Multi-factor Authentication: A Survey and Challenges in V2X Applications

Aleksandr Ometov and Sergey Bezzateev

***Abstract*—Today, the digitalization strides tremendously on all the sides of the modern society. One of the enablers to keep this process secure is the authentication. It touches many different areas of the connected world including payments, communications, and access right management. This manuscript attempts to shed the light on the authentication systems' evolution towards Multi-factor Authentication (MFA) from Single-factor Authentication (SFA) and through Two-factor Authentication (2FA). Particularly, MFA is expected to be utilized for the user and vehicle-to-everything (V2X) interaction which is selected as descriptive scenario. The manuscript is focused on already available and potentially integrated sensors (factor providers) to authenticate the occupant from inside the vehicle. The survey on existing vehicular systems suitable for MFA is given. Finally, the MFA system based on *reversed* Lagrange polynomial, utilized in Shamir's Secret Sharing (SSS), was proposed to enable flexible in-car authentication. The solution was further extended covering the cases of authenticating the user even if some of the factors are mismatched or absent. The framework allows to qualify the missing factor and authenticate the user without providing the sensitive biometric data to the verification entity. The proposed is finally compared to conventional SSS.**

I. Introduction and Background

The continuous growth of the smart devices number and related connectivity load has made it possible to avail services offered anywhere in the world [1]. In such a supercharged world, the thing keeping the transmitted data secure is, in the first place, *authentication* [2].

Authentication is a fundamental safeguard against the illegitimate access to the device or any other sensitive application being them offline or online [3], [4]. Back in time, the transactions were authenticated mostly by physical presence, i.e., for example, the wax seal [5]. Closer to our days and with the civilization advancement, it was realized that validation based on the sender identification only is not always enough in scale of the world[1].

Originally, just one *factor* was utilized to authenticate the transmitting entity. By that time, Single-factor Authentication (SFA) was mostly adopted by the community due to its simplicity and user friendliness [6], [7]. As an example, the use of a password to confirm ownership of a user ID could be considered. Evidently, this is the weakest level of authentication [8], [9]. By sharing the password, one can compromise the user account, i.e. unauthorized user can also attempt an access by utilizing the dictionary attack [10] or rainbow table [11]. Commonly, the minimum password complexity requirement is to be considered while utilizing this type of authentication[2].

Next, it was realized that authentication with just a single factor is not reliable to provide adequate protection due to the number of recent security threads [12]. As an intuitive step, Two-factor Authentication (2FA) [13], [14], [15] was proposed coupling the representative data (username/password combination) with the factor of personal ownership, such as a mobile phone [16]. Generally, the authentication evolution is shown in Fig. 1.

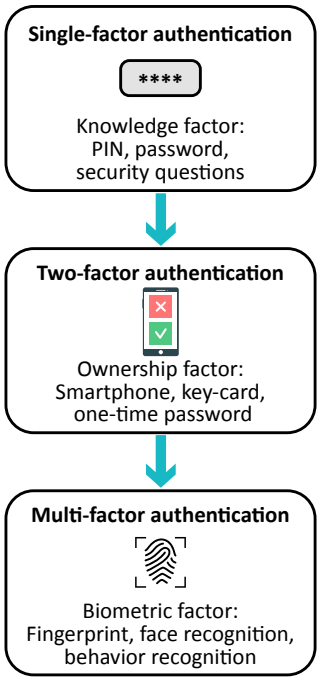

Fig. 1. Authentication methods evolution from SFA to MFA.

Almost immediately, Multi-factor Authentication (MFA) was proposed providing higher level of safety to facilitate continuous protection of computing devices and other critical

A. Ometov is with Tampere University of Technology, Tampere, Finland and (also) with Peoples' Friendship University of Russia (RUDN University), Moscow, Russian Federation.

S. Bezzateev is with Saint Petersburg University of Aerospace Instrumentation, St. Petersburg, Russia.

Correspondence email: aleksandr.ometov@tut.fi

[1]"MFA (Multi-factor Authentication) With Biometrics", 2017: https://www.bayometric.com/mfa-multi-factor-authentication-biometrics/

[2]"Your Password is Too Damn Short", 2015: https://blog.codinghorror.com/your-password-is-too-damn-short/

online services from unauthorized access [17], [18]. This offered an elevated level of security as user was required to present the evidence of the identity itself, which belong to two or more different factors [19].

MFA is supposed to be utilized in cases where safety requirements are higher than usual. For example, consider the daily use case of the ATM cash withdrawal. Here, the user has to provide a physical token (a card) representing an ownership factor, and accomplish it with a PIN code representing knowledge factor to be able to access his account and withdraw money. This system could be easily made more complex by adding the second channel like, for example, one-time password to be entered after the card and password are present [20]. Giving more interesting scenario, it could be done with, for example, facial recognition method [21]. Recent survey found that 30 percent of enterprises plan to implement an MFA solution in 2017, with 51 percent claiming they already utilize MFA, and 38 percent saying they use it in "some areas" of operation[3].

Based on the statistics[4], vehicle is stolen every 45 seconds in U.S. Current authentication method that allows to start and use the vehicle is immobilizer key, the MFA is the next big step towards secure ownership of the electronic devices [22]. When people talk about connected vehicular world or vehicle-to-everything (V2X) paradigm, authentication becomes a critical factor while checking the identity of the user and the car (or its connectivity system) [23], [24]; of the infrastructure [25]; and of the devices that might be interconnected with a vehicle, such as the smartphone, tablet, wearable device, or any other digital token (key dongle)[5]. Presently, the main challenge here is absence of the correlation between the identity of the driver and the identities of the smart sensors within the car [26]. In terms of security, this relationship must be established so that only the vehicles legal operator – whose identity is authenticated in advance – can control the various on-board connected devices, including the vehicle itself [27], [28].

At the same time, the authentication process of the ideal connected car in V2X should be as user-friendly as possible:

- Customers first register and authenticate at the service provider to activate and manage services they want to access in rented/owned car;
- Once next to the vehicle, user is required to pass a simple SFA with the fingerprint/token signed by the service provider;
- Once in the car, customer authenticates himself by logging into the car using the same username and password they set up for the customer portal (or social login);
- For additional security, the management platform could enable secondary authentication factors. Once the user has successfully passed all the tests, the vehicles device automatically authenticates to the services platform;
- The secondary authentication happens automatically based on the biometric MFA, so the user would be requested to enter an additional code or provide a token password only in case the MFA fails.

Biometrics indeed contribute to MFA scheme and can vastly improve identity proofing by pairing the knowledge factor with personal appearance factor [29], [30], [31], thus, making it much more difficult for a criminal to eavesdrop into system pretending to be another person. However, the utilization of biological factors has own issues mainly related to the ease of use [32].

From the user experience perspective, a fingerprint scanner provides the easiest user interface. This is mainly due to its wide adoption by smartphone vendors on the market [33]. On the other hand, it is not generally recommended to be utilized as a stand alone authentication method [34]. However, the use of any biometrics often requires a set separate sensing devices. The utilization of already integrated ones allows to reduce the authentication system deployment costs. The other issue is related to concerns around false negatives, or the biometric actually failing to authenticate the correct individual. In this case, the MFA should promptly react to this failure.

In our V2X scenario, the user would have a username/password/PIN/token [35], [36] and would then be asked to use a biometric, such as facial recognition or fingerprint, as it would be discussed later in this manuscript. If the authentication fails to establish trust using this combination of form factors, then the user could be asked to authenticate utilizing another previously registered form factor or a set of those. The MFA system can not only verify the accuracy of the user input, but also determine how user interacts with the devices, i.e. analyze the *behavior* [37], [38]. Basically, the more user interacts with the biometric system, the more accurate it operation becomes.

Finally, it is worth noting that another issue is the actual sensors usability [39], [40]. If a device (say a fingerprint reader) is being utilized and that device is not available from where the user is attempting to log in or gain access – the user experience is less than ideal. Having a dual-purpose device – smartphone or smartwatch (suitable for the information security primitives execution [41]), which the user already has in his or her possession – as an additional MFA factor not only as token makes the costs and usability much more reasonable for wider use in the future[6].

The rest of the manuscript is organized as following. In Section II the main MFA-suitable devices for car interface already integrated and meeting the market soon are described in context of V2X. Next, the developed MFA system is proposed Section III giving the preliminary overview on the previously used secret sharing solutions and improvements. Section IV

[3]"The Move to Multifactor Authentication: Are Passwords Past Their Prime?", 2016: https://securityintelligence.com/news/the-move-to-multifactor-authentication-are-passwords-past-their-prime/

[4]"Learn How To Protect Your Car", NHTSA, 2015: https://www.nhtsa.gov/vehicle-theft-prevention

[5]"Connected car security: why identity should be in the driving seat", 2016: http://www.information-age.com/connected-car-security-why-identity-should-be-driving-seat-123461078/

[6]"Making the case for the use of biometrics in multi-factor authentication", 2016: https://www.scmagazineuk.com/making-the-case-for-the-use-of-biometrics-in-multi-factor-authentication/article/545395/

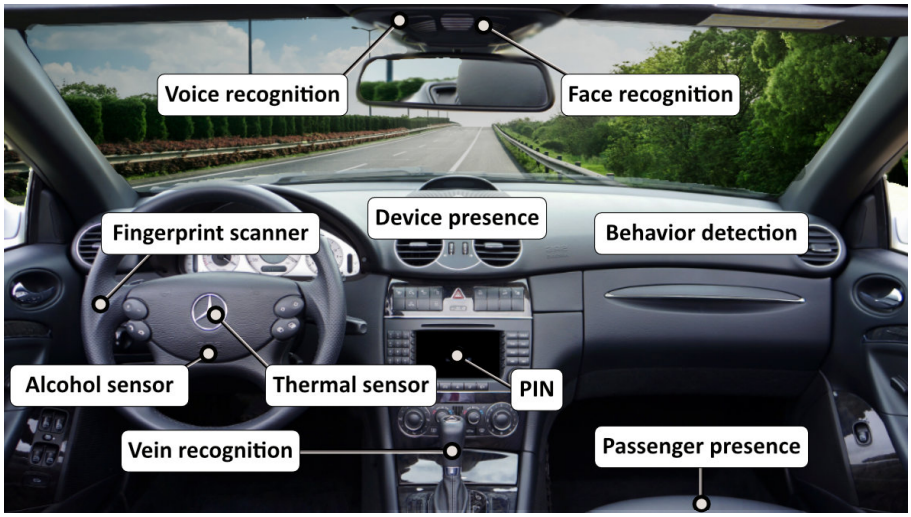

Fig. 2. Current and potential MFA sensors for vehicles.

provides brief security analysis and proofs of for the MFA framework. The last section concludes the manuscript.

II. MFA FOR VEHICLES

Today, vehicles are already equipped with a number of sensors providing an opportunity to identify the person inside. In this section, we elaborate on the market available sensors installed by the car manufacturers and provide some details on potentially used ones in the nearest V2X future. The general overview supported by the oncoming discussion is given in Fig. 2.

A. Currently deployed MFA solutions

In the connected car ecosystem, identification and authentication for vehicle security is one of the primary use cases for biometric technology in addition to the conventional sensors. Due to the market race, manufacturing luxury series of cars requires an integration of the smart services. We further list the sensors already deployed in most of the cars:

1) Token presence: Conventionally, the vehicle is protected by physical token, a key, which is required to initially access the car.
2) Password protection: The next intuitive way to authenticate the owner is to enter the PIN code or sequence of buttons clicks [42].
3) Face recognition: Modern cars are equipped with Camera Vehicle Surveillance Monitoring systems both facing the inside and the outside of vehicle [43]. The cabin facing one could be utilized for facial recognition purposes.
4) Voice recognition: The availability of the microphone allows to utilize voice recognition [44].
5) Occupant Classification Systems (OCS): A system of sensors that detect who is currently in the passenger/driver seat based on, for example, weight or posture [45], [46], [47].
6) Presence of specific non-vendor provided token [48]: smartphone, -watch, -wear, etc.
7) Alcohol sensor: The engine start function could be blocked in case the level of alcohol in the cabin is above the country-wise legal limit [49].
8) Location: Utilizing the device and user GPS coordinate to validate if the access to the device could be granted within given area [50].

B. Future of MFA for V2X

An acceleration of adoption across many industries and the increasing availability of biometric services in a wide range of readily-available consumer technology is pushing idea of wide MFA integration even more. Currently, the researchers and early technology adopters attempt to integrate new sensors to be used with MFA in vehicles:

1) Fingerprint scanner: Adding such a device to the door handle (or driving wheel) would allow user-friendly initial authentication [51].
2) Vein recognition: Integration of the vein recognizing sensor into the gearbox handle [52].
3) Thermal sensor: Fingerprint of the heat from our body is unique as well [53].
4) Behavior detection: The system allows to monitor the driver-specific features [54], [55], [56]. It could be analyzed from two perspectives. (i) Vehicle resulting behavior: steering angle sensor, speed sensor, brake pressure sensor, etc., or (ii) human factors: music played, calls made, presence of people in the car, etc.
5) Beam-forming techniques: would allow to precisely track the hand-held devices inside the car [57], [58].
6) Electrocardiographic (ECG) signal recognition: ECG data could be collected from natural driver's hand resting locations in the vehicle – the steering wheel or the gear handle [59].

Based on the above, allowing the MFA in vehicles is a promising direction even while utilizing the sensors already available on current vehicles. However, a lot of issues are still

to be addressed while integrating the MFA for vehicles. In the next section, we propose an authentication platform enabling the threshold MFA framework that is operating even in cases if some of the factors are not present or mismatched.

III. Authentication System Model

Presence of such high number of the sensor data brings us to the point of intuitive step towards it's application in MFA. We further elaborate on potential utilization of the corresponding factors to authenticate the user without providing the "verificator" with actual biometric data except for the real-time collected one.

A. Conventional approach

One of the approaches to be applied within the scope of this work is secret sharing based on Lagrange polynomial in Shamir's Secret Sharing (SSS) scheme [60]. The system secret S is usually split and distributed along the set of key holders and could be recovered later on, likewise in [61], [62] or numerous other works, as

$$\begin{aligned} f(x) &= S + a_1 x + a_2 x^2 + \cdots + a_{l-1} x^{l-1}, \\ f(0) &= S, \end{aligned} \tag{1}$$

where a_i is the generated polynomial indexes and x is a unique identification factor F_i. In such systems every key holder with factor ID obtain it's own unique key share S_{ID}

$$S_{ID} = f(ID).$$

In conventional systems it is required to collect any l shares $\{S_{ID_1}, S_{ID_2}, \ldots, S_{ID_l}\}$ of the initial secret to recover the system one while the curve may describe $n > l$ points, as it is shown in Fig. 3. The basic idea behind the approach is to specify the secret S and to use the generated curve based on random coefficients a_i to produce secret shares S_i. This methodology is successfully utilized in many secret sharing systems by means of Lagrange interpolation formula.

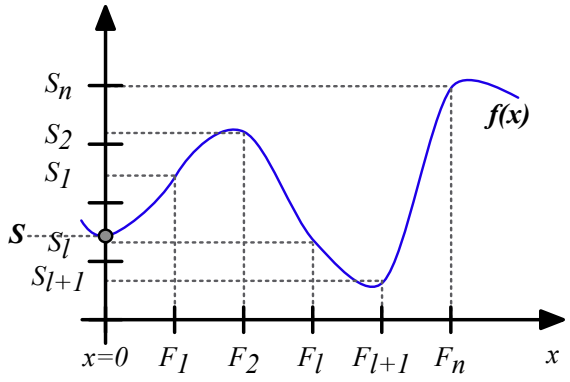

Fig. 3. Lagrange secret charing schema.

Unfortunately, this approach could not be applied for the MFA scenario since the biometric parameters are already in place, i.e. we neither can assign new S_i to a user nor to modify them. On one hand, user may set some of the factors himself, such as passwords, PIN-code, etc., on the other hand, some may be unchangeable (biometric parameters and behaviors attributes). In this case, the inverse task where the shares of the secret S_{ID_i} are known as factor values S_i is to be solved. Basically, S_i are fixed and become unique $\{S_1, S_2, \ldots, S_l\}$ set for a user. In this case, the system secret S is a secret for system access and should be obtained with the user factor values. Possible solution based on *reversed* Lagrange interpolation formula is proposed in the following subsection.

B. Proposed reversed methodology

In this manuscript, we consider MFA system with explicitly l factors F. Each factor F_i has unique secret S_i obtained with the corresponding procedure (PIN, fingerprint, etc.) from the user. In the worst case it is related to biological data, i.e. the probability of change over time is low. The corresponding factors and secrets could be then represented as

$$\begin{aligned} &F_1 : S_1, \\ &F_2 : S_2, \\ &\ldots \\ &F_l : S_L, \end{aligned} \tag{2}$$

where S_i is the secret value obtained from the sensor (factor) and l is a number of factors required to reconstruct the secret. Important to note, that providing the actual secrets to the verificator is not an option especially in case of sensitive biometric data due to the fact that our fingerprint is basically unchangeable factor, e.g. letting even a trusted instance obtain the corresponding data is a questionable step to make. Controversially to the method from subsection III-A, *the modified algorithm implies that S_i are obtained from our factors, i.e. the only one and only one polynomial describes the corresponding curve*, as it is shown in Fig. 4. In other words, the proposed methodology produces the system secret S based on the collected factor values S_i instead of assigning them in the first place.

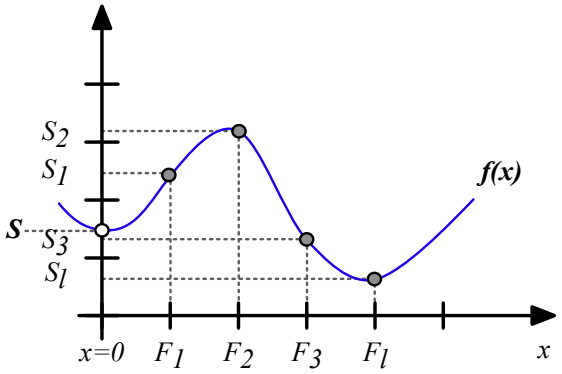

Fig. 4. Reversed method based on Lagrange polynomial.

A system of equations associated by Lagrange interpolation formula with the factors, their values and secret for system access is

$$\begin{cases} S_1 = S + a_1 F_1 + a_2 F_1^2 + \cdots + a_{l-1} F_1^{l-1} = f(F_1) \\ S_2 = S + a_1 F_2 + a_2 F_2^2 + \cdots + a_{l-1} F_2^{l-1} = f(F_2) \\ \cdots \\ S_l = S + a_1 F_l + a_2 F_l^2 + \cdots + a_{l-1} F_l^{l-1} = f(F_l) \end{cases}, \tag{3}$$

where $f(x) = S + a_1 x + a_2 x^2 + \cdots + a_{l-1} x^{l-1}$ and $f(0) = S$. The system of equations (3) has just one solution for S and it well-known from the Lagrange interpolation formula.

Lemma 1: One and only one polynomial curve $f(x)$ of degree $l-1$ could be described by l points on the plane $(x_1, y_1), (x_2, y_2), \ldots, (x_l, y_l)$

$$f_x = a_0 + a_1 x + \ldots + a_{l-1} x^{l-1}, \{f(x_i) = y_i\}_{i=1}^{l}.$$

Hence, the system secret S could be recovered based on l collected shares by ordinary Lagrange interpolation formula without the need to transfer the *original* factor secrets S_i to the verificator, i.e. the sensitive person-related data is kept private, as

$$S = (-1)^{l-1} \sum_{i=1}^{l} S_i \prod_{j=1, j \neq i}^{l} \frac{F_j}{F_i - F_j}. \tag{4}$$

C. Improvement considering possible factors' static behavior

The main drawback of the proposed solution in lack of continuous randomness in the factor shares due to the issue with our biometric data being preliminary unchanged over lifespan. The developed algorithm could be improved by simply adding one more factor F_{l+1} of a timestamp T as

$$\begin{aligned} &F_1 : S_1, \\ &F_2 : S_2, \\ &\cdots \\ &F_l : S_L, \\ &F_{l+1} : T. \end{aligned} \tag{5}$$

The ordinary approach of the hashing function with arguments as value of its factor F_{l+1} and collected system access secret could be utilized for additional randomization purpose. Instead, we continue to use here Lagrange interpolation to keep this system more natural. Then, the system of equations is updated accordingly

$$\begin{cases} S_1 = \overline{S} + b_1 F_1 + b_2 F_1^2 + \cdots + b_{l-1} F_1^{l-1} + b_l F_1^l \\ S_2 = \overline{S} + b_1 F_2 + b_2 F_2^2 + \cdots + b_{l-1} F_2^{l-1} + b_l F_2^l \\ \cdots \\ S_l = \overline{S} + b_1 F_l + b_2 F_l^2 + \cdots + b_{l-1} F_l^{l-1} + b_l F_l^l \\ T = \overline{S} + b_1 T + b_2 T^2 + \cdots + b_{l-1} T^{l-1} + b_l T^l \end{cases}, \tag{6}$$

where b_i are the corresponding generated coefficients.

Then, the secret recovery Lagrange interpolation formula is

$$S = (-1)^{l} \sum_{i=1}^{l+1} S_i \prod_{j=1, j \neq i}^{l+1} \frac{F_j}{F_i - F_j}, \tag{7}$$

where $F_{l+1} = T$. The proposed modifications are required to assure the uniqueness of the acquired data, for example, see Fig. 5.

Due to the feature of Lagrange system, there could be just one curve described by the corresponding polynomial (Lemma 1), therefore, each set of $\overline{[F_i : S_i]}$ would produce its unique $\overline{S}$.

However, if the biometric data collected by MFA has not been changing over time, the secret would be always the same, which is an obvious vulnerability of the developed system. On the other hand, the simple addition of the timestamp would always produce an unique curve, as it is shown in Fig. 5 for $T, \overline{T}$ and $\overline{\overline{T}}$.

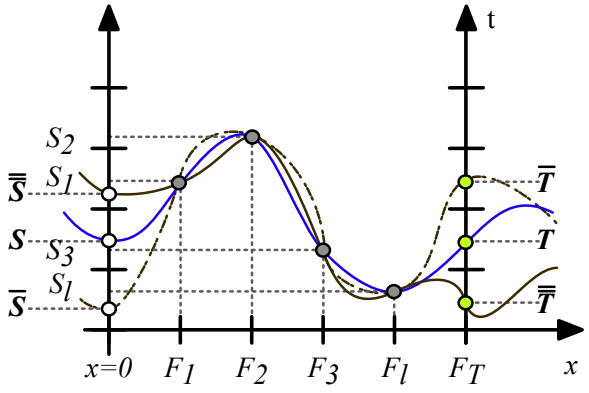

Fig. 5. Improved reversed method based on Lagrange polynomial.

D. Comparison of the MFA frameworks

Conventional SSS is based on the secret S and curve $f(x)$. The secret shares S_i are then generated and distributed between users, as it is shown in Fig. 3.

The first version of the proposed algorithm is based on existing secrets S_i, i.e. the collected biometric factors' values. The curve $f(x)$ is then generated and resulting S is calculated based on it, as it is shown in Fig. 4.

Final modification of the solution extends the first one and provides resistance against the case when all S_i are unchanged over time. This is achieved by adding unique factor of time T which enables the presence of unique factor F_l with the corresponding secret, as it is shown in Fig. 5. It is necessary to mention that the considered threshold scheme based on Lagrange interpolation formula utilizes the RSA or ElGamal encryption/decryption algorithm for authentication during the final step [63]. It is proven that in this case we obtain secure threshold scheme related to secrets S_i in [63].

IV. Proposed flexible MFA solution for V2X applications

Indeed, the proposed solution may operate out-of-the-box in case only all l factors are present. This may be crucial for a number of reasons:

1) Providing varied level of risk related to False Acceptance Rate and False Recognition Rate (FAR/FRR) [64], [65];
2) A possibility to distinguish and report outdated factor information, for example, weight fluctuation;
3) Access to the service automation in case some of the factors are not present.

In order to fulfil the listed goals, we have developed a flexible extension of the proposed solution. Assuming that the number of factors in our system is $l = 4$, then the system secret S could be represented in a simplified way as group of

$$S \leftarrow \left[\begin{array}{cccc} F_1 & F_2 & F_3 & F_4 \end{array} \right].$$

Here, if any of the S_i were modified – the secret recovery mechanism would fail. The improvement of the algorithm is delivered by providing separate system solutions $\overline{S_i}$ for lower number of factors collected. Basically, for $\bar{l} = 3$ the number of possible combinations of factors with a missing one would be equal to 4

$$\begin{array}{l} \overline{S_1} \leftarrow \left[\begin{array}{ccc} F_1 & F_2 & F_3 \end{array} \right] \\ \overline{S_2} \leftarrow \left[\begin{array}{ccc} F_1 & F_3 & F_4 \end{array} \right] \\ \overline{S_3} \leftarrow \left[\begin{array}{ccc} F_1 & F_2 & F_4 \end{array} \right] \\ \overline{S_3} \leftarrow \left[\begin{array}{ccc} F_2 & F_3 & F_4 \end{array} \right] \end{array} \tag{8}$$

The device may therefore grant access based on the predefined risk function. As the second benefit, it may inform the user (or authority) that F_1 should be updated based on the failed S_i combination. Indeed, this modification brings some marginal transmission overheads but, on the other hand, enables more flexibility in authentication and missing factor validation.

A. Trusted authority help in the case of factor lost

Another interesting scenario for the MFA is potential TA assistance in resistance against $F_i : S_i$ mismatch or loss. In case the user failed to provide enough the factors, the trusted authority could be requested for the temporary factor keys, as it is shown in Fig. 6.

For example, assuming that user forgot or lost two factors F_2, F_3 and corresponding keys $S_1 = f(F_1), S_2 = f(F_2)$, and the trusted authority is willing to assist in authentication – two temporary keys $S_{\Phi_1} = f(\Phi_1), S_{\Phi_2} = f(\Phi_2)$ are generated and sent to the user via secure channel. Obtaining these keys and applying Lagrange interpolation formula with RSA or ElGamal encryption/decryption-based threshold authentication procedure with factors and keys

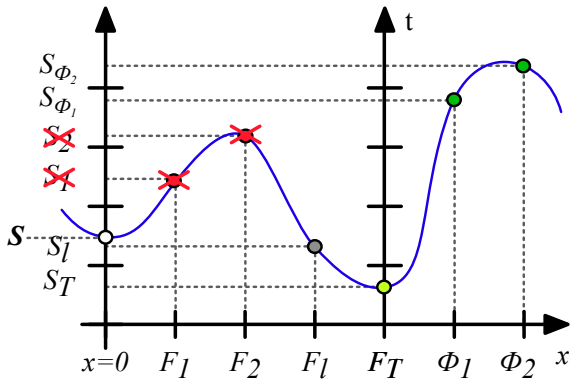

Fig. 6. Trusted authority assistance in authentication procedure in case when user lost/(forget) two factors

$$\begin{array}{l} F_1 : S_1, \\ F_2 : S_2, \\ \ldots \\ F_l : S_L, \\ F_{l+1} : T, \\ \Phi_1 : S_{\Phi_1}, \\ \Phi_2 : S_{\Phi_2}, \end{array} \tag{9}$$

as in [63], would allow to gain access for the device.

V. Discussion and conclusions

The digitalization of the modern world strides securely enabled by the authentication. In this work, we have shown the evolution of the authentication from single- through two- and towards multi-factor systems. Particularly, we focused on the factors to be utilized for vehicular MFA presenting state-of-the-art and future possible directions.

The proposed MFA solution is based on reversed Lagrange polynomial from Shamir's Secret Sharing Schema. It was extended covering the cases of authenticating the user even if some of factors being mismatched or absent, and further qualifying the missing factor without providing the sensitive data to the verificator.

Generally, the proposed solution is designed explicitly to fulfill the MFA step of the evolution, i.e. its usage for cases of SFA and 2FA is questionable. This is mainly due to the features of Lagrange interpolation formula. Basically, for the SFA case and without the $F_{l+1} : T$ factor, the equation could be simply represented as $S_1 = S + b_1 F_1$, i.e. it would be 'a point'. Even adding the random timestamp factor would not provide any valuable level of biometric data protection, since the eavesdropper would be able to immediately recover the factor secret.

In is not suitable for the 2FA neither, since providing two factors allows the curve to have linear behavior, i.e. the eavesdropper would require two attempts to recover the

secrets. However, the timestamp factor here allows to provide the necessary level of safety with 3 actual factors, as following.

Currently, authors are working on the implementation of the proposed solution and the corresponding secure communications protocol development.

ACKNOWLEDGMENTS

The work of the second author is supported by the Academy of Finland. The publication was prepared with the support of the "RUDN University Program 5-100".

REFERENCES

[1] VNI Cisco, "Global mobile data traffic forecast 2016–2021." White Paper, 2017.

[2] M. J. Dworkin, "Recommendation for block cipher modes of operation: The CMAC mode for authentication," *Special Publication (NIST SP)-800-38B*, 2016.

[3] C. Boyd and A. Mathuria, *Protocols for authentication and key establishment*. Springer Science & Business Media, 2013.

[4] A.-S. K. Pathan, *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press, 2016.

[5] A. M. Balloon, "From Wax Seals to Hypertext: Electronic Signatures, Contract Formation, and a New Model for Consumer Protection in Internet Transactions," *Emory LJ*, vol. 50, p. 905, 2001.

[6] R. K. Konoth, V. van der Veen, and H. Bos, "How anywhere computing just killed your phone-based two-factor authentication," in *Proc. of International Conference on Financial Cryptography and Data Security*, pp. 405–421, Springer, 2016.

[7] J.-J. Kim and S.-P. Hong, "A method of risk assessment for multi-factor authentication," *Journal of Information Processing Systems*, vol. 7, no. 1, pp. 187–198, 2011.

[8] D. Dasgupta, A. Roy, and A. Nag, "Toward the design of adaptive selection strategies for multi-factor authentication," *Computers & Security*, vol. 63, pp. 85–116, 2016.

[9] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "Passwords and the evolution of imperfect authentication," *Communications of the ACM*, vol. 58, no. 7, pp. 78–87, 2015.

[10] D. Wang and P. Wang, "Offline dictionary attack on password authentication schemes using smart cards," in *Information Security*, pp. 221–237, Springer, 2015.

[11] M. C. Ah Kioon, Z. S. Wang, and S. Deb Das, "Security analysis of md5 algorithm in password storage," in *Applied Mechanics and Materials*, vol. 347, pp. 2706–2711, 2013.

[12] N. Gunson, D. Marshall, H. Morton, and M. Jack, "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking," *Computers & Security*, vol. 30, no. 4, pp. 208–220, 2011.

[13] B. Schneier, "Two-factor authentication: Too little, too late.," *Communications of the ACM ACM*, vol. 48, no. 4, p. 136, 2005.

[14] T. Petsas, G. Tsirantonakis, E. Athanasopoulos, and S. Ioannidis, "Two-factor authentication: is the world ready?: quantifying 2FA adoption," in *Proc. of the 8th European Workshop on System Security*, p. 4, ACM, 2015.

[15] D. Wang, D. He, P. Wang, and C.-H. Chu, "Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 4, pp. 428–442, 2015.

[16] J. Sun, R. Zhang, J. Zhang, and Y. Zhang, "Touchin: Sightless two-factor authentication on multi-touch mobile devices," in *Proc. of Conference on Communications and Network Security (CNS)*, pp. 436–444, IEEE, 2014.

[17] E. M. Scheidt and E. Domangue, "Multiple factor-based user identification and authentication," Oct. 31 2006. US Patent 7,131,009.

[18] A. Bhargav-Spantzel, A. C. Squicciarini, S. Modi, M. Young, E. Bertino, and S. J. Elliott, "Privacy preserving multi-factor authentication with biometrics," *Journal of Computer Security*, vol. 15, no. 5, pp. 529–560, 2007.

[19] X. Huang, Y. Xiang, E. Bertino, J. Zhou, and L. Xu, "Robust multi-factor authentication for fragile communications," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 6, pp. 568–581, 2014.

[20] F. Aloul, S. Zahidi, and W. El-Hajj, "Two factor authentication using mobile phones," in *Proc. of International Conference on Computer Systems and Applications*, pp. 641–644, ACS/IEEE, 2009.

[21] D. Sunehra, "Fingerprint based biometric ATM authentication system," *International Journal of Engineering Inventions*, vol. 3, no. 11, pp. 22–28, 2014.

[22] H. Tahir and R. Tahir, "BioFIM: Multifactor Authentication for Defeating Vehicle Theft," in *Proc. of the World Congress on Engineering*, vol. 1, pp. 1–3, 2008.

[23] K. Han, S. D. Potluri, and K. G. Shin, "On authentication in a connected vehicle: secure integration of mobile devices with vehicular networks," in *Proc. of International Conference on Cyber-Physical Systems (ICCPS)*, pp. 160–169, ACM/IEEE, 2013.

[24] R. M. Ishtiaq Roufa, H. Mustafaa, S. O. Travis Taylora, W. Xua, M. Gruteserb, W. Trappeb, and I. Seskarb, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in *Proc. of 19th USENIX Security Symposium*, pp. 11–13, 2010.

[25] B. K. Chaurasia and S. Verma, "Infrastructure based authentication in VANETs," *International Journal of Multimedia and Ubiquitous Engineering*, vol. 6, no. 2, pp. 41–54, 2011.

[26] P. Kleberger, T. Olovsson, and E. Jonsson, "Security aspects of the in-vehicle network in the connected car," in *Proc. of Intelligent Vehicles Symposium (IV)*, pp. 528–533, IEEE, 2011.

[27] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proc. of the fourth ACM international workshop on Vehicular ad hoc networks*, pp. 19–28, ACM, 2007.

[28] Y. Yang, Z. Wei, Y. Zhang, H. Lu, K.-K. R. Choo, and H. Cai, "V2X security: A case study of anonymous authentication," *Pervasive and Mobile Computing*, 2017.

[29] A. De Luca, A. Hang, E. Von Zezschwitz, and H. Hussmann, "I Feel Like I'm Taking Selfies All Day!: Towards Understanding Biometric Authentication on Smartphones," in *Proc. of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pp. 1411–1414, ACM, 2015.

[30] A. Ometov, S. Bezzateev, J. Kannisto, J. Harju, S. Andreev, and Y. Koucheryavy, "Facilitating the Delegation of Use for Private Devices in the Era of the Internet of Wearable Things," *IEEE Internet of Things Journal*, 2017.

[31] N. Clarke, *Transparent user authentication: biometrics, RFID and behavioural profiling*. Springer Science & Business Media, 2011.

[32] S. Rane, Y. Wang, S. C. Draper, and P. Ishwar, "Secure biometrics: concepts, authentication architectures, and challenges," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 51–64, 2013.

[33] C. Bhagavatula, B. Ur, K. Iacovino, S. M. Kywe, L. F. Cranor, and M. Savvides, "Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption," *Proc. of USEC*, pp. 1–10, 2015.

[34] H. Wimberly and L. M. Liebrock, "Using fingerprint authentication to reduce system security: An empirical study," in *Proc. of Symposium on Security and Privacy (SP)*, pp. 32–46, IEEE, 2011.

[35] A. Ometov, D. Solomitckii, T. Olsson, S. Bezzateev, A. Shchesniak, S. Andreev, J. Harju, and Y. Koucheryavy, "Secure and Connected Wearable Intelligence for Content Delivery at a Mass Event: A Case Study," *Journal of Sensor and Actuator Networks*, vol. 6, no. 2, p. 5, 2017.

[36] T. Utter, D. Proefke, and R. Baillargeon, "Multiple vehicle authentication for entry and starting systems," July 1 2005. US Patent App. 11/173,617.

[37] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 136–148, 2013.

[38] Z. Jorgensen and T. Yu, "On mouse dynamics as a behavioral biometric for authentication," in *Proc. of the 6th ACM Symposium on Information, Computer and Communications Security*, pp. 476–482, ACM, 2011.

[39] L. F. Cranor and S. Garfinkel, *Security and usability: designing secure systems that people can use*. "O'Reilly Media, Inc.", 2005.

[40] V. Matyáš and Z. Říha, "Biometric authentication–security and usability," in *Advanced Communications and Multimedia Security*, pp. 227–239, Springer, 2002.

[41] A. Ometov, P. Masek, L. Malina, R. Florea, J. Hosek, S. Andreev, J. Hajny, J. Niutanen, and Y. Koucheryavy, "Feasibility characterization of cryptographic primitives for constrained (wearable) IoT devices,"

in *Proc. of International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, pp. 1–6, IEEE, 2016.
[42] A. L. Kun, T. Royer, and A. Leone, "Using tap sequences to authenticate drivers," in *Proc. of the 5th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*, pp. 228–231, ACM, 2013.
[43] J. Sun, Z.-h. Wu, and G. Pan, "Context-aware smart car: from model to prototype," *Journal of Zhejiang University-Science A*, vol. 10, no. 7, pp. 1049–1059, 2009.
[44] J. D. Lee, B. Caven, S. Haake, and T. L. Brown, "Speech-based interaction with in-vehicle computers: The effect of speech-based e-mail on drivers' attention to the roadway," *Human factors*, vol. 43, no. 4, pp. 631–640, 2001.
[45] T. Gioutsos, "Vehicle passenger weight sensor," Apr. 14 1998. US Patent 5,739,757.
[46] M. A. Mehney, M. C. McCarthy, M. G. Fullerton, and F. J. Malecke, "Vehicle occupant weight sensor apparatus," Mar. 21 2000. US Patent 6,039,344.
[47] M. Ferro, G. Pioggia, A. Tognetti, N. Carbonaro, and D. De Rossi, "A sensing seat for human authentication," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 451–459, 2009.
[48] C. Busold, A. Taha, C. Wachsmann, A. Dmitrienko, H. Seudié, M. Sobhani, and A.-R. Sadeghi, "Smart keys for cyber-cars: secure smartphone-based NFC-enabled car immobilizer," in *Proc. of the 3rd ACM Conference on Data and Application Security and Privacy*, pp. 233–242, ACM, 2013.
[49] K. H. Nothacker, P. A. Basaran, S. I. Rettus, M. J. Strasser, I. Aziz, J. P. Walton, Z. M. Saul, and C. T. Faykus, "Method and system for monitoring intoxication," Nov. 24 2015. US Patent 9,192,334.
[50] A. Hammad and P. Faith, "Location based authentication," Aug. 1 2017. US Patent 9,721,250.
[51] A. De Luca and J. Lindqvist, "Is secure and usable smartphone authentication asking too much?," *Computer*, vol. 48, no. 5, pp. 64–68, 2015.
[52] A. Kumar, M. Hanmandlu, V. K. Madasu, and B. C. Lovell, "Biometric authentication based on infrared thermal hand vein patterns," in *Proc. of Digital Image Computing: Techniques and Applications (DICTA'09)*, pp. 331–338, IEEE, 2009.
[53] A. M. Guzman, M. Goryawala, J. Wang, A. Barreto, J. Andrian, N. Rishe, and M. Adjouadi, "Thermal imaging as a biometrics approach
[62] M. H. Dehkordi and S. Mashhadi, "An efficient threshold verifiable multi-secret sharing," *Computer Standards & Interfaces*, vol. 30, no. 3, pp. 187–190, 2008.
to facial signature authentication," *IEEE Journal of Biomedical and Health Informatics*, vol. 17, no. 1, pp. 214–222, 2013.
[54] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, "Implicit Authentication through Learning User Behavior," in *ISC*, vol. 6531, pp. 99–113, Springer, 2010.
[55] N. Sae-Bae, K. Ahmed, K. Isbister, and N. Memon, "Biometric-rich gestures: a novel approach to authentication on multi-touch devices," in *Proc. of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 977–986, ACM, 2012.
[56] W. Wang, J. Xi, and H. Chen, "Modeling and recognizing driver behavior based on driving data: a survey," *Mathematical Problems in Engineering*, vol. 2014, 2014.
[57] N. Zhao, Z. Zhang, M. U. Rehman, A. Ren, X. Yang, J. Zhao, W. Zhao, and B. Dong, "Authentication in Millimeter-Wave Body-Centric Networks through Wireless Channel Characterization," *IEEE Transactions on Antennas and Propagation*, 2017.
[58] M. Gapeyenko, A. Samuylov, M. Gerasimenko, D. Moltchanov, S. Singh, E. Aryafar, S.-p. Yeh, N. Himayat, S. Andreev, and Y. Koucheryavy, "Analysis of human-body blockage in urban millimeter-wave cellular communications," in *Proc. of International Conference on Communications (ICC)*, pp. 1–7, IEEE, 2016.
[59] H. Silva, A. Lourenço, and A. Fred, "In-vehicle driver recognition based on hand ECG signals," in *Proc. of the 2012 ACM international conference on Intelligent User Interfaces*, pp. 25–28, ACM, 2012.
[60] C.-P. Lai and C. Ding, "Several generalizations of Shamir's secret sharing scheme," *International Journal of Foundations of Computer Science*, vol. 15, no. 02, pp. 445–458, 2004.
[61] C.-C. Yang, T.-Y. Chang, and M.-S. Hwang, "A(t,n) multi-secret sharing scheme," *Applied Mathematics and Computation*, vol. 151, no. 2, pp. 483–490, 2004.
[63] K. Kaya and A. A. Selçuk, "Threshold cryptography based on Asmuth–Bloom secret sharing," *Information Sciences*, vol. 177, no. 19, pp. 4148–4160, 2007.
[64] S. Bezzateev, A. Afanasyeva, N. Voloshina, and A. Ometov, "Multi-factor Authentication for Wearables: Configuring System Parameters with Risk Function," in *Proc. of Second International Conference on Advanced Wireless Information, Data, and Communication Technologies (AWICT 2017)*, pp. 1–7, ACM, 2017.
[65] P. Tuyls, A. H. Akkermans, T. A. Kevenaar, G. J. Schrijen, A. M. Bazen, and R. N. Veldhuis, "Practical biometric authentication with template protection," in *Proc. of AVBPA*, vol. 3546, pp. 436–446, Springer, 2005.