Vehicular Ad Hoc Network Security and Privacy: A Second Look

Jesse Lacroix, Khalil El-Khatib
Faculty of Business and Information technology
University of Ontario Institute of Technology
Oshawa, Canada
Emails: {Jesse.Lacroix, Khalil.El-Khatib}@uoit.ca

***Abstract*—VANETs are an emerging infrastructure that makes use of vehicles as the main objects within a network. These networks use either peer-to-peer communications to communicate with other vehicle objects directly or a more centralized client/server approach to communicate with its road side infrastructures to either authenticate, send or receive information. With this added ability implemented into modern and upcoming vehicles, the transportation infrastructure would greatly improve in terms of efficiency, safety and user-friendliness. Although communication introduces better ways of traveling, adding a network infrastructure to vehicles and their environments also introduces the possibility of security breaches inside the vehicles and respective surroundings through internal and external components embedded in Vehicular Ad Hoc Networks. It has been shown that multiple attack surfaces exist and proper defence mechanism must be implemented to properly secure and deploy this type of network. This survey will present an overview of VANETs and synthesize related works to demonstrate new security mechanisms and how much this type of network and in-house components of vehicles are exposed.**

Keywords—Vehicular Ad Hoc Networks; Security; Vulnerabilities.

I. INTRODUCTION

Modern vehicles are now embedded with Electronic Control Units (ECUs) and On-Board Units (OBUs) to send and receive information to other vehicles or Road Side Units (RSUs). RSUs and vehicles are used to send critical information to other peers and to communicate to other parts and types of network infrastructures such as the Internet. RSUs are important in the operation of VANETs because they are used as relays to send information to all vehicles (for e.g., safety-related messages such as an accident occurring within a specific region and authentication messages for system validation). This type of communication is called Vehicle-to-Infrastructure (V2I) communication. Since these are not mobile, it is much easier to have them deliver the messages to affected cars because RSUs are deployed in such a way that vehicle objects can maintain a constant connection or have an indirect way of communicating with them. RSUs are not the only way vehicles can communicate inside the VANET; Vehicle-to-Vehicle (V2V) communications will also allow vehicle objects to communicate together and exchange information. Vehicle tracking, vehicle speed, Basic Safety Messages (BSMs) and other related information can all be exchanged between the vehicles themselves directly to ensure efficient and safe operation of the vehicles in their respective environments. What is important about VANETs is that they incorporate other means of communications to facilitate their operation. Examples of these as shown by Checkoway et al. [4] are: Bluetooth; broadcast channels, such as radio and GPS channels); addressable channel, such as OnStar [4]; and cellular channels, including 3G/4G LTE and basic voice channels for cellular communications. Combining all of these technologies together offers much more robustness to VANETs; however, on a security aspect, it does compromise security standards since more attack surfaces are introduced in the formula.

Each vehicle in VANET has a number of components that are used by vehicles for internal operations and data flow presented by Everett and McCoy [7]. The internal components work in conjunction with the OBUs so that proper information is transmitted from one vehicle to another. The components are:

- CANs (Control Area Networks) – used as backbone channels
- LINs (Local Interconnect Networks) – used for low speed and low bandwidth applications
- FlexRay – used for high speed and high bandwidth safety critical applications
- MOST (Media Oriented System Transport) – used for high speed and high bandwidth media applications
- TPMS (Tire Pressure Monitoring System) – used to monitor tire condition, precise pressure, etc.
- HSM (Hardware Security Module) – Stores and secures sensitive data (for e.g., private keys)

These components produce the overall infrastructure implemented inside vehicles to properly function and work directly with ECUs to perform proper operations. Compromising one of these components potentially leads to the full compromise of the vehicle; proper mechanisms must therefore be implemented for safeguarding.

The IEEE 1609 standard, shown by the IEEE Standards Association [10], known as the Wireless Access in Vehicular Environments (WAVE) is a service recognized by the Intelligent Transportation System (ITS). It is employed in the United States and similar infrastructures employed around the world for VANETs so that vehicles and respective infrastructure can communicate. This standard can also be associated to the Dedicated Short Range Communications (DSRC) protocol for radio spectrum allocation used by WAVE technologies. WAVE embodies many standards for its secure and efficient communications. They are as followed (this survey relates to the 1609.2 standard):

- IEEE Std 802.11 (2012)—Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications for metropolitan and local networks as well as data exchange between systems
- IEEE Std 1609.2 (2013)—WAVE Security Services for applications and Management Messages; makes use of Elliptic Curve Cryptographic (ECC) as an encryption standard
- IEEE Std 1609.3 (2010)—WAVE Networking Services
- IEEE Std 1609.4 (2010)—WAVE Multi-Channel Operations
- IEEE Std 1609.11 (2010)—WAVE ITS over-the-air payment data exchange protocol
- IEEE Std 1609.12—WAVE Identifier Allocations

The European Telecommunications Standards Institute (ETSI) has developed its set of standards for VANET communication and information exchange for the ITS based off IEEE 802.11 technologies shown by Rizzo and Brookson [21]. ETSI ITS standards will take in consideration the IEEE 1609.2 data sets, but it will adopt them to fit explicit protocols developed for ETSI standards and will collaborate closely with the IEEE community. Here are some of the current ETSI ITS security standards:

- ETSI TS 102 867—ITS Security Service IEEE 1609.2 stage 3 mapping
- ETSI TS 102 940—ITS Security Service for communications security architecture and management
- ETSI TS 102 941—ITS Security Service for Trust and Privacy Management
- ETSI TS 102 942—ITS Security Service for Access Control
- ETSI TS 102 943—ITS Security Service for Confidentiality Services
- ETSI TS 103 097—ITS Security Service for headers and certificate formats

RSUs are also responsible for authenticating vehicles when one connects to the VANET network. At this moment, a centralize authentication scheme in combination with a Public Key Infrastructure (PKI) is the approach used to authenticate vehicles in the network with the use of trusted third parties (TPPs) as well as a central Certificate Authority (CA). This system would provide every vehicle with a valid certificate as long as they are part of the legitimate list of users located in the CA. This infrastructure makes use of what is known as a “legal authority” that binds certificates to the actual identities of drivers but is only accessible by the Central Authority. If a certificate is recovered, the driver’s personal details are not revealed and only linked to a given pseudonym. This authentication scheme is robust but faces computational issues when it comes to handling pseudonyms in an efficient and timely manner.

The contribution of this paper is to look at the current state of VANET security and privacy mechanisms and issues regarding all of its internal and external components so that a proper overview is provided to its audience. This paper can be used as reference to the challenges presented for future research when tackling presented problems and developing future platforms and systems. This survey will present and discuss the following topics to give a proper overview of Vehicular Ad Hoc Network security-related concepts and vulnerabilities at their current states of research. First, related works will be presented and split in subsections covering the main security concepts and new potential security mechanisms in each respective fields, including authentication and confidentiality, availability, non-repudiation, data trust and privacy. Proven vulnerabilities inside vehicles and on the network will then be discussed followed by the conclusion and future work.

II. SECURITY AND PRIVACY CHALLENGES IN VANET

The following section will present works and their research states with new security mechanisms in core concepts, such as authentication and confidentially, availability, non-repudiation, data trust and privacy.

A. *Authentication and Confidentiality*

Authentication plays a huge role in network security regardless of the infrastructure it is implemented in. Many methods and schemes exist to authenticate legitimate users to services, but a popular scheme employs the use of the public key infrastructure, as discussed by Fuentes, González-Tablas and Ribagorda [9]. This scheme employs a CA, TPPs and pseudonyms that form the Vehicular Public Key Infrastructure (VPKI). There are two proposals for the actual authentication process in the VPKI. The first method suggests that vehicle creates the pseudonyms and public keys themselves and send the information to RSUs so that they can be authenticated. The other method suggests that the HSM inside the vehicles takes care of authentication, since all stored information is already secured, and private keys are always contained inside the HSM; signed pseudonyms sent to the system are therefore much more secure. The main goal is to ensure that pseudonyms are changed at a regular interval so that enough confusion is caused within a network if someone is attempting to link acquired information to a specific car. Of course, other levels of addresses must be changed to limit how an attacker can link stolen information to cars such as the vehicle’s IP (Internet Protocol) and MAC (Media Access Control) addresses. An added proposal was suggested by Adigun et al. [2] for helping the VPKI re-allocate and change certificates to ensure that captured information does not link electronic license plate information to private information about drivers. The first method suggested is pretty straightforward and requires a regional CA to issue a new pseudonym to vehicle objects the instant a time “*t*” threshold is reached. The second approach presented is basically the same as above except that the vehicle itself generates a new pseudonym after the threshold “*t*” is reached. The difference in both approaches in this scheme is that the use of speed and distance between a vehicle object and RSU is the defining factor in determining the threshold. The bandwidth of the environment is also a factor that is considered to calculate the time. It was assumed that RSUs were equally distributed in the environment (for this example and presented scheme). The reasoning of this scheme suggests that if speed, distance and bandwidth are sufficient with respective categories, changing pseudonyms could be done more often and faster without impacting the overall authentication process of the vehicle object inside the VANET. This would make the current authentication scheme more robust.

As much as authentication is essential, certificate revocation methods must be properly implemented to remove illegitimate users off VANETs. Legitimate infrastructure and vehicle objects can malfunction so false information must be flagged and certificates revoked. The issue with this scheme is the maintenance poses a challenge because revocation lists, also known as CRLs, can be huge and hard to update on traveling vehicles. They might also not have access to RSUs depending on the area (for e.g., rural areas might have unequally distributed road side infrastructure in contrast to urban areas that have RSUs well distributed for constant communication). Compressed Certificate Revocation Lists (RC2RLs) presented by Fuentes, González-Tablas and Ribagorda [9] and Salem, Abdel-Hamid and El-Nasr [23] are the proposed mean for fixing this issue through the use of filters and subsets to speed up revocation lookup and updating revocation lists. This compressed method allows broadcast channels such as Radio Data Systems (RDS) to transmit the information through FM waves. In any case, most vehicles, regardless of their location, have access to radio waves so they can have their certificate revoked if malicious/accidental malfunctions occur. An extended method has also been presented by Zhang et al. [29] in hopes of making certificate revocation more efficient. It introduces a new algorithm that makes uses of a concept called “k-Means” clustering that basically uses nodes and centric points to create groups of vehicles to spread CRLs so that all vehicles are checked against these revocation lists. This scheme also adds two new fields to CRLs, and these are composed of an “Issued Data” and “Credibility” field. The credibility field receives an assigned value of 0 to 100 (0 means non-trustworthy and 100 means credible source) that will be based off how the source is perceived by the vehicular network. It uses correct and historical behaviour as factors in determining if the source is faulty, malicious or credible. The issued date field helps determine how long a certificate has been issued to determine if it should still be valid or not in regards to credibility.

Work shown by Whyte et al. [25] demonstrate the current leading authentication design for V2V communications. This scheme uses a PKI architecture for bootstrapping, provisioning of pseudonym certificates, reporting misbehaviour and certificate revocation. The designed Security Credential Management System (SCMS) used by this design would also allow for safe, reliable and private means of communicating and exchanging BSMs; it is similar in design to its European counter-part V2X PKI infrastructure. The SCMS mechanism would prevent privacy exposures from SCMS insiders and outsiders as well as mitigating false warning. These attacks are prevented with CRLs, constant changing of certificates and dividing operations with organizational separation employed by the SCMS. These work in conjunction with multiple authority figures to ensure efficient operation of the suggested scheme.

Xiong et al. [26] present the use of group signatures to achieve confidentiality and authenticity. In this work, it is shown that vehicles sending messages anonymize themselves for authentication among their respective groups and can only be identified by a trusted authority while doing this efficiently and secretly. To achieve this type of authentication, all vehicles’ OBUs within a group load public parameters from another group entity called the Member Manager (MM) to generate a private key. All private keys are assumed to be stored into their respective vehicle’s safe tamper-proof devices. This allowed the concept of “signcryption”. This concept makes it possible for a group to receive a message from the original sending one and have the sending one’s MM verify the true identity of the sender if dispute arises from the receiving group since it can only identify which group a message originates from. This allows confidentiality requirements to be achieved as well as conditional privacy/anonymity while maintaining efficiency for proper operation. The MM, by then, has all OBUs within the group registered and reveals identities of vehicles when required.

There can also be a dynamic approach to the PKI architecture elaborated by Salem, Abdel-Hamid and El-Nasr [23], which works with vehicles requesting dynamically for keys as they pass RSUs that are retrieved from CAs. The scheme shown in this work helps mitigate non-repudiation attacks, masquerade, man-in-the-middle attacks, Sybil attacks and replay attacks through the use of unique identifiers, nonces and information known between the source vehicle and certificate authority.

Public/private key infrastructures have shown to be effective in traditional networks that do not have much mobility. VPKI schemes show promise for authenticating vehicle objects efficiently with different options, but the amount of calculations and computation required to do this can be time consuming and compromise performance depending on network load and specific scheme used. Sulaiman et al. [24] present a different approach in authentication schemes to validate users on VANETs. They introduce methods that use one-way hashing chain methods or also known as Hashed-Chain based Authentication Protocol (HAP). The method employed by this type of authentication works in the following way:

- RSUs use HAP to generate public/private keys
- These keys are then distributed to newly introduced vehicle objects on the network
- These keys are also paired with a variable sized hash value and proof cipher
- Synchronized clocks employed by this scheme allows vehicles to verify each other using a combination of their respective public with the variable sized hash code

With this mentioned technique, computations are reduced, and authentication has less overhead, which are desirable characteristics in a mobile network. This protocol shows efficiency in regards to computation and processing when vehicle objects would authenticate. Although the PKI method shows more security, HAP does employ constant key changes to ensure randomization so that an attacker would have difficulty compromising key sets for attacks on the VANET. Since the traditional public key infrastructure offers more efficient security standards, HAP could potentially be deployed side-by-side to ECDSA (Elliptic Cryptography Digital Signature Algorithms) methods when delays in the network are inevitable and faster processing is required by the system, similar to a backup to the VPKI. The results shown by Sulaiman et al. [24] are promising and demonstrate that HAP has the potential to become a new method of authentication in VANETs; however, it will unlikely fully replace the already robust PKI architecture.

B. *Availability*

VANETs are mobile networks that require some data (for e.g., BSMs) to be sent and delivered to them in real time since some crucial decisions need to be done by end users. VANETs must be fully operational with barely any downtime if drivers are to become more dependent on them in the case of having the roadside infrastructure evolve and become more efficient. If any network entity was taken offline due to malfunction or lack of processing power, the vehicle objects would be directly affected since RSUs provide important information to vehicles. In a nutshell, availability is firstly about designing a network that is capable of handling the intended and predicted network load, properly processing it and remaining scalable while migrating any type of interference and malicious Denial-of-Service (DoS) attacks, distributed or not. The issue with VANETs is that they deploy prevalent wireless technologies and are therefore more susceptible to DoS attacks since wireless technologies are easier to access and exploit.

The issue with availability is that methods to mitigate these types of attack are harder to implement than it is to find new ways of attacking a network and attempting to block legitimate services, if not all. Kang, Lee and Gligor [11] present a new and ground-breaking type of Denial-of-Service attack that does not take in consideration the physical server it wants to bring down (or service in any case) but indirectly attacks it by forming a target area around it. This attack is called “The Crossfire Attack”. It mainly disconnects services and servers by attacking key links in the infrastructure with the use of layer 3 mapping. This work was presented in a non-VANET environment, but these concepts can be applied the same way since Road Side Units and its infrastructure are not mobile like vehicles. Here is a summary how such an attack works:

1. Select the target area where the desired servers/services are located
2. Select the links to attack (after doing a layer 3 mapping of the target area)
3. Select and attack decoy servers so traffic is directed to the target area and redirect flows from decoy server to the targeted links
4. Attacker then has the rest of the botnet target disjoint target links so that the targeted services/servers lose Internet connection

The employed technique clearly demonstrates how effective it can be in bringing down networks. The most efficient part of this attack is that only decoy servers and services are targeted, which makes it more difficult to pinpoint the source of origin of the attack. These decoy servers could so well spread out that the traffic to them might seem legitimate, but would instead be a target of this indirect Distributed Denial-of-Service attack. The evolution of attacks demonstrate that proper counter-measures must be taken if they are all to be mitigated, especially if attacks can be carried over to different types of infrastructures such as VANETs.

As mentioned above, Denial-of-Service attacks are hard to mitigate but not impossible. Methods do exist in attempts of stopping or rendering them less efficient so that network operations maintain tolerable flow and functionality with minimum requirements. Although the method presented by Abumansoor and Boukerche [1] is for unintended DoS attacks caused by high level congestion of vehicles, the presented concepts can be used to mitigate intended attacks. One way an attacker can deny service to an area or specific victim would be through the use of sending excessive amount of information and probes to the victim(s) and/or surroundings. The amount of cars in the area that send probes for useful information such as localization data and reply to other probes would obviously slow down the network infrastructure if there was an over-saturated amount of information being sent and received from any source, including malicious ones. The method used to counter such means would make use of vehicles using their sensors and acquired neighbour information to determine area congestion. Probing rates would then be adjusted so that network load heavily reduces. This method is entitled Adaptive Group Beaconing shown by Abumansoor and Boukerche [1]. Authority management nodes in charge of monitoring network activity and sending periodic messages can monitor the amount of probing and adjust its periodic message notifications and control Quality of Service (QoS) so that certain applications inside vehicles continue to operate properly regardless of the probing rate in the network. This type of adaptive probing behaviour can positively affect Denial-of-Service mitigation even if it is based off unintentional DoS attacks caused by a congested network.

Since general Denial-of-Service attacks tend to leave heavy traces of network traffic to successfully disable services, existing mechanism can be implemented with Vehicular Ad Hoc Network infrastructures to successfully detect abnormalities inside it. Intrusion Detection Systems (IDSs) make the use of signatures to detect and report attacks and malicious intent to system administrators or automated security service so that action can be taken. Even better would be Intrusion Prevention Systems (IPSs) since they can not only detect malicious attacks but stop them at the same time. The work discussed by Coussement, Bensaber and Biskri [5] demonstrates that these systems can be implemented into the vehicles themselves or into RSUs to ensure safety. There is only one issue with this approach and that is that these systems do not have a control mechanism with VANETs; this would need to be implemented. The employed mechanism presented by this paper would use a probabilistic scheme to determine incoming attacks. Normal behaviour of vehicles and known responses to vulnerabilities would be traced and recorded (in our case, high traffic load and congestion can be added in this probabilistic model to determine whether a DoS attack is occurring). Vehicles, when analyzed, would also be grouped into clusters to get more generalized predictions and behaviour in helping to determine if a vulnerability is exposed or services are being disrupted to targets in the same vicinity. With the use of this protocol/mechanism, IDSs/IPSs could potentially be implemented within VANETs to add more layers of security and rendering it safer. The true way to mitigate Denial-of-Service attacks is to ensure that all traffic is authenticated and that only legitimate users can send information. The use of message capacity mechanisms associated to each vehicle and network object can also be used with previous methods in attempts of mitigating the damages caused by DoS attacks, if not eliminating the threat altogether. The implementation of existing DoS mitigation methods must be considered to help eliminate them in VANETs since availability is crucial.

C. Non-Repudiation

Non-repudiation of origin consists of having vehicles acknowledge that they have sent messages to wherever it is destined. The use of digital signatures is employed to sign all messages that are being sent. The main encryption method employed by VANETs, which is mainly used by the IEEE 1609.2 standard because of high performance and complex cryptographic scheme, is ECC as shown by Fuentes, González-Tablas and Ribagorda [9] and the IEEE Standards Association [10]. This encryption type combined with non-repudiation of origin make it a strong method for sending and verifying messages' signatures. Signature checking isn't the only required step in signature verification: the certificate of the sender must also be checked to ensure that it is valid and isn't part of CRLs. A group signature method has also been suggested to add privacy to the non-repudiation of origin process. Clusters would only send one digital signature to destinations that represents the group that sent it. TPPs are the only entities that would have access in determining individual objects within the source cluster. Non-repudiation of origin allows every vehicle object to be held accountable for all action it performs on the network so this helps identify attackers when attempting to send bogus and/or harmful information, which is flagged by vehicle objects and road side infrastructure. Attackers would need to find a way to retrieve digital signatures or to duplicate another legitimate user's signature so that he/she can impersonate an unsuspecting victim and get away with the attack. Work developed in this area working in conjunction with security standards in all other security related concepts will help identify the sources of attacks so that mitigation is done much more easily and have the hackers held accountable. Strong authentication message as well as credential managements methods must be implemented in the authentication schemes to circumvent this type of vulnerability.

D. Data-Trust

Elliptic Curves Cryptography is the main encryption scheme used by the DSRC protocol for encryption and has proven to be efficient in terms of overall security and computation. Hash-based authentication presented by Sulaiman, Raja and Park [24] shows promise for speed and processing but lacks security compared to proven ECDSAs and other methodologies, such as those used by the 1609.2 standard, for example. ECC, being standardized, makes it hard for attackers to exploit, so data will remain unaltered and trustworthy. Methods shown by Fuentes, González-Tablas, and Ribagorda [9], such as two-direction reporting, threshold-based trust and the use of group signatures, which all incorporate static and dynamic factors, are some methods that can be used to ensure this aspect of security in VANETs.

To ensure that data trust is properly implemented as mentioned above, the correct approach would be to have a framework of trust implemented. Such a framework would greatly improve the performance of trust determination and credibility checks of data being received by vehicles. The work presented by Rostamzadeh et al. [22] proposes the implementation of such a framework called FACT. Successfully implementing this would greatly reduce delays in network communications and maximize performance since trust verification would greatly be minimized. This paper proposes that network segmentation should be implemented based on individual roads, neighbourhoods and road segments, to name a few. Then, depending on known reputation of the area and risk factors, these segmentations would be assigned a trust factor that reflects upon messages a vehicle sends when in a specific area. FACT would then classify all traffic into three categories ranking their overall importance. They are as follows:

- Category A – Holds all the critical infrastructure messages
- Category B – Holds all road side service information
- Category C – Holds all third party service messages

All of these categories employ QoS priorities to ensure that the respective messages are sent accordingly to their respective destinations in regards to their level of trust assigned. For category “A” messages, delay, data integrity and reliability are the key security concepts that must be considered when delivering these messages since the delay with critical information can directly affect a driver’s ultimate reaction and decision in the given framework. Category “B” messages are more concerned with reliability, access control, source anonymity and authentication to ensure the source is legitimate as well as access to the information is available and accurate. Source authentication and reliability are the main security concepts applied to category “C” messages since the third parties must be legitimate and allow message to be delivered efficiently in large numbers. The mechanisms being developed in this area of VANET will directly impact a user’s reaction and decision making process so data trust must be kept under constant check. This field shows that is on the right direction. This framework will further strengthen authentication schemes and underlying data trust protocols so that data being sent and received by legitimate users is trustworthy, authentic and authorized, especially if data trust protocols are supported by robust standardized protocols that employ ECC or other ECDSA methodologies.

E. *Privacy*

Users are legally entitled to know how their provided information will be used, stored and secured when agreeing to use a provided Internet service. Law and regulations have been put in place by some national/regional governments, but these laws vary and are applied in different ways based off the user’s location. Some organizations are enforced to communicate how they will protect the sensitive data and how they are implementing these procedures. The work elaborated by Kosa, Marsh and El-Khatib [12] proposes a framework that will be used to calculate the privacy states that would be automated and used for representing privacy concerns and states in VANETs, which are shown in the figure below. This would then lead to determine how data is collected and handled by its respective regulators across the system. The framework developed by Kosa, Marsh and El-Khatib [12] uses Canadian standards and laws as an example but can be extended to fit other country laws for adaptation into their transportation system’s VANET.

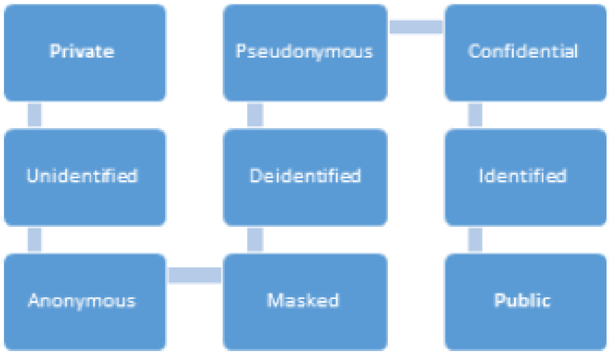

Figure 1. Different privacy states [12]

In Canada, there are multiple legal documents that regulate privacy concerns, what organizations need to do to protect this data, and how to communicate this to the users so they are made aware. The documents are as follows:

- PIPEDA (Personal Information Protection and Electronic Document Act) – covers non-profit organization and the private sector [17]
- Privacy Act – Information collected by the federal Government [19]
- MFIPPA (Municipal Freedom of Information and Protecting Privacy Act) – covers municipal organizations [15]
- FIPPA (Freedom of Information and Protection of Privacy Act) – covers provincial organizations [8]
- PHIPA (Personal Health Information and Protection Act) – covers all health organizations [18]

These acts are used to protect information collected by each respective organization according to their specific criteria that must be followed and, for this specific case, be used in Canada for privacy representation in VANETs. Any other country would adopt their laws and regulation documents with this framework to determine its privacy representation. Five privacy requirements must be respected when organizations collect information in this framework, shown by Kosa, Marsh and El-Khatib [12]. They are as follows:

- Privacy Regulation
- Inter-Jurisdiction

- Model Complexity
- Interoperability
- Access Regulation

The framework would employ a Finite-State-Machine (FSM) to determine what the result of a given communication between two entities would be in when an information transaction occurs. The given framework would help identify what to expect in terms of what type of communications are occurring so that users are made aware of how information is being handled. It basically gives consent on what users are expected to disclose and what users are expecting in regards to what sensitive information is being protected when collected. Privacy in VANETs must have the correct guidelines applied to them and must rely on current technologies and mechanism to ensure that private data is kept safe in accordance to their respective state and ruling government. Any country could adopt this framework to its respective laws and regulations for determining privacy representation for VANETs. Overall, such a framework helps determine privacy evaluation and decision making for end users regarding when and how data is collected/stored by respective governments, and how it would be handled.

III. PROVEN VULNERABILITIES

VANET security shows that there are many mechanisms being developed to ensure that all security concepts are enforced and maintain a standard of efficiency for the operation of vehicular networks. The mechanisms being developed do have specific reasons and are made to fend off many types of attacks that are present and could potentially target a VANET. Work shown by Rawat, Sharma and Sushil [20] demonstrates these types of attacks. Here is a list of network attacks that affect network communications when it comes to V2V and V2I communications:

- DoS attacks – as mentioned above, these attacks can target any specific object within the network in hopes of disrupting network service and functionality so that all operations are delayed or rendered useless with the use of excessive traffic and/or over-utilizing key resources in the infrastructure
- Sybil attacks – also elaborated by Yu, Xu and Xiao [28], Sybil attacks are done when a malicious users impersonates multiple identities hoping to fool legitimate users in taking different routes due to traffic congestion protocols
- Message suppression/alteration/falsification – a malicious user manages to drop legitimate traffic in the network in attempts of falsifying road conditions. Alteration is when legitimate messages are altered to fool legitimate users with incorrect data. Falsification is when an attacker broadcasts false information to influence the traffic to his liking or cause havoc
- Replay attack – legitimate messages are captures and used later in legitimate circumstances for illegitimate means
- GPS spoofing – an attacker falsifies GPS information to fool other vehicles into thinking they are at a different location with his/her own GPS simulator
- Tunneling attack – two physically separated parts of a VANET are connected through a tunnel thinking they are neighbours so an attacker could analyze the traffic of perform selective forwarding attacks
- Timing attack – time slots are altered so that safety critical message are delayed and received after their useful lifetime is outlived
- Man-in-the-middle attack – the attacker is between a legitimate communication session and intercepts traffic to see the content but forwards it to the right end destinations to remain invisible
- Home attacks – malicious user attempts to take control of the vehicle's internal components with the use of the Internet
- ID disclosure – a target's location is disclosed and made publicly available so that anyone can view the location of the vehicle
- Brute-force attack – an illegitimate user attempts to break cryptographic keys used in secure communication sessions

All these types of attacks have the potential of affecting VANETs and end users. That is why security standards are being developed so that all fronts are reinforced and that these attacks greatly reduced, if not rendered completely ineffective. These attacks, if well-coordinated, could also lead to the compromise of internal components if vehicles are lured to specific locations which allow an organized attacker to perform more sophisticated types of attacks.

A different attack has been introduced that basically fully compromises a node in the Vehicular Ad Hoc Network. The work presented by Lin et al. [13] demonstrates that a malicious user attempts to physically capture nodes inside the network. Once physical access is acquired, the adversary implements malware as well as attempts to reveal secret keys so that all communications with compromised nodes are known and traffic is exposed. Privacy concerns also arise as location could then be disclosed, not to mention other attacks could be launched including Denial-of-Service, spamming, Sybil attacks, etc. A compromised node could then affect further nodes attached to it so it can spread into the network and increase its potential regional reach, if not global up until the entire network is compromised. The only downfall to this attack is that physical access is required so some parts of the infrastructure are not reachable (e.g., highway RSUs) and/or publicly exposed; however, if managed correctly and not caught in the act, RSUs that are not easily physically accessible could fall prey to one that is and compromised. This type of attack is dangerous as it enables a platform to launch all mentioned above attack through a seemingly legitimate node of the infrastructure. Overall, many methods are available for attacking a network. Many methods and mechanisms must therefore be deployed and further researched to ensure end user security.

Vehicular Ad Hoc Networks show definite promise in the functionality it is intended to provide. The ability to send information about road conditions, accidents, congestion warnings from indirect neighbours, to name a few, is useful as discussed by Younes and Boukerche [27]. The wireless technology employed to do this is quite efficient in enabling the operations of VANETs, but like any other infrastructure, specifically wireless oriented ones, vulnerabilities to attack the network arise. Rawat, Sharma and Sushil [20] present home attacks that are directed towards taking control of vehicles using, and not limited to, the Internet, so that internal vehicle components are exploited and taken over. Works shown in [4][6][11][14][16] present multiple attack surfaces that are exposed through external components and allow compromise of the internal network components of the vehicle objects. There are many attack vectors that are of the following:

- OBD II port – direct physical access to internal components of the vehicle
- “PassThru” device – Device that connects to OBD II port for analysis of system buses and firmware updates
- Media devices (e.g., MP3s, USBs, CDs, etc.) – direct physical access to internal components of the vehicle
- Bluetooth – short range communications access to internal components of the vehicle
- Cellular – long range communications access to internal components of the vehicle
- Broadcast Channels – long range communications access to internal components of the vehicle

The work presented by Checkoway et al. [4] explains how full vehicle compromise (for e.g., vehicle acceleration and braking, to name a few) was attained and all possible ways they have managed to successfully do it. Figure 2 shows all the multiple attack surfaces. Vehicle objects have shown vulnerability from direct physical access to the vehicle’s OBD II port. If an attacker manages to get access to this port when the driver is not present, he can listen in on the internal network components and debug the communication in attempt of reverse-engineering the internal protocols. The user can use packets that he/she crafts, based off the debug output, to make the vehicle do as he/she pleases. This is the most efficient way of compromising a vehicle, but physical access to the port is hard and is noticeable by users since the car has to be broken into. “PassThru” devices, which are used by vehicle manufacturers, authorized dealerships and mechanic shops, are used to update and gain access to a vehicle’s internal network components (CANs, LINs, FlexRay, etc.). Once this device is connected, they can update and maintain the firmware, which would be periodically done when a vehicle comes in for maintenance schedules and safety checks. These devices can also use wireless communications and allow an untrusted third party to connect to it. When the device connects to the OBD II port, the attacker could gain access to the internal components of the vehicle shown by Checkoway et al. [4]. No authentication checks are done by the internal components when a PassThru device connects to it, meaning anyone connected to the PassThru gains automatic access to the OBD II port. Authentication means would need to be implemented to stop this from happening. An attacker could also upload malicious packages to the PassThru device so that whenever it connects to a vehicle, the files are uploaded to the vehicle to compromise the internal network. This method would allow multiple unsuspecting vehicle objects to be infiltrated. Media devices such as CDs and USB devices can also be used to upload malicious information to vehicles if inserted in the proper access channels. It has been show by Checkoway et al. [4] that if CDs contain malformed audio files, they can update the firmware inside the vehicle through a buffer overflow attack.

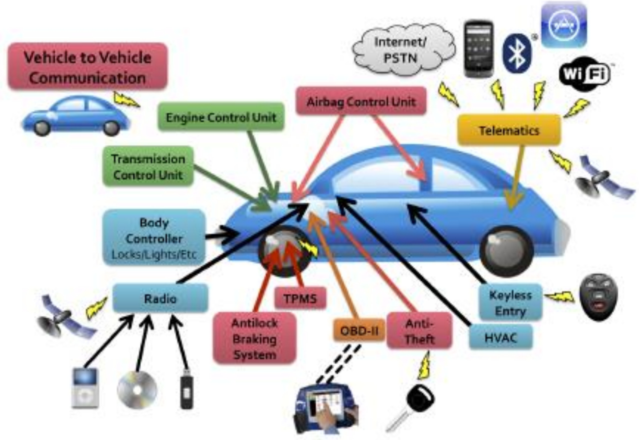

Figure 2. Attacks surfaces in VANETs [4]

Bluetooth has also shown to be a vulnerability inside vehicles. This work demonstrates that through device and car pairing, the vehicle can be compromised. With the use of “Bluesniff”, which is used to sniff and capture Bluetooth MAC addresses, brute-forcing methods can be done to pair to the vehicle. Approximately 9 PINs per minute can be brute forced to pair to a vehicle according to trials successfully made by Checkoway et al. [4]. Although this does not sound like a lot of attempts in the given time frame, this technique could be done in a public garage where thousands of vehicles may be present, brute-forcing one within seconds. This is plausible as tests presented by Checkoway et al. [4], demonstrate that a single vehicle was compromised within 15 minutes. This time significantly reduces when there's more than one vehicle, and, once the device of the attacker is paired to the vehicle, custom applications can be used to gain access to the vehicle's network.

Just like Bluetooth, long range communication means can also be used to exploit buffer overflow vulnerabilities inside the vehicle to fully compromise it. Cellular communication can be used to breach a vehicle's security, which demonstrate how volatile and dangerous wireless communications can be when exploited. AqLink, a protocol used to send and receive voice communication on cellular channels, has been reverse-engineered by Checkoway et al. [4]. This protocol changes analog bits to digital ones so that they can be interpreted by the internal systems. This opens up the possibility of using audio playback to trigger an exploit that was successfully done in the presented research. They were able to phone a remote vehicle that is within cellular range and play an audio file through an audio device, and it compromised the vehicle through a buffer overflow exploit. The issue with this type of attack is that the transmission speed is limited and can only send data at a certain limited rate; a certain amount of data must therefore be delivered before a timeout occurs to trigger the attack. Well-crafted and short code must be done to successfully exploit the vehicle object. Other mediums such as 3G or addressable channels, such as OnStar, allow for faster delivery mechanism with a much bigger payload, but the vehicle must be within range of 3G transmitters to be contacted. Work discussed by Cai et al. [3] shows that Bluetooth can further be exploited with the use of antennas to boost signals and coupling with devices that have more than one antenna (in this case vehicles). The vehicles do not need to be in line of sight, and with the use of multiple antennas, the vehicle object and Bluetooth device can be paired, making it much harder for an attacker of being detected since visual cues are not available. Many attack surfaces exist in vehicles for targeting internal components of vehicles that interact with the vehicular network of this infrastructure, if not targeting the external components of VANETs to launch attacks through them, and many different types of attacks exist. Security standards must be kept under constant revision to ensure that all components are secured and cannot be easily exploited, if not impossible, since security in VANETs is extremely important to ensure end user safety and well-being.

IV. CONCLUSION AND FUTURE WORK

A. Conclusion

There is a little doubt that VANETs offer great potential in the advancement of vehicles and the development of the ITS. The functionality of this network architecture does come at a price since it requires high efficiency with no room for security flaws. Current technologies in authentication, localization, information access and so forth show promise, but better mechanisms must be implemented to ensure that all standards are met. Current research works have shown present alternate solutions with promising potential that will possibly be implemented in future instances of VANETs as its development cycle extends and nears completion. Plenty of vulnerabilities have also been discovered and reported to ensure that none of them are present when VANETs are publicly available to the masses. These vulnerabilities demonstrate to what extent a VANET can be exploited, even to the point of full car control that is unacceptable considering the damage it could cause to the end users. As much as the efficiency of the transportation system would increase if the deployment of VANET was sooner than later, extended research in its security related aspects must be done before being fully implemented.

B. Future Work

Future work from the VANET research community must put emphasis not only on developing security mechanisms to counter all potential vulnerabilities, but also on platforms that could be used by researchers to perform further testing on the internal and external components of VANETs. These types of networks are not as readily available as the more standard Internet architecture platforms so it is important that research goes into developing ways for researchers to be able to directly test potential solutions to VANET issues, security related or not. Work must also be put into testing all these proposed solutions unto larger and scalable models to ensure that the mechanisms work as predicted. It also goes to show that future research must be done to test out all the possible security angles of VANETs since room for vulnerabilities cannot be tolerated. The extent of such work would help ensure the protection of VANET users, which is paramount in an architecture that is directly tied to the transportation system.

ACKNOWLEDGMENT

This work is partially sponsored by NSERC DIVA Research Network grant.

REFERENCES

[1] O. Abumansoor and A. Boukerche, “Preventing a DoS threat in Vehicular Ad Hoc Networks using Adaptive Group Beaconing.” Proc. 3rd Annual DIVA Workshop, NSERC DIVA workshop, 2013, pp. 233-240.

[2] A. Adigun B. A. Bensaber, and I. Biskri, “Protocol of change pseudonyms for VANETs.” Proc. 3rd Annual DIVA Workshop, NSERC DIVA workshop, 2013, pp. 150-155.

[3] L. Cai, K. Zeng, H. Chen, and P. Mohapatra, “Good neighbor: ad hoc pairing of nearby wireless devices by multiple antennas.” in NDSS, 2011.

[4] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, “Comprehensive experimental analyses of automotive attack surfaces.” in USENIX Security Symposium, 2011.

[5] R. Coussement, B. A. Bensaber, and I. Biskri, “Decision support protocol for intrusion detection in VANETs.” Proc. 3rd Annual DIVA Workshop, NSERC DIVA workshop, 2013, pp. 41-47.

[6] L. Ertaul and S. Mullapudi, “The security problems of Vehicular Ad Hoc Networks (VANETs) and proposed solutions in securing their operations.” in ICWN, 2009, pp. 3–9.

[7] C. E. Everett and D. McCoy, “OCTANE: Open Car Testbed And Network Experiments bringing cyber-physical security research to researchers and students.” in Cyber Security Exper. and Test, 2013.

[8] Freedom of Information and Protection of Privacy Act of Canada (2011). [Online]. Available: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm [accessed: May, 2014].

[9] J. M. de Fuentes, A. I. González-Tablas, and A. Ribagorda, “Overview of security issues in Vehicular Ad hoc Networks.” *Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts*, 2010.

[10] IEEE Standards Association, “IEEE guide for wireless Access in vehicular environments (WAVE) architecture,” 2013.

[11] M. S. Kang, S. B Lee, and V. D. Gligor, “The crossfire attack.,” in *IEEE Symposium on Security and Privacy*, 2013.

[12] T. A. Kosa, S. Marsh, and K. El-Khatib, “Privacy representation in VANET.” Proc. 3rd Annual DIVA Workshop, NSERC DIVA workshop, 2013, pp. 48-52.

[13] C. Lin, G. Wu, F. Xia, and L. Yao, “Enhancing efficiency of node compromise attacks in Vehicular Ad hoc Networks using connected dominating set,” *Mobile Networks and Applications*, vol. 18, no. 6, pp. 908–922, Dec. 2013.

[14] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, “Security in Vehicular Ad Hoc Networks.” Communications Magazine, IEEE, vol. 46, no. 4, pp. 88–95, 2008.

[15] Municipilaty Freedom of Information and Protection of Privacy Act of Canada (2007). [Online]. Available: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90m56_e.htm [accessed: May, 2014].

[16] B. Parno and A. Perrig, “Challenges in securing vehicular networks.” in Workshop on hot topics in networks (HotNets-IV), 2005, pp. 1–6.

[17] Personal Information Protection and Electronic Document Act of Canada, (2011). [Online]. Available: http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html [accessed: May, 2014].

[18] Personal Health Information Protection Act of Canada (2010). [Online]. Available: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm [accessed: May, 2014].

[19] Privacy Act of Canada (2014). [Online]. Available: http://laws-lois.justice.gc.ca/eng/acts/P-21/ [accessed: May, 2014].

[20] A. Rawat, S. Sharma, and R. Sushil, “VANET: Security attacks and its possible solutions.,” *Journal of Information & Operations Management*, vol. 3, no. 1, 2012.

[21] C. Rizzo and C. Brookson, “ETSI white paper No. 1 security for ICT – the Work of ETSI.,” ETSI, 2014.

[22] K. Rostamzadeh, H. Nicanfar, S. Gopalakrishnan, and V. C. M. Leung, “A context-aware trust-based communication framework for VNets.” Proc. 3rd Annual DIVA Workshop, NSERC DIVA workshop, 2013, pp. 156-161.

[23] V A. H. Salem, A. Abdel-Hamid, and M. A. El-Nasr, “The case for dynamic key distribution for PKI-based VANETS,” *International journal of Computer Networks & Communications*, vol. 6, no. 1, pp. 61–78, Jan. 2014.

[24] A. Sulaiman, S. V. Kasmir Raja, and S. H. Park, “Improving scalability in vehicular communication using one-way hash chain method,” Ad Hoc Networks, vol. 11, no. 8, pp. 2526–2540, Nov. 2013.

[25] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, “A security credential management system for V2V communications,” in *Vehicular Networking Conference (VNC), 2013 IEEE*, 2013, pp. 1–8.

[26] H. Xiong, G. Zhu, Z. Chen, and F. Li, “Efficient communication scheme with confidentiality and privacy for vehicular networks,” *Computers & Electrical Engineering*, vol. 39, no. 6, pp. 1717–1725, Aug. 2013.

[27] M. B. Younes and A. Boukerche, “Efficient traffic congestion detection protocol for next generation VANETs.” Proc. 3rd Annual DIVA Workshop, NSERC DIVA workshop, 2013, pp. 208-212.

[28] B. Yu, C.-Z. Xu, and B. Xiao, “Detecting Sybil attacks in VANETs,” *Journal of Parallel and Distributed Computing*, vol. 73, no. 6, pp. 746–756, Jun. 2013.

[29] Q. Zhang, M. Almulla, Y. Ren, and A. Boukerche, “An efficient certificate revocation validation scheme with k-means clustering for Vehicular Ad Hoc Networks.” Proc. 3rd Annual DIVA Workshop, NSERC DIVA workshop, 2013, pp. 249-254.