A Survey on Vehicle Security Systems: *Approaches and Technologies*

Kudakwashe Mawonde
Department of Computer Science
North-West University
Mafikeng, South Africa
kuda.mawonde@gmail.com

Bassey Isong
Department of Computer Science
North-West University
Mafikeng, South Africa
isong.bassey@ieee.org

Francis Lugayizi
Department of Computer Science
North-West University
Mafikeng, South Africa
francis.lugayizi@nwu.ac.za

Adnan M. Abu-Mahfouz
Modelling and Digital Science
CSIR
Pretoria, South Africa
a.abumahfouz@ieee.org

***Abstract*—Vehicle security is an emergent issue in the technology sector that has benefited from the continuous advancement in technology through the creation of more complex and advanced security systems. This serves to address the pandemic of vehicle theft that is prevalent in numerous countries due to inadequate security in vehicles. Consequently, security devices in vehicles are susceptible to attacks such as man-in-the-middle, replay attacks, deciphering attacks and signal disruption, all of which caused the devices to function below the expected parameters. Current technology has loopholes in its security implementation creating attack vectors from benign devices such as the infotainment system to more severe systems like the CAN bus network. Therefore, this paper presents analysis of the numerous works and approaches that exists in the literature to tackle this menace. Moreover, we performed an in-depth comparative analysis of the type of technology implemented, the strengths and the weaknesses of the proposed systems. Based on the analysis, we found that there is a need for more holistic approaches to tackling the pre-existing security vulnerabilities in an effective manner that reduces chances of compromise to the most minimal degree.**

***Keywords*— Vehicle, Theft, Security System, Attacks.**

I. Introduction

Vehicle security refers to the numerous technologies put in place in a vehicle to prevent unauthorized access and use. It's a concept which goes beyond access and extends to other aspects like accountability and vehicle identification. Early forms of vehicle security were created to address the fundamental problems that arose when vehicles were a new transportation technology, with aspects like anonymity being key among the tasks to be tackled as vehicles looked identical in the early days. License plates [1] were created to combat this issue as they provided accountability through uniquely identifying vehicles and thereby making it easier for law enforcement to identify the owners of vehicles used in criminal activities. Next advancement was in the form of mechanical immobilizers in an attempt to thwart vehicle theft whereby steering locks and gear locks were used to secure a vehicle when it was not in use [2] which worked until adversaries found a way to defeat the mechanisms and compromise the vehicles to a point where the mechanical immobilizers could be disabled in seconds [3]. This inevitably led to the use of electronic immobilizers [4] which awe a more effective security measure and exponentially more advanced in their implementation. They worked through the disabling of critical vehicle systems like the fuel system or the ignition system when activated and are still used up to now. Other systems were put in place like in [5] to prevent the illegitimate registration of stolen vehicles by increasing the complexity of vehicle registration systems thereby reducing the vehicle laundering. Other systems like license plate recognition [6] have been used to augment the effectiveness of law enforcement in detecting stolen vehicles on the road and this acts as a layer to the overall countermeasure suite used in vehicle theft prevention.

Vehicle security has been an issue since the creation of vehicles, starting from the simplistic problem of anonymity tackled through the use of Vehicle Identification Numbers and License Plates [7] to the use of more advanced problems like man-in-the-middle attacks (MITM) carried out by more technical adversaries in the current vehicle theft landscape. The main issue is the undeniable fact that as security technology advanced, methods used by adversaries to circumvent them have also advanced and in most cases the adversaries have managed to circumvent the countermeasures put in place to stop them from accessing a vehicle or vehicle system. This paper aims to offer clarity on the state of current vehicle security implementations and to outline the weaknesses that are resulting in the compromise of vehicle security apparatus as well as a comparison of the proposed solutions with an emphasis on what they bring to the table in terms of improvements and their shortcomings. This paper present previous works on evaluations made pertaining to vehicle security and threats, the solutions proposed to address the predominant weaknesses of current vehicle security and will discuss the proposed solutions according to their merits and shortcomings.

The remaining parts of the paper are organized as follows; Sect. II presents the analysis of the existing works, Sect. III presents existing implementations and solutions, Sect. IV is the paper discussions and Sect. V is the conclusion.

II. Analysis of Existing Technologies and Threats

This section will detail the various studies conducted by other researchers and the approaches proposed in assessing trends in vehicle security. Graham *et al.* [8] conducted a study on the various security technologies that have been implemented over the years as technology advanced and developed a tool to assess the impact of vehicle security implemented from different eras, among other factors, on the rate of vehicle theft. They concluded that the use of combination of various security technologies that favourably augment each other's functions as part of a suite and the use of a favourable environment would drastically reduce the chances of vehicle theft. In descending order, the most effective security systems were a combination of an alarm, central locking, electronic immobilizer and tracker with the highest security protection factor, followed by central locking, electronic immobilizer and mechanical immobilizer as the second and alarm system, central locking, electronic immobilizer and mechanical immobilizer being the third.

Copes *et al.* [9] investigated the rate of vehicle theft using the routine activity theorem which takes aspects like availability and proximity and correlates them to vehicle theft. The framework was used to reflect the effect of the size of the offender pool, the availability of a vehicle and the level of guardianship on vehicle theft. A qualitative vulnerability based risk assessment was conducted by Kelarestaghi *et al.* [10] which focused on Intelligent Transport Systems (ITS). ITS are a new form of vehicular technology which utilises mobile communication technologies like mobile networks, Wi-Fi and Vehicular Ad hoc Networks (VANETS) [11] to facilitate inter-vehicular communication (V2V) and vehicle to infrastructure communication (V2I). Concerns arose as a result of an article by [12] detailing the successful remote access and control of a Jeep Cherokee by security researchers who used the vehicle's infotainment system's wireless communication as an attack vector to compromise the vehicle Controller Area Network (CAN) bus and control vehicle functions including but not limited to the steering and braking systems. This highlights the prevalent problem of improper implementations of security measures in deploying connected systems in motor vehicles. A risk model was then proposed, which aimed at mitigating security vulnerabilities in intelligent systems through pre-emptive measures like proper implementation and securing of controllers that affect the vehicle functions and communicate with the Engine Control Units (ECU) in vehicles. Wu *et al.* [13] detailed and tabulated the various attacks that can be conducted on vehicle systems as a result of the increased connectivity between vehicle systems and vehicles with external networks as detailed in Fig. 1. The vulnerabilities mainly stem from the inadequately protected CAN busses that transmit control information from different critical vehicle systems.

This includes non-invasive methods like side channel attacks in which the attacker monitors non critical information leaked from the devices in order to approximate the data or operations being conducted by the critical devices. It also includes invasive attacks like the use of the On Board Diagnostics (OBD2) port to directly interface with the vehicle's ECU and inject malicious code which gives the attacker access to functions they are not authorized for. Other invasive attacks involve packet fuzzing and spoofing which means the falsifying of data used by the vehicle's systems in order for the attacker to illicit a certain response from the vehicle. The study also detailed remote attacks such as jamming which can be used to disrupt vehicle sensors from obtaining crucial information and Global Positioning System (GPS) spoofing in which the vehicle is fed with false location data.

Zheng *et al.* [14] proposed a test bed for analysing vehicle systems based on a virtual environment. Although such tests have been done on actual vehicles, their approach involved a highly configurable environment which would cater to numerous vehicle systems and provide a uniform set of results for all the tests run on the different vehicle systems. The data obtained can be used to model attacks that can be tested against the vehicle ECU.

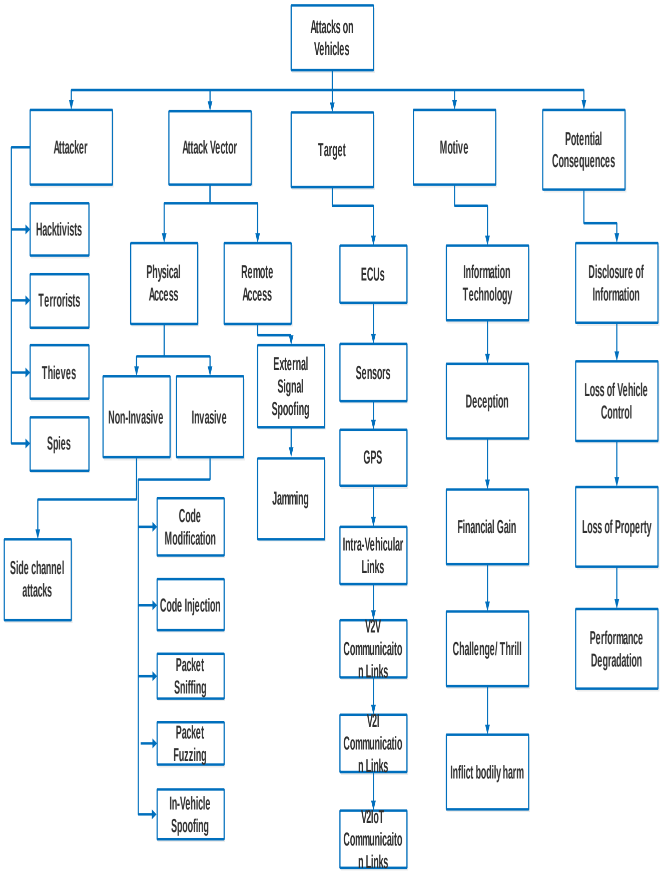

Fig. 1 Taxonomy of attacks [13]

III. Existing Implementations and Solutions

This section covers the different approaches proposed in numerous works to solve the problem of vehicle security and aims to address the shortcomings of traditional security systems that are considered ineffective and in need of replacement or augmentation in order for them to function within acceptable security margins.

Wut *et al.* [13] also proposed a defensive approach to combat attacks to vehicle systems as detailed in Fig. 2. This involved the use of passive countermeasures like user authentication to verify the identity of the individual attempting to access the vehicle. This would prevent the issue of unauthorized access to the vehicle by attackers. The use of a firewall was also considered as it could be used to prevent spoofing by blocking malicious traffic sources and monitoring network traffic in untrusted environments.

The use of encryption was also proposed so as to secure the communications between devices and vehicles. This would prevent the leaking of any data that could be used by an attacker to infiltrate the system. Active countermeasures involve the use of intrusion detection systems (IDS) to monitor the vehicle systems for indicators of compromise (IoC) that would reflect malicious activity by an attacker. This would create an alert if the vehicle system is under attack and would enable other intervention systems to take the appropriate countermeasures to resolve the issue and mitigate the damage. Another countermeasure is antimalware which can be used to identify and eradicate malicious code injected into the ECU by an attacker in an effort to compromise the vehicle system. The defence model is aimed at ensuring the protection of critical data in crucial vehicle systems in the event of an attack that has the potential to compromise said systems and data.

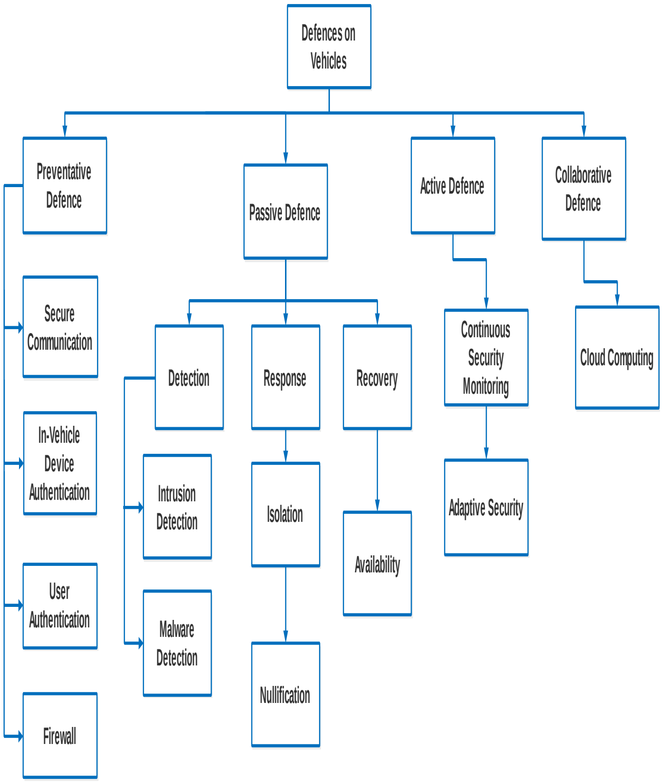

Fig. 2 Taxonomy of defences on vehicles[13]

Krishna *et al.* [15] proposed a vehicle security and antimalware approach which verified the identity of the user and checked the presence of malware through the use of a java based program. The system uses facial recognition to identify the user by comparing the image captured for verification to the image stored in a secure database during setup. If the images match then the user is authorized otherwise the user is denied access and the vehicle security remains armed.

Alrabady *et al.*[16] conducted an analysis on remote keyless entry systems and proposed a few approaches to mitigate the security natively offered in these systems. Remote keyless entry refers to entry systems on vehicles which enable the user to be authenticated and granted access to a vehicle through the use of a keyfob which is in possession of the user and communicates with the vehicle reader, thereby exchanging security information. The problem with this system is the lack of robust security measures to protect the code which is transmitted so as a result, an attacker can intercept the code with ease.

An embedded antitheft system was suggested in [17] which uses an embedded chip and an inductive proximity sensor to alert the user when a key has been inserted in to the ignition. The system then prompts the user for a password which is needed for the vehicle functions to be activated. In the event of failure to enter the password, the system alerts the police using a GSM module and transmits its coordinates using a GPS module which is also part of the vehicle. The lock can be disabled by the owner who's in possession of a second security code exclusively used with the locking system.

Lui *et al.* [18] proposed a system that incorporates the use of a GMS and GPS module as well as few sensors to provide continuous tracking information of a stolen vehicle to a partner application on the owner's mobile device enabling the owner to track the vehicle to in a timely manner.

Ecker [19] proposed a security system which disabled the critical components of a vehicle until a security code was entered and validated to disable the security using solenoids and relays so that in the event of unauthorized access, the attacker would not be able to operate the vehicle. The system works in conjunction with a keyless entry system which grants the owner access to the vehicle through the driver door before they have to enter a passcode to unlock the locked functions of the vehicle.

Berman *et al.* [20] used a secret sequence of actions to authenticate the user and enable vehicle functions. However this approach severely lacks in security robustness as the sequence can be merely observed by an attacker and later used to circumvent the same security.

A rolling code keyless entry system was suggested by Waraksa *et al.* [21] that is similar to one mentioned earlier in [16], using RFID based technology and an algorithm that cycles among a set of codes to validate the user's beacon device and unlock the vehicle and its functions. It utilizes a motion sensor as a basis for activating the beacon and continuously changing signal between the beacon and the receiver in an effort to deter theft.

Tsuria *et al.* [22] proposed a vehicle theft prevention system that uses a central control station to transmit control signals to a receiver located in the vehicle and disable interference on a critical component in the vehicle, enabling the component for use in the vehicle. While the concept is interesting, it provides additional points of failure for the system and creates unnecessary dependencies on an auxiliary system that does not seem practical.

TABLE I. Summary of Proposed Vehicle Security Technologies

Ref.	Technology	Implementation	Strengths	Weaknesses
[15]	SMS, GSM, GPS, Biometrics	-Disables vehicle engine automatically. -Detects vehicle theft. -Transmits vehicle coordinates to cellphone.	-Tracking enables recovery of vehicle. -Uses facial recognition. -Uses malware detection.	-GSM messages can be jammed. -Facial recognition can be tricked in some instances with high resolution copies of owner.
[16]	RFID	-Uses keyfob to authenticate user. -Transmits a code from the keyfob to vehicle for validation. - Could use fixed code, rolling code or challenge response.	-Ease of use of keyless entry. -Rolling code offers different codes for validation. -Utilises some cryptographic functions.	-The keyfob can be probed by rogue interrogation signal without user knowledge. - Susceptible to RollJam attack[31]. -Weak encryption.
[17]	GSM, GPS, Inductive proximity sensor	-Uses a sensor to detect key insertion. -Transmits a notification to vehicle owner. -Uses password to validate user and activate vehicle. -Locks vehicle if password incorrect after 3 attempts.	-Multistage security. -More secure than conventional lock and key security. -User is notified of any activity with vehicle being started. -Secondary system lock provides additional security.	-Subject to signal jamming. -Susceptible to hardware. tampering -Password has fixed portion in the form of key number. -Attacker with second password could intentionally trigger system lock.
[18]	GPS, GSM, IoT, RFID	-Uses vibration sensors to sense movement. -Sends coordinates to Android app.	-Can potentially detect vehicle being moved whilst locked. -Immediate notification of user. -Tracking information which can be used to locate vehicle.	-Subject to GSM jamming. -Subject to GPS spoofing -No countermeasures to disable stolen vehicle.
[19]	Solenoids, Relays, RFID	- Unlocks only driver door using RFID device. -Uses passcode to unlock functions.	- Limits initial physical access. -Requires auxiliary validation to enable vehicle functions.	-RFID code cloning will grant attacker physical access to vehicle. -Security code length affects security.
[20]	Secret sequence	-Vehicle stalls unless secret sequence is entered.	-Additional security over conventional lock and key.	-Secret sequence can be observed and repeated by attacker. -No flexibility.
[21]	RFID	-Uses a motion sensor to activate key -Unlocks vehicle using keyfob	-Motion activated keyfob saves battery -Rolling codes prevent traditional replay attacks	-Key can be probed without user knowledge -Susceptible to RollJam [31]
[22]	Control station, Radio	-Central station transmits control signals to unlock vehicle.	-Additional layer of security.	-Susceptible to jamming. -Susceptible to eavesdropping.
[23]	Encryption, Keyless entry	-Uses encryption functions to validate user	-Offers secure encryption	-Its strength is dependent on the effectiveness of the encryption algorithm used
[24]	Biometrics	-Uses fingerprint to authenticate user. -Uses password as a backup system.	-Biometrics enhance the traditional security. -Password provides contingency.	-Possibly susceptible to fingerprint spoofing. -Access to password by attacker will enable biometrics bypass.
[25]	GPS, GSM	-Uses password system when vehicle is lost.	-Provides tracking capabilities.	-Security can be bypassed with just a key.
[26]	Keyless entry	-Uses identification information on a transceiver to validate user.	-Augments traditional security.	-Susceptible to interception.
[27]	OBD2, CAN	-Checks messages sent to the CAN bus through a security mechanism.	-Protects vehicle system from unauthorised access.	-Possible vulnerability to spoofed messages.
[28]	GPS, Accelerometer	-Uses GPS and accelerometer to detect vehicle location and movement.	-Facilitates vehicle tracking.	-Does not prevent unauthorized access by attackers.

IV. Discussions

In this paper, we have performed a thorough analysis of security issues in vehicles and their solutions. In Table I, a variety of solutions proposed by different researchers have been analysed according to the categories of the type of technology, the way in which the proposals are implemented in the vehicle, the strengths and weaknesses of each solution. As shown in Table I, it indicates the clear differences among the proposed solutions and reflect the type of problems being targeted in each scenario. However, it also clearly indicate areas lacking in each implementation where the proposed solution does not completely address all pre-existing vulnerabilities or creates new attack vectors for attackers to manipulate and compromise the vehicle security. From Table I, one can conclude that solutions that use multiple technologies in a single system such as [15, 17, 18, 23, 27] offer more robustness as they cover a multitude of areas and aim to eliminate multiple vectors with some extending functionality to tracking in the event of a system compromise which leads to the vehicle being stolen. Solutions with single technologies such as in [16, 20, 21, 24] have their own strengths in their implementations but they focus on a single avenue of vehicle security and neglect other areas which are otherwise crucial in achieving their desired goal more effectively. It is worth noting though that, either approach will increase the efficiency of the security implemented in the vehicle and reduce the possibility of theft.

The fact of the matter is that the current state of security in vehicles is not adequate to prevent unauthorized access and use. This raises concerns in the terms of the safety of the driver and occupants that could be potentially compromised as a result of the vehicle system being compromised and the potential loss of vehicles due to theft. With the rush to automate and implement smart systems, a lack of a fundamentally strong base on which to implement these smart systems has created vectors for exploitation which were previously non-existent or at the very least very difficult to access. A prime example of this is the connectivity of vehicle CAN busses and by extension, vehicle ECUs to a networking interface for a more user friendly and easy access without putting in place the adequate security measures to prevent the illegitimate access of these systems remotely and locally through interconnected systems.

An example of such a case is the Nissan Leaf [31] which used networking to connect the vehicle remotely to an application on a mobile phone enabling the user to control and monitor several features of the vehicle. Due to poor security and implementation, it was discovered that it was relatively easy to communicate with the vehicle system from an internet browser and without proper authorization after obtaining the vehicle’s VIN which is not a secret as it is not hidden on the chassis of the vehicle. This enabled potential attackers to target a remote vehicle located on a different continent successfully and with relative ease. Such a prospect raises concerns as to the usefulness of smart or interconnected systems if they compromise the security of the vehicle and the safety of the user to this extent.

The pre-existing security solutions have their own set of problems as they are based on RFID technology and that has inherent weaknesses that can be manipulated by adversaries with the relevant hardware and knowhow. This presents a problem in that retrofitting patched hardware to the millions of vehicles already in use is impossible. Therefore, the danger of the vulnerabilities is ever present. In some of the solutions discussed earlier, alternative approaches based on technology other than RFID were proposed and that facilitates investigation of a new and more secure security scheme to ensure the ineffectiveness of most if not all attacker attempts.

V. Conclusion

This paper discussed the existing and proposed vehicle security systems that aimed to address pre-existing weaknesses found in the current vehicle security technology. We compared the solutions on the basis of the type of technology used to implement the systems or proposed in the systems as well as the strengths and weaknesses of the systems. Based on the findings of the analysis performed, we surmise that there are strong contenders to the augmentation of current vehicle security, however there still lacks a solution with a quintessential silver bullet of sorts that will tackle all of the underlying problems without creating or leaving any pre-existing weaknesses that can be exploited by malicious actors.

Acknowledgment

This research was supported by FRC and the Department of Computer Science at the NWU-Mafikeng and CSIR, South Africa.

References

[1] G. Newman, "Car safety and car security: an historical comparison," Understanding and Preventing Car Theft. Crime Prevention Studies, vol. 17, 2004.

[2] B. Webb, "Steering column locks and motor vehicle theft: Evaluations from three countries," Crime prevention studies, vol. 2, pp. 71-89, 1994.

[3] C. Corbett, Car crime: Willan, 2013.

[4] N. Tilley, G. Farrell, A. Tseloni, and J. Mailley, "Curbing Vehicle Theft: Experience beyond the United States," Report to Rutgers School of Criminal Justice as part of a larger study of vehicle theft prevention devices for the National Highway Traffic Safety Administration, 2009.

[5] B. Webb, M. Smith, and G. Laycock, "Designing out crime through vehicle licensing and registration systems," ed: Willian Publishing, 2004.

[6] B. Taylor, C. Koper, and D. Woods, "Combating Vehicle Theft in Arizona: A Randomized Experiment with License Plate Recognition Technology," Criminal Justice Review, vol. 37, pp. 24-50, 2012.

[7] J. Bässmann, "Vehicle Theft Reduction in Germany: The Long-Term Effectiveness of Electronic Immobilisation," European Journal on Criminal Policy and Research, vol. 17, p. 221, June 14 2011.

[8] G. Farrell, A. Tseloni, and N. Tilley, "The effectiveness of vehicle security devices and their role in the crime drop," Criminology & Criminal Justice, vol. 11, pp. 21-35, 2011.

[9] H. Copes, "ROUTINE ACTIVITIES AND MOTOR VEHICLE THEFT: A CRIME SPECIFIC APPROACH," Journal of Crime and Justice, vol. 22, pp. 125-146, 1999/01/01 1999.

[10] K. B. Kelarestaghi, K. Heaslip, and R. Gerdes, "Vehicle Security: Risk Assessment in Transportation," arXiv preprint arXiv:1804.07381, 2018.

[11] S. Yousefi, M. S. Mousavi, and M. Fathy, "Vehicular Ad Hoc Networks (VANETs): Challenges and Perspectives," in 2006 6th International Conference on ITS Telecommunications, 2006, pp. 761-766.

[12] A. Greenberg, "Hackers remotely kill a jeep on the highway—with me in it," Wired, vol. 7, p. 21, 2015.

[13] V. L. L. Thing and J. Wu, "Autonomous Vehicle Security: A Taxonomy of Attacks and Defences," in 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016, pp. 164-170.

[14] X. Zheng, L. Pan, H. Chen, R. D. Pietro, and L. Batten, "A Testbed for Security Analysis of Modern Vehicle Systems," in 2017 IEEE Trustcom/BigDataSE/ICESS, 2017, pp. 1090-1095.

[15] A. S. Krishna and S. A. Hussain, "Smart vehicle security and defending against collaborative attacks by malware," Int. J. Embed. Softw. Comput, 2015.

[16] A. I. Alrabady and S. M. Mahmud, "Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs," IEEE transactions on vehicular technology, vol. 54, pp. 41-50, 2005.

[17] V. K. Sadagopan, U. Rajendran, and A. J. Francis, "Anti theft control system design using embedded system," in Proceedings of 2011 IEEE International Conference on Vehicular Electronics and Safety, 2011, pp. 1-5.

[18] Z. Liu, A. Zhang, and S. Li, "Vehicle anti-theft tracking system based on Internet of things," in Proceedings of 2013 IEEE International Conference on Vehicular Electronics and Safety, 2013, pp. 48-52.

[19] E. Ecker, "Automotive theft-prevention system using a key pad and a remote signaling module," ed: Google Patents, 1997.

[20] L. C. Berman and J. C. Noe, "Car theft prevention device," ed: Google Patents, 1995.

[21] T. J. Waraksa, P. A. Michaels, S. A. Slaughter, J. A. Poirier, and I. B. Rea, "Rolling code for a keyless entry system," ed: Google Patents, 1995.

[22] Y. Tsuria and D. Handelman, "Theft prevention system and method," ed: Google Patents, 1999.

[23] H. Brinkmeyer, M. Daiss, G. Schwegler, and B. Kruger, "Vehicle security device with electronic use authorization coding," ed: Google Patents, 1998.

[24] S. Dashore and N. Verma, "ANTI-THEFT VEHICLE SECURITY SYSTEM USING FINGERPRINT SCANNER AS WELL AS MANUAL," 2018.

[25] F. Shaikh, N. Chikhal, and S. Joshi, "Advanced Vehicle Security and Safety System for Two Wheelers," International Journal of Engineering and Management Research (IJEMR), vol. 6, pp. 28-30, 2016.

[26] J. Harvey, T. F. Doyle, and M. L. Segal, "Vehicle security system and method," ed: Google Patents, 2014.

[27] T. R. Markham, "Vehicle security module system," ed: Google Patents, 2017.

[28] K. E. Flick, "Vehicle control system including accelerometer based security warning and related methods," ed: Google Patents, 2016.

[29] H. Sasaki, "Vehicle antitheft system and vehicle security device," ed: Google Patents, 2017.

[30] (2015, February 23, 2018). Anatomy of the Rolljam Wireless Car Hack. Available: https://makezine.com/2015/08/11/anatomy-of-the-rolljam-wireless-car-hack/

[31] T. Hunt, "Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs," Blog post, February, 2016.

[32] Sherwood, R., *et al., Flowvisor: A network virtualization layer.* OpenFlow Switch Consortium, Tech. Rep, 2009. 1: p. 132.

[33] K. M. Modieginyane, B. B. Letswamotse, R. Malekian, and A. M. Abu-Mahfouz, ‘‘Software defined wireless sensor networks application opportunities for efficient network management: A survey,’’ Comput. Elect. Eng., no. 3, pp. 1–14, 2017.

[34] A. De Gante, M. Aslan, and A. Matrawy, ‘‘Smart wireless sensor network management based on software-defined networking,’’ in Proc. 27th Biennial Symp. Commun., Jun. 2014, pp. 71–75.

[35] Dhamecha, K. and B. Trivedi, Sdn issues-a survey. International Journal of Computer Applications, 2013. 73(18).

[36] Kreutz, D., F. Ramos, and P. Verissimo. Towards secure and dependable software-defined networks. in Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. 2013. ACM.

[37] Jacobsson, M. and C. Orfanidis. Using software-defined networking principles for wireless sensor networks. in 11th Swedish National Computer Networking Workshop (SNCNW 2015) Karlstad, May 28-29, 2015. 2015.

[38] Nunes, B.A.A., *et al.*, A survey of software-defined networking: Past, present, and future of programmable networks. IEEE Communications Surveys & Tutorials, 2014. 16(3): p. 1617-1634.

[39] Lantz, B., B. Heller, and N. McKeown. *A network in a laptop: rapid prototyping for software-defined networks*. in *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*. 2010. ACM.

[40] Anadiotis, A.-C.G., *et al.*, *SD-WISE: A Software-Defined WIreless SEnsor network.* arXiv preprint arXiv:1710.09147, 2017.

[41] Gupta, M., J. Sommers, and P. Barford. Fast, accurate simulation for SDN prototyping. in Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. 2013. ACM.

[42] Dargahi, T., *et al.*, *A survey on the security of stateful SDN data planes.* IEEE Communications Surveys & Tutorials, 2017. 19(3): p. 1701-1725

[43] Scott, R.C., *et al.*, *What, where, and when: Software fault localization for sdn.* EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2012-178, 2012.

[44] Reitblatt, M., *et al. Fattire: Declarative fault tolerance for software-defined networks*. in *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*. 2013. ACM.

[45] J. Louw, G. Niezen, T.D. Ramotsoela and A.M. Abu-Mahfouz, "A Key Distribution Scheme using Elliptic Curve Cryptography in Wireless Sensor Networks," in *Proceedings of the IEEE 14th International Conference on Industrial Informatics*, 18-21 July, Futuroscope-Poitiers, France, 2016. pp. 1166–1170.

[46] A.M. Abu-Mahfouz and G.P. Hancke, "Evaluating ALWadHA for providing secure localisation for wireless sensor networks," in *Proceeding of the IEEE AFRICON 2013 conference*, 9-12 September, Mauritius, 2013, pp. 501-505.