Adaptive KPSD Model for Insider Attack Detection in VANET

Kalaivani.S#1, Haripriya.S#2, Mallesan.C#3, Jayanthi.A #4
#1 Department of Computer Science, SNS College of Technology
Coimbatore, Tamil Nadu, India

Abstract— In Vehicular networks (VANETs) to make future deployment successful, it is important that all applications are provided with proper security mechanisms. Current proposals mostly focus on entity authorization by establishing a public key infrastructure. Such proactive security efficiently excludes non-authorized entities from the network. However, in the case of insider attackers possessing valid key material, we need to consider data-centric methods to complement entity-centric trust. The inside attackers possessing valid key material could be able to cause accidents due to false information. Signing packets with digital signatures and by establishing a public key infrastructure (PKI) security is provided. In the proposed system, to facilitate vehicles to achieve high-level location privacy, Signature with respect to an effective pseudonym changing at social spots (PCS) strategy with Key-Insulated Pseudonym Self-Delegation Model is used rather than the DSA used in the existing system. Key-Insulated Pseudonym Self-Delegation Model provides short life keys that are used in small social spots. In PCS strategy, each vehicle is equipped with OBU which is used for communication that possesses large number of short life keys authorized by TA. The security of the proposed KPSD scheme can be guaranteed, i.e., it can effectively achieve anonymous authentication with conditional tracking to fulfill the requirements of location privacy. In addition, the proposed KPSD scheme can mitigate the hazards due to vehicle theft, because the authorized anonymous key insulated, i.e., it is stored in a secure environment; then, vehicle thieves cannot obtain keys from the stolen vehicle and, consequently, cannot arbitrarily generate new self-delegated short-life keys.

Keywords—Data consistency, vehicular networks, public key infrastructure.

I. INTRODUCTION

The future applications that make use of vehicular networking span a wide range of use cases. We can differentiate three main groups of applications namely safety applications, traffic efficiency applications and infotainment services. The goal of safety applications is to provide the driver with additional information that can prevent potential accidents. Examples are hard breaking warning or a lane-change assistant. The goal of traffic efficiency applications is to optimize travel time beyond the possibilities of current navigation systems. For example, information about current average speed, which is disseminated to approaching vehicles, can help to better plan alternate routes. The infotainment services include applications like video streaming or map updates while on the road. For some of the above mentioned applications, information from the single-hop broadcast area around a vehicle is sufficient. In particular, safety applications often depend on one-hop broadcasts because of tight real-time constraints. However, other applications, particularly those for traffic efficiency, need to disseminate information in larger areas. In these multi-hop scenarios, competition for available wireless bandwidth is an issue. Consequently, numerous proposals exist for efficient multi-hop information dissemination protocols. Two major dissemination patterns that are employed are geocast and aggregation[1]. Geocast disseminates information in a predefined geographical region, for example, a stretch of road or a city region. Depending on whether the origin of information is within the destination region, information is either first forwarded toward the destination region or disseminated directly. Examples for geocast are the dissemination of emergency vehicle warnings to the approaching vehicles and disseminating accident warnings. The goal of aggregation mechanisms is to collaboratively create and disseminate an approximate view of the real world. Instead of forwarding information like average speed unmodified, vehicles combine known information and only disseminate summaries in larger regions. In contrast to geocast, information is modified while it is forwarded in the network. Examples are traffic information systems and parking spot availability information. To prevent spreading of malicious information, all proposed protocols need to be properly secured[2] [3] [4]. Otherwise, attackers could be able to reroute traffic if they insert malicious messages into traffic
information systems, for example, in cases of safety applications, attackers could be able to cause accidents due to false information, in the worst case scenario. The original approach to protect vehicular communication is based on entity-centric trust, which is established by signing packets with digital signatures and by establishing a public key infrastructure (PKI) that issues certificates to vehicles. Entity-centric trust ensures that the originators of messages are actual vehicles or other infrastructure that is authorized to participate in vehicular networks. Attacks using arbitrary commodity devices are effectively prevented. However, prohibitive cost and complex management of trusted hardware make it likely that knowledgeable attackers will be able to access key material in vehicles they physically own. Using the obtained keys, attackers can generate wrong information or modify the information they process as a part of multi-hop dissemination protocols. Hence, cryptographic signatures cannot guarantee that the messages contain correct information. This problem is worse in multi-hop protocols. If geocast is used to forward messages over large distances, it is likely that the receivers of messages do not have any previous interactions with the originators of messages. Hence, messages cannot be judged based on the originator’s previous good or bad behaviour. If aggregation is used, the originators can no longer be identified. Because the forwarding nodes actively modify and combine messages, which invalidates the originator’s signatures Therefore, a number of research papers [5][6] as well as standardization activities [7], propose to complement entity-centric trust with data-centric methods, which detect attacks based on data consistency rather than entity trust. Data-centric methods are well known in intrusion detection systems for closed networks or servers. The central idea is to depend on physical models, local sensors, or data redundancy to detect spurious data. As VANET applications highly depend on communicated data, checking that such data correctly reflect a specific real world situation is fundamental. Entity-centric trust helps to filter spurious data by excluding non-authorized devices from the network. However, additional data consistency checks are needed to detect attacks from insiders who possess the valid key material. The central idea of data consistency checking is to depend on multiple independent sources of information to detect inconsistencies between different alleged information. The detection of inconsistencies can be used as a source for mechanisms that filter wrong information and exclude attacker vehicles from the network. We differentiate three main types of sources for data consistency mechanisms. They are real world models, local sensors and Dissemination redundancy. Real world Models can be used to compare claimed information against known models, such as the physical behaviour of vehicles. For example, vehicles cannot accelerate arbitrarily fast and cannot move at infinite speed. The particle-hopping models are used to represent statistical physics of vehicular traffic, which define the physical behaviour of vehicles and captures all possible events and uses their statistical properties (e.g., probability of occurrence) to detect spurious information[8]. The Local sensors can be used to verify information received from vehicles in the direct vicinity. In case of conflicts between the perceived environment and information from other vehicles, the precedence can be given to local sensor information. For example a system that uses sensors to analyse vehicle behaviour and check the position information[9]. Finally, the dissemination redundancy exploits the fact that messages are often delivered through multiple routes to compensate for packet loss, and that events are often observed by multiple vehicles. As a result, vehicles can detect spoofed information by observing inconsistencies between the different received messages about the same event. For example, the notion of proof of relevance (PoR), [10]which is accomplished by collecting authentic consensus on the event from witness vehicles in a cooperative way. Event reports from attackers who fail to provide this PoR are disregarded, making the network immune to incorrect data.

II. PUBLIC KEY INFRASTRUCTURE

A public-key infrastructure (PKI) is a system for creating, storing, and distributing the digital certificates which are used to verify that a particular public key belongs to a certain vehicle in vanets. The PKI creates digital certificates which relates public keys to vehicles, safely stores the certificates in a central repository and revokes them if required. A PKI consists of a certificate authority (CA) that
issues and verifies the digital certificates, registration authority which verifies the identity of vehicles requesting information from the CA, central directory which is a safe location to store and index keys, certificate management system and a certificate policy [5]. In cryptography, a PKI is an arrangement that binds public keys with respective vehicle identities by means of a certificate authority (CA). The vehicle identity must be unique within each CA domain. The third-party validation authority (VA) can provide this information on behalf of CA. The binding is created through the registration and issuance process, which, relying on the assurance level of the binding, may be carried out by software at a CA or under human supervision. The registration authority (RA) takes care of this binding and ensures that the public key is bound to the vehicle to which it is assigned in a way that ensures non-repudiation. Public key cryptography is a cryptographic technique that enables users to safely communicate on an insecure public network, and reliably verify the identity of a vehicle through digital signatures.

III. ADAPTIVE GEOCAST ROUTING

A basic aggregation scheme is used similar to [12] as representative for in-network aggregation protocols. The scheme uses fixed-size road segments, for which all atomic observations are averaged. An assumption is made such that a message from the source reaches the destination if the destination receives an aggregate that the source message is contributed to. All vehicles gather known aggregates in a real world model and periodically disseminate a subset of the world model using one-hop link layer broadcast. For dissemination, a fixed packet size is configured. In case the world model content exceeds the packet size, priority is given to information about the direct vicinity of the disseminating vehicle. Both the segment size and the dissemination packet size can be adjusted. An adaptive probabilistic gossiping protocol, namely, Advanced Adaptive Geocast (AAG) [13] is used for efficient adaptation. In AAG, each node determines the message forwarding probability based on the current perceived node density according to two-hop neighbourhood information. The protocol performance can be adjusted by configuring an average reception percentage, which states the percentage of nodes that should, on an average, receive a message. In high node density scenarios, AAG uses a logistic function to automatically reduce the forwarding probability further. A target region can be specified which determines the area for which an observation is relevant. For our simulations, we set the target region to the whole network, because of the assumption that a traffic information application where all vehicles are interested in the speed of the other vehicles in the network. The aggregation protocol could be adapted to perform less aggregation in low node density scenarios to maintain a higher redundancy due to more redundant atomic observations. AAG automatically reduces redundancy by reducing the forwarding probability in high node density scenarios. [11] AAG reacts well to high node densities from an efficiency point of view, but it is problematic from a security point of view. Even when a large number of nodes, and consequently redundant observations, are available, a cleverly positioned insider attacker will still be able to insert the wrong information. The distribution
performance decreases with higher number of nodes due to reduced forwarding probabilities according to the logistic function. The distribution percentage represents the distribution of a particular message and not a number of messages about the same event. Since AAG does not aggregate messages about a single event, like the aggregation protocol, it is likely that at least some messages about an event will still reach the destination, if the source sends enough messages over the network.

IV. KPSD MODEL

We assume a single insider attacker whose aim is to alter the message that is transferred from source to destination, who are both honest. Further, the attacker possesses at least one valid certified key pair [11]. While cases of colluding attackers are possible, we consider single attackers to be the most likely, particularly assuming that attackers need to physically own cars to extract key material. Whenever the attacker receives source’s message for forwarding, the content will be modified. We assume that we cannot differentiate the attacker from the normal vehicles beforehand, because the attacker vehicle creates messages that conform to the communication protocol. In general, we assume that the attacker behaves according to the protocol except for modifying the message content. This attack scenario cannot be solved with a simple message integrity protection scheme using digital signatures. The reason is that the destination does not know the identity of the source. Therefore, the destination cannot check whether the message has been signed with source’s private key. Instead, the destination can only verify that the signer of the message is an authorized participant of the network under consideration. However, since we assume that the attacker possesses one or more valid key pairs, destination cannot differentiate source’s messages from attacker’s messages only using signatures. We consider the attacker to be successful if it is able to modify all messages that the destination receives from source. To be successful, the attacker needs to be in and part of all possible paths from source to destination, i.e., the attacker needs to be a critical node.

A Key-Insulated Pseudonym Self-Delegation Model is used for detecting the insider attack, which provides short life keys to the vehicles that are used in small social spots. In PCS strategy, [2] each vehicle is equipped with on-board unit (OBU) which is used for establishing communication that possesses large number of short life keys authorized by TA. In VANETs, vehicles can communicate with each other. (V2V, Vehicle-to-Vehicle communications) and they can also communicate to an infrastructure(V2I, Vehicle-to-Infrastructure), i.e. Road Side Units to get some service. This infrastructure is assumed to be located along the roads to provide service to the vehicles. Each vehicle should contain some amount of pseudonyms. In this model, TA provides the key to the user of the vehicle instead of preloading the authorized keys. Then the user stores the provided authorized keys in a secure environment.

When a user is ready to travel, these short life keys are used to sign the messages. The security of the proposed KPSD scheme can be guaranteed, i.e., it can significantly achieve anonymous authentication with conditional tracking to satisfy the requirements of that particular location privacy. Moreover, the proposed KPSD scheme can mitigate the hazards due to vehicle theft, because the authorized
anonymous key is insulated, i.e., it is stored in a secure environment. The vehicle thieves cannot obtain the insulated keys from the stolen vehicles and, consequently, cannot arbitrarily generate new self-delegated short-life keys.

V. CONCLUSION

Safety applications in vanet often depend on one-hop broadcasts because of the tight real-time constraints. Attackers could be able to cause accidents due to false information, in the worst case scenario. Signing packets with digital signatures and by establishing a public key infrastructure (PKI) that issues certificates to vehicles take large time for computation. It also provides routing overhead. To achieve location privacy, a popular approach that is recommended in VANETs is that vehicles periodically change their pseudonyms when they broadcast safety messages. To reduce computation cost, Signature with respect to a Pseudonym is used rather than DSA used in the existing system. We utilize the unique feature of social spots, i.e. several vehicles temporarily stop at the social spot, to propose the PCS (pseudonym changing at social spots) strategy. A holistic protocol will use both absolute cryptographic security mechanisms and probabilistic approaches together to ensure data consistency and protect VANETs against both outsider and insider attackers. Hence, to facilitate vehicles to achieve high-level location privacy in VANETs, an effective pseudonym changing at social spots (PCS) strategy with Key-Insulated Pseudonym Self-Delegation Model is used.

REFERENCES