Ann. Telecommun. (2017) 72:283–295
DOI 10.1007/s12243-016-0551-6

Attacks and countermeasures in the internet of vehicles

Yunchuan Sun[1,2] · Lei Wu[3] · Shizhong Wu[1] · Shoupeng Li[1] · Tao Zhang[1] · Li Zhang[1] · Junfeng Xu[1] · Yongping Xiong[4] · Xuegang Cui[2]

Received: 13 January 2016 / Accepted: 20 October 2016 / Published online: 15 November 2016

Abstract As a typical application of Internet of Things (IoT) in the field of transportation, Internet of Vehicles (IoV) aims at achieving an integrated intelligent transportation system to enhance traffics efficiency, avoid accidents, ensure road safety, and improve driving experiences by using new IoT technologies. Different from other Internet, it is characterized by dynamic topological structures, huge network scale, non-uniform distribution of nodes, and mobile limitation. Due to these characteristics, IoV systems face various types of attacks, such as authentication and identification attacks, availability attacks, confidentiality attacks, routing attacks, data authenticity attacks, etc., which result in several challenging requirements in security and privacy. Many security scientists made numerous efforts to ensure the security and privacy for the Internet of Vehicles in recent years. This paper aims to review the advances on issues of security and privacy in IoV, including security and privacy requirements, attack types, and the relevant solutions, and discuss challenges and future trends in this area.

Keywords Internet of vehicle · Security · Privacy · Countermeasure · Cloud computing

✉ Yunchuan Sun
yunch@bnu.edu.cn

Lei Wu
bill31415926@qq.com

Xuegang Cui
cxg@bnu.edu.cn

[1] China Information Technology Security Evaluation Center, Beijing, 100085, China

[2] Business School, Beijing Normal University, Beijing, 100875, China

[3] College of Information Science & Technology, Beijing Normal University, Beijing, 100875, China

[4] State Key Laboratory of Networking & Switching Technical, Beijing University of Posts & Telecommunications, Beijing, 100876, China

1 Introduction

Internet of vehicles (IoV) is becoming a new emerging paradigm with the rapid development of wireless and mobile communication technologies. Aiming to the intelligent traffic and smart driving, wireless sensor networks (WSN) have been gradually implemented on devices of vehicles and roadside, and the network of vehicles has been connected to the Internet. Internet of vehicles is a complex system which contains many kinds of resource types such as vehicle, human, and sensors. In IoV, vehicles with various sensors are the primary nodes that connect to other resources. As a heterogeneous network, IoV is a dynamic mobile communication system which communicates between vehicles and public networks using vehicle-to-vehicle (V2V), vehicle-to-road (V2R), vehicle-to-human (V2H), and vehicle-to-sensor (V2S) interactions [1] to improve the safety on road, traffic management, and provide convenience to drivers. By information gathering and sharing among vehicles, roads and their surroundings, the system can effectively guide vehicles, and provide mobile Internet application services [2].

Nowadays, IoV can provide more comprehensive and convenient services, combined with the concept of cloud computing system, especially in driving status and traffic

data analysis [3]. Vehicle dynamic data recording, including vehicle information, map and weather data, etc., high-precision location service, and Intelligent driving are all promising trends in IoV development which are based on the computation and synchronization of cloud platform [4].

IoV can be viewed as a kind of the Internet of Things (IoT). Comparing with other Internet such as smart cities, IoV is mobile and changing dramatically, while Internet such as smart cities are changing slowly and always stable in a long time till new buildings or equipment with sensors are constructed. The general structure of IoV is shown in Fig. 1. IoV has the following special characteristics:

- Dynamic topological structures. With high mobility and short connection cycle, the topological structures of IoV are intrinsically dynamic and thus difficult to predict and model. Comparing with other network such as smart family devices, vehicles are mobile and move quickly, which leads to the frequent changes of vehicles in the IoV. Because a vehicle may have different drivers, V2H will change. The neighbors of vehicles on the road will change frequently, so the V2V will change. A vehicle will run on the different roads, so the V2R will change. The different actions of drivers will lead to the changes of sensors, so the V2S will change. So IoV will change frequently according to the changes of vehicles, drivers, roads, and sensors.
- Huge network scale. IoV may consist of millions of vehicles equipped with wireless communication capabilities which are decided by the scale of a city. The scale of IoV network should be scalable according to the entering or leaving of vehicles. With the advance of vehicle manufacturing and the construction of roads, more vehicles are running on the roads. The scale of IoV is drastically changing, especially in the time when people go to work in the morning or go home in the afternoon.
- Non-uniform distribution of nodes. The distribution of vehicles is affected by many factors including the road network topological structure, geographical location, driver's driving habit, etc. The connectivity of the network can be totally different, for example, in the downtown of a metropolis and a rural area in a developing country. So the structure of sub-IoVs keeps on changing continuously, although vehicles are in the whole IoV. A vehicle may enter different sub-IoVs according to the changes of its locations.
- Different granularities. Vehicles on the same road, in the same district, city, province, or a country formulate different IoVs with different granularities. IoVs with smaller granularities (called sub-IoVs) will formulate the IoVs with larger granularities (called super-IoVs).
- Mobile limitation. Vehicles in IoVs are connected via wireless communication network. So IoVs are

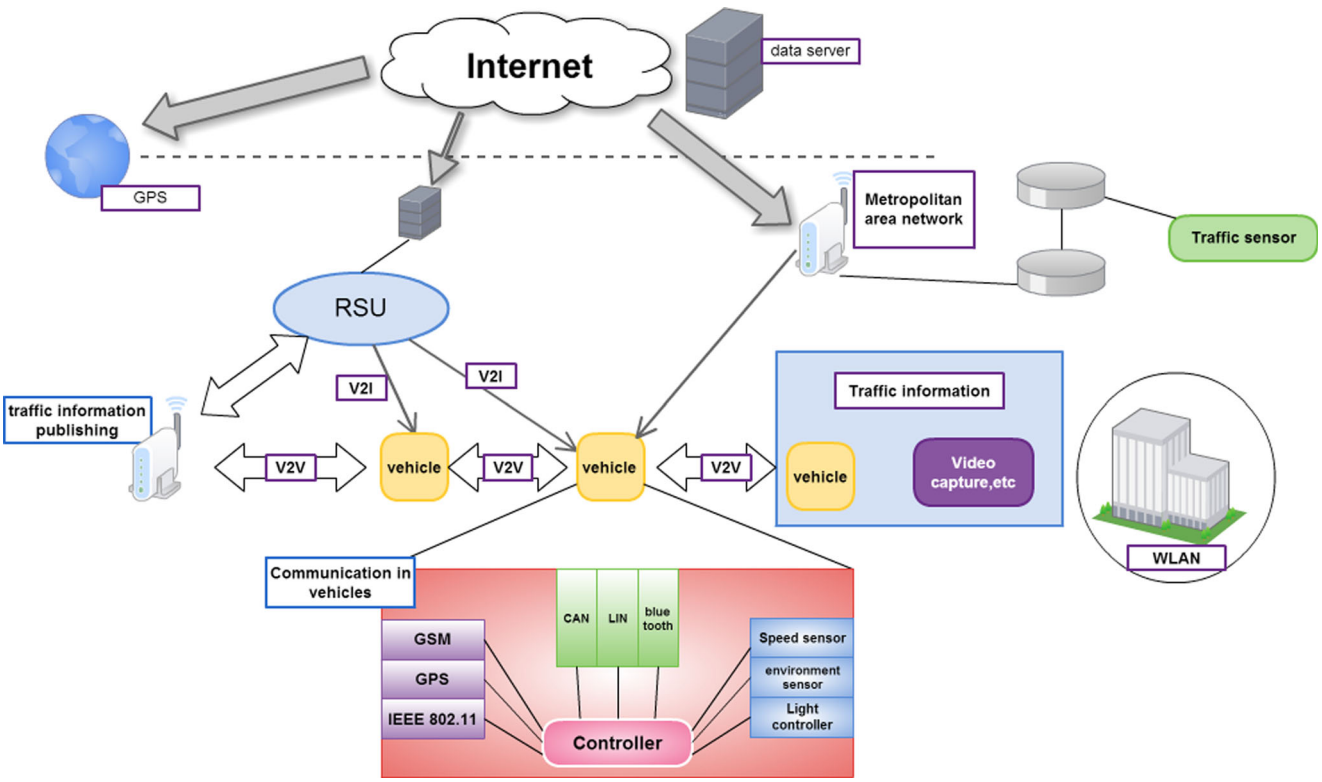

Fig. 1 General structure of IoV

heavily limited by the signals of wireless communication network. If the distance is too large, the wireless network will not work, and then the signals will be weak, thus, the IoVs also will be hard to be formulated. Since nodes in IoV are expected to move on the road with determined track in some extent, its predictability is better than those of free running, which is a benefit.

Security and privacy of IoV are serious issues because the traffic disaster caused by erroneous information from IoV leads directly to the loss of people lives. If network intrusion happens in IoV, the vehicles may be controlled by hackers with ulterior motives, and this will lead to traffic accidents. So the security of IoV is a very serious issue. At the same time, driving tracks are the privacy of people. People may not want to let others know where and when they have been. However, the IoV could capture and driving track of vehicles, which will reveal the privacy. What is more, as vehicles access into cloud more and more, the security and privacy in IoV are facing with more challenges. Some information in IoV could be public, while some information must be protected as privacy. Security could assure the safety of vehicle driving and protect the privacy of people.

2 Attack types in IoV

In information security, attacks and threats can be classified into six main categories in STRIDE Threat Model [5], including spoofing identity, tampering with data, repudiation, information disclosure, denial of service, and elevation of privilege. Specially, Internet of Vehicles system may get attacked from various of aspects by different methods like jamming, interference, eavesdropping, and so on, which will decease the stability, robustness, real-time, security, and privacy of IoV and make it lose the ability to provide effective services, and even cause serious accidents [6–11], due to its characteristics of dynamic topology, bandwidth limitations, transmission power limitations, abundant resources, mobile limitation, non-uniform distribution of nodes, perception of data depending on the vehicle trajectory, and large-scale network.

This section introduces attack types in the Internet of Vehicles. The main structure is shown in Fig. 2.

2.1 Attacks on authentication

- Sybil attack. One can have, some claim, as many electronic persons as one has time and energy to create [12]. This words just tells what the Sybil attack is. In wireless networks, a single node with multiple identifications can damage the system by controlling most nodes in the system. In a word, Sybil attack means that a malicious device or node appears in the system with multiple illegal identities [12–16]. Because IoV is dynamic, the vehicles always access in IoV temporarily and unstably, which makes it easy for Sybil nodes to find chance to attack. Normal vehicles are easy to be attacked and they cannot have their normal services and private data of these vehicles are leaked [17].
- GPS deception. GPS deception can provide a node with fake information about its location, speed, and some other GPS information. When such information has been accepted by applications about safety or financial issues, the adversary can feign enough untrue but unable-to-deny evidences to escape from tracking [16]. In IoV, GPS information plays an important role in many applications such as navigation tools and payment applications, and inaccurate location may cause fake evidence and unpredictable property damage.
- Masquerading attack. In a normal network environment, one entity must have the unique identification. Masquerading attacks can threaten chaos by allowing more than one node in such circumstance to have the identical ID. Subsequently, the IoV systems would not work properly and would be puzzled with such a chaos state [16, 18].
- Wormhole attack. The fundamental idea of wormhole attack is that two or more malicious nodes hide the true distances among them entice other normal nodes to route across these dangerous nodes to absorb data flow and cause network conjunction or cooperate with other attackers [19, 20]. This kind of attack always has fatal influences on IoV system due to its characteristics of change and high dependence on efficient routing algorithm. Every type of IoV elements will lose their normal response when they are attacked by wormholes [11, 21].

2.2 Availability attacks

Attacks like denial of service and channel interference are common types of attacks on availability. This type of attack mainly utilizes the limitations of bandwidth and transmission power to make the IoV system collapse [16, 22]. Most of major significant components of IoV are exposed outside and have deficient protection, as a result they are facile to be interfered, controlled, and totally destroyed. The influence of an availability attack depends on which type of nodes to be attacked, i.e., damagment on a core unit will have larger impacts on IoV system than a destroyed vehicle [23].

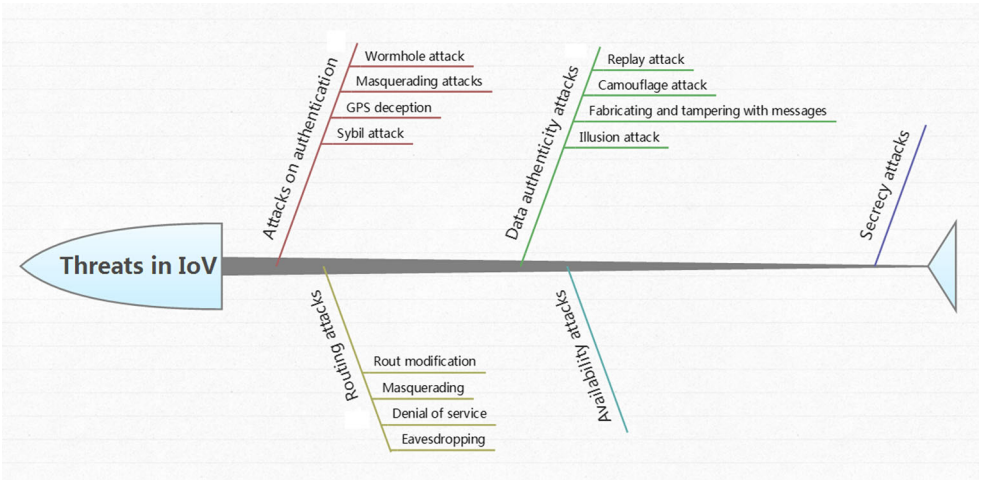

Fig. 2 Types of attacks in IoV

2.3 Secrecy attacks

The data and resources are always the most important parts of a system, and secrecy is needed to guarantee that these sensitive data can only be accessed by legal nodes which are authorized correctly. The secrecy attacks steal data by eavesdropping or interception. In most cases, an attacker compromises a normal entity like a vehicle or a road side unit (RSU), then this attacker can have the ability to access the secret resources through eavesdropping this entity, causing the leakage of users' privacy [7, 17].

2.4 Routing attacks

There are four different attack types in routing process [24, 25].

- Eavesdropping. Due to the openness of wireless links, routing nodes in network are easily to be eavesdropped and implementing eavesdropping can be difficult to be detected because this type of attack has no disruption for original data [22].
- Denial of service. Malicious nodes may send a large number of repeating requests or invalid data to other nodes and make them too busy to provide normal services properly. This would lead to a serious security threat no matter how it takes place [21, 26].
- Masquerading. Malicious nodes can obstruct routing process and obtain vital information by masquerading as a legitimate node. Masquerading can bring deadly threats to the network and attackers can hide identity with the help of the impersonated objects [22, 27].
- Route modification. Malicious nodes in the network modify the routing information or change the number of hops in forwarding routing request packets. Then, the routing process will not be completed correctly, and data cannot be delivered rightly [22, 28].

Routing algorithm and its quality imply the effect of IoV communications among RSUs, vehicles, and other TPMs, and the routing mechanisms of IoV are always relatively complex due to the IoV's limitations of bandwidth, transmission power, and mobility. Subsequently, this complicacy brings about the loopholes and vulnerability of IoV routing process [29–32].

2.5 Data authenticity attacks

When data packets are transmitted in the network, it is necessary to ensure that the source data has not been modified. Data authenticity attacks can be categorized into the following types.

- Replay attack. Unlike other types of attacks, replay attacks have a unique feature, i.e., it can be conducted by illegitimate nodes. A large amount of message replays increase the cost of precious bandwidth, resulting in the dropping of priority messages from the queue. The efficiency of the system would be greatly decreased because of the frequently replaying and deleting, and this system activity cannot be prevented by using digital signature technology like message forgery [33, 34].
- Camouflage attack. A camouflage node hides itself under a false identity and utilizes this appearance from a legitimately authenticated node, and spreads fake and harmful messages, or executes blackhole attacks, or other fatal attacks [35].
- Fabricating and tampering with messages. Such attacks manifest through generating fake messages and disseminating untrue information, masquerading, and hiding sensed evidence to hide different kinds of vehicle

attacks [25]. The path of multi-hop message distribution will also be broken because the routine nodes (vehicles) are prevented from joining in the traffic normally. Message modification can also bring about false reaction of traffic emergencies [26].

– Illusion attack. In this kind of attacks, some voluntary sensors that generate false or meaningless information in the network will be placed. These malicious sensors are always properly authenticated and identified in some ways or by some other attackers. Authentication mechanisms are unable to deal with this type of attack [25].

As for the motives of attacks in IoV, there are two main aspects.

– Motivated by challenges. Such type of attacks are always support by researches and specific security institutions. Challenging various IoV systems can be helpful for security study and also give efficient enhancements to the defense of IoV attacks. In 2010, researchers at the University of South Carolina and Rutgers University tracked the movement of a car and modified the displayed tire pressure arbitrarily by hacking its tire-pressure-monitoring systems [36]. This is quite difficult to implement without the hardworking for professional researchers.
– Motivated by profit. As the number of the applications in IoV grows rapidly, except for typical applications such as navigation service, multimedia platforms, some new types of applications comes out which may contain more information about private account or finance of the users. What is more, attackers can have chances to make profits by threatening the IoV customers or stealing vehicles. Therefore, like attacks on other different networks, profit-motivated attackers also play important roles in IoV attacks.

The property of openness makes IoV data flow easy to be captured, fabricated, and forwarded, especially in routing and wireless communication. Data authenticity attacks makes the applications of IoV not credible and this destruction may have profound and lasting effects on IoV [37].

3 Security requirements in IoV

In general, when facing with increasing threats, the first step is to specify proper policies is to clarify the requirements in IoV. Specific and reasonable requirements can help researchers to propose practical and effective mechanisms to ensure enough security and privacy for the participants of IoV (Fig. 3).

– Availability. A high availability requirement is mandated in IoV especially because of its safety-critical nature by providing fail-safe, resilient, and fault-tolerant operations [38, 39]. A mature IoV system must have the ability of working in emergency situations, for example, if the auto-control module breaks down, the on board IoV system can switch into manual operating urgently to ensure the vehicle still in control.
– High mobility of IoV entities. Frequently changing network topology and high mobility of entities result in the transient nature of V2V and V2I communication interactions, and this attribute makes it much more difficult to ensure security and non-repudiation [39]. More specifically, data packets must keep complete and not modified during the whole uncertain routing process, and efficient routing algorithm to save time to ensure arriving on time is also necessary. After all, any tiny mistake or delayed information may bring about traffic chaos or even accidents.
– Key distribution management. Vehicle manufacturers, government, wholesalers, etc. are all important participants in IoVs, so it is hard to judge who is more authoritative among these stakeholders. As a result, determining who should be certificate authority (CA) responsible for public key distribution can always be challenging when taking into account the benefit of these participants. What is more, because of the differences in standard of vehicles, rules, and policy, cooperation of different units in different situations can be difficult to implement and this difficulty which may cause problems in the work of certificate authorities [40].
– Low errors tolerance. In many practical network systems, like IoV, there is no so-called tiny error, because any minor mistake can lead to unimaginable disasters especially in systems like IoVs. For instance, a car may hit another vehicle because of an infinitesimal delay of deceleration. In IoVs, the limited bandwidth and unstable network quality constrains the communication of real-time in Internet of vehicle. To ensure fatal errors do not appear or do not cause accidents, placing more focus on preventive security measures is always much more meaningful than coppering with problems [41], i.e., make the drivers realize where will be congested and avoid it early is always much better than dispatching traffic police to ease the terrible traffic.
– Paradox between requirements of privacy and security. Generally speaking, more security commonly means less privacy and vice versa. Many drivers are unwilling to give up their privacy for some perceived security benefit and worry about the security at the same time. Therefore, balancing strong security with good

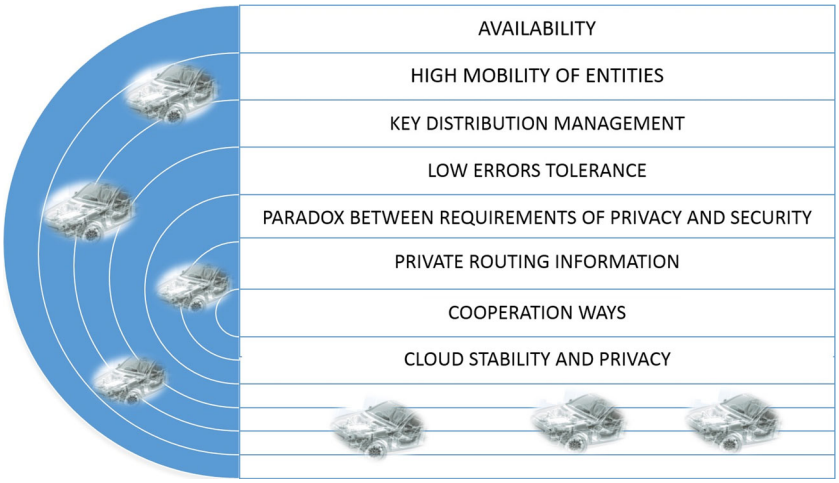

Fig. 3 Security requirements of IoV systems

performance is another major challenge [42]. For example, the navigation service providers cannot give consumers better services without more accurate location information of them, while consumers hesitate to share their such information because of their protection of the privacy data.

– Private routing information. IoV is a typical delay tolerate network (VDTN) where routing packets in routing are forwarded in the form of store-carry-forward because of uncertain intermittent node connections. In packets routing process, a node will compare the routing utilities of the nodes it is encountering with for the destinations of all the packets carried by it. Generally speaking, the probability of forwarding packets to the destination determines the routing utility of a node for a certain destination [43, 44]. The routing utility is a dynamic attribute and a node will choose the node with highest routing utility as the forwarder to forward the corresponding packets. In addition, the routing utility of a node can be always determined by its social properties such as the meeting frequency, network distance, and network position [15, 45–47]. In fact, the social activities of nodes are their private information so it is necessary to pay enough attention to think about the privacy protection [48]. Obviously, the choice a node made for selecting its packets forwarder reflects the utilities of the nodes it meet, and this choice also reflects the social attributes of these nodes which are private and should not be leaked to others, for example, whom a person always meets, and when a person often visit a certain place, both of which are private issues. In many routing algorithms [43, 44, 49], a malicious node can have opportunities to learn the routing utilities of other nodes and take advantage of these information to fabricate a router with higher utilities to attract, drop, or tamper packets to disseminate viruses [50–54]. As a result, protecting such private information in routing of IoV can be significant, but this information is also imperative to guarantee correct routing.
– Cooperation ways. Because of divergent interests and goals among different IoV participants such as manufacturers, consumers, government, etc., it is challenging to align the interests of them properly. For instance, many consumers nowadays may fiercely resist IoV use and will be reluctant to adopt it because they believe that they are being monitored by the system [55, 56].
– Cloud stability, security, and privacy. There is no doubt that cloud services will play increasing important roles in IoV as the development of IoV have based on big data and high performance computing [57]. The interactive data process between cloud platforms, vehicles, and other IoV units should be attached great importance to its stability, security, and privacy at the same time considering the data transmission could has potential hazards in both directions concurrently that toward the users and the cloud platforms. Besides, the data credibility should also be checked to escape the dangerous data injection caused by malicious input which can bring about unknown instruction execution and improper reactions of drivers when meet with traffic accidents. For privacy, efficient encryption algorithm should be also utilized in both sensitive data transmission and storage. Consequently, providing stable service and ensuring the and security and privacy of IoV users must be the basic requirements in IoV.

4 Countermeasures for the threats in IoV

Most of the countermeasures to attacks for general computer networks can work for attacks in IoV. However, the characteristics of the attacks in IoV leads to the special requirements for countermeasures. Many works have been made in this area in last decades (Fig. 4).

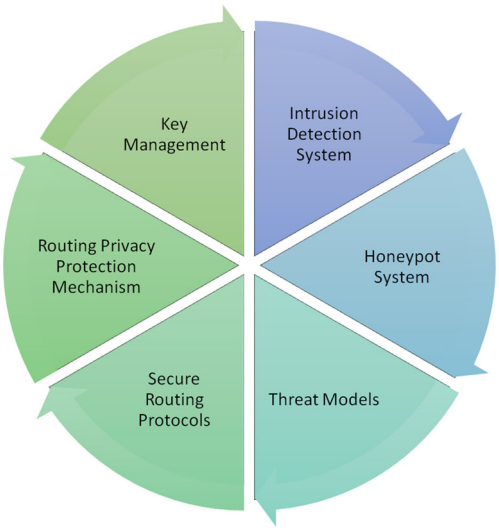

Fig. 4 Countermeasures for IoV threats

4.1 Threat model

Modeling different attacks is important for understanding and analyzing their impacts on IoV. Microsoft's STRIDE is a popular threat modeling technique commonly used to find the security weakness of various systems [58]. Graph-based approaches and mathematical modeling approaches are two main methods for describing the modeling network attacks [59, 60].

Both static and dynamic graph-based techniques are well known for attack modeling. They provide graphics to describe the relationships between different parts so that people who use them could conveniently make the model clear and easy to focus on the behavior of the attack in the network [61–63]. Petri net modeling approaches [64], for example, have been used in modeling the network attacks in large cyber physical infrastructures [65], such as smart grids, as a more flexible method. Hierarchical methods for constructing large petri nets from smaller size petri nets have also been proposed for such a complex IoV. Although graph-based approaches have many advantages for engineering applications in designing the attack detection methods for improving security analysis and security design in large scale IoV, they are too complex to be used in industrial fields. Mathematical approaches for modeling the attacks in Supervisory Control and Data Acquisition have been used for IoV, such as power networks and smart grids, instead of graph-based models.

Considering mathematical approaches, IOV are typically modeled as time-varying or time invariant linear systems, while network attacks, such as integrity attack, false data injection, or deception attack and denial of service, are modeled as disturbance injected as an external control input system. An IoV integrity attack is modeled as a disturbance, which is injected by external control input devices or fake sensor measurements in linear time invariant systems [66, 67]. In [68], it is assumed that those IoV adversaries will act as uncertainly parameters in IoV, which is modeled as a linear time-invariant system, and will not change the system's dynamic features. However, unlike cyber ones which may cause immediate perturbations at many respects of IOV, the adversaries can change the whole dynamics of the system.

4.2 Intrusion detection system

Intrusion detection system (IDS) is an important supplementary measure of network security. IDSs provide protections against internal and external attacks by collecting and analyzing information from internal network systems to check if there exist system behaviors which violate security strategy or signs of attack [69]. Signature-based detection and anomaly-based detection are the two main classes of detection methods [70].

- Signature-based detection. This type of detection will build up a database to store various signatures of known attacks for retrieving and making comparisons. Signature-based detection identifies attack by comparing the signatures in the database with the IoV states. The IDS based on signature will trigger the corresponding resistance measures when a network state matches an attack stored in the database. Though the detection results are always accurate for recorded attacks, however, when new, unknown attacks take place, this type of detection will have high false negative (FN) rates, which makes the detection lag indicators. In IoV, with the fast development of onboard applications, more sensors and more types of devices are integrated in vehicles, which makes signature-based detection invalid sometimes.
- Anomaly-based detection: Anomaly-based detection predefines the baseline of normal environment attributes in a system, and it can detect new types of attacks through the data observed which shows abnormal information beyond the baseline. This detection method has high false positive (FP) rates, costs much, and it is hard to find proper metrics to determine the baseline [71]. More accurate data analysis algorithms are needed for current and future use.

Beisdes, SVM-based context aware security framework has also been proposed to distinguish the malicious nodes in IoV network [72]. This framework implements the detection by construct a SVM to process the synthesis of both behavioral data and context data.

In addition, stateful protocol analysis can provide much more accurate detection information than the methods above, but it will cost much more resource because of its

complex analysis. Typically, higher accuracy means less efficiency in an IDS.

4.3 Honeypot

Spitzner defined a honeypot as a security resource whose value lies in being probed, attacked, or compromised [73]. Honeypots complement most other security mechanisms by running as normal system computing resources to tempt attackers. Honeypots aim at diverting attackers' attention away from the vital system resources and analyzing the behaviors of attackers to create signatures for intrusion detection system, so the real targets, the important system services and data can be protected by the attraction of attackers, and this is the reason why IDSs need honeypots [74]. In IoV, authorization module and communication module are the components which get attacked more often, and these related parts exist components which have the role of honeypot to absorb damage and record the attack data. Because they consume the system resource, these function should be switch off in some relatively safe situations [75]. The structure of the Honeypot in IoV is shown in Fig. 5.

4.4 Secure routing protocols

In order to effectively resist attacks like eavesdropping, denial of service, counterfeit, route modification, black hole, etc., a series of security routing protocols are presented based on traditional routing protocols. These security routing protocols can achieve normal routing functions and can effectively resist common routing attacks at the same time. There are three most common security routing protocols: SAODV, Ariadne, and SRP.

– SAODV protocol. The main method that SAODV [76] protocol ensures the security of routing is verifying multiple fields in routing messages by using digital signature and one-way hash function to verify the hop count. SAODV protocol generates the digital signatures for the key field in the route request packet. Therefore, intermediate nodes cannot modify the information of source node and the destination node freely, and the hop counts have been calculated through a hash function to forbid intermediate nodes to tamper hop count to prevent malicious nodes from reporting false hop information.
– Ariadne protocol. To verify the integrity and authenticity of routing information, Ariadne [77] protocol utilizes broadcast authentication mechanism–TESLA authentication scheme based on the one-way hash message authentication code. TESLA authentication scheme uses one-way hash function chain as a one-way key chain and each node selects a chain value as the TESLA key to calculate the MAC attached to the routing packet. Ariadne protocol prevents a malicious node forged false information or inserted into the routing information and avoid attacks initiated by routing black hole and other external malicious nodes through the application of one-way hash function.
– SRP protocol. The premise of using the SRP [78] protocol is that a secure connection between a source node and a destination node must be established with shared keys. The basic ad hoc routing protocol attaches SRP package head which carries the request sequence number and identification symbols and message authentication code (MAC). SRP protocol calculates MAC with the shared secret of the two nodes, verifies the dependability of the end nodes, and identifies new routing with the request sequence number to prevent routing replay attack. In addition, the limitation of request frequency also prevents the destination node from the hazards of denial of service attacks.

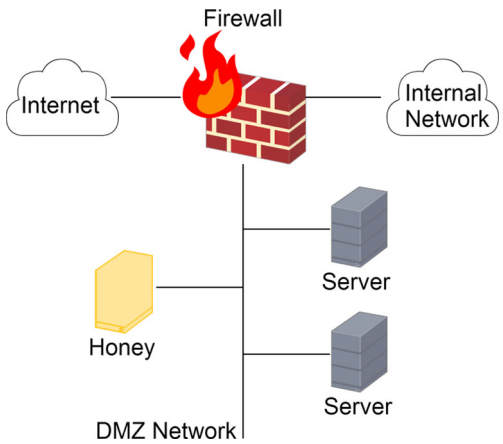

Fig. 5 Structure of honeypot

4.5 Routing privacy protection mechanism

To ensure that the routine nodes data will not be leaked during the routing process, a routing privacy protection mechanism is necessary for IoVs. Hiding the value of each utility using the idea of "The Millionaire's Problem" [79] can be a feasible method which is designed to compare two objects without leaking their actual values. SLPD [80], ALAR [81], and STAP [82] are three algorithms to protect the location privacy of mobile nodes in DTNs. SLPD makes a node's location information circumvent the social friends of this node to prevent the service providers from obtaining the location data of the node. ALAR divides the source packet into different parts, use different keys to encrypt

them, and forward them separately. After these treatments, it is almost impossible for the attackers to figure out the private information of the nodes from packets. STAP uses the idea of cache and caches packets for a node on locations where it appears frequently. Then, others nodes which meet with it do not need to know the node's location to send their packets to it [83, 84].

4.6 Key management

Encryption is the fundamental means to ensure information security. Encryption technology can meet the requirements of authentication, message confidentiality, data integrity of vehicular ad hoc networks, and non-repudiation. Effective encryption requires appropriate key management.

The goal of key management is to ensure the security of the key, that is, authenticity and validity. Key management includes key generation, distribution, transmission, preservation, destruct, and backup. In traditional networks, the distribution and management of keys are generally completed by the key distribution center (KDC) or certificate authentication center (CA) (Fig. 6) [85].

Moreover, distributed authentication protocol for IoV employed efficient pseudonym signature to protect privacy and use certificateless signature technology to assist vehicles receive keys secretly [86].

5 Future trends

In this section, we will discuss the future trends of the security and privacy issues in the Internet of Vehicles. We argue that there are eight different trends which would attract more efforts in the coming future.

– Reduce the defects of intrusion detection system. There are many differences between IoV and traditional wired networks. The intrusion detection technology based on wired networks can hardly be applied to IoV due to the unavailability of fixed basic network architecture. Network-based intrusion detection systems in wired network rely on real-time traffic analysis. Traffic monitoring is usually implemented on the switches, routers and gateways node. However, there are no flow centralized monitoring points which is available to collect the entire network data in IoV. For example, the node sending fake routing message might be captured nodes, but also may be due to a temporary loss of mobility and synchronization. Intrusion detection, in a way, is difficult to identify the true invasion and temporary system failure [55].
– Privacy protection in routing. In the package routing processing of IoV, the meeting frequency, social closeness, and network centrality and other social

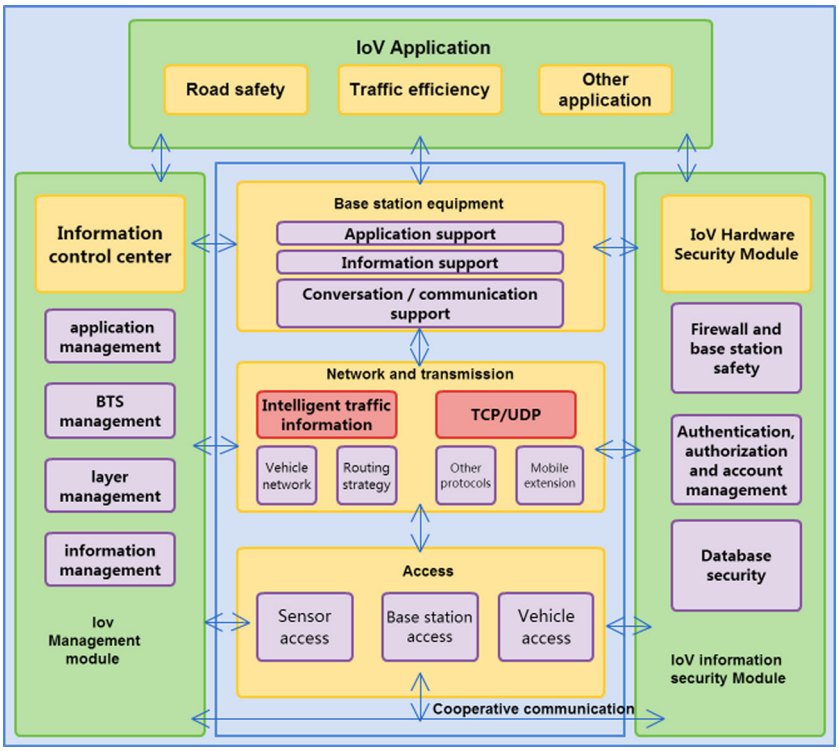

Fig. 6 Collaborative architecture of IoV

attributes of routing nodes play important roles in routing [87]. Correct and efficient routing needs the genuine utility information to be revealed and shared between the two nodes and most of the routing algorithms cannot be executed properly if such data are concealed from the two nodes. Here comes the paradox: how to protect the private routing information, i.e., a node's routing utilities and selected reasonable forwarders at the same time in IoV routing while guaranteeing the correct operations in routing are big challenges to be adequately addressed [88].

- Risk analysis and management. Risk analysis and management are used for the identification and management of potential threats and attacks in vehicle communication. Though the solutions to this kind of attack have been proposed very early, the behavior model-recording the user's behavior and extract rules-of this attack is still not clear [89].
- Trust and verification of data center. Data center provides the security of data communication through the trust and the audit of data [90]. The trust and verification of data center protect the vehicles in IoV from network threats and attacks, but the standard is not unified and this disunity hindered the further integration of IoV. Social network in IoV is an important aspect in view of trust management [91, 92]. How to verify trust-based recommendation in IoV social network is also a challenge currently [93].
- Forwarding algorithm. The goal of routing is to select the best route to reach the destination while the purpose of forwarding is to determine how the package is sent from one node to another after the route has been selected, and give consideration to the instability of bandwidth and topological structure in IoV [53].
- Delay constraint. The data packets sent by applications of IoV usually have a special significance in the aspects of time and position. The major challenge of designing vehicle communication protocols is how to provide good delay performance under the restrictions of vehicles' speed, unstable connection, and quickly changing network topology [94].
- Cross layer transmission and its reliability. Due to the characteristics of wireless communication between vehicle and vehicle or vehicle and network, connections may end abruptly [95]. Traffic safety is difficult to obtain stable security in this case. Therefore, designing the cross layer transmission protocol is really important for IoVs to support real-time and multimedia applications. [96] systematically proposes a layered adaptive security architecture to prevent adversaries from breaking-through all layers of security by simply compromising one particular security measure.
- Privacy and security protection in mobile cloud computing. Protecting the data of mobile cloud participants and allowing users to decide how to expose or hide their information are the main targets of mobile cloud computing [97]. The mobile nodes always become temporarily disconnected, so the data of mobile applications can be delegated to mobile cloud computing. The devices that have been penetrated by different type of attackers should also be protected by mobile cloud computing. However, protection mechanisms always mean negative impact on functions, for example, how to determine the right lifetime of certificate can be difficult, fixed lifetime, location-dependent or speed-dependent can have various effects in different situations [98].
- Dealing with big data. More and more modern vehicle models can access into Internet by lots of types of communication modes, for example, General Motors Co.GM −1.25 % has rolled out built-in LTE 4G broadband connections in more than 30 vehicle models [99]. Therefore, automakers are facing the challenge of handling large quantities of data generated by millions of vehicles to maintaining the security and privacy of customer information. In [100, 101], a two-levels of event linked network model is proposed to represent both the big status data and changing data independently with an efficient way and to manage and apply the knowledge produced in the Internet of Things. The model would be useful for IoV big data management and analytics.

6 Discussion and conclusion

Due to the broad prospects of IoV, more and more countries and institutions participate in the study of IoV application to make intelligent transportation penetrate into traditional transportation, which lefts increasing unfathomed security problems, and such fact also catches people's attention. The US released Fair Information and Privacy Principles directed at its intelligent traffic system (ITS) since 1999, and National Institute of Standards and Technology devised Cybersecurity Risk Management Framework Applied to Modern Vehicles [102]. EU also started ITS Action Plan to restrict the use of IoV data to ensure the security. However, the security problems still exist such as the security hole of Connected-Drive of BMW which could make more than 200,000,000 vehicles get attacked, and the flaws of the OnStar system General Motors, the most famous veteran of the ITSs, cause vehicles could be manipulated remotely [103].

Obviously, each aspect of IoV technologies has made great progress, but security and privacy issues in IoV

applications have always been in spotlight. Security and privacy are also technical difficulties in IoV and still exist a long list of unresolved problems. In one sense, security and privacy will also determine the promotion and popularization degree of IoV and they are also the crucial premise and foundation for IoV would be put into large scale of use. Vehicle users, vehicle manufacturer, suppliers, insurance companies, public agencies, and anyone effective connected in the transportation network all play important roles in IoV. Vehicle manufacturers, communication service providers, and middleware service providers need a more unified standards and development strategies to make IoV play its value steadily in all of these things connected world. Nevertheless, in addition to the technical factors, the constraint and supervision of governments are also significant.

In this paper, we first give a brief introduction to IoV, propose five characteristics of IoV system from the security view including dynamic topological structures, huge network scale, non-uniform distribution of nodes, granularity diversity, and mobile limitation. According to these characteristics, a summarization on five different types of attacks to IoV systems is presented. These attacks are mainly on authentication, availability, secrecy and privacy, routing, and data authenticity. We also overview existed countermeasures for IoV security issues from six aspects: threat models, intrusion detection system, honeypot system, secure routing protocols, routing privacy protection mechanism, and key management. Finally, we propose the future research trends of the Internet of Vehicles. Generally speaking, this paper makes an overall introduction on the present situation of security and privacy in IoV which could contribute to the further study.

Acknowledgment This research is sponsored by the National Natural Science Foundation of China (No. 61371185, 61571049) and China Postdoctoral Science Foundation (No.2015M571231).

References

1. Leng Y, Zhao L (2011) Novel design of intelligent internet-of-vehicles management system based on cloud-computing and internet-of-things. In: 2011 International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT), vol 6. IEEE, pp 3190–3193
2. Kolls HB (2003) Communicating interactive digital content between vehicles and internet based data processing resources for the purpose of transacting e-commerce or conducting e-business. uS Patent,6,615,186
3. Ahmed SH, Bouk SH, Yaqub MA, Kim D, Song H, Lloret J Codie: Controlled data and interest evaluation in vehicular named data networks
4. Wang J, Cho J, Lee S, Ma T (2011) Real time services for future cloud computing enabled vehicle networks. In: 2011 International Conference on Wireless Communications and Signal Processing (WCSP), pp 1–5
5. Lazarevic A, Srivastava J, Kumar V (2002) Cyber threat analysis–a key enabling technology for the objective force (a case study in network intrusion detection). In: 23rd Army Science Conference Proceedings of the IT/C4ISR
6. Yu L, Deng J, Brooks RR, Yun SB (2015) Automobile ecu design to avoid data tampering. In: Proceedings of the 10th Annual Cyber and Information Security Research Conference. ACM, p 10
7. Sicari S, Rizzardi A, Grieco L, Coen-Porisini A (2015) Security, privacy and trust in internet of things: the road ahead. Comput Netw 76:146–164
8. Singh R, Singh P, Duhan M (2014) An effective implementation of security based algorithmic approach in mobile adhoc networks. Human-centric Comput Inf Sci 4(1):1–14
9. Othmane LB, Weffers H, Mohamad MM, Wolf M (2015) A survey of security and privacy in connected vehicles. In: Wireless Sensor and Mobile Ad-Hoc Networks. Springer, pp 217–247
10. Yan G, Wen D, Olariu S, Weigle MC (2013) Security challenges in vehicular cloud computing. IEEE Trans Intell Transp Syst 14(1):284–294
11. Li W, Song H (2016) ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks. IEEE Transactions on Intelligent Transportation Systems 17(4):960–969
12. Wang L, Kangasharju J (2013) Measuring large-scale distributed systems: case of bittorrent mainline dht. In: 2013 IEEE Thirteenth International Conference on Peer-to-Peer Computing (P2P). IEEE, pp 1–10
13. Bellare M, Rogaway P (1993) Random oracles are practical: a paradigm for designing efficient protocols. In: Proceedings of the 1st ACM Conference on Computer and Communications Security. ACM, pp 62–73
14. Aura T, Nikander P, Leiwo J (2001) Dos-resistant authentication with client puzzles. In: Security Protocols. Springer, pp 170–177
15. Burgess J, Gallagher B, Jensen D, Levine BN (2006) Maxprop: Routing for vehicle-based disruption-tolerant networks. In: INFOCOM, vol 6, pp 1–11
16. Mershad K, Artail H (2013) A framework for secure and efficient data acquisition in vehicular ad hoc networks. IEEE Trans Veh Technol 62(2):536–551
17. Marian S, Mircea P (2015) Sybil attack type detection in wireless sensor networks based on received signal strength indicator detection scheme. IEEE
18. Chen C-Y, Yein AD, Hsu T-C, Chiang JY, Hsieh W-S (2014) Secure access control method for wireless sensor networks
19. Wang X, Wong J (2007) An end-to-end detection of wormhole attack in wireless ad-hoc networks. In: 131st Annual International Conference on Computer Software and Applications 2007, COMPSAC 2007. IEEE, pp 39–48
20. Tun Z, Maw AH (2008) Wormhole attack detection in wireless sensor networks. World Acad Sci Eng Technol 46:2008
21. Ji S, Chen T, Zhong S (2015) Wormhole attack detection algorithms in wireless network coding systems. IEEE Trans Mob Comput 14(3):660–674
22. Shah N, Valiveti S (2012) Intrusion detection systems for the availability attacks in ad-hoc networks. Int J Electron Comput Sci Eng (IJECSE, ISSN: 2277-1956) 1(03):1850–1857
23. Shah V, Modi N (2014) Responsive parameter based an anti-worm approach to prevent wormhole attack in ad hoc networks. Int J Netw Secur 5(1):1

24. Ko Y-B, Vaidya NH (2000) Location-aided routing (lar) in mobile ad hoc networks. Wirel Netw 6(4):307–321
25. Kannhavong B, Nakayama H, Nemoto Y, Kato N, Jamalipour A (2007) A survey of routing attacks in mobile ad hoc networks. IEEE Wirel Commun 14(5):85–91
26. Zargar ST, Joshi J, Tipper D (2013) A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. IEEE Commun Surv Tutorials 15(4):2046–2069
27. Wallgren L, Raza S, Voigt T (2013) Routing attacks and countermeasures in the rpl-based internet of things. Int J Distrib Sensor Netw 2013
28. Xia H, Jia Z, Li X, Ju L, Sha EH-M (2013) Trust prediction and trust-based source routing in mobile ad hoc networks. Ad Hoc Netw 11(7):2096–2114
29. Gite P, Thakur S (2015) An effective intrusion detection system for routing attacks in manet using machine learning technique. Int J Comput Appl 113(9)
30. Virmani D, Soni A, Chandel S, Hemrajani M (2014) Routing attacks in wireless sensor networks: A survey. arXiv:1407.3987
31. Pavani K, Damodaram A (2014) Anomaly detection system for routing attacks in mobile ad hoc networks, vol 6
32. Bakiler H, Şafak A (2015) Analysis of current routing attacks in mobile ad hoc networks. Int J Appl Math, Electron Comput 3(2):127–132
33. Mejri MN, Ben-Othman J, Hamdi M (2014) Survey on vanet security challenges and possible cryptographic solutions. Veh Commun 1(2):53–66
34. Zhao M, Walker J, Wang C-C (2012) Security challenges for the intelligent transportation system. In: Proceedings of the First International Conference on Security of Internet of Things. ACM, pp 107–115
35. Rawat DB, Yan G, Bista B, Weigle MC (2014) Trust on the security of wireless vehicular ad-hoc networking
36. Ellison G, Lacy J, Maher D, Nagao Y, Poonegar A, Shamoon T (2012) The car as an internet-enabled device, or how to make trusted networked cars. In: Electric Vehicle Conference (IEVC), pp 1–8
37. Anwar RW, Bakhtiari M, Zainal A, Abdullah AH, Qureshi KN (2014) Security issues and attacks in wireless sensor network. World Appl Sci J 30(10):1224–1227
38. Al Ameen M, Liu J, Kwak K (2012) Security and privacy issues in wireless sensor networks for healthcare applications. J Med Syst 36(1):93–101
39. Qu F, Wu Z, Wang F-Y, Cho W (2015) A security and privacy review of vanets
40. Almeida J, Shintre S, Boban M, Barros J (2012) Probabilistic key distribution in vehicular networks with infrastructure support. In: 2012 IEEE Global Communications Conference (GLOBECOM). IEEE, pp 973–978
41. Aouzellag H, Ghedamsi K, Aouzellag D (2015) Energy management and fault tolerant control strategies for fuel cell/ultracapacitor hybrid electric vehicles to enhance autonomy, efficiency and life time of the fuel cell system. Int J Hydrog Energy 40(22):7204–7213
42. MaliK V, Bishnoi S (2014) Security threats in vanets: A review
43. Serna-Olvera JM, Medina Llinás M., Luna Garcýa A. (2013) A trust-driven privacy architecture for vehicular ad-hoc networks
44. Qabajeh LK, Kiah MLM, Qabajeh MM (2009) A scalable and secure position-based routing protocols for ad-hoc networks. Malays J Comput Sci 22(2):99–120
45. Lindgren A, Doria A, Schelén O. (2003) Probabilistic routing in intermittently connected networks. ACM SIGMOBILE Mob Comput Commun Rev 7(3):19–20
46. Balasubramanian A, Levine B, Venkataramani A (2007) Dtn routing as a resource allocation problem. ACM SIGCOMM Comput Commun Rev 37(4):373–384
47. Costa P, Mascolo C, Musolesi M, Picco GP (2008) Socially-aware routing for publish-subscribe in delay-tolerant mobile ad hoc networks. IEEE J Sel Areas Commun 26(5):748–760
48. Sharef BT, Alsaqour RA, Ismail M (2014) Vehicular communication ad hoc routing protocols: a survey. J Netw Comput Appl 40:363–396
49. Daly EM, Haahr M (2007) Social network analysis for routing in disconnected delay-tolerant manets. In: Proceedings of the 8th ACM International Symposium on Mobile ad hoc Networking and Computing. ACM, pp 32–40
50. Wu J, Xiao M, Huang L (2013) Homing spread: Community home-based multi-copy routing in mobile social networks. In: INFOCOM, 2013 Proceedings IEEE. IEEE, pp 2319–2327
51. Gao W, Cao G (2010) On exploiting transient contact patterns for data forwarding in delay tolerant networks. In: 2010 18th IEEE International Conference on Network Protocols (ICNP). IEEE, pp 193–202
52. Zhang X, Cao G (2013) Transient community detection and its application to data forwarding in delay tolerant networks. In: 2013 21st IEEE International Conference on Network Protocols (ICNP). IEEE, pp 1–10
53. Hui P, Crowcroft J, Yoneki E (2011) Bubble rap: Social-based forwarding in delay-tolerant networks. IEEE Trans Mob Comput 10(11):1576–1589
54. Daly EM, Haahr M (2007) Social network analysis for routing in disconnected delay-tolerant manets. In: Proceedings of the 8th ACM International Symposium on Mobile ad hoc Networking and Computing. ACM, pp 32–40
55. Hussain R (2014) Cooperation-aware vanet clouds: providing secure cloud services to vehicular ad hoc networks. J Inf Process Syst 10(1):103–118
56. Md Nawaz Ali G, Mollah S, Abdus M, Samantha SK, Mahmud S (2014) An efficient cooperative load balancing approach in rsu-based vehicular ad hoc networks (vanets). In: 2014 IEEE International Conference on Control System, Computing and Engineering (ICCSCE). IEEE, pp 52–57
57. Sun Y, Zhang J, Xiong Y, Zhu G (2014) Data security and privacy in cloud computing. Int J Distrib Sens Netw 2014
58. Scandariato R, Wuyts K, Joosen W (2014) A descriptive study of microsoft's threat modeling technique. Requir Eng 20(2):163–180
59. Cohen F (1999) Simulating cyber attacks, defences, and consequences. Comput Secur 18(6):479–518
60. Cheung S, Lindqvist U, Fong MW (2003) Modeling multistep cyber attacks for scenario recognition. In: DARPA Information Survivability Conference and Exposition, 2003. Proceedings, vol 1. IEEE, pp 284–292
61. Wu J, Yin L, Guo Y (2012) Cyber attacks prediction model based on bayesian network. In: 2012 IEEE 18th International Conference on Parallel and Distributed Systems (ICPADS). IEEE, pp 730–731
62. Ingols K, Chu M, Lippmann R, Webster S, Boyer S (2009) Modeling modern network attacks and countermeasures using attack graphs. In: Computer Security Applications Conference, 2009. ACSAC'09. Annual. IEEE, pp 117–126
63. Camtepe SA, Yener B (2007) Modeling and detection of complex attacks. In: Third International Conference on Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. IEEE, pp 234-243
64. Chen TM, Sanchez-Aarnoutse JC, Buford J (2011) Petri net modeling of cyber-physical attacks on smart grid. IEEE Trans Smart Grid 2(4):741–749
65. Ekedebe N, Yu W, Song H, Lu C (2015) On a simulation study of cyber attacks on vehicle-to-infrastructure communication (v2i) in intelligent transportation system (its). In: SPIE Sensing Technology+ Applications. International Society for Optics and Photonics, pp 94 970B–94 970B

66. Mo Y, Sinopoli B (2009) Secure control against replay attacks. In: 47th Annual Allerton Conference on Communication, Control, and Computing, 2009. Allerton 2009. IEEE, pp 911–918
67. Yilin Mo BS, chabukswar R (2014) Detecting integrity attacks on scada systems. IEEE Trans Control Syst Technol 22(4):1396–1407
68. Kwon C, Liu W, Hwang I (2013) Security analysis for cyber-physical systems against stealthy deception attacks. Am Control Conf (ACC) 2013:3344–3349
69. Weimerskirch A, Thonet G (2002) A distributed light-weight authentication model for Ad-hoc networks. Springer, Berlin Heidelberg
70. Scarfone K, Mell P (2007) Guide to intrusion detection and prevention systems (idps), NIST SP - 800–94
71. Garca-Teodoro P, Daz-Verdejo J, Maci-Fernndez G, Vzquez E (2009) Anomaly-based network intrusion detection: techniques, systems and challenges. Comput Secur 28:188
72. Li W, Joshi A, Finin T Svm-case: An svm-based context aware security framework for vehicular ad-hoc networks. In: 82nd IEEE Vehicular Technology Conference. IEEE
73. Spitzner L (2003) Honeypots: tracking hackers, vol 1. Addison-Wesley Reading
74. Nikolaidis J (2003) Honeypots, tracking hackers [book reviews]. IEEE Netw 17(4):5–5
75. Gantsou D, Sondi P (2014) Toward a honeypot solution for proactive security in vehicular ad hoc networks. Lecture Notes in Electrical Engineering
76. Guerrero M, Guerrero M (2001) Secure ad hoc on-demand distance vector (saodv) routing. Internet Draft Ietf Mob Ad Hoc Netw Work Group 6(7):106–107
77. Hu YC (2002) Perrig a, johnson db. ariadne: a secure on-demand routing protocol for ad hoc networks. Proc Acm Int Conf Mob Comput Netw 11(1-2):21–38
78. Ping YI, Jiang YC, Zhong YP (2005) A survey of secure routing for mobile ad hoc networks. Comput Sci 1(3):27–31
79. Yao CC, Yao CC (1982) Protocols for secure computations (extended abstract), Pcr—O(1/n) = O(1) points from P Pcr in Si, since Pr[p Si] = (n 1/c) is, pp 160–164
80. Zhang X, Wang X, Liu A, Zhang Q, Tang C (2012) Pri: a practical reputation-based incentive scheme for delay tolerant networks. Ksiitransactionsoninternetandinformationsystems 6(4):973–988
81. Lu X, Hui P, Towsley D, Pu J, Xiong Z (2010) Anti-localization anonymous routing for delay tolerant network. Comput Netw Int J Comput Telecommun Netw 54(11):1899–1910
82. Lin X, Lu R, Liang X, Shen X (2011) Stap: a social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in vanets. Proc - IEEE INFOCOM 28(6):2147–2155
83. Ozturk C, Zhang Y, Trappe W (2004) Source-location privacy in energy-constrained sensor network routing, Acm Sasn, pp 88–93
84. Chen Y, Xu W, Trappe W, Zhang Y (2005) Enhancing source-location privacy in sensor network routing. In: 2013 IEEE 33rd International Conference on Distributed Computing Systems, pp 599–608
85. Yong HK, Lee H, Dong HL, Lim J (2006) A key management scheme for large scale distributed sensor networks. Lect Notes Comput Sci:437–446
86. Zhang C, Lu R, Lin X, Ho P-H, Shen X (2008) An efficient identity-based batch verification scheme for vehicular sensor networks. In: INFOCOM 2008. The 27th Conference on Computer Communications. IEEE. IEEE
87. Shah N, Huang D (2010) A-weor: Communication privacy protection for wireless mesh networks using encoded opportunistic routing. In: INFOCOM IEEE Conference on Computer Communications Workshops, pp 1–6
88. Li Y, Ren J (2009) Preserving source-location privacy in wireless sensor networks. In: 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON '09, pp 1–9
89. Sherer SA (1992) Risk analysis and management. Appl Modern Technol Bus 269(1):13–24
90. Raman B, Mao ZM et al (2002) The sahara model for service composition across multiple providers. In: Pervasive Computing, pp 1–14
91. He Z, Cai Z, Wang X (2015) Modeling propagation dynamics and developing optimized countermeasures for rumor spreading in online social networks. In: The 35th IEEE International Conference on Distributed Computing Systems, pp 205–214
92. Wang Y, Cai Z, Yin G, Gao Y, Pan Q (2016) A game theory-based trust measurement model for social networks, Computational Social Networks
93. Wang Y, Yin G, Cai Z, Dong Y, Dong H (2015) A trust-based probabilistic recommendation model for social networks. J Netw Comput Appl 55:59–67
94. Salama HF, Reeves DS, Viniotis Y (1997) A distributed algorithm for delay-constrained routing. IEEE/ACM Trans Netw 8(2):84
95. Raisinghani VT, Iyer S (2004) Cross-layer design optimizations in wireless protocol stacks. Comput Commun 27(8):720–724
96. Wang S, Bie R, Zhao F, Zhang N, Cheng X, Choi H.-A (2015) Security in wearable communications. IEEE Network. (In press)
97. Whaiduzzaman M, Sookhak M, Gani A, Buyya R (2014) A survey on vehicular cloud computing. J Netw Comput Appl 40(1):325–344
98. Casetti C, Torino PD (2012) Security and privacy in ivc. In: Proceedings CCNC 2012 Tutorial
99. King R (2015) Gm grapples with big data, cybersecurity in vehicle broadband connections. The Wall Street Journal, p 10
100. Sun Y, Jara AJ (2014) An extensible and active semantic model of information organizing for the internet of things. Pers Ubiquit Comput 18(8):1821–1833
101. Sun Y, Yan H, Lu C, Bie R, Zhou Z (2014) Constructing the web of events from raw data in the web of things. Mob Inf Syst 10(1):105–125
102. Mccarthy C, Harnett K (2014) National institute of standards and technology (nist) cybersecurity risk management framework applied to modern vehicles, Risk Management
103. Zhang T, Delgrossi L (2012) Vehicle safety communications: protocols, security, and privacy, vol 103. Wiley