A Review on Security and Challenges for Vehicular Ad Hoc Networks

Manjunath P S¹, Narayana Reddy²
¹Dept. of Telecommunication Engineering, BMS College of Engineering
²Dept. of Electronics and Communication, S V U College of Engineering

Abstract— Vehicular Ad-hoc Networks (VANETs) are the most prominent enabling network technology for Intelligent Transportation Systems (ITS). VANETs provide many new exciting applications and opportunities albeit transportation safety and facilitation applications are their core drivers. Security of vehicular networks remains the most significant concern in VANETs deployment – because it is mandatory to assure public and transportation safety. In this paper, we review the various dimensions of VANETs security including security threats, challenges in providing security in vehicular networks environment, requirements and attributes of security solutions. We also provide taxonomy and critically review of the notable security solutions – available for VANETs in literature.

Keywords— Vehicular Ad-hoc Networks (VANETs), Intelligent Transportation Systems (ITS)

I. INTRODUCTION

The development of intelligent transportation systems (ITS) is due to the inherent human desire for change, progress, mobility, entertainment, safety and security and so Vehicular Ad-hoc networks are the most prominent enabling technology for ITS. The participating nodes in VANET communication networks (i.e. vehicles) interact and cooperate with each other by short-range direct communications, by anticipating messages through vehicles (Vehicle-to-Vehicle) and road side posts (Vehicle-to-Infrastructure). Conventionally, information about traffic on a road is only gained through inductive loops, cameras, roadside sensors and studies. VANETs offer new locations for collecting real time information— from onboard sensors on vehicles and its quick distribution. The information collected through individual vehicles participating in the network can be integrated together to form a real time picture of the road situation. Many new applications have been enabled through VANETs, though safety and transportation efficiency applications are the most important driver for them. The various ITS stakeholders such as governments, tele-communication companies and car manufacturers are working together to make “VANET based ITS” a reality.

Hundreds of projects are in progress in the United States, Europe, Japan, China, India and other countries of the world, supporting the cause with research, innovation, testing and correction activities [1][2]. It is predictable – up till 2015 – that software and electronics will cover 50% of the total cost of an automobile [9]. Today, automobiles are fully equipped with IT and software technologies. However, these systems are not mainly concentrating on security aspects. Fig. 1 shows a view of Vehicular Ad Hoc Network.

Fig. 1: Vehicular Ad Hoc Network

On the other hand, Vehicular ad hoc networks are mainly designed for safety applications (to ensure the safety of drivers and vehicles and also to avoid or minimize the road accidents). VANET is a special type of Mobile ad hoc networks (MANET) [5] customized for automobiles with some distinctive features e.g. predictable mobility patterns, movement of nodes along predefined paths instead of random directions. There are no battery constraints in VANET therefore it is suitable for long range communications through vehicles. In addition to safety applications, various other applications like collision avoidance, traffic management, trip planning and infotainment are also developed for them [6]. Safety applications must be protected from hackers and crafty attacker because a compromised safety application could result in the loss of human life [8].
Commercial applications need security to protect the potential loss of revenue. Without security, a Vehicular Ad hoc network can be affected by many attacks like denial of service, message suppression and propagation of false message attacks etc. that may cause accidents.

Our focal point in this survey paper is to indicate and underline the major security issues, threats, core requirements & challenges to design a fail-safe security framework.

The rest of the paper is organized as follows. Section 2 summarizes the major security threats in VANET landscape. In section 3, we enlist the background challenges for designing the security frameworks for vehicular networks. Finally, we conclude the survey in section 4 with a few possible future directions.

II. MAJOR SECURITY THREATS IN VANETS

There exist number of security threats & attacks which are quite non-trivial for VANETs due to open wireless nature. The security of VANETs is crucial as their very existence relates to critical life threatening situations. It is imperative that vital information cannot be inserted or modified by a malicious person. The system must be able to determine the liability of drivers while still maintaining their privacy.

These problems are difficult to solve because of the network size, the speed of the vehicles, their relative geographic position, and the randomness of the connectivity between them.

An advantage of vehicular networks over the more common ad hoc networks is that they provide ample computational and power resources. For instance, a typical vehicle in such a network could host several tens or even hundreds of microprocessors [2]. Raya et al. [1] classify attackers as having three dimensions: “insider versus outsider”, “malicious versus rational”, and “active versus passive”. The types of attacks against messages, can be described as follows: “Bogus Information”, “Cheating with Positioning Information”, “ID disclosure”, “Denial of Service”, and “Masquerade”. The reliability of a system where information is gathered and shared among entities in a VANET raises concerns about data authenticity. For example, a sender could misrepresent observations to gain advantage (e.g., a vehicle falsely reports that its desired road is jammed with traffic, thereby encouraging others to avoid this route and providing a less congested trip). More malicious reporters could impersonate other vehicles or road-side infrastructure to trigger safety hazards. Vehicles could reduce this threat by creating networks of trust and ignoring, or at least distrusting, information from untrusted senders.

2.1. Threats to availability, authenticity, and confidentiality

Attacks can be broadly categorized into three main groups: those that pose a threat to availability, those that pose a threat to authenticity and those that pose a threat to driver confidentiality. The following sections present threats posed to each of the areas of availability, authenticity, and confidentiality.

2.1.1 Threats to availability

The following threats to the availability of vehicle-to-vehicle and vehicle-to-roadside communication (including routing functionality) have been identified:

- **Denial of Service Attack**: DoS attacks can be carried out by network insiders and outsiders and renders the network unavailable to authentic users by flooding and jamming with likely catastrophic results. Flooding the control channel with high volumes of artificially generated messages, the network’s nodes, onboard units and roadside units cannot sufficiently process the surplus data.

- **Broadcast Tampering**: An inside attacker may inject false safety messages into the network to cause damage, such as causing an accident by suppressing traffic warnings or manipulating the flow of traffic around a chosen route.

- **Malware**: The introduction of malware, such as viruses or worms, into VANETs has the potential to cause serious disruption to its operation. Malware attacks are more likely to be carried out by a rogue insider rather than an outsider and may be introduced into the network when the onboard units and roadside units receive software and firmware updates.

- **Spamming**: The presence of spam messages on VANETs elevates the risk of increased transmission latency. Spamming is made more difficult to control because of the absence of a basic infrastructure and centralised administration.

- **Black Hole Attack**: A black hole is formed when nodes refuse to participate in the network or when an established node drops out. When the node drops out, all routes it participated in are broken leading to a failure to propagate messages.

2.1.2 Threats to authenticity

Providing authenticity in a vehicular network involves protecting legitimate nodes from inside and/or outside attackers infiltrating the network using a false identity, identifying attacks that suppress, fabricate, alter or replay legitimate messages, revealing spoofed GPS signals, and impede the introduction of misinformation into the vehicular network. These include:
International Journal of Emerging Technology and Advanced Engineering

• **Masquerading:** Masquerading attacks are easy to perform on VANETs as all that is required for an attacker to join the network is a functioning onboard unit. By posing as legitimate vehicles in the network, outsiders can conduct a variety of attacks such as forming black holes or producing false messages.

• **Replay Attack:** In a replay attack the attacker re-injects previously received packets back into the network, poisoning a node’s location table by replaying beacons. VANETs operating in the WAVE framework are protected from replay attacks but to continue protection an accurate source of time must be maintained as this is used to keep a cache of recently received messages, against which new messages can be compared.

• **Global Positioning System (GPS) Spoofing:** The GPS satellite maintains a location table with the geographic location and identity of all vehicles on the network. An attacker can fool vehicles into thinking that they are in a different location by producing false readings in the GPS positioning system devices. This is possible through the use of a GPS satellite simulator to generate signals that are stronger than those generated by the genuine satellite.

• **Tunneling:** An attacker exploits the momentary loss of positioning information when a vehicle enters a tunnel and before it receives the authentic positioning information the attacker injects false data into the onboard unit.

• **Position Faking:** Authentic and accurate reporting of vehicle position information must be ensured. Vehicles are solely responsible for providing their location information and impersonation must be impossible. Unsecured communication can allow attackers to modify or falsify their own position information to other vehicles, create additional vehicle identifiers (also known as Sybil Attack) or block vehicles from receiving vital safety messages.

• **Message Tampering:** A threat to authenticity can result from an attacker modifying the messages exchanged in vehicle-to-vehicle or vehicle-to-roadside unit communication in order to falsify transaction application requests or to forge responses.

• **Message Suppression/Fabrication/Alteration:** In this case an attacker either physically disables inter-vehicle communication or modifies the application to prevent it from sending to, or responding from application beacons.

• **Key and/or Certificate Replication:** Closely related to broadcast tampering is key management and/or certificate replication where an attacker could undermine the system by duplicating a vehicle’s identity across several other vehicles.

The objective of such an attack would be to confuse authorities and prevent identification of vehicles in hit-and-run events.

• **Sybil Attack:** Since periodic safety messages are single-hop broadcasts, the focus has been mostly on securing the application layer. For example, the IEEE 1609.2 standard does not consider the protection of multi-hop routing. However, when the network operation is not secured, an attacker can potentially partition the network and make delivery of event-driven safety messages impossible.

2.1.3 Threats to confidentiality

Confidentiality of messages exchanged between the nodes of a vehicular network are particularly vulnerable with techniques such as the illegitimate collection of messages through eavesdropping and the gathering of location information available through the transmission of broadcast messages. In the case of eavesdropping, insider and/or outsider attackers can collect information about road users without their knowledge and use the information at a time when the user is unaware of the collection. Location privacy and anonymity are important issues for vehicle users. Location privacy involves protecting users by obscuring the user’s exact location in space and time. By concealing a user’s request so that it is indistinguishable from other users’ requests, a degree of anonymity can be achieved.

III. VANET RESEARCH CHALLENGES

In this section, we discuss some of the VANET-related research challenges that still need further investigation and innovative solutions to enable VANET infrastructures, communications, security, applications, and services.

3.1 Routing protocols

Routing plays an important role in VANET applications but the high-speed mobility of vehicles and their rapidly changing topology results in conventional MANET routing protocols being inadequate to efficiently and effectively deal with this unique vehicular environment as intermediate nodes cannot always be found between source and destination and end-to-end connectivity cannot always be established. This has prompted researchers to find scalable routing algorithms that are robust enough for the frequent path distributions caused by vehicle mobility [4, 5, 6], new and novel approaches that can deliver improved throughput and better packet delivery ratio [3, 4]. Sun et al. [4] propose a novel vehicular ad hoc routing protocol that utilizes both Zone Routing Protocol (ZRP) and Global Positioning Information (GPSR).
Using the history cache to store the movement information of intra-zone vehicles and destination location information, the proposed routing protocol can predict an efficient path. By applying GPSR function on ZRP border nodes only (and not for all of its neighbors), better routing performance can be achieved for VANETs. Chung et al. [6] address the problem of spectrum access to deal with channel dynamics due to highly mobile nodes. A multi-channel Media Access Control (MAC) design that supports concurrent transmissions by allocating the channel for every beacon interval, is inadequate for fast-fading VANET environments. In contrast, a MAC design based on opportunistic spectrum access that selects a channel for each transmission cannot provide fair share of spectrum among devices. To address deficiencies of these MAC designs, Chung et al. [6] present the design and evaluation of a Cognitive MAC for VANET (CMV). CMV utilizes both long-term and short-term spectrum access, which not only provides a fair share but also exploits multi-user diversity, while achieving a significant increase in the overall network throughput. Their results show that CMV improves previous multi-channel MAC protocols throughput by up to 72% when compared with traditional dedicated and split protocols. Okada et al. [8] propose a novel selection scheme for the next-hop node in VANET. In their scheme, a new link metric called ‘expected progress distance’ is introduced in order to consider both forwarding distance and the transmission quality of the wireless link. They demonstrate that their approach can achieve much higher throughput and a better packet delivery ratio over existing conventional schemes such as greedy perimeter stateless routing, flooding-based geo-casting protocols, beaconless routing algorithms and contention-based forwarding. Yu and Ko [3] introduce a novel Delay/Disrupted Tolerant Network (DTN) routing scheme that uses a Message Ferry technique for VANETs. Geographic information is used to divide the road into blocks and control block size to ensure 1-hop communication between vehicles. Speed selection is designed for a minimum number of ferries and fast packet delivery. Simulation results show that their scheme has better delivery ratio when the delay is over 400 seconds and more messages are delivered to their destinations in the case of heavy load when compared with the Distance-Aware Epidemic Routing (DAER) scheme [5].

In addition, different performance comparisons with other DTN protocols are also required to further demonstrate the performance efficiency of the proposed scheme. Ali and Bilal [7] propose a VANET routing protocol that is especially designed for city environments. It consists of the selection of the next junction dynamically and an intelligent greedy strategy is used to forward packets between two junctions. The authors, inspired by the work of Jerbi et al. [9] proposed a geographical routing protocol using digital maps and vehicle density to select the next junction. Their work addresses some of the issues associated with the Improved Greedy Traffic Aware Routing (GyTAR) protocol [9] namely an intersection-based geographical routing protocol capable of finding robust routes within city environments. GyTAR, moves a packet successively closer to the destination along streets where there are enough vehicles to provide connectivity. Although GyTAR outperforms previous routing protocols in terms of packet delivery ratio, routing overhead, and end-to-end delay, GyTAR suffers large end-to-end delays and decreased packet delivery ratio when there are vehicles on the road opposite the direction of desired destination (such as one-way roads). Other issues such as the integration of VANETs with cellular networks, situation aware vehicular routing, and group formation still require further investigation.

3.2 Security frameworks

As we discussed above, efficient security support is an important requirement of VANETs. Several VANET security challenges still need to be addressed in the areas of authenticity, driver confidentiality, and availability. We need lightweight, scalable authentication frameworks that are capable of protecting vehicular nodes from inside and/or outside attackers infiltrating the network using a false identity, identifying attacks that suppress, fabricate, alter or replay legitimate messages, revealing spoofed GPS signals, and prevent the introduction of misinformation into the vehicular network. Early work in this area has been undertaken by Verma and Dihiang [10]. As far as driver confidentiality is concerned, we need reliable and robust secure protocols that can protect message exchanges among nodes of a vehicular network from threats such as unauthorized collection of messages through eavesdropping or location information (through broadcast messages). Choi and Jung [11] propose a prototype security framework aimed at mitigating threats to confidentiality in VANETs. To ensure availability, we also need mechanisms in place that can detect and mitigate attacks (such as Denial of Service) that can deny authenticated users access to the network.
Some early works in this area is also presented in [10, 11]. Secure, efficient message exchange and authentication schemes operating for Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communications are required.

For instance, mechanisms that can perform fast authentications between vehicles and roadside infrastructure units are needed to avoid delays. The use of a central, trusted authority and the use of public/private key-based solutions for vehicle-to-vehicle communication not only suffer high operational costs and response times but are also not scalable. We need to investigate innovative fast, low-cost message exchange solutions whose communication overheads remain constant as the number of vehicles in the communication range increases. We need novel encryption protocols that can operate at high speed compared to traditional public key-based solutions which incur more delays and overheads when encrypting messages from neighboring vehicles. The Secure Group Communications (SeGCom) scheme proposed in [10] is a lightweight solution that addresses some of these challenges for the V2V scenario by exploiting only one encryption method when creating and disseminating emergency messages. The authors in [11] proposed an ID-based cryptosystem (for safety-related applications) that implements strong repudiation and privacy while eliminating the overheads associated with certificate management prevalent in Public Key Infrastructure (PKI) systems.

However, the use of a trusted third party to verify a vehicle’s identifier may not lead to a scalable solution as mentioned previously.

3.3 Quality of service

Although current efforts [12] have attempted to optimize the available bandwidth to improve latency of messages, QoS support over VANETs remains a challenge because of the various factors we discussed earlier. We need to develop adaptive QoS routing approaches that can quickly and efficiently set up new routes when current routing paths becomes no longer available as a result of changes in node velocity, node positioning, network topology or distance between vehicular nodes. Well-defined QoS metrics for VANETs still need to be agreed upon given the wide variations of performance metrics (including popular QoS ones such as delay and jitter) being used by the VANET community. Initial results by Boban et al. [13] demonstrate that the real QoS challenges are packet delivery ratio and connection duration (rather than typical QoS metrics such as end-to-end delay and jitter [14]) are hard to achieve for unicast-based applications.

Although multipath routing improves global QoS [13] metrics we need more in-depth research to investigate the impact of the multipath approach on the available bandwidth and processing load of intermediate vehicular nodes involved in the various paths used.

3.4 Broadcasting

Broadcasting continues to be a strong research area of focus by VANET researchers because a significant number of messages transmitted in VANETs are broadcast messages. Novel broadcasting algorithms are required to minimize broadcast storms that arise as a result of packet flooding. In addition, the underlying 802.11 wireless communication technology used by VANET is not well suited at handling broadcast transmissions because of frequent message collisions leading to frequent retransmissions by vehicles. These collisions in turn affect the message delivery rate and increases the delivery time of the messages. Further research is required to investigate intelligent flooding schemes, distributed algorithms that can efficiently handle asymmetric communications among vehicles for different transmission ranges. Providing reliable broadcast messages with minimal overheads for VANETs introduces several other technical challenges including: the selection of the next forwarding node, the maintenance of communications among vehicles as they leave and join a group, hidden terminal problems since broadcast messages do not use the typical Request to Sender/Clear to Sender (RTS/CTS) message exchange employed by IEEE 802.11. Research proposals [14–16] have only recently begun to investigate broadcasting techniques for VANET but more research is required to enable highly efficient, reliable broadcasting techniques for VANET.

IV. Conclusions

In near future, it is expected that Vehicular ad hoc networks will not be restricted to deploy in any countries. Security of such networks is very vital because people’s lives may be at stake due to it. In this paper we have described why this problem has such particular requirements. We also define different types of threats that are possible in vehicular ad hoc networks. We also surveyed the literature on several security issues specifically related to VANETs. These security issues make a potential stumbling block to deploy VANETs. From the analysis in survey, we came to know that – up till now – there doesn’t exist a broad security protocol or structure that covers all security aspects of VANET.
So, there is need to develop such a structure which mitigates all these security problems; more research is required in this area.

REFERENCES


