online games, security related applications, etc.

In the scenario, there are two vehicles, five access points and five authentication servers/road side units. The movement path of the vehicles is shown as the arrows. The links shows services of RSUs and vehicles. In scenario access points AP1, AP2, AP3 and Vehicle 1 are in the same trust group and the Vehicle 2, AP4 and AP5 are in the other trust group. The network nodes in the same trust groups trusting other nodes in the same group and are exchanging services and security related information messages. When the Vehicle 1 joins the vehicular network, it selects the AP with the strongest signal strength - AP1. The AP1 initiates a complete authentication procedure to generate the group session key (GSK) [2] and the PTK. If the vehicle successfully authenticates to the AP, the AS1 calculates the trust value and ID and passes the table to other authentication servers in the same trust group. When the vehicle is moving towards its destination and the signal drops below the threshold, it is probing the network and selects the other AP with the strongest signal in its trust group and then is establishing connection to it. If access AS

identifies the vehicle as trustable it authenticates it without all the procedure described in 802.11i standard. If the wireless probing shows that there are no networks in the same trust group with reasonable signal strength it selects network from other trust group with the strongest signal and the whole authentication procedure is repeated.

**Trust value calculation**

In this section it is analyzed the calculation of the trust value (TRV). The trust value in our proposed scheme plays the key role in handoff latency time reducing, because vehicles connecting to the same trust group AP or other vehicle do not have to repeat full authentication procedure and time required for authentication are significantly reduced. The trust value is a hash function and is calculated by the 1st equation:

$$T_{ID_{vehicle}} = \left(t_1\left(hash\left(R_{vehicle}\right)\right) \cap t_1\left(hash\left(R_{trustRSU}\right)\right)\right) \cap t_3\left(hash\left(PTK\left(ID_{trust}, ID_{vehicle}, GSK_{vehicle}, R_{vehicle}, R_{trustRSU}\right)\right)\right). \quad (1)$$

Here when the vehicle wants to join the *RSU* in its trust group, it generates a random number $R_{vehicle}$ and sends the authentication request packet to the *RSU*. The *RSU* first checks the trust table to find out if the vehicle is in its trust group. The *RSU* responds by sending an authentication response packet (*ASP*) with a generated random number $R_{trustAP}$. When the vehicle receives the *ARP*, both the vehicle and the *RSU* know the random generated numbers. Then both nodes can generate the *PTK* using the group session key (*GSK*), vehicle *ID*, *ID* of the *RSU* and two generated random numbers based on hash functions. The trust value plays the key role in the reduction of the handoff latency time; because vehicles that are connecting to the same trust group *RSU*s do not have to repeat the full authentication procedure. Vehicle trust based authentication (*RTV*) for *V2V* is expressed as (2):

$$T_{ID_{vehicle}} = t_1\left(RTV\left(mean\left(R_e, O_{sc}, ID_{vehicle}\right)\right)\right) \cap t_2\left(hash\left(PTK\left(ID_{trust}, ID_{vehicle}, GSK_{vehicle}\right)\right)\right). \quad (2)$$

Here $R_e$ are the used resources by the ($ID_{vehicle}$) device and $O_{sc}$ are the successfully completed services provided operations (based on history). The proposed authentication scheme can significantly reduce the time of the handoff procedure and thus be more efficient compared to general VANET authentication systems.

**Conclusions**

The essence of the proposed system is that authentication process is based on trust between vehicles and APs and full authentication process is initiated only when it is connected to a new AP or vehicle. The servers or vehicles in the same trust group treat the connected node as secure and do not repeats authentication procedure. The authentication servers passes thru a regularly updated table with connected nodes trust values and information about successfully authenticated nodes and of those who are blocked from entry to the system. Using the proposed authentication scheme it would significantly reduce the time needed for handoff procedure. In future works we are planning to perform simulations and to perform real life measurements of our proposed scheme.

*The authors would like to thank project LLII-061 "Development of Joint Research and Training Centre in High Technology Area" (Latvia-Lithuania Cross Border Cooperation Programme under European Territorial Cooperation Objective 2007-2013 Subsidy Contract Nr. LV-LT/1.1/LLII-061/2010/) for the financial support while writing and publishing the manuscript*

REFERENCES

[1] Chun-Ta L., Min-Shiang H., Yen-Ping C., A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks, *Computer Communications*, 31 (2008), 2803-2814

[2] Zhang Z., Boukerche A., Ramadan H., Design of a lightweight authentication scheme for IEEE 802.11p vehicular networks, *Ad Hoc Networks* (2010), In Press

[3] Gerla M., Kleinrock L., Vehicular networks and the future of the mobile internet, *Computer Networks*, 55 (2011), No. 2, 457-469

[4] Mishra A., Shin M.H., Petroni N.J., Proactive key distribution using neighbor graphs, *IEEE Wireless Communications*, 11 (2004), 26-36

[5] Pazzi R., Zhang Z., Boukerche A., Design and evaluation of a novel MAC layer handoff protocol for IEEE 802.11 Wireless networks, *The Journal of Systems and Software*, 83 (2010), 1364-1372

[6] Xu C., Teng J., Jia W., Design and evaluation of a novel MAC layer handoff protocol for IEEE 802.11 Wireless networks, *Computer Communications*, 33 (2010), 1795-1803

[7] IEEE Std 802.11i™-2004 IEEE, 2004

***Authors:*** *prof. dr Arunas Andziulis, Msc. Mindaugas Kurmis, assoc. prof. dr. Jonas Vaupsas, Msc. Sergej Jakovlev, Msc. Valdemaras Pareigis, Klaipeda University, 17 Bijunu Str. E-mail: arunas.iik.ku@gmail.com, mindaugask01@gmail.com, prodekanas.jtf@ku.lt, s.jakovlev.86@gmail.com, valdevaldas@gmail.com*