Security and Privacy in Emerging Wireless Networks

Di Ma
Computer and Information Science Department
University of Michigan-Dearborn
dmadma@umd.umich.edu

Gene Tsudik
Computer Science Department
University of California, Irvine
gts@ics.uci.edu

***Abstract*—Wireless communication continues to make in-roads into many facets of our society and gradually becomes more and more ubiquitous. While, in the past, wireless communication (as well as mobility) was largely limited to first and last transmission hops, today's wireless networks are starting to offer purely wireless, often mobile, and even opportunistically connected operation. The purpose of this paper is to examine security and privacy issues in some new and emerging types of wireless networks and identify directions for future research.**

***Index Terms*—wireless networks, security and privacy, sensor networks, vehicular networks, disruption-tolerant networks**

I. Introduction

Wireless communication plays an increasingly important role in many spheres of our society. It has become an essential (and, in some cases, ubiquitous) means of communication. The number of wireless phones exceeded that of wired ones and soon there will be more smart-phones than PCs [24]. Wireless LANs are commonplace; they are being routinely used at home, work, and many other public venues, such as cafes and malls. Most current wireless networks are employed in the context of personal communication where end-users are human beings. In such networks, wireless communication typically occurs only at the first and last hops. For example, cell phones communicate indirectly, via base stations that are, in turn, connected to wired networks. Similarly, wireless LANs are usually connected to wired access points that are, in turn, connected to larger wired LANs and/or Internet Service Providers (ISPs). We refer to these networks collectively as: *infrastructure-based wireless networks*. Since communications originating (or terminating) in cell-phones or WiFi-capable devices usually transit a fixed network infrastructure, few (if any) *new* security and privacy issues arise from such networks.

Recent advances in technology have motivated new application domains for wireless networks. For example, wireless sensor networks (WSNs) are used for environmental monitoring in both civilian and military settings. Vehicular *a*d hoc networks (VANETs) promise safer roads and improved driving experience, while disruption-tolerant networks (DTNs) bring low-cost best-effort connectivity to challenged environments with little or no infrastructure. At the same time, there has been a surge of interest in body-area networks (BANs) with envisaged applications in military, law enforcement, sports and medical domains. These emerging wireless networks extend the network function beyond purely personal communication and potentially offer a world of truly ubiquitous computing. One of their distinctive features is the lack of (or non-reliance on) any wired or fixed infrastructure. Nodes communicate either directly or via peers, instead of using infrastructure elements, such as base stations or access points. Since nodes themselves are responsible for forwarding messages, they play an increasingly active role in networking mechanisms. Also, network formation does not need to follow some pre-defined fashion: nodes might move independently, and the network topology can be formed on an *a*d hoc basis.

In general, we observe that wireless networking is in the process of transition from conventional infrastructure-based last-hop-wireless networks to more dynamic, self-forming, self-organizing (autonomous) peer-to-peer networks. This transition has significant implications for both security and privacy:

- In traditional (first- and/or last-hop) wireless networks, the high cost of setting up the infrastructure limits network operators to sufficiently large entities that presumably care about their brand name and overall reputation. Thus, they are expected to be trusted by end-users. Accordingly, security in these networks is centered on protecting end-user data from being exposed to outsiders and preventing the infrastructure from being accessed by unauthorized parties. Whereas, in emerging wireless networks, most communication is via peers. Even if there is some form of central authority, it might be less trusted (as in wireless mesh networks). In fact, there might be no central authority at all, at least not one that is present all the time. Consequently, nodes can be compromised, removed or destroyed without immediate or rapid detection. Moreover, without a centralized authority, devices have to work together to accomplish tasks, such as network formation, routing and adjusting to network dynamics. They might also need to take part in mitigating attacks. All these changes require dramatically different security and privacy techniques.
- In current wireless networks, end-users (or end-devices) are not concerned with network topology, since they communicate directly to some fixed infrastructure. Whereas, emerging wireless networks might evolve in a decentral-

ized fashion, and topology formation might be dynamic and *a*d hoc. In the absence of permanent connections communication may take place over opportunistic links. Efforts to secure wireless communication with non-permanent and opportunistic connections must consider specific constraints of dynamic network topology and intermittent connectivity.

Many valuable lessons were learned from securing wired networks, such as the Internet, where security has been treated incrementally. Typically, newly discovered (or previously underestimated) security problems and vulnerabilities are fixed by painstakingly applying *a*d hoc patches. This constitutes an unsystematic and reactive approach which is unfortunately fraught with problems. We believe that a proactive approach (i.e., one that anticipates threats) should be taken in the context of emerging wireless networks.

In this paper, we consider security and privacy issues in certain emerging wireless networks: wireless sensor networks (WSNs), vehicular *a*d hoc networks (VANETs) and disruption-tolerant networks (DTNs). These types of networks were picked based on our view of their perceived importance and popularity in the near future. In doing so, our goal is to identify new problems, i.e., attacks, threats, and other issues not previously encountered.

Disclaimer: This paper's scope of coverage is not intended to be exhaustive. This is due partly to our (clearly subjective) decision about what types of wireless networks are new and/or emerging, and partly – to our opinion about what security and privacy problems are *new* in these wireless networks.

II. General Security Issues

As is well-known, wireless networks are inherently more vulnerable than their wired counterparts. Also, complications arise in the presence of node mobility and dynamic network topology. Moreover, intermittent connectivity, whether caused by mobility or periodic node sleep (or hibernation), brings about additional challenges. At the same time, node resource constraints – due to battery operation (power), weak transceivers (bandwidth), and small memory/storage – make direct adoption of existing security solutions difficult, if not impossible. Finally, in some settings, network size and/or physical inaccessibility of nodes further exacerbates security problems.

Key factors contributing to security problems include the following:

- **Channel.** Wirelessness usually (though not always, e.g., Infra-Red and laser) involves broadcast communication which makes eavesdropping and jamming easier.
- **Mobility.** Although not all wireless devices are mobile, wirelessness, by its very nature, enables mobility. In wireless communication, physical connection is replaced by logical association. The latter can be interrupted and must be renewed whenever a wireless device moves beyond transmission range. Establishing secure association in the presence of mobility is challenging, especially, in high-mobility settings, such as VANETs. At the same time, if a wireless device is affiliated with a human user, tracking the device reveals the user location and mobility patterns. Thus, privacy becomes an important concern.
- **Resources.** Some modern high-end wireless devices (e.g., PDAs and smart-phones) have fast processors and run actual operating systems (e.g., Symbian and Windows Mobile), thus blurring the distinction between them and laptops. However, most wireless devices are still resource-constrained. One fundamental reason is the need to keep physical size small to enable mobility and embeddability. Also, even high-end wireless devices are battery-powered, which limits computation and communication ability as well as the size of RAM and secondary storage. Such limitations open the door for denial of service attacks aimed at battery depletion.
- **Accessibility.** While some devices are personal and usually attended by their owners, others (e.g., sensors or robots) are generally left unattended and are placed in remote and/or hostile locations. This greatly increases their vulnerability to physical attacks.

III. Wireless Sensor Networks

The original motivation for wireless sensor network (WSN) research stemmed from the vision of Smart Dust in the late 1990-s [26]. This entailed an integrated computing, communication and sensing platform consisting of small devices, enabling applications such as dense environmental monitoring and smart home/office. Since then, progress in WSN research has yielded major advances toward the original Smart Dust vision.

A typical WSN encountered in the research literature consists of a large number of small, cheap and resource-constrained sensors and a few base stations or sinks. In most WSN settings, sensors collect data from the environment and forward the collected data hop-by-hop to the sink. A sink is a more powerful entity. It may serve as a gateway to another network, a data processing or storage center, or an access point for human interface. WSN deployment can be *a*d hoc, e.g., sensors might be air-dropped over a designated area without exact pre-positioning. Because of their allegedly easy deployment, WSNs appeal to a wide range of applications in military, environmental, disaster relief, and homeland security domains.

Security has always been considered to be an important factor in the eventual success of WSNs, especially, in security-sensitive applications such as military or homeland security. A flurry of research results appeared in early 2000-s, addressing a number of WSN security issues, including key management, secure routing, DoS attacks, and clone detection. Due to sensor resource constraints, many prior results involved impressive cryptographic contortions aimed at miniaturizations of security functionalities (e.g., key management) that are not specific to WSNs. However, some research addressed issues unique to WSNs, e.g., clone detection and certain DoS attacks. Also,

there has been some notable research in application-specific WSN security, such as secure aggregation and secure statistical sampling.

Despite oft-claimed successes, the current range of deployed WSN applications is still far from the ubiquitous and autonomic sensing and computing platform envisaged by Smart Dust. First, although WSN deployment can be *a*d hoc, the underlying network model is usually not infrastructure-less and information flow is funneled at the sink. The sink is a powerful entity that plays an important security and privacy role for the entire network. Indeed, most WSN security efforts have assumed continuous presence of the sink. Once a sink receives data collected by individual sensors, it takes care of storage of, and access control to, that data. (In the remainder of this paper, we use the term "sink" to collectively denote all management and collection entities, including mobile collectors and static sinks). Also, most WSNs suffer from limited network life span due to finite-capacity sensor batteries. Once the battery runs out of power, the sensor dies. This makes WSNs ill-suited for settings where replacing sensors or recharging sensor batteries is difficult or impossible.

However, two new WSN types bring us closer to the Smart Dust vision. The first is Unattended WSNs (UWSNs) that operate in unattended mode without constant presence of the sink, and the second – WSNs composed of sensors equipped with RFID tags. In the following sections, we overview security issues in these WSN types.

A. Unattended WSNs

Unattended WSNs, or simply UWSNs, operate without continuous presence of (or supervision by) a sink. Instead, sensor data is collected by an itinerant sink that visits the network intermittently, with a certain upper bound on the interval between successive visits. Because sensors cannot communicate with the sink at will, they must accumulate data in situ and wait for the sink. The unattended nature of the network might be promoted by some design requirements to avoid any central point of failure. (For example, in military applications, a constantly present sink represents an attractive and valuable attack target.) The unattended nature might also be caused by the inaccessibility of the WSN deployment area.

Since, in a UWSN, data is stored on individual sensors, securing that data is both important and challenging. Clearly, sensors operating in unattended mode face greater risk of compromise. Once a sensor is compromised, its data and all secrets are learned by the adversary. Consequently, UWSN security must take into account undetectable sensor compromise.

Distinctive characteristics of UWSNs prompt a new mobile adversary model [37]. In particular, the adversary can compromise a subset of sensors within a certain time interval (see Figure 1). While in control of a sensor, the adversary can read, and possibly write to, that sensor's memory, storage and communication interfaces. In the next interval (round), the adversary can either continue occupying the same subset of sensors or migrate to another subset. Given enough rounds, the adversary can gradually compromise the entire network. Time between successive sink visits represents periods of vulnerability that motivate mobile adversary attacks. (We note that a similar *parasitic* adversary was investigated in [36], however, in the more traditional WSN context, where a sink is always present.)

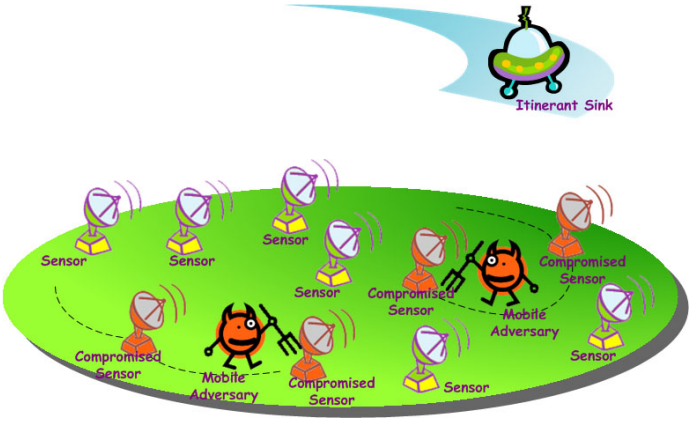

Fig. 1. A mobile adversary in a UWSN setting.

The main challenge is protection of data accumulated on unattended sensors from a mobile adversary. Considering that compromise of a given sensor has a certain duration, sensor-resident data can be classified into three categories, based on the exact time of compromise: (1) before compromise, (2) during compromise, and (3) after compromise. Security of category (1) data is referred as **Forward Security**. It means that, even if the adversary obtains the sensor's current secrets, it cannot decrypt (or forge authentication tags for) data collected and encrypted (or authenticated) before compromise. Whereas, security of category (3) data is referred as **Backward Security**: even if the adversary obtains the sensor's current secrets, it cannot decrypt (or forge authentication tags for) data in category (3). Of course, nothing can be done about security of category (2) data since, during that time, the adversary is in full control of the sensor. Therefore, the UWSN security challenge can be viewed as the ability to achieve both forward and backward security.

In prior UWSN results (e.g., [56]), forward security is attained by periodically updating secret keys (used for encryption or data integrity and origin authentication) through a one-way function. Time is divided into fixed-length intervals and a different key is used in each interval. An adversary that compromises a sensor and obtains its current key cannot compute pre-compromise keys due to the one-wayness property of the key update function. Data location privacy has been considered in data-centric UWSNs where sensor data of a given type is sent to and stored at some designated nodes [52]. To prevent the adversary from identifying storage nodes for a certain data type, a secret key (updated periodically through a one-way function) is used to determine these special nodes. UWSNs have also been considered in the context of minimizing storage and bandwidth overhead due to data authentication [38], [58]. Proposed forward-secure sequen-

tial aggregate authentication techniques provide both forward security and storage/communication efficiency. However, all these schemes do not offer backward security.

Recently, a suite of techniques were proposed specifically to defend against mobile adversary attacks in UWSNs. They addressed different types of attacks based on the adversary's goal: data survival [12]–[14], [48], secrecy [11], [39], and authentication [16]. The main common feature of all these techniques is *cooperation among all sensors*.

The central question in data survival is how to cope with a mobile adversary that aims to *surgically* erase specific data that it considers to be of value. To achieve data survival, sensors play a hide-and-seek game by moving all data around the network [12]–[14]. However, as shown in [12], [13], this is ultimately a losing game, unless cryptography is used [14]. Moreover, the use of cryptography is not at all intuitive. In particular, there is no security advantage in using public key (over symmetric) cryptography. (There is, however, an advantage as far as protocol robustness.) More recent work [48] utilizes secret sharing and error-correction coding to improve dependability among sensors in order to achieve higher data survival rate. It also uses a network coding approach to further enhance communication efficiency.

Subsequent results [11], [39] deal with a mobile adversary aiming to learn sensors' secrets in order to later decrypt data. Proposed techniques allow sensors to probabilistically recover from compromise by simultaneously providing and obtaining help to/from peer sensors and re-gaining secrecy through cooperation. Cooperation comes in two flavors: (1) in [39], sensors explicitly ask randomly chosen peers for help, and (2) in [11], sensors volunteer help to randomly chosen peers. One notable disadvantage of these collaborative self-healing techniques is their high bandwidth cost.

To cope with a mobile adversary that wants to modify sensor data, collaboration is once again suggested in [16]. The proposed technique involves sensors co-signing data of their peers. As long as at least one of the co-signers is not compromised, the sink can later verify both integrity and authenticity of collected data.

Another related result [15] considers intrusion-resilience in a mobile UWSN setting. In a mobile UWSN, sensors move according to some common mobility model (e.g., random jump or random walk) within a fixed deployment area. In this environment, the mobile adversary does not actually need to move physically. Instead, it can occupy (control) a certain fixed deployment sub-area and merely wait for unsuspecting sensors to migrate there. Analytical and simulation results show that collaboration among sensors remains a very effective way of regaining security. However, mobility facilitates and simplifies collaboration, since sensors no longer need to send or solicit contributions to/from random peers. Instead, after every move, each sensor exchanges random contributions with its immediate neighbors. The set of neighbors changes randomly, based on the specific mobility model. This results in much more efficient protocols than those in [11] and [39].

Besides data security, mobile sink compromise and user privacy have been considered in the context of UWSNs. UWSNs are assumed to employ mobile sinks for periodic data collection and network maintenance. Compromise of a mobile sink is obviously quite dangerous. To this end, privilege restriction schemes were proposed to grant a mobile sink the least privilege while not impeding its ability of carrying out its intended tasks [61]. Also, a UWSN might be accessed by multiple clients (subscribers). To prevent malicious network operators from linking users with their data access patterns, some privacy-preserving schemes have been proposed to hide either client identify [60], or client search interest and query patterns [9].

B. RFID WSNs

As mentioned earlier, battery operation is the bane of most commodity sensors. Although many research efforts have focused on (and succeeded in designing) energy-efficient communication and computing mechanisms for WSNs, there is no way to mitigate the fact that, as batteries get depleted, sensors gradually "die", regardless of techniques used to minimize power consumption.

Recently, *RFID sensors* (RSensors) have emerged as a means of addressing the problem of battery-powered WSNs [6], [23]. RSensors are powered by harvesting Radio Frequency (RF) power from a reader sink (RSink). Harvested energy is stored on a capacitor that can sustain virtually unlimited charging cycles, enabling an RSensor to have a potentially very long lifespan and few or no requirements vis-a-vis maintenance. To reduce reliance on RSink, RSensors can be further equipped with other energy harvesting means that derive power from environmental sources, such as solar, thermal, vibrational or ambient RF energy [1], [7], [27], [28], [49]. Also, being battery-less, RSensors can have *smaller form factor*, which allows them to be used for sensing and computation in places where a battery-powered device cannot be placed.

Intel's Wireless Identification and Sensing Platform (WISP) is the first fully-passive RSensor that uses an ultra-low power 16-bit general-purpose micro-controller for sensing, computation and RFID communication [53]. The Intel Passive Data Logger (PDL) is an RFID sensor data logging platform [8]. It extends the WISP platform by attaching a storage capacitor (the size of pea) and has an additional property: it can (unlike passive WISPs) collect data while not in presence of an RFID reader.

This new paradigm opens up numerous promising applications for ubiquitous sensing and computation. Although RSensor WSNs (RWSNs) are not expected to totally replace WSNs, they facilitate new application domains where long life and small size (as well as, possibly, deployment in inaccessible locations) are important.

Very little research on RSensor or RWSN security has been done thus far. We are aware of one result that deals with backup checkpoint status integrity of RSensor [50]. Since RSensors operate intermittently (depending on the availability of RSink), one problem occurs due to energy constraints

in executing cryptographic computations. Power derived by the sensor from a single cycle of harvested energy might be insufficient to perform a realistic cryptographic operation. CCCP (Cryptographic Computational Continuation Passing) [50] suggests that an RSensor can perform demanding computations despite limited energy and power interruptions. The main idea is for a sensor to backup its RAM state just before it loses power (e.g., when the sink leaves). When the sink reappears, the sensor can retrieve its backed up state and resume unfinished operations, without having to re-start from scratch.

C. Summary

Considering the trends discussed above, we envision a new class of WSNs characterized by one or both of: (1) unattended nature, and (2) intermittent operation. The latter causes sporadic connectivity, since only a subset of the nodes is "on" at any given time. Such networks (referred to as IUWSNs - Intermittently-connected Unattended WSNs) are expected to be useful in remote, inaccessible and/or hostile environments (e.g., conflict zones, international borders, disaster areas and nature reserves). During periods of unattended operations, IUWSNs are subject to threats different from those facing other WSNs. In particular, detection and mitigation of attacks is greatly complicated by the fact that sensors have to essentially fend for themselves. Whereas, intermittent sensor operation and potential depletion of battery power (before the next sink visit) motivate integration of sensors and RFID technology in order to facilitate "post-mortem" data collection (from *dead* sensors) by a mobile sink that acts as an RFID reader. Since IUWSNs face distinct security threats, research is needed to develop effective and efficient attack countermeasures. We note that further research issues arise in the presence of sensor mobility, whether voluntary (i.e., self-locomotion) or not (e.g., air- or water-borne deployment).

IV. Vehicular Ad Hoc Networks

Vehicular Ad Hoc network (VANET) technology allows an automobile to become both a wireless node and a router. Vehicles can communicate with each other, with road-side infrastructure nodes (that may, in turn, connect to the Internet) as well as with pedestrians equipped with wireless devices, such as smart-phones or PDAs. Because of the pervasiveness of roads and highways, VANET deployment can cover very large areas.

VANETs enable a wide range of applications. Basic applications are aimed at improving road safety (e.g., collision warnings, weather and road hazard alerts, road closure and detour information) as well as providing driver convenience (e.g., notification of real-time traffic information, parking availability, and location-based services) [5]. Due to potential wide-area coverage, non-energy-starved nodes and infrastructure-less operation, many other VANET-based applications have emerged. VANET-based file distribution systems such as SPAWN [41], CarTorrent [30], and Code Torrent [35], allow efficient distribution of entertainment or location-relevant content, such as local attractions, events, and tourist information, among traveling vehicles through cooperative downloading or network coding. VANET-based urban sensing platforms such as MobEyes [31]–[33] and VITP [17] provide proactive urban monitoring (e.g., traffic and pollution) services where vehicles continuously monitor their environment, store, process, and communicate sensed data to other vehicles in their vicinity. FleaNet offers a virtual VANET-based marketplace that allows a mix of mobile and stationary users to buy and sell goods [34].

Figure 2 illustrates an example VANET usage scenario. Safety messages are periodically sent out by participating vehicles over the 5.9 GHz band specifically allocated by the U.S. Federal Communications Commission (FCC) for vehicular communications (also known as Dedicated Short Range Communications (DSRC) [4]). Emergent information such as collisions can be spread out through the network quickly to surrounding vehicles in order for them to prepare accordingly. Meanwhile, vehicles equipped with cameras can form a vehicular sensing network and take (and exchange) pictures of their surroundings. Pictures as well as other information can be later retrieved by the authorities for the purpose of accident scene investigation.

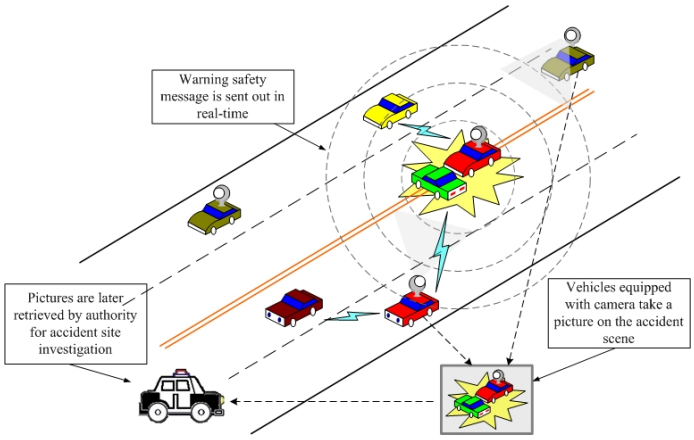

Fig. 2. Example VANET usage scenario.

We distinguish vehicular safety from other applications due to its highly time-critical message delivery and liability requirements. Safety messages are very time-sensitive, since they must be delivered within a specified time window in order for other vehicles to respond and possibly avoid accidents and other hazards. Also, security is particularly important in VANET safety applications. If security is not properly handled, new safety concerns might arise. For example, as cars start to communicate via the wireless channel, they become subject to remote attacks. We claim that the full potential of these systems for improving road safety will not be realized until network security issues are fully resolved. Because of our society's reliance on transportation systems, VANET applications and their security issues can and will have profound societal impact.

Fortunately, unlike nodes encountered in other types of *a*d hoc networks, vehicles are typically not subject to energy

constraints and can thus be equipped with high-end processors, sizable memory/storage, and powerful wireless transceivers. Thus, a broad range of security and cryptographic tools can be used. Although different VANET applications have specific security requirements, most security issues are not unique to VANETs.

In the following, we first survey existing communication security solutions in safety-related VANET applications and then discuss whether current solutions for secure communication are suitable for other VANET applications that take advantage of infrastructure-less inter-vehicle communications.

A. VANET Safety Applications

The earliest work discussing security issues in vehicular networks is due to [59]. Several subsequent papers examined security challenges in VANETs and discussed basic mitigation measures [43], [44], [46], [47].

Securing vehicular communication in the context of safety-related applications calls for several conflicting security properties. First, VANET-based safety applications involve high liability which incentivizes authentication and non-repudiation. It is not hard to imagine accidents, injuries or even deaths occurring when vehicles receive – and/or respond to – false information. Before taking actions, a vehicle must establish that the message it received is indeed coming from a legitimate user and that the message has not been tampered with in transit. Ideally, vehicles should only respond to legitimate events. Although authentication itself does not guarantee legitimacy of information conveyed in the message, it makes sure that a sender cannot deny originating a message.

As mentioned above, responding to false safety messages can have dangerous consequences. By examining messages exchanged before accidents, vehicles that originated false information must be identified. However, authentication raises certain privacy concerns. VANET communication, is subject to easy eavesdropping. If a plain digital signature scheme is used for authentication, all messages from the same vehicle are signed with the same private key and verified using the same public key. This allows an observer to link messages emitted by the same vehicle at different locations and times, thus enabling tracking. Hence, unlinkability with respect to observers (which include intended recipients) must be provided.

In general, VANET nodes operate in a very dynamic environment. Vehicles move at high speeds and connectivity time windows are short, with respect to both other vehicles and roadside infrastructure. Hence, security mechanisms need to be very time-efficient in order to meet such stringent real-time constraints.

Many schemes have been proposed to address VANET security, including authentication, non-repudiation and privacy. Taking advantage of safety messages being disseminated via broadcast, an extension of the symmetric key-based TESLA authentication protocol was developed for VANET message authentication in [54]. However, a symmetric key-based approach does not provide non-repudiation. Digital signatures are the most widely accepted and natural approach for message authentication with non-repudiation [46]. However, if a vehicle's public key is associated with vehicle identity, e.g., Electronic License Plate (ELP), identification and tracking become trivial. One way to mitigate this problem is by assigning each vehicle an anonymous public key pseudonym unrelated to any identity. As pointed out in [47], this conceals vehicle identity but still allows tracking.

The simplest way to simultaneously achieve authentication, non-repudiation and anonymity, is to supply each vehicle with a large set of certified public/private keys during the periodic re-registration process (e.g., yearly safety inspection) [47]. Each key is then used only for a brief period of time, such as a day. Another way is to use group signatures [22]. However, group signatures are computationally expensive and cannot meet strict delay requirements in safety-related VANET applications. Furthermore, efficient revocation poses a problem considering the potential immense scale of the network.

Recently, a hybrid scheme that utilizes a combination of group and plain signatures is proposed in [55]. In it, Regional Authorities (RA) issue temporary public/private keys (not linked to node identity) to participating vehicles that enter a specific region. Both RAs and vehicles are certified by a Managing Authority (MA) which serves as the root of trust, such as the Department of Motor Vehicles. When a vehicle enters a region, it sends an authenticated request to the local RA asking for a temporary anonymous certified key (TACK). A vehicle is equipped with a group user key issued by the MA and its request is authenticated using a group signature generated under its group user key. After getting a TACK from the RA, the vehicle uses it for subsequent V2V communication. Since each TACK is short-lived, the scheme satisfies the aforementioned security requirements with efficient authentication and revocation. However, it requires non-trivial set-up of the infrastructure units (such as RAs).

B. Security in Other VANET Applications

As discussed above, besides safety applications, VANETs motivate other applications that could benefit the car industry and network operators.

Non-safety (general-purpose) VANET applications might have similar general security requirements: authentication, non-repudiation and privacy, albeit, without criticality of strict timing constraints on message delivery. Security mechanisms for safety applications might not be re-usable in general-purpose applications. This is because general-purpose applications, at least in the near future, are unlikely to use the roadside infrastructure. A ubiquitous and reliable roadside infrastructure takes years to deploy and, even when deployed, its purpose would be to primarily support safety-related applications, while other uses might be either discouraged, disallowed or simply priced too high. Therefore, infrastructure-reliant schemes such as TACK could be unsuitable for general-purpose VANET applications and there is motivation to consider infrastructureless (*a*d hoc) solutions.

C. Summary

We view VANETs as a very important class of emerging wireless networks and VANET application security has the potential of having great impact on the daily lives of many millions of drivers. There has been quite a bit of prior work addressing security issues in safety-related VANET applications. However, the state-of-art requires the existence of reliable and ubiquitous roadside infrastructure. Exclusivity of this infrastructure (for safety applications) prompts considering the use of infrastructureless inter-vehicular communication (as well as security techniques) for general-purpose VANET applications. Finally, we note that technology alone cannot solve all VANET security issues. In particular, deployment of functional VANETs will require participation of public transportation agencies at national, state, and local levels. Large scale of the network, high mobility of vehicles, and involvement of both private and public sectors complicate the design of secure VANETs.

V. Disruption-Tolerant Networks

Advances in wireless communication allow mobile devices – vehicles, smart phones, PDAs and sensors – to form infrastructure-less *a*d hoc networks. Such networks can be rapidly deployed and are very useful in many real-world settings, e.g., military, law enforcement, disaster relief, and wildlife and environmental monitoring. Infrastructure-based networks assume existence of real-time end-to-end paths. However, this assumption does not hold in some infrastructure-less *a*d hoc networks where frequent communication disruptions occur, for various reasons such as limited radio range, mobility, obstacles, sparse coverage, and energy limitations. Traditional networks are unsuitable for handling disruptions. They simply drop messages when interruptions occur. However, failure of message delivery in some critical applications may have very serious consequences [40].

Disruption-Tolerant Networking (DTN) technology recently emerged as a means of providing connectivity (though in a non-real-time fashion) in networks with frequent interruptions. DTN was originally developed for deep space networking and inter-planetary communication [42]. However, the increased popularity of wireless networks, has given DTN many potential terrestrial applications. DTN technology introduces an overlay network atop the transport layer and delivers data over opportunistic links in a store-and-forward fashion. A DTN node is called a storage node: it retains data during periods of unavailability of the next hop. Stored data is forwarded whenever the next hop pops up. As long as subsequent links in an end-to-end path exist in ascending order, messages can be delivered to the intended recipient(s).

Ability to deliver messages in the presence of disruptions makes DTN an attractive technology for a range of applications from military [21], [25], [40] to civilian [3], [19]. DTNs are very applicable to sensor-based networks, terrestrial wireless networks, satellite networks, underwater acoustic networks as well as airborne networks. For example, the vehicular content delivery application [35] can take advantage of DTN technology to help cars deliver or share information when normal network coverage is either unavailable or too costly.

Although many DTN applications originate in the military, the most vaunted application for DTNs comes from the civilian milieu as a means of bringing low-cost best-effort connectivity to challenged environments with limited or no fixed network infrastructure. One typically cited scenario is a rural-area DTN providing Internet connectivity to remote and/or disadvantaged communities in developing regions. For example, a rural bus line can act as a store-and-forward message switch (similar to an SMTP server) with limited RF communication capability [19]. It can provide service to nearby clients and communicate with distant entities to be visited in the near future. An example DTN usage scenario is shown in Figure 3 where a traveler (Alice) passing through a distant village with no direct Internet connection uploads her latest travel content onto the bus (Bus A). Bus A then carries data to the nearest town with Internet connectivity. On its way to the town, Bus A encounters another bus (Bus B) which carries latest tourist information of the town which A will visit. Bus B shares the information with Bus A so that Bus A does not need to take the hassle to stop at a WiFi station to download such data. After Bus A comes to the town, Alice's content is forwarded to her friends via the Internet.

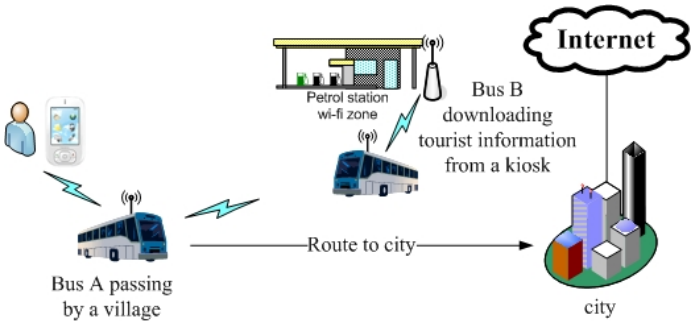

Fig. 3. Example DTN usage scenario.

A. Security Issues and Challenges

DTN security requirements include [3]:

- *Authentication* of origin (sender) and, possibly, of intermediate hops.
- *Integrity* of messages and, possibly, of message fragments.
- *Confidentiality* of end-to-end communication.

Although other types of wireless networks have the same or similar requirements, traditional network security approaches do not generally apply to DTNs mainly because they assume the existence of end-to-end paths. Frequent network partitions and intermittent connectivity in DTNs prompt some unique security issues and challenges.

Due to scarcity of network resources that characterizes many DTN settings, unauthorized access to and use of DTN resources is a serious concern. This motivates authentication

of origin on both end-to-end (transport) and link (hop-by-hop) bases. The latter is needed to allow intermediate storage nodes to validate traffic in order to avoid carrying unauthorized data. Furthermore, before forwarding data, the next-hop intermediate node must be authenticated. This is because, unlike traditional networks – where messages are routed through infrastructure nodes which are usually trusted to route data – DTN messages are routed through peers. Hence hop-by-hop authentication is needed to prevent malicious nodes from dropping messages.

Message authentication is further complicated if a message must be fragmented en route. DTN connections might last only a very short time. For example, if buses are used as storage nodes, connection between two fast-moving buses is likely to be very brief. Thus, it might be impossible to transfer an entire message before DTN nodes move out of each other's transmission range and fragmentation becomes a necessity. Ideally, both hop-by-hop and end-to-end authentication should support fragmented messages.

As usual, confidentiality is needed to protect sensitive communication. Encryption, either symmetric- or public-key based, is the standard way to achieve data confidentiality. Purely symmetric encryption requires the availability of Kerberos-like on-line key distribution servers (KDCs). Whereas, public key encryption requires a PKI, complete with directory servers to distribute peers' public keys and revocation information. (An alternative is to use Identity-Based Encryption; see below). Both are problematic in the DTN environment.

We now overview current security approaches and attempt to identify some open problems.

B. Using Identity-Based Cryptography

The usual PKI-based approach of bootstrapping secure communication is not well-suited for DTNs, since access to on-line servers (CAs, RAs) to retrieve public keys and check certificate revocation status is not guaranteed, due to lack of fixed infrastructure and intermittent connectivity. To this end, the use of identity-based cryptography (IBC) is proposed as a way of enabling message encryption and signature verification in DTNs [20].

In IBC, an entity's (e.g., user's) public key is derived from some unique identity information of that entity, e.g., an email address or a phone number. The corresponding private key is generated by a trusted third party called Private Key Generator (PKG). Anyone who knows the identity information of an entity party can easily generate the corresponding public key. Thus, without relying on any on-line servers or third parties to retrieve public keys, one can verify signatures from or encrypt information for any entity, knowing only its identity information. This feature is naturally quite attractive in the DTN context.

A DTN is expected to cover multiple geographical regions and DTN users in different regions need to acquire their private keys from different PKGs. To allow users in different regions to communicate securely, [51] proposed a security architecture using Hierarchical Identity-Based Cryptography (HIBC) where different regions contain sub-regions, each maintaining its own PKGs. Trust relationships between PKGs allow messages sent between users in different sub-regions to be authenticated and/or encrypted. Subsequently, [29] designed another HIBC-based security infrastructure which is more efficient and also offers anonymity.

One major problem with IBC-based schemes is revocation. This is particularly the case with Identity-Based Encryption (IBE). [1] Since user identity functions as that user's public key which is used for encryption, revoking a public key requires an identity change. This is not always feasible. One way to address this issue is to use time-dependent identities, e.g., adding timing information to identity strings. However, this triggers another problem since the receiver of an encrypted message has to contact its PKG to obtain the corresponding private key. The applicability of IBC for DTNs is studied in [2], [3] and it is showed that IBC is no better than traditional PKI in terms of authentication and only a little better than traditional PKI in terms of encryption since network connectivity is not necessarily needed at the time of reception and decryption.

In IBC-based schemes, kiosks operating in rural areas can be used as PKGs to generate their constituent users' private keys. Although a security architecture using a combination of physical and cryptographic mechanisms is proposed to protect rural Internet kiosks [57], it remains an open question how a kiosk PKG can verify whether a particular user has the right to a particular identifier.

C. Security Initialization

As discussed above, neither PKI- nor IBC-based approaches work particularly well in DTNs. A PKI requires on-line servers in order for users to retrieve public keys of peers or check their revocation status, while IBC requires rural-area PKGs to be capable of verifying the association between a user and a well-know identifier. Initializing secure DTN communication remains a difficult problem.

It is suggested that one viable way of bootstrapping DTN security is by leveraging existing infrastructure [3]. The proposed solution is to start with the current cellular telephone security infrastructure since it is, by far, the most widely deployed authentication scheme. However, this requires a DTN node to be securely paired with a GSM cell-phone – something that is not always practical. Another proposal [10] suggested taking advantage of casual information, such as knowledge of current and previous affiliations or social contacts of peers, in order to establish an initial security context between DTN nodes with no security history. Instead of establishing a shared key, a sender encrypts its message with multiple keys shared with some affiliated entities (AEs). As long as these AEs are also AEs of the receiver, the message can be decrypted by the latter.

[1] Identity-Based Signatures (IBS) do not exhibit this problem, since a signed message can be always accompanied by the sender's public key certificate (in the form of a non-identity based signature from a CA) and timely revocation information.

D. Fragment Authentication

The natural way to authenticate message fragments is to attach a signature to each [18]. However, the message source cannot foresee all potential fragment boundaries. Hence, precomputing signatures for all possible fragments is not viable.

Two techniques for authenticating fragments are presented in [45]. The first entails authenticating each fragment by computing a hash over all previous fragments. The amount of work required from the receiver is less than in the naïve approach, since multiple fragments can be authenticated by verifying one signature. The second techniques is to authenticate fragments using so-called *f*unction definitions that require a "special" authentication function. However, no efficient construction of such a function is provided. Subsequently, a scheme based on Merkle Hash Trees is proposed as an alternative scheme for DTN fragment authentication [3]. Despite these exiting ones, efficient and flexible solutions remain elusive.

E. Summary

Security issues specific to DTNs arise from intermittent network operation and connectivity which makes efficient authentication challenging. The same DTN features also complicate end-to-end confidentiality whenever end-points have no prior security context. Finally, DTN message fragmentation makes it very difficult to authenticate the origin of individual fragments.

VI. Conclusion

In this paper, we examined security and privacy issues in some new and emerging wireless networks. In surveying relevant literature, we tried to identify new security and privacy challenges as well as inadequacies of current approaches. Certain challenges arise from the unattended, intermittently connected and possibly mobile, network operation. Consequently, we need to anticipate threats arising from malicious exploitation of such network features and design appropriate security counter-measures. Also, since some emerging wireless networks are *a*d hoc in nature, infrastructure-independent security and privacy techniques are particularly suitable. Finally, emerging wireless devices such as RSensors motivate the development of new cryptographic primitives and protocols.

References

[1] R. Amirtharajah and A. Chandrakasan. Self-powered signal processing using vibration-based power generation. *IEEE Journal of Solid-State Circuits*, 33:687–695, 1998.

[2] N. Asokan, K. Kostiainen, P. Ginzboorg, J. Ott, and C. Luo. Applicability of identity-based cryptography for disruption-tolerant networking. In *MobiOpp*, 2007.

[3] N. Asokan, K. Kostiainen, P. Ginzboorg, J. Ott, and C. Luo. Towards securing disruption-tolerant networking. Technical Report NRC-TR-2007-07, Nokia Research Center, 2007.

[4] ASTM Standard E2213, 2003. ASTM E2213 - 03 standard specification for telecommunications and information exchange between roadside and vehicle systems 5 ghz band dedicated short range communications (dsrc) medium access control (mac) and physical layer (phy) specifications. ASTM International, West Conshohocken, PA, 2003. DOI: 10.1520/E2213-03, www.astm.org.

[5] F. Bai, T. Elbatt, and G. Hollan. Towards characterizing and classifying communication-based automotive applications from a wireless networking perspective. In *IEEE Workshop on Automotive Networking and Applications (AutoNet)*, 2006.

[6] M. Buettner, B. Greenstein, A. Sample, J. R. Smith, and D. Wetherall. Revisiting smart dust with RFID sensor networks. In *ACM Workshop on Hot Topics in Networks (Hotnets-VII)*, October 2008.

[7] S. Clark, J. Gummeson, K. Fu, and D. Ganesan. Towards autonomously-powered CRFIDs. In *Workshop on Power Aware Computing and Systems (HotPower 2009)*, October 2009.

[8] R. Prasad D. Yeager, D. Wetherall, P. Powledge, and J. Smith. Wirelessly-charged UHF tags for sensor data collection. In *IEEE RFID'08*, 2008.

[9] E. De Cristofaro, X. Ding, and G. Tsudik. Privacy-preserving querying in sensor networks. In *IEEE ICCCN 2009*, 2009.

[10] K. El Defrawy, J. Solis, and G. Tsudik. Leveraging social contacts for message confidentiality in delay-tolerant networks. In *33rd Annual IEEE International Computer Software and Applications Conference (COMPSAC 2009)*, 2009.

[11] R. Di Pietro, D. Ma, C. Soriente, and G. Tsudik. POSH: Proactive co-operative self-healing in unattended sensor networks. In *27th IEEE International Symposium on Reliable Distributed Systems (SRDS'08)*, pages 185–194, 2008.

[12] R. Di Pietro, L. Mancini, C. Soriente, A. Spognardi, and G. Tsudik. Catch Me If You Can: Data survival in unattended sensor networks. In *6th IEEE International Conference on Pervasive Computing and Communications (PerCom'08)*, pages 185–194, 2008.

[13] R. Di Pietro, L.V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik. Data security in unattended sensor networks. *IEEE Transactions on Computers, Special Issue on Autonomic Network Computing*, 2009.

[14] R. Di Pietro, L.V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik. Maximizing data survival in unattended wireless sensor networks against a focused mobile adversary. *Ad Hoc Networks (Elsevier). Special Issue on Privacy and Security in Wireless Sensor and Ad Hoc Networks*, 2009.

[15] R. Di Pietro, G. Oligeri, C. Soriente, and G. Tsudik. Intrusion-resilience in mobile unattended wsns. In *Infocomm*, 2010.

[16] R. Di Pietro, C. Soriente, A. Spognardi, and G. Tsudik. Collaborative authentication in unattended wsns. In *ACM Conference on Wireless Network Security (ACM WiSec'09)*, 2009.

[17] M.D. Dikaiakos, T. Nadeem, S. Iqbal, and L. Iftode. VITP: An information transfer protocol for vehicular computing. In *in: VANET05: Proceedings of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks, ACM*, pages 30–39, 2005.

[18] DTNRG. Delay tolerant networking research group: dtn-interest mailing list archive. [Online]. Available: http://mailman.dtnrg.org/pipermail/dtn-interest/2005-April, April 2005.

[19] K. Fall. A delay tolerant network architecture for challenged internets. In *SIGCOMM*, 2003.

[20] K. Fall and A. Chakrabarthi. Identity-based cryptosystem for delay-tolerant networking. May 2004.

[21] G. Goth. Delay-tolerant network technologies coming together. *IEEE Distributed Systems ONLINE*, 7(8), 2006.

[22] J. Guo, J. Baugh, and S. Wang. A group signature based secure and privacy-preserving vehicular communication framework. In *Mobile Networking for Vehicular Environments (MOVE) workshop in conjunction with IEEE INFOCOM*, 2007.

[23] M. T. Isik and O. B. Akan. Wireless passive sensor networks. *IEEE Communication Magazine*, 47(8):92–99, August 2009.

[24] M. Jakobsson. Mobile malware - an outlook and a new defense paradigm. RSA Conference 2010, March 2010.

[25] T. Jonson, J. Pezeshki, V. Chao, K. Smith, and J. Fazio. Application of delay tolerant networking DTN in airborne networks. In *Milcom'08*, 2008.

[26] J. Kahn, R. Katz, and K. Pister. Emerging Challenges: Mobile networking for 'smart dust'. *Journal of Communication Networks*, pages 188–196, 2000.

[27] A. Kansal, D. Potter, and M. Srivastava. Performance aware tasking for environmentally powered sensor networks. In *ACM SIGMETRICS'04*, 2004.

[28] A. Kansal and M. Srivastava. An environmental energy harvesting framework for sensor networks. *ACM/IEEE ISLPED*, 2003.

[29] A. Kate, G. Zaverucha, and U. Hengartner. Anonymity and security in delay tolerant networks. In *3rd International Conference on Security and*

Privacy in Communication Networks (SecureComm 2007), September 2007.

[30] K.C. Lee, S.H. Lee, R. Cheung, U. Lee, and M. Gerla. First experience with CarTorrent in a real vehicular ad hoc network testbed. In *Move'07*, 2007.

[31] U. Lee, E. Magistretti, M. Gerla, P. Bellavista, and A. Corradi. Dissemination and harvesting of urban data using vehicular sensor platforms. *IEEE Transaction on Vehicular Technology*, 58(2):882–901, 2009.

[32] U. Lee, E. Magistretti, M. Gerla, P. Bellavista, P. Lio, and K.W. Lee. Bio-inspired multi-agent data harvesting in a proactive urban monitoring environment. *Ad Hoc Networks Journal (Elsevier), Special Issue on Bio-Inspired Computing and Communication in Wireless Ad Hoc and Sensor Networks*, 7(4), 2009.

[33] U. Lee, E. Magistretti, B. Zhou, M. Gerla, and A. Corradi. MobEyes: Smart mobs for urban monitoring with vehicular sensor networks. *IEEE Wireless Communications*, 13(5):51–57, 2006.

[34] U. Lee, J. Park, E. Amir, and M. Gerla. FleaNet: A virtual market place on vehicular networks. In *Annual International Conference on Mobile and Ubiquitous Systems*, 2006.

[35] U. Lee, J. Park, J. Yeh, G. Pau, and M. Gerla. Code Torrent: Content distribution using network coding in VANET. In *MobiShare'06: Proceedings of the 1st international workshop on Decentralized resource sharing in mobile computing and networking*, pages 1–5. ACM Press, 2006.

[36] J. Luo, P. (Panos) Papadimitratos, and J. P. Hubaux. GossiCrypt: Wireless sensor network data confidentiality against parasitic adversaries. In *IEEE SECON 2008*, 2008.

[37] D. Ma, C. Soriente, and G. Tsudik. New adversary and new threats: Security in unattended sensor networks. *IEEE Network*, March 2009.

[38] D. Ma and G. Tsudik. Forward-secure sequentical aggregate authentication. In *Proceedings of IEEE Symposium on Security and Privacy 2007*, May 2007.

[39] D. Ma and G. Tsudik. DISH: Distributed self-healing in unattended wireless sensor networks. In *10th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS'08)*, pages 47–62, 2008.

[40] Donna Miles. Developing system gives hope to improved battlefield communications. [Online]. Available: http://www.defense.gov/news/newsarticle.aspx?id=53894, April 2009.

[41] A. Nandan, S. Das, G. Pau, M. Gerla, and M.Y. Sanadidi. Co-operative downloading in vehicular ad-hoc wireless networks. In *WONS'05*, 2005.

[42] NASA. NASA DTN project page. [Online]. Available: http://www.nasa.gov/mission_pages/station/science/experiments/DTN.htm.

[43] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J. Hubaux. Secure vehicular communication systems: design and architecture. *IEEE Communications*, 2008.

[44] B. Parno and A. Perrig. Challenges in securing vehicular networks. In *ACM Workshop on Hot Topics in Networks (HotNets-IV)*, 2005.

[45] C. Partridge. Authentication for fragments. In *4th Workshop on Hot Topics in Networks (HotNets-IV)*, 2005.

[46] M. Raya and J. Hubaux. The security of vehicular ad hoc networks. In *ACM workshop on Security of Ad Hoc and Sensor Networks*, 2005.

[47] M. Raya, P. Papadimitratos, and J. Hubaux. Securing vehicular communications. *IEEE Wireless Communications*, 2006.

[48] W. Ren, J. Zhao, and Y. Ren. Network coding based dependable and efficient data survival in unattended wireless sensor networks. *Journal of Communications*, 4(11):894–901, Dec 2009.

[49] S. Roundy, P. K. Wright, and J. M. Rabaey. *Energy scavenging for wireless sensor networks: with special focus on vibrations*. Kluwer Academic Publishers, 2003.

[50] M. Salajegheh, S. Clark, B. Ransford, K. Fu, and A. Juels. CCCP: Secure remote storage for computational RFIDs. In *18th USENIX Security Symposium*, page August, 2009.

[51] A. Seth and S. Keshav. Practical security for disconnected nodes. In *1st IEEE ICNP Workshop on Secure Network Protocols (NPSec)*, November 2005.

[52] M. Shao, S. Zhu, W. Zhang, and G. Cao. pDCS: Security and privacy support for data-centric sensor networks. In *INFOCOMM'07*, pages 1298–1306, 2007.

[53] J. R. Smith, A. P. Sample, P. S. Powledge, S. Roy, and A. Mamishev. A wirelessly-powered platform for sensing and computation. In *Ubicomp 2006*, pages 495–406, 2006.

[54] A. Studer, F. Bai, B. Bellur, and A. Perrig. Flexible, extensible, and efficient VANET authentication. *Journal of Communications and Networks*, 11(6):574–588, December 2009.

[55] A. Studer, E. Shi, F. Bai, and A. Perrig. Tacking together efficient authentication revocation, and privacy in VANETs. In *IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, 2009.

[56] N. Subramanian, C. Yang, and W. Zhan. Securing distributed data storage and retrieval in sensor networks. *Pervasive and Mobile Computing Journal (Special Issue for PerCom 2007)*, 3(6):659–676, 2007.

[57] S. Ur Rahman, U. Hengartner, U. Ismail, and S. Keshav. Practical security for rural Internet kiosks. In *NSDR '08: Proceedings of the second ACM SIGCOMM workshop on Networked systems for developing regions*, pages 13–18, New York, NY, USA, 2008.

[58] A. Yavuz and P. Ning. Hash-based sequential aggregate and forward secure signature for unattended wireless sensor networks. In *the Sixth Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous 2009)*, 2009.

[59] M. El Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian. Security issues in a future vehicular network. In *EuroWireless 2002*, February 2002.

[60] R. Zhang, Y. Zhang, and K. Ren. gDP^{2}AC: Distributed privacy-preserving access control in sensor networks. In *INFOCOM'09*, 2009.

[61] W. Zhang, H. Song, S. Zhu, and G. Cao. Least privilege and privilege deprivation: towards tolerating mobile sink compromises in wireless sensor networks. In *ACM MobiHoc'05*, pages 378–389, May 2005.