Impact of the Pre-authentication Performance in Vehicular Networks

Juan A. Martinez
Dept. of Information and Communications Engineering
University of Murcia
Murcia, Spain E-30100
Email: juanantonio@um.es

Pedro M. Ruiz
Dept. of Information and Communications Engineering
University of Murcia
Murcia, Spain E-30100
Email: pedrom@um.es

Rafael Marin
Dept. of Information and Communications Engineering
University of Murcia
Murcia, Spain E-30100
Email: rafa@um.es

***Abstract*—The possibility of connecting vehicles to fixed IP networks through roadside units (RSUs) or even access gateways is seen as a very interesting alternative to fully infrastructure-less VANETs. However, getting access to those fixed networks must be controlled and only authorized users should be able to use those RSUs or gateways. However, that authentication process incurs in a not-negligible delay which can result in packet losses and other issues during handoffs. In this paper we assess the performance benefit provided by pre-authentication schemes in which vehicles use the current gateway to authenticate with nearby gateways before they finally attach to them. Our simulation results show that pre-authentication offers important benefits in terms of packet delivery ratio and handoff delays both in urban and inter-urban scenarios.**

I. Introduction and Motivation

Mobile ad-hoc networks (MANETs) have been a really interesting research area during the last few years because of their wide applicability. They are able to facilitate communications in scenarios where nodes move randomly and with different speeds. To do so, a source node uses neighboring nodes as forwarding nodes to reach the destination through multihop relaying. They are particularly interesting in emergency scenarios without infrastructure support.

A new type of MANETs are vehicular ad-hoc networks (VANETs). In this case nodes are vehicles equipped with wireless devices. Car manufacturers, as well as traffic authorities, have shown their interest in these networks as an important tool for reducing road accidents, and also giving the opportunity to offer value added services for drivers and passengers.

However, VANETs have their own specific features that make them different from generic MANETs. In particular, VANETs nodes are vehicles, which means that their average speed is higher than MANET nodes. Their movement is not random because they can only move along roads and streets. Nodes have also other mobility restrictions such as intersections, traffic lights, and so on. These create groups of cars (a.k.a. platoons) in different moments which can dynamically split and merge over time. On the other hand, VANETs do not have strong energy consumptions requirements. Thus, nodes can be equipped with high performance on board units (OBUs). Moreover, they can also have different wireless devices (WIFI, WIMAX, UMTS) allowing them to connect to their neighbors as well as the infrastructure.

An isolated VANET without the support of some infrastructure is able to take on basic services: for instance, it can react to a road accident by transmitting information to the involved vehicles that travel in the direction where the accident happened. However, connecting the VANET to the infrastructure, allows us to benefit from the services and information available in existing networks. Therefore, that external connectivity opens up a lot of novel services and simplifies the implementation of the existing ones (e.g. traffic management, ...).

Nevertheless, in general, it is expected that these services will only be used by authenticated and authorized users. So, in order to provide access control to these services, AAA *(Authentication, Authorization and Accounting)* infrastructures are deployed to assist this process [1]. Integrated with AAA infrastructures, the *Extensible Authentication Protocol* EAP provides flexible authentication and key management for network access control.

The following three entities are defined in EAP: an authenticator, a peer and an EAP server. An *authenticator* is an end of a link and responsible for initiating EAP authentication. A *peer* is the other end of the link and responds to the authenticator. An *EAP server* is an entity (e.g. a AAA server) that terminates an EAP authentication method (or an *EAP method* hereafter) such as EAP-TLS [2] with the peer. The transport of EAP between the peer and the authenticator is referred to as the *EAP lower-layer*. On the contrary, typically an AAA protocol, such as RADIUS [3] or Diameter [4], is used to transport EAP between the authenticator and the EAP server. The peer and authenticator are typically implemented on a mobile node (e.g. a car) and a network point of attachment such as a gateway, respectively.

However, a typical authentication based on EAP, which is detailed below, requires multiple messages to complete and adds a significant latency to obtain network access when mobile node changes to its network connection to another gateway. Thus, if we apply this scheme to a multi-hop network we must be aware of the cost in terms of overhead and the authentication delay.

978-1-4244-3574-6/10/$25.00 ©2010 IEEE

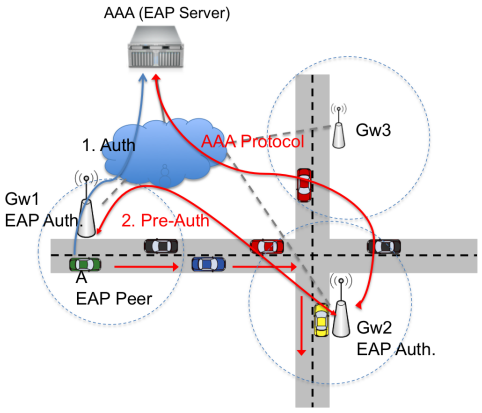

Fig. 1. Example of scenario of pre-authentication.

For the particular case of VANETs, the continuous network partitions and the high speed of the nodes causes a degeneration of the access control behavior increasing the number of messages needed to complete an authentication or restarting the whole authentication process. The high speed of the nodes also provokes that nodes are attached to gateways during a shorter period of time comparing with nodes in MANETs.

In this paper, our target is not only to analyze the impact of the authentication scheme with the infrastructure over VANETs but also the impact of an improvement to reduce the authentication latency based on a pre-authentication scheme [5] in the same type of scenario. By this pre-authentication scheme, a mobile node is able to carry out an authentication process with a close gateway *before* the attachment through the current and authenticated gateway. Thus, the node will not have to start the authentication process with this new gateway making *after* the movement, and this handover will be faster than with the traditional scheme.

Fig. 1 shows an example of the use of pre-authentication by a vehicle. The selected vehicle moves along the scenario following the path indicated by the arrows. Therefore, the vehicle is authenticating with each gateway it finds along its path in order to access the services available in the infrastructure. If the node was able to pre-authenticate with these gateways before it makes the handover we will save time and we also get as a result a better performance because the new gateway will be able to forward the traffic straight away.

The remainder of this paper is organized as follows: In section II we analyze relevant existing works. Our proposal will be explained in section III describing the pre-authentication process and their advantages. This work will be reflected in section IV where simulations and results are commented. Finally in section V we will comment the benefits obtained in this article as well as our future research directions on this topic.

II. Related work

A solution for authentication and authorization based on the deployment of PKIs (*Public Key Infrastructures*) is proposed in [6]. However, the deployment of purely-based PKIs solutions for network access control is less common than the use of AAA infrastructures. In this sense, some solutions [7], [8] provide access control and authentication in hybrid MANET by using deployed AAA infrastructures and EAP over 802.11i link-layer frames. However, a protocol which transports EAP between the mobile node and the gateway through multiple hops independently of the underlying wireless technology is more appropriate in the context of MANETs or VANETs. Examples of these protocols are IKEv2 [9] or PANA [10] since they use UDP as transport protocol, although PANA provides a lighter way of operation. In this sense [11] proposes an extension to Mobile IPv4 to allow ad-hoc nodes to connect to the Internet. However this scheme is well-known to have performance limitations and the authentication mechanism is specifically designed for Mobile IPv4. Also, solution [12] designs a new public-key based protocol to provide an efficient and fast authentication process between the mobile node and the gateway, contacting the AAA server after the successful authentication. However, the solution assumes a complete change in the current AAA model and the standards defined for traditional network access control. In this sense, the pre-authentication scheme that we study in this paper follows the standard model for network access control based on EAP defined in [13].

Nevertheless, an authentication based on EAP may require of the exchange of several messages as well as a certain time to process and complete the exchange the keys between the client and the server. The total time spent in completing an authentication can vary from several milliseconds to seconds [14].

In a VANET this problem is becoming important due to the innate properties of the mobile networks like the network mobility or the link breaks that can cause a longer delay in the delivery of the data increasing the time necessary to complete an authentication process. Along the path covered by a vehicle this authentication process can be repeated several times with different gateways, so a lot of link losses will happen deteriorating the performance of the authentication process. This is the reason why is interesting to reduce the time spent by a node to be connected and authenticated with a gateway.

Authors in [15], have contributed solutions to the authentication process in MANETs making it more efficient by the use of a media-independent pre-authentication scheme [16]. The proposal presented in these articles consists in an utility based control scheme employed to perform efficiently the pre-authentication process.

Every node willing to connect to the infrastructure network will execute this scheme periodically to select the most promising gateways to pre-authenticate with. Therefore, the pre-authentication will not be done with all the gateways that the node finds along its path but just with the better candidates.

The key aspect of this scheme is the way to make the prediction to know which gateway is a good candidate to pre-authenticate with. This prediction will be carried out by taking into account the positions of the closer gateways in

the current evaluation instant and in the previous evaluation instant. Thus, with this information, a new position of the gateway is estimated for the next evaluation instant.

III. Pre-authentication in VANETs

Without loss of generality and for the purpose of our analysis, we have considered the use of EAP-TLS since it is one of the most common EAP methods nowadays. Moreover, in order to transport EAP between the mobile node (EAP peer) and the gateway (EAP authenticator) we have considered PANA as an EAP lower-layer which is able to operate in multi-hop networks. Finally, Diameter (commonly used in 3G networks) have been considered to deliver these EAP messages from the gateway to the AAA server.

After a first discovery stage to know the PANA agent (PAA)'s IP address (which acts as EAP authenticator and is located in the gateway), the EAP Peer exchanges several EAP messages of the specific EAP-method with the AAA/EAP server through the PAA, obtaining as a result from the EAP authentication process. Once this stage successfully ends, the AAA will send a Master Session Key (MSK) to the PAA. This MSK will be also derived by the own EAP Peer so both PAA and the Peer will be able to generate new session keys to establish a security association between them. This way, like both entities have common shared keys, they gateway will easily check whether the traffic sent by a mobile node is authorized or not. The whole process to authenticate a mobile node could last several seconds in some cases.

As commented above, the authentication process requires of the awareness of the location of the gateways which will act as PAA, as well as their IP addresses in order to start the authentication process with them. Using a gateway discovery protocol, a node will be able to select the gateway to authenticate with depending on its location. Going a step further, a mobile node can gather information about several gateways and bring forward an authentication with a near gateway because it is more likely to authenticate with it in a close future. Thus, when the mobile node is attaching to this new gateway it will save time when obtaining network access in the handover between gateways.

From the point of view of the protocol, the pre-authentication process is quite similar to the authentication process explained before, however the pre-authentication process will be sent by the mobile node through an authenticated gateway with the purpose of establish a new authentication with a new gateway because there exists a high probability to attach to it in a close future.

The use of the pre-authentication scheme has been studied under a MANET environment obtaining successful results enhancing the current authentication scheme performance [15]. However, VANETs have different characteristics which make them compared to MANETs: Nodes in a VANET cannot move freely due to the restriction of the roads. Network partitions also occur very often due to the traffic signs. Finally, their speed is higher than nodes of a MANET because in VANETs, nodes represents cars traveling along the roads.

However, the behavior of the authentication process will be affected by these specific conditions making more difficult to establish and maintain an authentication with a gateway. The intermittent connectivity with other nodes will also cause that these authentication associations will be lost quite often, restarting the authentication process to attach again the node to the gateway.

For this reason, our proposal introduces a cache of authenticated or pre-authenticated gateways for every mobile node. Thus, although the links between nodes are lost, the authentication state shared by both the node and the gateways will be saved for a period of time.

In the mobile node side, however, this cache will be used by the pre-authentication scheme to store the more promising gateways to pre-authenticate with. Therefore, a mobile node will evaluate periodically the announces of the nearer gateways. It will gather information about the gateways positions and will be able to calculate the distance to each gateway and from all the announces received, it will select just the more promising ones and once the pre-authentication is completed will be introduced in the cache.

Our point in this paper is to analyze the impact of this pre-authentication scheme in the VANET environment obtaining information about metrics like the packet delivery ratio, control overhead, average delay of the packets.

IV. Simulations and results

We have carried out simulations using the version 2.33 of the NS-2 network simulator [17] and the authentication process have been simulated according to data sizes and processing times obtained from an estimation of EAP-TLS-over-PANA authentication flow messages [15].

We have represented two kind of scenarios that fits to the different environment where a car could move along. On the one hand, an inter-urban scenario represented by a highway of 4 km where the car travels at a high speed and, on the other hand, a grid of 1 km x 1 km representing the movement of the vehicles in a urban scenario.

In both scenarios we have some common simulations parameters: The simulations have been defined varying the number of sources (5, 10 and 15), transmitting the information with a rate of 512kbps and in both cases the cover range of the nodes has been fixed at 250m. As commented above a cache has been also defined in order to store the authenticated and/or pre-authenticated gateways with a size of two entries.

Due to the necessity of receiving gateways advertisements the pre-authentication scheme has been integrated in the simulator with a gateway discovery algorithm and a vehicular routing protocol defined within the MARTA project[1].

Regarding the performance metrics. We have considered that the most representative ones are, the packet delivery ratio, average delay of the data and the control overhead of the authentication process in order to take an impression of the

[1]MARTA. Movilidad y Automocion con Redes de Transporte Avanzadas. http://www.cenitmarta.org/lotus/quickr/marta

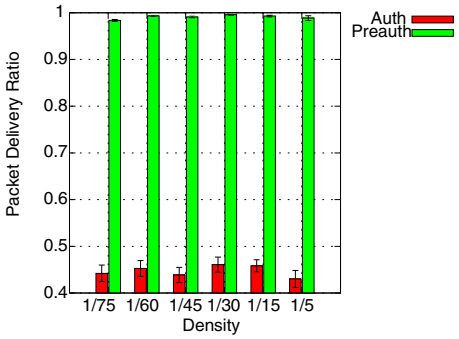

Fig. 2. Packet Delivery Ratio for the inter-urban scenario

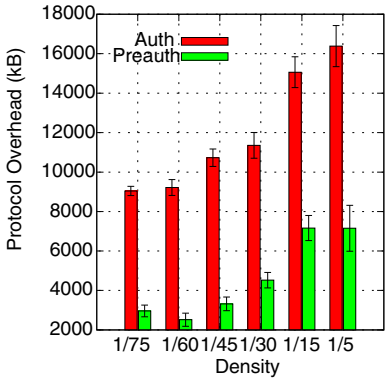

Fig. 3. Control overhead introduced by both authentication schemes in the inter-urban scenario

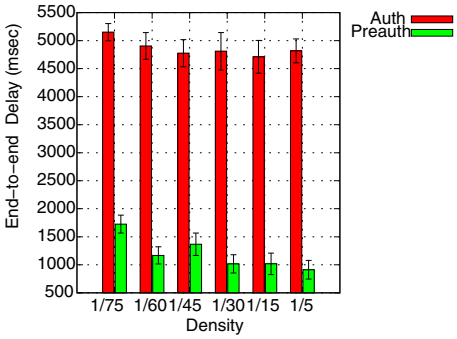

Fig. 4. Average delay of the messages in the inter-urban scenario

impact of the authentication and pre-authentication process in the VANET.

A. *Inter-urban scenario*

For this scenario we have simulated a 4019m x 20m highway with different traffic densities: 1/75, 1/60, 1/45, 1/30, 1/15 and 1/5 veh/s. Along the highway 5 gateways have been located in the following positions: gateway 1 (414.6, 30), gateway 2 (1243.8, 30), gateway 3 (2073, 30), gateway 4 (2902.2, 30) y gateway 5 (3131.4, 30) covering the whole highway. The maximum speed selected for the vehicles traveling along the highway is 33m/s.

Taking a look at figure 2 we can see that the algorithm has a good performance with a packet delivery ratio (PDR) of about 98%. Looking at this graph, we can deduce that the hit rate of the pre-authenticated gateways is really high. Letting mobile nodes to carry out fasts hand-overs between gateways without wasting time performing authentication processes and therefore the gateway will not discard packets sent by mobile nodes increasing the PDR compared with the traditional scheme.

Figure 3 shows the control overhead of both authentication processes. In the moment that the node starts receiving the announces of the gateway is when the node is farther from it. So in the traditional scheme, is in this moment when the authentication process starts increasing the possibility of losing packets due to the far distance. However, under the pre-authentication scheme the process does not happens this way. The mobile node is getting closer to its current and authenticated gateway so, when the node starts the pre-authentication the distance to its current gateway is really short, reducing the overhead because the packets sent will follow the path from the node to the authenticated gateway. The graph also shows that the overhead introduced by the pre-authentication scheme despite the fact that mobile nodes carry out authentication and pre-authentication sessions is lower than the traditional scheme.

In figure 4 we can see the average delay of both authentication schemes. The better performance of the pre-authentication scheme reflects the utility of this scheme. A mobile node, along the way to its destination, will make a handover as soon as it detects that there is a better gateway with respect to its position.As commented above, in the traditional scheme, this will be the moment where the authentication process would start. Nevertheless, when the authentication process is completed the mobile node has wasted a period of time getting closer to the gateway without sending data to it. On the other hand, applying the pre-authentication scheme the node will send the information to the gateway as soon as it detects that its the closer one reducing the average delay of the data.

B. *Urban scenario*

For this scenario, a grid of 1049m x 1049m with three roads horizontally and three vertically and four gateways have been placed in the following positions: gateway 1 (11, 505); gateway 2 (505, 11); gateway 3 (1045, 505); gateway 4 (505, 1045) with a cover range of 250m. Regarding the density we have tested this scenario with 1/30, 1/25, 1/20, 1/15 and 1/10 veh/s. Vehicles in this scenario will travel at lower speeds than in a highway, about 16m/s.

Looking at figure 5 we can see the packet delivery ratio for this scenario. Unlike the previous one, despite the fact that these results are also better than the traditional scheme, they are not as good as in the previous scenario. The difference between both scenario is the possibility to choose among several promising gateways. Whereas in the highway it is clear that there is only one gateway better than the rest this does not happen in the grid scenario. So the pre-authentication cache hit rate could fail provoking a new authentication process and therefore decreasing the packet delivery ratio.

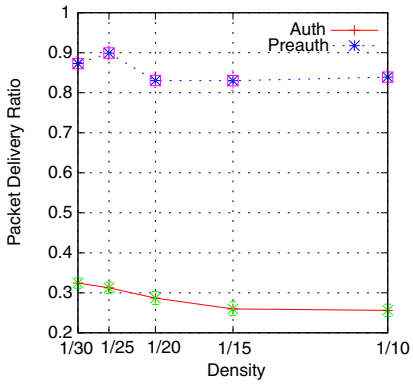

Fig. 5. Packet delivery ratio for the urban scenario

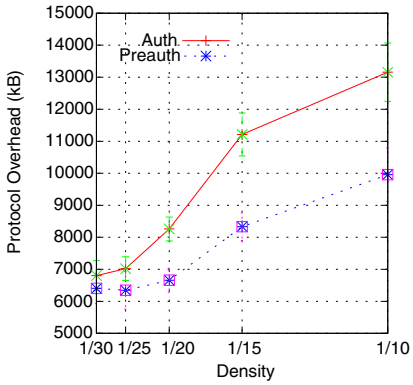

Fig. 6. Control overhead introduced by both authentication schemes in the urban scenario

Figure 6 shows control overhead of the authentication schemes. As in the previous graph, this is also affected by the same reason, due to the simplicity of the pre-authentication scheme the possibility to not being success in selecting a promising gateway affects to this overhead increasing it. The average delay also reflects this behavior as you can see in figure 7 if we compare it with the results obtained in the highway scenario.

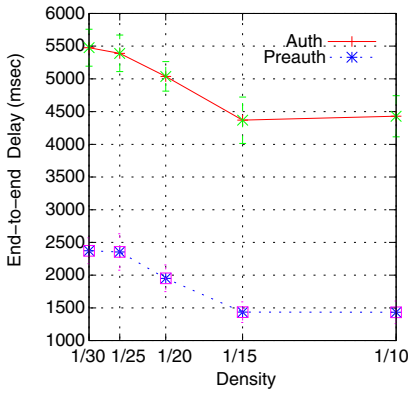

Fig. 7. Control overhead introduced by both authentication schemes in the urban scenario

V. Conclusions

From the aforementioned results, we can see that the pre-authentication scheme is a good way to improve the authentication and access control in VANETs because it improves the performance of the traditional scheme increasing the packet delivery ratio and reducing the delay of the messages. Besides, the overhead introduced by this scheme does not impair the overhead of the traditional scheme so it corroborates the performance of the pre-authentication scheme in these mobile networks. However, in light of these results, a better performance will be obtained if a more intelligent mechanism of selecting the more promising gateways is developed. Therefore, a next step for this research could be to define this method to select the promising gateways.

Acknowledgment

This work has been funded in the framework of a collaboration with Telefónica I+D through the MARTA research project (CENIT-2007-2008).

References

[1] E. Coronado, S.Cherkaoui, An AAA Study for Service Provisioning in Vehicular Networks In Proc. of lcn, pp.669-676, 32nd IEEE Conference on Local Computer Networks (LCN 2007), 2007
[2] B. Aboba, D. Simon and R. Hurst. The EAP-TLS authentication protocol. RFC 5216, March 2008.
[3] C. Rigney, S. Willens, A. Rubens, and W. Simpson (2000). *Remote Authentication Dial In User Service (RADIUS)*. RFC 2865.
[4] P. Calhoun and J. Loughney (2003). *Diameter Base Protocol*. RFC 3588.
[5] Y. Ohba (ed). Extensible Authentication Protocol (EAP) Early Authentication Problem Statement. draftietf-hokey-preauth-ps-12 IETF Internet Draft, Jan. 2010. Work in Progress.
[6] V. Casola, J. Luna, A. Mazzeo, M. Medina, M. Rak and J. Serna. An interoperability system for authentication and authorisation in VANETs International Journal of Autonomous and Adaptive Communications Systems 2010 - Vol. 3, No.2 pp. 115 - 135
[7] A. Hafslund and J. Andersson. 2-Level Authentication Mechanism in a Internet connected MANET. 6th Scandinavian Workshop on Wireless Ad-hoc Networks, May 3-4, 2005, Johannesberg Estate, Stockholm.
[8] H. Moustafa and G. Bourdon and Y. Gourhant An AAA Study for Service Provisioning in Vehicular Networks. In Proc. of the 2nd ACM international workshop on Vehicular ad hoc networks, 2005, Cologne, Germany
[9] Open IKEv2. http://openikev2.sourceforge.net/.
[10] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, and A. Yegin.
[11] U. Jnsson, F. Alriksson, T. Larsson, P. Johansson and GQ. Maguire. MIPMANET-mobile IP for mobile ad hoc networks. International Symposium on Mobile Ad Hoc Networking and Computing, August 2000; 75?85.
[12] J. Choi, S. Jung, Y. Kim and M. Yoo. A Fast and Efficient Handover Authentication Achieving Conditional Privacy in V2I Networks Lecture Notes in Computer Science (LNCS) Vol. 5764/2009, pp. 291-300, 2009.
[13] B. Aboba, D.Simon, and P. Eronen. Extensible Authentication Protocol (EAP) Key Management Framework. RFC 5247, Aug. 2008.
[14] M Georgiades, N. Akhtar, C. Politis and R. Tafazolli. AAA Context Transfer for Seamles and Secure Multimedia Services. 5th European Wireless Conference (EW'04), February 2004, Barcelona, Spain.
[15] Pedro M. Ruiz, Rafa Marin, Francisco J. Ros and Juan A. Martnez. Enhanced Access Control in Hybrid MANETs Through Utility-Based Pre-Authentication Control. Wireless Communications and Mobile Computing, John Wiley & Sons, December 2008.
[16] A. Dutta, D. Famolari, S. Das, Y. Ohba, V. Fajardo, K. Taniuchi, R. Lopez, and H. Schulzrinne (2008). *Media-Independent Pre-Authentication Supporting Secure Interdomain Handover Optimization. IEEE Wireless Communications, 15(2), 55–64*. Protocol for Carrying Authentication for Network Access (PANA). RFC 5191, May 2008.
[17] The Network Simulator - ns-2. http://www.isi.edu/nsnam/ns.