National Journal of Multidisciplinary Research and Development
ISSN: 2455-9040; Impact Factor: RJIF 5.22
Received: 30-12-2018; Accepted: 02-02-2019
www.nationaljournals.com
Volume 4; Issue 2; April 2019; Page No. 01-03

Security and privacy issues in recent emerging wireless networks

Amit Kumar[1], NK Singh[2]
[1-2] Department of Applied Science, Institute of Engineering & Technology, MIA, Alwar, Rajasthan, India

Abstract
Recent rapid advances in Wireless networking have extended its application from mobile networks and wireless sensor networks to emerging wireless networks including wireless mesh networks, delay-tolerant networks, vehicular networks, and urban sensing networks. While facilitating ubiquitous network access and also social interactions, these emerging networks are particularly vulnerable to numerous privacy and security threats. For example, attackers may jeopardize the privacy of users in vehicular and urban sensing networks; the adversary may also compromise selected nodes in a tactical delay-tolerant network and thus fail the critical mission of the network. There is clearly an urgent need to protect emerging wireless networks from various security and privacy threats, thereby eliminating a major impediment to their widespread adoption of such networks. This paper hence describes the security and privacy issues in some new and emerging types of wireless networks.

Keywords: wireless networks, security and privacy, sensor networks, vehicular networks, disruption-tolerant networks

1. Introduction
Wireless network refers to any type of computer network that is not connected by cables of any kind. It is a method by which telecommunications networks and enterprise (business), installations avoid the costly process of introducing cables into to a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using a transmission system called radio waves. This implementation takes place at the physical level, (layer), of the network structure. 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 ad 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.

2. Important security issues
It is well known that wireless networks are inherently more vulnerable than their wired counterparts. Also, complications arise in the presence of node mobility and dynamic network topology. However, intermittent connectivity, whether caused by mobility or periodic node sleep (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. The Factors responsible for Security problem are:-

- **Channel:** Wireless ness 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, wireless ness, 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 embed ability.
- **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.

3. Wireless sensor networks
The term wireless sensor network (WSN) practically came into existence in late 1960s [1]. This entailed an integrated computing, communication and sensing platform consisting of small devices, enabling applications such as dense environmental monitoring A 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 ad 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. 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. 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. 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-à-vis maintenance. To reduce reliance on RSink, RSensors an be further equipped with other energy harvesting mean that derive power from environmental sources, such as solar, thermal, vibration or ambient RF energy. 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 [5]. 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.

4. 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 [6], CarTorrent [7], and Code Torrent [8], 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 and VITP provide proactive urban monitoring (e. g. Traffic and pollution) services where vehicles are 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 [4]. 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 ad 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.

5. Disruption-tolerant networks

Advances in wireless communication allow mobile devices vehicles, smart phones, PDAs and sensors to form infrastructure-less ad hoc networks. Such networks can be rapidly deployed and are very useful in many real-worlds 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 ad 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. 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. 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 to civilian. 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 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. It can provide service to nearby clients and communicate with distant entities to be visited in the near future. DTN security requirements include Authentication of origin (sender) and, possibly, of intermediate hops. Integrity of messages and, possibly, of message fragments. Confidentiality of end-to-end communication.

6. 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 ad hoc in nature, infrastructure-independent security and privacy techniques are particularly suitable. Finally, emerging wireless devices such as R Sensors motivate the development of new cryptographic primitives and protocols.

7. References

1. Buettner M, Greenstein B, Sample A, Smith JR, Wetherall D. Revisiting smart dust with RFID sensor networks. In ACM Workshop on Hot Topics in Networks (Hotnets-VII), 2008.
2. Kansal Srivastava M. An environmental energy harvesting framework for sensor networks. ACM/IEEE ISLPED, 2003.
3. Lee U, Magistretti E, Gerla M, Bellavista P, Corradi A. Dissemination and harvesting of urban data using vehicular sensor platforms. IEEE Transaction on Vehicular Technology. 2009; 58(2):882-901.
4. Di Pietro R, Mancini LV, Soriente C, Spognardi A, Tsudik G. Data security in unattended sensor networks. IEEE Transactions on Computers, Special Issue on Autonomic Network Computing, 2009.
5. Ma D, Soriente C, Tsudik G. New adversary and new threats: Security in unattended sensor networks. IEEE Network, 2009.
6. Papadimitratos P, Buttyan L, Holczer T, Schoch E, Freudiger J, *et al*. Secure vehicular communication systems: design and architecture. IEEE Communications, 2008.
7. Raya M, Papadimitratos P, Hubaux J. Securing vehicular communications. IEEE Wireless Communications, 2006.
8. Seth Keshav S. Practical security for disconnected nodes. In 1st IEEE ICNP Workshop on Secure Network Protocols (NPSec), 2005.