Securing Vehicular Networks with VIBES

Samuel C. Nelson and Robin Kravets
Department of Computer Science
University of Illinois at Urbana–Champaign
snelso20@cs.uiuc.edu, rkh@cs.uiuc.edu

ABSTRACT
One of the biggest challenges in making vehicular networks a reality is security. Aside from the clear need for vehicles to be able to authenticate messages from certain personnel, such as police officers and ambulances, secure end-to-end communication will also benefit numerous distributed applications that will be running over these vehicular networks.

In this paper, we argue that four design goals must be met for any feasible VANET security system: it must (1) be scalable and allow for correct and efficient authentication, encryption, and key distribution and revocation, (2) be delay tolerant, (3) be DoS resistant, and (4) utilize existing infrastructure in a fashion such that it is readily deployable today, with minimal infrastructure changes. We present and analyze VIBES, a system using Identity-based Encryption and Signatures that meets these design goals and addresses much of the practical issues surrounding the implementation of a vehicular network security system. Furthermore, we show a performance evaluation comparing it to popular certificate-based schemes.

1. INTRODUCTION
Vehicle technology in the near future will look vastly different than it does today. As vehicles become equipped with short-range radios, large scale vehicular networks will enable numerous vehicle-based distributed applications. Characteristics of this network will include both areas of high connectivity and density, resembling a highly connected ad hoc network, as well as areas of intermittent connectivity and partitioning, resembling a delay tolerant network. The environment will therefore be highly dynamic and very large.

This technology will enable new communication options for companies and individual users. One important set of applications include end-to-end vehicle-to-vehicle communication. As an example, consider a trucking company wishing to utilize this network to collect and disseminate data to their trucks for automated route planning or other “smart car” functionality. Individual trucks could automatically and periodically, with no user intervention, contact other trucks along possible paths and obtain real-time road conditions, traffic reports, and weather conditions which aid in the route planning process. This periodic data will allow the on-board computer to make educated guesses when planning the optimal route. For application such as these, end-to-end vehicular communication is ideal. In many cases, VANETs are a cost-efficient alternative to cellular technology.

Due to the shared, open nature of the network, practical end-to-end security must be available to prevent malicious entities from interrupting or stealing confidential business or individual information. Faking trucker identities or editing in-transit data can, depending on what materials or information the truck may be carrying, have devastating results.

Therefore, practical end-to-end security is necessary to support upcoming distributed applications.

Since vehicular networks are still in the design phase, it is important to integrate them with effective security solutions. We identify four main requirements for supporting security for distributed applications running over VANETs, which provide the minimum functionality for deploying these networks today. First, the system must provide efficient, manageable, and correct authentication and encryption, as well as key distribution and revocation. Second, it must be delay and disruption tolerant, since many sparse portions of the VANET will likely have intermittent connectivity. Third, the system must be resistant to denial of service attacks. Fourth, the system must utilize existing infrastructure, where infrastructure is both information (e.g., license plate numbers) and physical objects (e.g., existing car radios), in a fashion that is readily deployable today, or in the very near future, with little infrastructure-based upgrades.

Although not specific to security solutions, utilizing current infrastructure is important for the rapid, near-term deployment of distributed applications. For about a decade, highways and mass transit have been part of the United States’ critical infrastructure [9]. The result of this, as well as much attention in the private industry, indicates that security must be an integral part of vehicular networks from the start, and hence must rely on the current infrastructure to support these applications. However, there is little practical end-to-end security work for vehicular networks that could be deployed in the near-term.

In this paper, we present VIBES (Vnet with Identity-Based Encryption/Signatures), an end-to-end security system that provides manageable authentication and encryption to both centrally distributed and peer-to-peer applications. The novelty of VIBES comes from the integration of Identity-Based Encryption (IBE) and Identity-Based Signatures (IBS), as opposed to other popular techniques like Public Key Infrastructure, into the existing transportation and communication infrastructure. VIBES, utilizing IBE, fits very well into vehicular networks, since it offers a high level of security while providing some delay tolerance and denial of service protection. Since public keys in VIBES are inherently bound to user identification, no certificate is required to authenticate a foreign party. VIBES also introduces a novel key revocation and restoration scheme that uti-
lizes both time-based keys as well as wide-area radio broadcasts. Additionally, by utilizing the existing infrastructure, VIBES will be deployable in the very near future.

The remainder of this paper is organized as follows. Section 2 goes into depth about VANET security design decisions and goals. Section 3 describes our approach to security using IBE, including how authentication, encryption, and key distribution and revocation are performed. Section 4 provides a realistic performance evaluation comparing our approach to a popular CA-based scheme. Related work is presented in Section 5. Finally, Section 6 concludes.

2. SECURING VEHICULAR NETWORKS

The basis for any secure vehicular network starts with effective mechanisms for providing adequate levels of security in a scalable fashion [6]. This necessarily includes the ability to efficiently distribute and revoke keys. Furthermore, since the density of vehicles in any area is far from evenly distributed, many partitions will exist at any given time. Therefore, security solutions in these environments must operate despite unpredictable delays and disruptions. Finally, security systems must be readily deployable with existing infrastructure.

2.1 Trustworthy, Scalable Systems

The security infrastructure in vehicular networks must provide an adequate level of security as well as be scalable. Symmetric-key based cryptosystems using pairwise shared keys between all nodes quickly become infeasible due to scalability as well as key distribution issues. While public key cryptosystems do not suffer from such scalability problems, not all public key solutions are applicable to vehicular networks. In the rest of this subsection, we discuss the main public key approaches and in the next two subsections discuss how well suited they are for vehicular networks.

PKI (public key infrastructure) approaches are the most popular popular public key cryptosystem and are widely used on the Internet. Certificate authorities (CAs) are responsible for issuing certificates to individuals that allow parties who trust the CA to authenticate one another. Centralized PKI is in wide-spread use, is scalable (popular examples include VeriSign [2] and Thawte [1]), and provides high levels of security. Distributed PKI (e.g., COCA [15]) can also be used to lessen the load of a centralized server, while remaining quite scalable and providing strong levels of security. Here, a node is required to contact at least $k$ of these $n$ CAs (referred to as the cryptographic threshold) to perform general certificate operations.

Identity-Based Encryption (IBE) provides a means of eliminating certificates altogether, and was proposed in 1984 [12]. IBE uses alphanumeric strings that are well-known or easy to obtain through out-of-band channels (e.g., email addresses or, in our case, license plate numbers) as public keys. These keys are assumed to be inherently bound to parties’ identities such that the certificate “look-up step” is not required. When a user joins the network, it contacts a private key generator (PKG) and obtains a private key for the chosen public key. To communicate with any party, one simply has to recall the party’s identity to verify their signature. This technique provides high levels of security and is centralized via the PKG, and so, sufficiently scalable.

In decentralized web-of-trust based systems, like PGP [16], trust chains are not signed by any trustworthy centralized servers, but rather signed by individual clients that vouch for another party in a transitive fashion. Since this type of approach removes the centralized, trusted component, the level of security may be compromised. Therefore, decentralized web-of-trust systems are not appropriate for vehicular network applications that require high levels of security.

2.2 Disruption Tolerance

A security system for VANETs must have some degree of disruption tolerance. The rational for this design decision is that any network formed over vehicles will be heavily partitioned due to vastly different vehicle densities in any given area. It is clearly advantageous to be able to communicate within one connected component without having to first communicate with parties outside of the partition.

Centralized PKI solutions clearly fail in partitioned networks. When two unauthenticated nodes wish to communicate, look-up steps must be performed for both nodes to obtain the other’s public key in a trustworthy fashion. Unless the nodes are in the same partition as the CA, they will not be able to perform these lookup steps. This issue is realized in literature as a solid reason to not use centralized PKI as a security solution for intermittently connected networks [11]. While distributed PKI alleviates the problem slightly, since there are more CAs that can be contacted, there would have to be $k$ of the $n$ total CAs in each foreseeable partition to eliminate the problem. This is not feasible for many reasons, one being that partitions are dynamically created. In comparison, IBE works well in intermittently connected environments since the lookup steps are eliminated.

2.3 DoS Resistance

A third characteristic of any practical vehicular network security system is denial-of-service resistance. If an attacker is able to deny service in security-related lookup steps, such as preventing certificates or certificate revocation lists from propagating, then they can cripple the entire system.

A DoS attack on a relatively small portion of the network should not cause the entire network to suffer substantially. In the centralized PKI approaches, attacks launched at nodes near the CA may prevent communication to and from the CA, severely limiting network functionality. While centralized PKI is not DoS resistant, distributed PKI may be since an attacker must affect a larger number of nodes $(n-k+1)$ to cripple the network. IBE is DoS resistant during normal operations since the lookup step is removed. There are cases, however, where IBE must be secured against DoS attacks. Two of these operations are obtaining a private key from the centralized (or possibly hierarchical) PKG, as well as obtaining public key revocation lists. In Section 3, we discuss how to make these operations DoS resistant in vehicular networks.

2.4 Utilization of Existing Infrastructure

For deployment purposes, a security approach should utilize as much of the existing infrastructure as possible, so as to not demand major infrastructure changes and to allow the system to be practical and monetarily attractive. Minimal or no changes to the infrastructure allow the system to be implemented in the near-term without major investments by corporate or government parties.

Centralized PKI solutions require centralized infrastructure capable of communicating with the vehicular network
and quickly processing requests on-the-fly. While this is not a large infrastructure change, it does constitute a certain amount of investment. However, the major disqualification of centralized PKI fall within the first two design goals. Distributed PKI, on the other hand, requires a much larger infrastructure investment, since multiple CAs must be installed and maintained. Furthermore, out-of-band channels must be set up or purchased for the CAs to communicate, assuming their control and management channels are not, for security reasons, traveling over the ad hoc vehicular network. In this case, the monetary investment as well as the infrastructure change may be significant.

In IBE-based solutions, we show it is possible to keep infrastructure change to a minimum by utilizing existing infrastructure as much as possible. While a PKG must be setup, it does not have to process requests in real-time and can be contacted out-of-band. The two popular means of revocation, particularly expiration of time-based keys and revocation lists, can also utilize existing infrastructure. For instance, wide broadcasts of revocation lists can be done via existing radio towers and/or satellites with vehicles using standard antenna for reception, as shown in Section 3.

In summary, IBE offers the best characteristics to quickly and practically deploy, and use a vehicular network security system. Therefore, the design of VIBES is based on IBE as a fundamental building block.

3. A SECURITY SYSTEM USING IBE

VIBES is designed primarily for standard communication between applications and users in a vehicular network. VIBES is scalable, and secure, while being both denial of service resistant and usable in intermittently connected networks. Furthermore, it offers quick key revocation and key restoration. Therefore, public keys, which are inherently bound to IDs, and in our case license plate numbers, can be safely restored and reused after compromise due to the use of the time-based key structure. In this section, we first present a threat model that describes the power of an attacker, and then present a detailed description of VIBES.

3.1 Threat Model

To highlight the effectiveness and limitations of VIBES, in this section we present a realistic threat model.

We assume that a malicious attacker has the ability to: (1) read and store all data transmitted across the wireless medium, without repercussion, (2) physically compromise one or more nodes (i.e., vehicles) in the network, with the stipulation that proper authorities (i.e., police) will be quickly (but not instantly) notified of the compromise, and (3) obtain any sensitive cryptographic information, including stored keys, from physically compromised nodes.

However, the attacker cannot compromise entities that are not part of the standard vehicular network. In the case of IBE, this involves private key generators (PKG) and standard radio towers. It also cannot jam a large portion of a dedicated, police-monitored radio frequency.

3.2 VIBES Public Keys

In VIBES, standard vehicle-to-vehicle authentication and/or encryption is done via IBE. IBE allows any alphanumeric string to act as a public key, while the corresponding private key is mathematically generated and distributed by a private key generator (PKG). In VIBES, a public key for a vehicle is the vehicle’s license plate number. When a vehicle wishes to send an authenticated message to another vehicle, the sending vehicle digitally signs it with the private key obtained from the PKG. The receiving node, knowing the identity of the sender and hence the sender’s public key, can verify the signature using the sender’s public key. Note that the only “lookup step” required is to obtain a private key from the PKG. This, however, can be done off-line or, in the case of time-based keys, pushed from the PKG.

In VIBES, public keys are the concatenation of the State, license plate number, and current day, month, and year. The first two components guarantee that public keys are unique throughout the nation (a country code could be added to make this system world-wide), and the time component allows the key to be time-based, which is used for the property of key restoration. For example, a public key for a vehicle registered in California may look like:

California.123.ABC.25/5/2010

This public key format allows for existing infrastructure to be utilized, meaning there is no need for extra information such as electronic license plate numbers.

In VIBES, public keys expire every day and hence new private keys must be pushed from the PKG to every vehicle every day. This, however, is clearly infeasible. Therefore, we introduce the concept of an Annual Key Card (AKC) that contains a set of 365 private keys, one for each day of the year. We envision these AKCs being obtained out-of-band during annual visits to vehicular organizations such as Motor Vehicle Services. These AKCs will be simple USB cards that can interface with the on-board computer in a way that a human can easily load the day’s key into the vehicle. Note that this requires little to no infrastructure change since USB sticks are inexpensive and can easily hold 365 private keys.

3.3 Key Revocation and Restoration

The key revocation is a fundamental issue with IBE, since public keys are inherently bound to identities. For this reason, it is common to use time-based public keys that expire. This allows the period of compromise to be limited to the current time slice. However, we view this solution as unacceptable since there is still a non-negligible period of time where an attacker can do substantial damage via “identity theft”. Therefore, to meet the design goal of being secure, VIBES uses key revocation broadcasts that are able to be sent in a reasonable amount of time after a compromise.

VIBES utilizes the existing infrastructure of radio towers (and/or satellite radio) and vehicle antennas to immediately broadcast key revocations and “key un-revocations” over a dedicated channel. Every time police are informed of a stolen car, that license plate number is sent over the dedicated radio station. To give a perspective of the amount of data that will need to be sent using this scheme, in 1997 the FBI estimated that there was a car stolen in America once every 23 seconds [3]. It therefore seems feasible that revocation lists for the current day would introduce a minimal amount of processing overhead for vehicles. Determining the frequency of these broadcasts is left for future work. Once a vehicle learns of a revoked license plate or public key, it does not send data to that vehicle. This technique does require a little infrastructure change. A second antenna is needed per vehicle tuned to the dedicated frequency. Additionally,
radio towers need a way to receive revocation lists, which is quite feasible via satellite radio broadcasts to radio receivers in the towers.

VIBES utilizes the time-based keys for key restoration. We define key restoration as the process of allowing the reuse of the same public identifier after that identifier has been compromised. This is an attractive property for VIBES since one does not have to give up one’s identity (e.g., public key, or license plate in our case), after compromise. Furthermore, while it is not acceptable to wait for some non-negligible period of time for a key to be revoked, it generally is acceptable to wait for a period of time for a key to be restored. When a compromised (e.g., stolen) vehicle is recovered, the owner may immediately use the same public key (assuming the AKC was not compromised). In the case that the vehicle was returned on the same day, the owner would have to wait until the end of the day, since the daily private key may still be compromised. A “key un-revocation” can be immediately issued to the network via the same broadcast mechanism as key revocations.

Note that this is a different, and somewhat reverse, approach than that which is common. Time-based keys are generally used for key revocation, and the concept of key restoration is often overlooked. We propose that time-based keys be used for the less time-critical step of restoration, and immediate broadcasts should be used for the more time-critical step of revocation. For key restoration to properly occur, we do not recommend preloading all of the keys into the vehicle. This is because if a vehicle is compromised, key restoration will not be able to occur until the end of the year, although the key will still be revoked immediately.

The aforementioned use of a license plate-based public key scheme, as well as VIBES’ approach to key revocation and restoration, makes VIBES both delay tolerant and DoS resistant. VIBES is delay tolerant since the PKGs must only be contacted once a year, and not during live message exchanges. Furthermore, with the prominence of radio towers and the wide coverage of satellites, it is unlikely that many vehicles will be unable to receive messages from the dedicated channel. The system is also DoS resistant since the PKGs are contacted out-of-band, and our threat model assumes attackers cannot jam a large area of the dedicated frequency without being detected.

4. PERFORMANCE EVALUATION

The primary goal of our evaluation is to gauge the performance benefits of IBE (the basis for VIBES), compared to a standard certificate authority (CA) scheme. Our evaluation shows that IBE always performs better than standard CA schemes in terms of message delivery ratio and message delay, as expected. We were particularly interested in the potential of an IBE scheme, compared to a CA scheme. The performance benefits of IBE become very large as the network becomes more disconnected.

To evaluate the performance of IBE against a standard CA scheme, we capture both the message delivery ratio as well as the average message delay for the authenticated messages that were delivered. As an additional metric supporting the hypothesis that a CA scheme results in high message delay, especially in poorly connected environments, the CA-based scheme is evaluated using the average message delay for messages from a source whom the destination has not yet seen and so does not have a certificate for. This metric indicates how long it takes for the first message sent from a source to a destination to be received and verified.

To highlight the benefits of IBE in an intermittently connected network and to test our second design goal of being delay tolerant, it is interesting to evaluate both metrics over the level of connectivity in the network. To capture and control the connectivity level in the network, the transmission range of the nodes is adjusted, decreasing it to obtain less connected scenarios and increasing it to obtain more connected scenarios. We use the Spray and Wait [13] routing protocol to route data through the network, since it is a delay tolerant networking protocol and much better suited for intermittently connected networks than standard MANET routing protocols (such as AODV [7] and DSR [4]).

Simulations are executed using the ONE [5] DTN simulator. Each datapoint is an average of 10 runs with a 95% confidence interval. All simulations are performed using 100 vehicles (with the addition of a stationary CA node in the CA set) traveling over true roadway paths, in a random fashion, in a 4.5km by 3.4km section of Helsinki, Finland. Vehicle speeds vary between 10km/hr and 50km/hr. Every vehicle generates 1 message per minute of size 20kB destined for another random vehicle. Vehicles are equipped with 5MB of buffer space. Packets are generated for the first 1800 seconds of the total 3600 seconds in a simulation.

In the IBE scheme, when a destination first obtains a message from a sender, it immediately verifies the message without having to contact a CA. In the CA scheme, a sender generates a message and transmits it to the destination. Upon reception, the destination checks to see if it has a proper certificate for the source. If so, the destination verifies the message at that time. If not, the destination sends a certificate request to the CA and buffers the message. If a certificate request for that source is already outstanding, the destination does not send a further request. When the appropriate certificate is received, the vehicle attempts to authenticate any buffered messages from the source and stores the certificate in a certificate list. We estimate the size of certificate requests to be 4kB, and certificate replies to be 1kB.

The IBE scheme strongly outperforms the CA scheme in both message delivery ratio and average message delay. In terms of message delivery ratio, IBE operating at the lowest level of connectivity (tx range of 8 meters) outperforms the CA scheme even at a very high level of connectivity (transmission range 128 meters). This is illustrated in Figure 1a. Furthermore, in low levels of connectivity, the CA scheme virtually collapses with less than a 30% delivery ratio, while the IBE scheme remains at higher than an 80% delivery ratio. This illustrates the delay tolerance of IBE and the delay intolerance of CA-based schemes.

For average message delay, a similar trend occurs. In lower connectivity environments, IBE greatly outperforms the CA scheme, delivering messages with lower delay. In higher connectivity environments, we notice improvements in both IBE and CA schemes, with IBE always performing better (see Figure 1b). Finally, when the destination does not have a certificate for the source in the CA scheme, the average message delay of the first message is extremely high. Only the CA scheme is shown here, because for the IBE scheme, the first message is no different than any other message in terms of latency, and hence results will be similar to that of Figure 1b. These results show that IBE has a higher performance potential than CA-based schemes.
5. RELATED WORK

The specific use of IBE in securing vehicular networks has been briefly proposed in the literature, although most of this work only suggests the idea and provides little or no details of how to design and deploy such a system. One particular system, VDTLS [8], was developed specifically for vehicular networks. It, however, introduces new infrastructure, named Roadside Equipment (RSE), as well as requires servers to run in network infrastructure. For this reason, we believe it is not readily deployable. Raya et. al. have proposed a Vehicular Public Key Infrastructure in which keys are uploaded and bound to an Electronic License Plate (ELP) [10]. However, this approach is not complete and faces many challenges including revocation, since keys are uploaded for a long period of time, CAs and what their role would be in message-to-message authentication, and denial of service attacks. Furthermore, it requires the deployment of new infrastructure, ELPs. In contrast to current solutions, VIBES was designed from the beginning to extensively utilize existing infrastructure and not require major infrastructure changes.

The use of existing infrastructure in vehicular networks has been briefly touched upon in literature. Yan et al. prevent Sybil and position-based attacks by using on-board radar, which is available in some vehicles today and probably most in the future, as an “eye” to verify claimed GPS positioning data [14]. By using data obtained from radar, along with neighbor reports, vehicles attempting to fake position information can be caught. This is a useful technique; however, it does not concentrate on general authentication, only secure position information.

6. CONCLUSION

In this paper, we present VIBES, a means of securing vehicular networks using Identity-based Encryption. VIBES was developed to be secure, scalable, and efficient; delay tolerant; DoS resistant; and easily integrated with existing infrastructure. In the future, we plan to fully develop and implement VIBES in a semi-transparent fashion, as clean and functional application layer API. This will allow distributed applications easy access to security. Furthermore, we plan to explore more in-depth how the vehicular network can securely transport key revocation lists when vehicles are out of radio tower range, but still connected to the vehicular network. Finally, we plan to explore different proposed routing options, including delay-tolerant network routing, to better understand the interplay between the routing layer and VIBES, allowing for fine-tuned optimizations.

7. REFERENCES