TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

AKI ROUHIAINEN

INTERNET OF THINGS SECURITY SURVEY: SOLUTIONS, STANDARDS AND OPEN ISSUES

Master of Science Thesis

Examiners: Professor Jarmo Harju,
M.Sc. Joona Kannisto
Examiner and subject approved by
Faculty of the Computing and Electrical Engineering Council on 8th of
November 2013

ABSTRACT

TAMPERE UNIVERSITY OF TECHNOLOGY
Master's Degree Programme in Signal Processing and Communications Engineering
ROUHIAINEN, AKI: Internet of Things Security Survey: Solutions, Standards and Open Issues
Master of Science Thesis, 61 pages
February 2014
Major: Communication Networks and Protocols
Examiners: Professor Jarmo Harju, M.Sc. Joona Kannisto
Keywords: Internet of Things, security, wireless sensor networks, vehicular ad-hoc networks, authentication, localization, standardization

Internet of Things (IoT) extends the Internet to our everyday objects, which enables new kind of applications and services. These IoT applications face demanding technical challenges: the number of 'things' or objects can be very large, they can be very constrained devices, and may need to operate on challenging and dynamic environments. However, the architecture of today's Internet is based on many legacy protocols and technology that were not originally designed to support features like mobility or the huge and growing number of objects the Internet consists of today. Similarly, many security features of today's Internet are additional layers built to fill up flaws in the underlying design. Fulfilling new technical requirements set by IoT applications requires efficient solutions designed for the IoT use from the ground up. Moreover, the implementation of this new IoT technology requires interoperability and integration with traditional Internet. Due to considerable technical challenges, the security is an often overlooked aspect in the emerging new IoT technology.

This thesis surveys general security requirements for the entire field of IoT applications. Out of the large amount of potential applications, this thesis focuses on two major IoT application fields: wireless sensor networks and vehicular ad-hoc networks. The thesis introduces example scenarios and presents major security challenges related to these areas. The common standards related to the areas are examined in the security perspective. The thesis also examines research work beyond the area of standardization in an attempt to find solutions to unanswered security challenges. The thesis aims to give an introduction to the security challenges in the IoT world and review the state of the security research through these two major IoT areas.

TIIVISTELMÄ

TAMPEREEN TEKNILLINEN YLIOPISTO
Signaalinkäsittelyn ja tietoliikennetekniikan koulutusohjelma
ROUHIAINEN, AKI: Asioiden Internetin tietoturva: ratkaisuja, standardeja ja avoimia ongelmia
Diplomityö, 61 sivua
Helmikuu 2014
Pääaine: Tietoliikenneverkot ja protokollat
Tarkastajat: professori Jarmo Harju, diplomi-insinööri Joona Kannisto
Avainsanat: Asioiden Internet, tietoturva, sensoriverkot, tieliikenneverkot, autentikointi, paikannus, standardit

Asioiden Internet (engl. Internet of Things, IoT) mahdollistaa suuren määrän uusia sovelluksia erilaisiin käyttötarkoituksiin. Näiden IoT-sovellusten on täytettävä tiukkoja teknisiä vaatimuksia, kuten toiminta erittäin resurssiniukoilla laitteilla tai toimintakyky haastavassa ja dynaamisessa verkkoympäristössä. Laitteiden määrä verkossa voi myös olla huomattavan suuri. Nykyisen Internetin rakenne perustuu kuitenkin moniin vanhoihin protokolliin ja tekniikoihin, joita ei alun perin suunniteltu tukemaan objektien liikkuvuutta eikä niiden miljardeihin nousevaa lukumäärää. Myös monet nykyisessä Internetissä käytettävät tietoturvaratkaisut ovat lisäkerroksia, jotka on rakennettu paikkaamaan löytyneitä tietoturva-aukkoja. IoT-sovellusten teknisten vaatimusten täyttäminen vaatii tehokkaita erityisesti IoT-käyttöön suunniteltuja ratkaisuja. Niiden käyttöönotto vaatii kuitenkin yhteensopivuutta vanhan Internet-tekniikan kanssa. Huomattavien teknisten haasteiden vuoksi tietoturva on usein jätetty vähemmälle huomiolle IoT-tekniikan suunnittelussa. Tämä työ keskittyy tähän vähemmän tutkittuun aihealueeseen.

Työssä määritellään yleiset tietoturvavaatimukset koko IoT:n sovellusmahdollisuudet huomioiden. Sovellusten osalta työ on rajattu käsittelemään kahta suurta kokonaisuutta: langattomia sensoriverkkoja ja älykkään tieliikenteen tietoliikenneverkkoja. Alueilta mainitaan esimerkkejä käyttötapauksista ja määritellään niihin liittyvät suurimmat tietoturvahaasteet. Käyttötarkoitusalueisiin liittyvät yleisimmät standardit esitellään tietoturvan osalta. Määriteltyihin tietoturvahaasteisiin haetaan vastauksia myös standardoinnin ulkopuolisesta tutkimuksesta. Työn tarkoituksena on tarjota lukijalle valittujen sovellusalueiden kautta esittely IoT:n tietoturvahaasteiden maailmaan ja siihen liittyvään tutkimukseen.

PREFACE

This thesis was carried out at Tampere University of Technology in the Department of Computer Science. Professor Jarmo Harju provided me with the research topic based on our discussions in February 2013. Around a year later, the project was completed.

I would like to express my gratitude to my supervisors Prof. Jarmo Harju and M.Sc. Joona Kannisto, who provided invaluable feedback on our meetings throughout the past year. I also like to thank Prof. Jarmo Harju for providing me the opportunity to work for the university, M.Sc. Joona Kannisto for being an exemplary co-worker and all the fellow workers in our department for creating a friendly working atmosphere.

Tampere, 27th of January 2014

Aki Rouhiainen

CONTENTS

LIST OF SYMBOLS AND ABBREVATIONS

4G	4G is the common name of 4th generation of cellular network technology, including Mobile WiMAX and Long Term Evolution.
6LowPAN	IPv6 over Low power Wireless Personal Area Networks is standard developed by a working group in IETF that finished its work in 2012. 6LowPAN definition allows IPV6 packets to be sent and received over IEEE 802.15.4 based networks.
BER	Bit error rate is the number of received bits of a data stream, that has been altered due to interference, noise, distortion or bit synchronization errors.
C2C-CC	The Car2Car Communication Consortium is a non-profit organisation initiated by six European car manufacturers (Audi, BMW, DaimlerChrysler, Fiat, Renault and Volkswagen) with aim to develop a open industrial standard for inter-vehicle communication to ensure interoperability, using IEEE 802.11 WLAN standards.
CA	Certificate Authority is the name for a trusted third party in PKI.
CPU	Central Processing Unit is hardware to carry out the instructions of a computer program by performing the basic arithmetical, logical, and input/output operations of the system.
CSMA	Carrier sense multiple access is a MAC method in which a node verifies absence of other traffic before transmitting on a shared medium.
CSMA/CA	Carrier sense multiple access with collision avoidance is a variation of CSMA, with the addition of collision avoidance mechanisms to better cope with hidden terminal problem.
DDoS	Distributed-denial-of-service attack is a variation of denial-of-service attack, which originates from multiple locations.
DNS	Doman name system is a hierarchical distributed naming system designed for Internet. DNS is designed to resolve information associated to domain names.
DoS	Denial-of-service attack is an attack method, designed to compromise service's availability to legitimate users.
DSRC	Dedicated short-range communications is a one- or two-way short- to medium-range wireless communication method specially designed for vehicular use.

ECC	Elliptic curve cryptography is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.
FCC	Federal Communications Commission is an independent agency of United States government. FCC regulates the use of non-federal radio spectrum.
FFD	Full-function device is a PAN coordinator node defined in IEEE 802.15.4 standard.
GPS	Global positioning system is a satellite positioning system developed by United States Department of Defence.
GPSM	GPS multicast routing is a GPS-based routing scheme, based on atoms and partitions.
HART	Highway Addressable Remote Transducer Protocol is an early implementation of Fieldbus, an industrial automation protocol. It is able to communicate over legacy instrumentation wiring, making it one of the most popular industrial communication protocols today.
IEEE	Institute of Electrical and Electronics Engineers is international professional association dedicated to advancing technological innovation.
IETF	Internet Engineering Task Force is an organization that develops and promotes Internet standards. IETF was formed in 1986.
INSENS	Intrusion-tolerant routing protocol for wireless sensor networks is a suggestion for secure wireless sensor network routing protocol introduced in article by J. Deng, R. Han and S. Mishra in 2003.
IoT	Internet of Things is a broad term used for to uniquely identifiable objects in an Internet-like structure
IP	Internet protocol is the principal communications protocol in the Internet protocol suite.
LR-WPAN	Low-rate wireless personal area network links devices together using wireless distribution method in a personal area with low transmission rate. For example, ZigBee networks are a LR-WPANs.
MAC	Medium access control is part of the data link layer in a seven-layer OSI model of computer networking. MAC provides channel access control mechanisms that allow several nodes to communicate using shared medium.
OBU	On-board unit is a communication device installed on vehicles communicating in VANETs.

OFDM	Orthogonal frequency-division multiplexing is a modulation scheme that involves encoding digital data ton multiple carrier frequencies.
PAN	Personal area network is a network for interconnecting devices centered on an individual person's workspace.
PGP	Pretty Good Privacy is a widely used data encryption and decryption method that uses combination of hashing, data compression, symmetric-key, and public-key cryptography.
PHY	Physical layer is the bottom layer in a seven-layer OSI model of computer networking. When using wireless medium, PHY layer consists of transceivers, digital signal processor and communication algorithm processing.
PKI	Public Key Infrastructure is a key management method relying on digital certificates issued by trusted third party.
QoS	Quality of Service refers to an ability to provide different priority levels between applications, users or data flows.
RAM	Random-Access Memory allows stored data to be accessed directly in any random order.
RFD	Reduced-function device is a basic PAN node defined in IEEE 802.15.4 standard.
RFID	Radio frequency identification is a wireless method of data transfer using electromagnetic fields. Passive RFID tags use inducted power from the reader device to transmit their data.
RIPS	Radio Interferometric Positioning System is a positioning method that relies on two external radio signals at different frequencies and calculation of phase offset between the signals.
RSU	Roadside unit is a static node placed on roadside in VANETs.
SPINE	Secure Positioning Method in Sensor Networks is a positioning method based on verifiable multilateration, developed for wireless sensor networks.
VANET	Vehicular ad hoc network is a mobile ad hoc network consisting of moving vehicles as nodes.
WAVE	Wireless access in vehicular environments is a framework of standards consisting of IEEE 802.11p standard and IEEE 1609 standard family.
WirelessHART	Wireless Highway Addressable Remote Transducer Protocol is an extension to HART specification, extending the protocol to communicate over wireless medium.

WLAN	Wireless local area network links devices together using wireless distribution method in a local area.
WSN	Wireless sensor networks consist of autonomous sensor nodes distributed to monitor physical or environmental conditions, like temperature.

1 INTRODUCTION

The term Internet of Things (IoT) can be shortly defined as uniquely identifiable objects in Internet-like structure [1]. The IoT extends the Internet and the Web into the physical world by means of smart objects. The objects or 'things' are Radio-Frequency Identification (RFID) tags, sensors, actuators, embedded and wearable computers etc. The unique addressing scheme allows objects to be linked to over traditional Internet structure in order to cooperate towards a common goal.

The IoT has been known as a term for almost 15 years [2], but still can be considered in many ways as a novel paradigm in present-day wireless telecommunications. The future IoT world allows linking of digital and physical entities by the means of appropriate communication technology. IoT will have a big impact on everyday life of its users. Assisted living, health monitoring and enhanced learning are application fields that private users can directly benefit from. Corporations can use IoT to improve automation, logistics, manufacturing and business processes. The potential applications scale up even to a global level, like intelligent transportation systems.

The introduction of IoT presents a new set of technical challenges. The modern heterogeneous objects are equipped with varying hardware capabilities and will greatly outnumber traditional computers. The communication, as well as the network itself will be more dynamic and despite differences, interoperability with traditional Internet has to be maintained. Progress has been made, but many technical challenges still need to be addressed before IoT can be widely accepted.

The pressing technical issues have left security with a lesser attention among the IoT research and standardization work. Even though security should be considered as a part of the system design from the beginning, many pioneering IoT technologies, like many ad-hoc routing protocols, are fundamentally insecure by their design. However, the IoT security research has gained considerably more attention in the past 5 years [3] [4].

IoT consists of a huge field of technology with diverse security issues to cover. This field is limited to two major topics in this work. First one is wireless sensor networks (WSNs). WSNs can be used for varying applications, of which many are for industrial use. The standardization work has also advanced furthest on the industrial WSN applications and the amount of WSN implementations continues to grow.

The second major area of this thesis is vehicular ad-hoc networks (VANETs). VANETs have been researched for a long time, but in many ways, it can be considered as an emerging field in comparison to WSNs. There are still many important security issues that have not yet progressed to the standardization phase. Still, it is possible that

VANETs will become world largest ad-hoc networks at some point in not too distant future [5].

The main objective of this thesis is to serve as an introduction to the current state of security research on the two selected major IoT fields. The attempt is not to try to find comprehensive answers to the presented security challenges, but to give the reader an opportunity to understand what has been done and what issues still remain to be addressed.

The structure of this thesis is as follows: Chapter 2 defines some general security requirements for all IoT technology. Chapter 3 presents major security challenges in WSNs. Chapter 4 introduces common WSN standards from the security perspective and research work beyond standardization is examined in an attempt to find answers to the remaining unanswered security challenges. Chapters 5 and 6 present security challenges, standards and research work for VANETs, similarly as Chapters 3 and 4 did for WSNs. Finally, conclusions are drawn in Chapter 7.

2 DEFINING INTERNET OF THINGS SECURITY REQUIREMENTS

This Chapter sets a broad definition to security requirements for Internet of Things (IoT) technologies in comparison to today's Internet. In the context of this thesis, today's Internet refers to traditional Internet structure, in which Internet Protocol (IP) is a global basis for connecting entities over mostly wired network infrastructure. This thesis covers two major fields in the IoT field, but the topics in this Chapter are discussed in the scope of the entire IoT concept.

2.1 Security requirements and interest groups

To start with IoT security requirements, some basic security principles are defined. The same general security requirements apply to the IoT world that we are familiar with on the today's Internet. Security requirements consist of confidentiality, authenticity, integrity, non-repudiation and availability. Following definitions are used in the context of this thesis.

- Confidentiality: Information is disguised from unauthorized receivers. In other words, only the sender and intended receiver or receivers are able to understand the message. When communicating on a wireless pathway, eavesdropping and intercepting the message only requires eavesdropper to be within the transmission range of a transmitting node. For this reason, achieving confidentiality usually requires the use of encrypted messages. [6]

- Authenticity: All parties involved in the communication should be able to confirm the identities of the other parties. In a face-to-face human communication this happens simply with the visual recognition, but in a digital world, other methods are required. Digital authentication might require signed certificates and a special network entities acting as a neutral third party for the authentication process. [6]

- Integrity and non-repudiation: Communicated messages cannot be altered by unauthorized party. Successfully completed authentication process does not yet guarantee message integrity and non-repudiation. Data may be altered in the transit either by maliciously or by accident. Providing message integrity

and non-repudiation usually requires checksumming and other cryptographic methods. [6]

- Availability: For a system to serve its purpose, information and resources must be available when needed. This is a key requirement for any communication to happen in a first place, but also easily compromised by denial-of-service (DoS) attacks. The requirement of keeping attackers from gaining access to the infrastructure leads to the requirement of access control, which falls into the scope of availability requirement in the context of this thesis. [6]

The future chapters of this thesis show that guaranteeing these requirements is a different task in the IoT world. Providing confidentiality using public key cryptography might be considered well known and even trivial task in traditional Internet, but is considerably harder in Internet of Things setting.

The listed general security requirements are set by different interest groups associated with the use of the service. Different security requirements have different priorities among different interest groups on each particular use scenario. On a large part of use scenarios, the interest groups directly associated with the scenario can be divided into users and service providers. When future network architecture is designed, we need to take account the laws and restrictions set by the society. From a security standpoint, we need also to take an important fourth group into account, the attackers. In the context of this thesis, the interest groups are shortly defined as follows.

- Users: Their interest is mainly in the utilization of services and the infrastructure and properties associated with such use [7]. Depending on the usage scenario, they may be represented by the devices, software or people.

- Service providers: They provide services and infrastructure. Their main interest is to gain profit from the service and run profitable business enterprises. [7]

- Society: Their interest is to protect society at large with the legal framework, which is enforced by government authorities. This group can also be extended to include standardization bodies, which advance people's interest to have globally interoperable technologies and sustainable free market. [7]

- Attackers: Their interest will vary, depending on the particular type of attacker. Attackers act according to their own set of moral rules, which are usually at least partially in conflict with one or more of the former groups.

In addition to attackers, other interest groups can also have colliding interest with each other and the roles of the interest groups may overlap. Design goal of new network architecture is an optimized compromise between users, service providers and society.

2.2 Different attackers and attack types

When new network architecture is designed, the ideal solution is to meet as many requirements set by the users, service providers and society, but also at same time maintain a strong network security, thus keeping attackers from fulfilling their goals. For this reason, attackers are usually defined as some outsider group when describing the network use scenario, even though not all the attackers are the same. Examining their motives, expertise, resources and willingness to take risks, allows us to better prioritise network's security requirements. Hackers, lone criminals, malicious insiders, industrial spies, terrorists and national intelligence organisations are distinctly different attacker types. Following list of different attacker types is not comprehensive.

- Hackers: Real hackers have considerable expertise, often greater than that of the system's original designers. In terms of resources, they usually have a lot of time, but few financial resources. They are motivated by curiosity and desire to understand. Their willingness to take risks depends on an individual. Some of them are risk averse and some engage illegal activities with no fear of prosecution and risk involved. [8]

- Lone criminals: Lone criminals often lack expertise and resources. They don't have money or access to the system. They are motivated by financial gain and thus target commercial systems. [8]

- Malicious insiders: Malicious insiders are dangerous attackers. They may have considerable expertise and could have even been involved in the design of the system. They also have one ultimate resource. They have insider access to the system and are considered trusted. Most standard computer security measures, like firewalls are powerless against insiders, as they can simply bypass them. Malicious insiders are particularly problematic adversaries in IoT world as they require special security measures that can be hard to implement due to system limitations. [8]

- Industrial spies: Industrial espionage attacks have precise motivations: to gain as advantage over the competition by stealing competitor's trade secrets. Industrial spies have usually at least medium expertise and are well funded. A rational company will devote enough resources to gain acceptable return of investment. These attackers have medium risk tolerance, as

they risk company's reputation in order to gain considerable competitive advantage, both of which are considered valuable. [8]

- Terrorists: A wide range of different ideological groups can be considered terrorists. Terrorists are usually more concerned with causing harm and gaining publicity than gathering information, so they tend to prefer denial-of-service -type of attack methods. Majority of terrorists have low expertise, and unless funded by a rich idealist, also low financial resources. Terrorists generally consider themselves to be personally in a state of war, so they have a very high risk-tolerance. [8]

- National intelligence organisations: A national intelligence organisation is extremely well funded, as it is considered a branch of military. This funding can buy a lot of equipment and expertise. A national intelligence organization is also a very risk averse. They don't want their operations to get exposed and even the knowledge about them possessing certain information is considered valuable. [8]

Internet of Things applications are often designed for specific purpose, which can help to rule out certain attacker types due the lack of their motivation to target the specific application. Like in traditional Internet, this can help backtracking the attacker in publicly available networks, where the complete prevention of attacks is very hard due to adversary's easy access to the network. The majority of all IoT technology can well be considered to be state of the art technology, which requires attackers to have considerable expertise and usually a specialized hardware to perform attacks. Moreover, industrial application is a particular field in IoT technologies that has advanced well in to deployment stage already. These considerations hint that first attacks against deployed IoT technologies to gain publicity will most likely be performed by adversaries with considerable funding and expertise.

To achieve their goals, attackers employ various attack techniques. Practicality of each technique depends on the network design and architecture, some being specially crafted for the specific network type. The following list is compiled from most of the commonly problematic attacks against Internet of Things technologies.

- Eavesdropping attack: Attacker passively monitors the communication session between two parties using the network in an attempt to determine the contents of the messages [9]. IoT technologies use almost exclusively wireless medium at least in some parts of the network, therefore the only precondition is that the attacker is within transmission range of the communication. Attacker may even use specialized equipment, like directional antennas to eavesdrop communication outside standard specified communication range. Eavesdropping can be passive or active. During

active eavesdropping, the attacker actively injects messages into the communication channel in order to assist him or her deciphering the contents of the messages [9]. Many IoT applications are solely designed to transmit monitoring data over the network. This makes eavesdropping attack particularly harmful, as performing it successfully might reveal adversary all the necessary information with no need to further attack the network operation and risk detection.

- Man-in-the-middle attack: Attacker positions himself or herself in between the two communicating parties. The purpose of the attack is to make both parties of the communication to believe they are communicating with each other, when in reality, they are communicating with the attacker. Successful employment of man-in-the-middle attack allows attacker to bypass cryptographic methods protecting the message confidentiality and read the plain contents of the messages. Attacker can also modify the contents of the message, thus violating the integrity of the session [9].

- Wormhole attack: This is a variation of man-in-the-middle attack performed in wireless networks. The attacker connects two remotely located compromised nodes with an external connection. The compromised node listens and tunnels packets with an external connection to the location of the other compromised node, which retransmits the messages. If performed successfully, the other nodes in the network will misinterpret the location of the compromised node, which results in erroneous routing decisions by network's routing protocol. [10]

- Sybil attack: Sybil attack is another attack type performed against wireless networks and particularly harmful against many IoT applications. In this attack, the malicious node generates an arbitrary amount of fake identities, which it claims to be able to connect to. This attack aims to corrupt routing tables of neighbouring nodes or otherwise take advantage of network accepting multiple identities. Some IoT security solutions are based on majority voting and plausibility checks, which can effectively be manipulated by multiple malicious identities. [11] [12]

- Denial-of-service attack: As the name suggests, a denial-of-service (DoS) attack is designed to compromise service's availability to legitimate users. This is done by flooding network nodes with extensive amount of messages. Effectiveness of different flood messages varies depending on the network design and the protocols used, but the main principle remains the same. The purpose of the flood messages is to

cause targeted node to instantiate data structures out of a limited pool of resources. Once the resources are exhausted, the node is unable to serve new legitimate connections, thus denying service's availability. A TPC SYN packet flooding is a popular example of a denial of service attack on IP networks. Distributed-denial-service (DDoS) attack is a variation of denial-of-service attack. DDoS attack is performed simultaneously from multiple locations. [13] [14]

- Denial-of-sleep: In the IoT world, a battery powered network nodes can also be attacked with a specially crafted denial-of-service attack designed to exhaust device's power supply. This attack, usually referred as denial-of-sleep attack, aims to send flood messages with certain frequency in an attempt to deny a network node entering an energy saving sleep state and eventually draining the node's battery. [15]

As seen from the listing, the basic attacks against wireless networks are very much viable on the IoT world. The list of attack types can also be extended with specialized attacks against devices with limited power supply, which covers almost the whole range of IoT applications. There is also one considerable difference in the threat of various attacks in comparison to traditional Internet. Many of the more advanced attacks, like wormhole attack and Sybil attack require an attacker to posses at least one compromised node. This prerequisite is far more easily achieved with many IoT applications as the number of nodes is large and most of the nodes are unattended. This is discussed in more detail on future chapters of this thesis.

2.3 Risk analysis and management

Deriving basic security requirements in their relation to different interest groups is quite straightforward for the IoT world. The same basic principles apply as in the today's Internet. However, future chapters of this thesis show that fulfilling these goals can be immensely harder in constrained IoT environments. Examining attacker types and attack tools at their disposal shows that various constrains, battery powered nodes and challenging operation environments make IoT technologies more vulnerable. For secrecy reasons, there is hardly any public research available on military IoT technologies, but it is clear that IoT technology has various potential military uses, in which security is a concern not to be taken lightly. Other technical challenges have kept researchers busy and security issues have started to get more attention only in the recent years [3] [4]. The following picture taken from the reference [16] is an example of things that need to be considered in relation to IoT security.

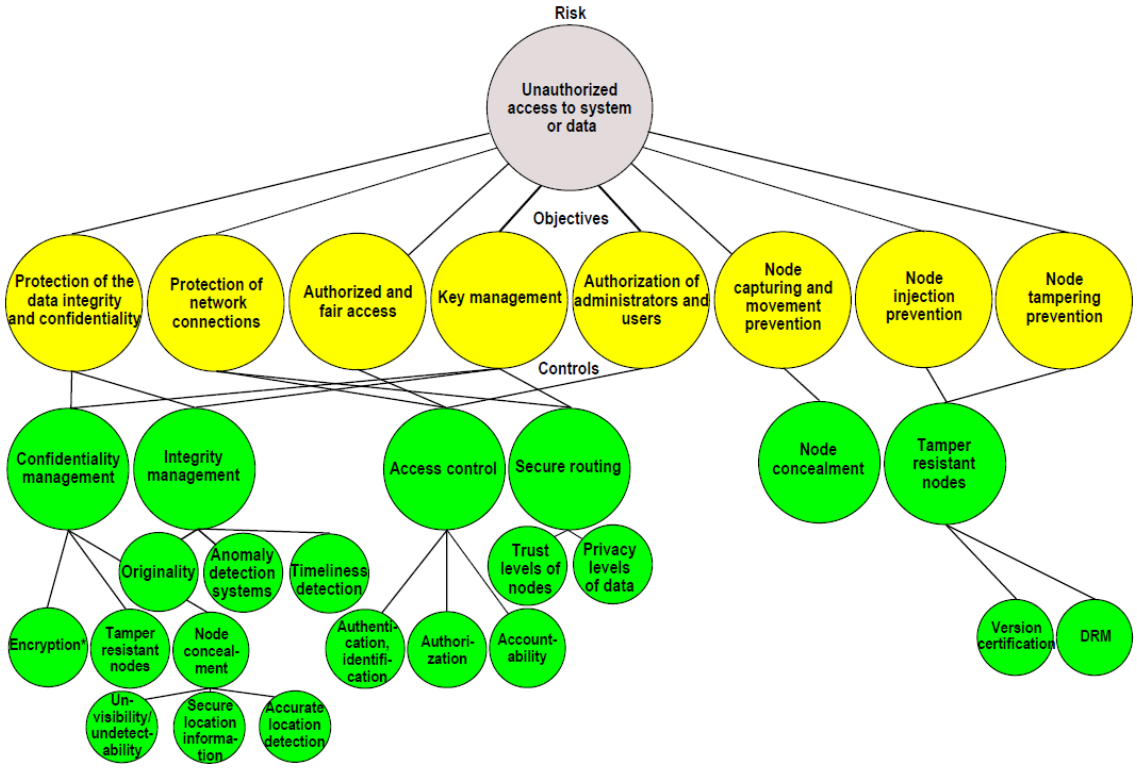

Figure 1: From risks to objectives and control – example [16].

The picture gives an overview of various methods to protect the system from certain types of security threats. Challenging nature of IoT technology requires compromises in security, at least on many early IoT implementations. The risk management is not a well researched topic in IoT perspective, even though pioneer papers exist [17]. Some basic assumptions can still be made, like the most common motive for a network attack being a financial gain in one form or another. If there is no way to gain financial advantage from a certain type of attack, the probability of it happening is significantly smaller [8].

This thesis does not try to form a complete coverage of all the potential risks in the presented IoT scenarios, but to concentrate on the most probable threats and well researched topics. The thesis presents security definitions of the most common standards in the selected IoT scenarios, as well as the most researched security challenges beyond standardization work. The presented answers to these challenges are not comprehensive and most of them prioritize security on the threats that are assumed to be the most common on the particular application.

3 SECURITY CHALLENGES IN WIRELESS SENSOR NETWORKS

The first major IoT area of this thesis is wireless sensor networks (WSNs). WSNs have a wide range of applications. These include ocean and wildlife monitoring, manufacturing machinery, different kinds of performance monitoring, building safety, earthquake monitoring and various military applications. The range of applications is likely to broaden even more in the future, including pollution, wildfires, building security and all kinds of health monitoring. A common working principle for a wireless sensor network is that the large number of sensor nodes record data streams and direct them to a single or multiple aggregation points in the network. Wireless sensor networks introduce unique challenges to the network design which render traditional network security techniques suboptimal or even useless. Sensor nodes are usually designed to be as inexpensive as possible, which limits their computation, communication and energy capabilities. They are often deployed in an accessible location, which makes physical tampering of the nodes a threat. A close interaction with physical world and people also presents new security problems, like an attacker purposely feeding the node with false data. [18]

These are all aspects to consider when designing a WSN system. The next section presents some of the WSN application scenarios in more detail. Many of these networks are already at least on the real world testing phase. After example scenarios, Section 3.2 lists general technical challenges and design goals that have to be met on WSN design.

3.1 Example use scenarios

Industrial automation can be improved by deploying IoT technologies and on some branches of industry, technology is already widely deployed. Applications range from storage management, production and quality control, assembly line machinery monitoring and worker safety monitoring. Current industrial applications are mostly deployed in more static field of activities, like production lines in industrial plants but more dynamic work environments like construction sites have yet seen few applications. The range of applications is likely to get considerably wider in the future.

The first example in a variety of industrial WSN applications is chemical plants and inventory management. Chemical inventories carry a tremendous value in a company's supply chain. Traditionally, inventory management has been based on manual methods and dedicated hard-wired computing systems. Both methods offer limited ability to disseminate accurate and timely information across widely distributed sensor points. Specific safety requirements for bulk storage tanks and tank farms can also make wiring

prohibitive and manual monitoring a hazardous task. Tank management system based on WSN can benefit supply chain by providing instant access to real-time inventory data for both producers and their suppliers, allowing them to manage and schedule replenishment of inventory stocks to ensure a constant supply of raw materials. This application is designed to integrate with the process logic controller, so that data from the additional sensors can be overlayed to input from existing fixed installation. [19]

Another industrial WSN application is pulp and paper mills. WSNs can be used to monitor machines for diagnostic and preventive maintenance purposes. The rolling machines at pulp and paper mills are massive and have complex mechanisms. The smallest variations in temperature, speed or the alignment of the rollers can have serious effects on quality of the operation. WSNs are ideal solution for investigating and resolving circumstances such as unanticipated variations in output quality, unusual vibration, noise, or other signs of potential problems. Whether the need is to measure temperature, speed, pressure or vibration, technicians can attach the required sensor nodes to appropriate areas of the machine process line and the sensor nodes will connect by themselves. Equipped with smart I/O system to identify the sensor types, the nodes identify the data to be measured and relay it wirelessly to a handheld base station device. These ad-hoc or overlay systems can be quickly installed and rapidly removed once problems are identified and resolved. [19]

Industrial WSNs can also be used in oil refineries. Heat tracing solutions have been delivered to continuous process manufacturers in oil refineries in extreme locations. To keep pipes and systems operating efficiently, heat tracing is used to keep pipes from freezing or within a particular temperature range. Traditionally, these systems have used wired connectivity for temperature sensing and heat trace control. As the number of temperature monitoring points can run into thousands, wiring costs can become prohibitively expensive. Errors in wiring installation can result in a plant shutdown, where costs become extreme. Outfitted with WSN modules, and embedded networking software, the temperature sensors can be more densely distributed with a reduced installation cost. Sensor networking allows a flexible deployment and the network adapts to the structure of the installation. The network allows peer-to-peer communication, and can help identify malfunctioning sensors before they lead to system failure.[19]

In addition to industrial applications, WSNs are well suited for environmental monitoring. The environmental monitoring applications can monitor jungle wildlife in their native habitats, where human presence has to be minimized. WSNs can also be used to monitor vibrations on the edge of a volcano to provide early warning from any seismic activity. Commonly, WSNs can monitor areas which are hard to access, dangerous for humans, or human presence is dangerous for the environment. These networks can be deployed from aerial vehicle, or even ballistically scattered over deployment area [20].

Governments are also very interested in military applications for WSNs. Usually these applications involve detecting, tracking and intelligence gathering on enemy troops. There is even an example of ad-hoc based WSN network to locate enemy snipers based on trajectory and speed of the fired bullet [21]. Military applications share

many similarities with environmental monitoring applications due to hostile area they are usually deployed to. Similarly, the deployment method is usually random scattering and the number of nodes is large. However, the security has significantly higher priority on military applications.

There are also many WSN applications in which the locations of sensor nodes are not static. These applications include: tracking nodes planted on animals, advanced military intelligence applications, ocean monitoring with nodes that flow along with oceanic currents or even nodes planted in human circulatory system. There is well over 10 years of research available on the nodes so tiny, that they can travel with the wind [22]. Nodes on these systems are usually very limited in their ability to actively communicate over radio transmission, leading to very specialized communication systems. For this reason, these types of WSNs have been excluded from this thesis. Node mobility also presents unique challenges to routing algorithms and allows new ways for adversaries to perform attacks. These subjects are discussed in more detail in chapters related to VANETs.

3.2 Technical requirements and design goals

WSNs in general share a set of technical challenges and restrictions. Examining these challenges helps to outline the technical nature of WSNs. Most restrictions also affect the implementation of WSN security mechanisms. The major technical challenges for WSNs are outlined below.

Firstly, WSN nodes are constrained in many ways. The design of many WSNs aims on having physically very small nodes with the cost of the individual node being very low. The nodes also have to almost always rely on a small battery or a limited amount of energy gathered from the operating environment. All this limits the nodes in three ways: Energy, memory and processing power are all very limited resources. Project Smart Dust is an example of very constrained nodes with the physical size of only few cubic millimetres [22]. [23]

Many WSN applications also require nodes operating in harsh environmental conditions. This also affects network connectivity. In industrial conditions, like on our example scenarios, the topology and connectivity of the network may vary due to link and sensor-node failures. Furthermore, sensors may also be subject to RF interference, vibrations, dirt, dust, high humidity levels or even highly caustic or corrosive environments. The harsh conditions may hinder node performance, but the result can also be malfunctions, like some nodes reporting invalid or unreliable sensor readings [24]. [23]

The varying WSN applications have different QoS requirement specifications. The definition of QoS in the context of WSNs differs from the traditional QoS definition. The QoS provided by WSNs refers to the accuracy between the data reported to the sink node and what is actually occurring in the environment. In addition, sensor data is typically time sensitive, like alarm notifications for the industrial facilities. If data has long latency due to processing or communication, it may lead to wrong decisions in the

monitoring system. In comparison to performance in wired networks, the attainable capacity of each wireless link depends of the interference level perceived at the receiver. Typically, high bit error rates (BER = 10^{-2} – 10^{-6}) are expectable. Additionally, wireless links suffer from varying characteristics in both, time and space. This is due to noisy environment and obstructions. Therefore, capacity and delay attainable at each link are location dependent and vary constantly. All this makes QoS provisioning challenging. [23]

However, there are a few advantages to QoS provisioning in WSN context as well. High density of sensor nodes in WSNs offers a good data redundancy in many situations. Sensor observations are highly correlated in the space domain. The nature of certain physical events also offers temporal correlation between each consecutive observation of the sensor node. [23]

One fundamental importance of WSNs is to be commercially viable. This requires WSNs to provide services that allow the querying of the network to retrieve useful information from anywhere and anytime. This leads to the requirement of WSNs to be remotely accessible from the Internet and, hence the need to be integrated with the IP architecture. The current sensor network platforms use gateways for integration between WSNs and the Internet [25] [26]. The integration may change in the future, extending IP connectivity all the way to the sensor nodes. [23] [27]

3.3 Authentication and key distribution

After initial deployment and discovering direct neighbours, WSN nodes require some sort of authentication scheme as a basis for fulfilling authenticity security requirement. Authentication schemes require of nodes having the necessary cryptographic information available. Secure distribution of this key information is a major security matter on WSN context. The unique nature of WSNs affects suitability of each particular authentication scheme and key distribution method.

The constrained nature of the nodes sets limits to possible authentication solutions. Limited memory resources dictate that individual nodes do not possess resources to establish unique keys with every other node in the network. Bandwidth and transmission power are also very limited. For example, the UC Berkeley Mica platform's transmitter has a bandwidth of 10 Kbps, and a packet size of about 30 bytes [28]. Due to high bit error rates, the transmission reliability is often low, making the communication of large blocks of data particularly expensive. The resource limitations make most of the public key cryptosystems impractical for WSNs, such as Diffie-Hellman key agreement [29] and RSA signatures [30]. RSA operations are problematic due to limited amount of memory available on the nodes. Both cryptographic methods also suffer from the problem that using longer and stronger keys will increase the processing delay exponentially [31]. The long processing delay in performing public key authentication gives adversary an opportunity to perform DoS attacks against node authentication [32]. An adversary

can exhaust node's energy source by sending arbitrary authentication requests, which will result in an exhaustive decryption and encryption of packets by the receiving node.

The threat of a physical node capture also needs to be taken into account when designing authentication solutions for WSNs. Many applications involve deploying nodes in public or hostile locations. Furthermore, the large number of nodes and the low-cost requirement makes it hard to manufacture tamper-resistant nodes or supervise physical access to the nodes effectively. If an attacker manages to capture a node, he or she also gains access to all the keys stored in node's memory. [28]

A particularly harmful attack against WSNs in is known as the Sybil attack [11]. This attack is based on a node illegitimately claiming multiple identities. We refer these additional identities as Sybil nodes. The ease of physical capture makes this attack considerably easier to perform against WSNs. The attack can be performed by fabricating new node identities, or stealing identities from existing nodes. If a node is identity is a certain integer value, an attacker can simply fabricate nodes by assigning them random integer values as Sybil node identities. If an authentication scheme with an intentionally limited name space is used, the attacker may need to assign Sybil nodes identities stolen from other legitimate nodes. This can go undetected when performed in conjunction with destroying or temporarily jamming the corresponding legitimate nodes. When analyzing each particular authentication scheme for WSNs, we will need to also examine its ability to resist Sybil attacks. [12]

Resource testing is known defence mechanism against Sybil attacks [11]. It can be done as part of the authentication procedure, but also as a periodic security measure to maintain WSN authenticity. Resource testing is based on the assumption that each node is limited in some resource. Verifier is sent to ensure that each identity has as much of the tested resource as a physical device. Normally, the resources tested are computation power, storage capacity and communication ability. Testing the first two is not suitable for WSNs, as adversary may use physical device with several orders of magnitude more computation power and storage capacity than the standard sensor node in the network. The traditional method of testing communication ability is to broadcast request for identities and then accept replies within a given time interval. This method is also unsuitable for WSNs, because all the replies converging at the verifier will result in that part of the network becoming congested. We will later examine radio resource testing method that is better suited for WSNs. [12]

After initial deployment of nodes and several weeks of operation, some nodes in the network may exhaust their power supply because of the uneven distribution of traffic load or malicious attacks. Some sensor nodes may be destroyed by hazardous environmental events, like chemical leakage in a chemical plant or exposure to extreme heat in an oil refinery. Besides the natural loss of sensor nodes, some nodes may even be destroyed by adversaries in an attempt to cripple communications in the entire WSN. Therefore, WSN authentication scheme must be able to accept authentication of new nodes that are added to the network after initial deployment. This implies that bootstrapping information must always be present and cannot simply be erased after de-

ployment to prevent compromise in the event of capture [28]. The possibility of the situation that all of the newly deployed nodes may not be legitimate also needs to be considered. An adversary may capture, re-program and then re-deploy compromised nodes back to the network or try to authenticate completely new malicious nodes to the WSN. [33]

The role, density and capabilities of base stations also vary between different WSNs. WSN base stations are typically few and expensive. Relying on them as a source of trust invites attackers to target base stations and also limits the application of protocol security. The communication patterns of sensor networks also differ from traditional networks. Nodes usually need to set up keys with their neighbours and with data aggregation points. Key establishment also needs to scale to the networks with hundreds or even thousands of nodes. Therefore, an authentication scheme that minimizes the communication with a base station working as arbiter or verifier is highly desirable. [28]

3.4 Secure localization

Most WSNs contain a large number of sensor nodes, hundreds to thousands or even more, which might be spread randomly over the deployment area. The method can be for example a random scattering from an airplane. This means that WSN protocols cannot know beforehand which nodes will be within communication range of each other after deployment. Moreover, the lack of predetermined network infrastructure necessitates the WSNs to establish connections and maintain network connectivity autonomously. [23] [28]

The problem of determining the node's geographical position and relative location within the WSN is referred to as localization. The term is similar to corresponding localization concept in VANETs. However, WSNs have radically different applications and a lot more constrained, but usually less mobile nodes. The nature of the problem and potential solutions are very different in comparison. The localization needs to be a part of the same initial bootstrapping procedure, where node discovers its neighbours, performs authentication, determines its location in the network, and establishes communication routes.

Existing direct localization methods include GPS or manual location preconfiguration. Equipping nodes with GPS receiver is simple solution to the problem. However, GPS-based system is not usable for indoor WSN applications and it is unreliable when sensors are deployed in an environment with obstructions such as dense foliage areas. Additionally, even though GPS-receivers are small in size, they cause considerable battery drain and increase the cost of constrained sensor nodes [34]. Preconfiguring node locations manually is also a possibility, but sets severe limitations to the WSNs. The node locations have to be completely static and random deployment methods cannot be used. This makes manual configuration method very cumbersome and expensive in terms of time consumption. Additionally, this method scales very poorly, which makes it unusable for any large scale WSNs. [35] [36]

The constraints of sensor nodes and impracticality of manual configuration has lead researchers to search for alternative secure localization solutions. The indirect localization methods are based on nodes positioning themselves relative to other nodes in their vicinity. They were introduced to overcome the problems of direct localization methods, while still maintaining location accuracy. Most of the indirect localization methods are based on the use of beacon nodes. The beacon nodes, which know their own position, help sensor nodes determine their position. Beacon nodes are few in numbers in relation to sensor nodes, so they can be equipped with GPS receiver or their location can be manually configured. This method also has its own security problems. The beacon nodes often work in a same hostile environment as sensor nodes, so they can be suspect to physical node capture as well as other attacks. The possibility of beacon nodes providing wrong location information has to be taken into account. Other localization methods are examined in more detail in Chapter 4. [35] [36]

3.5 Routing and data aggregation

After the initial authentication and localization procedure, we need to consider security aspects of routing in WSNs. There are some excellent papers written on routing techniques in WSNs [37] [4]. In short, WSN routing protocols can be classified based on the underlying network topology. Routing can be based on flat or hierarchical topology, or it can be completely location-based. In flat networks, each node typically plays the same role and nodes collaborate to perform the sensing and delivering information to the network sink. The hierarchical topologies use cluster-based routing to optimize energy consumption by aggregating communication through more powerful nodes that are higher on the network hierarchy. On location based routing, nodes are addressed by their locations. Nodes have only knowledge of their direct neighbours and forward packets to the neighbours who are determined to be closer to the packet destination.

Like traditional networks, most sensor network applications require protection against eavesdropping, injection and modification of packets [18]. Despite what type of routing protocol is used, WSNs are designed to transmit data produced by sensor nodes to sink nodes and further to the data processing server. Eavesdropping attacks are at particular interest of adversaries on this type of network. Passive eavesdropping of certain critical data streams on WSN might provide an adversary all the information of interest, with no need to risk detection by interfering network communication by injecting or modifying data packets. Cryptography is the standard defence against the attacks listed above. Integrating cryptography to sensor networks results in certain trade-offs.

In point-to-point communication, end-to-end cryptography achieves high level of security, but it requires key setup between all the end points. This makes encrypted communication incompatible with passive participation and local broadcast. Link-layer cryptography with a network wide shared key provides simple key setup and supports passive participation and local broadcast. However, a single shared key also makes

eavesdropping and packet modification easy for the adversary with the requirement of compromising just one of the intermediate nodes [18]

Modern sensor nodes can be fitted with camera sensors that produce live video data streams. Such multimedia sensor networks can produce huge amounts of delay sensitive data and usually require in-network processing techniques to reduce the amount of information flowing in the network. This usually requires a hierarchical topology, where sink nodes, which work as aggregation points of incoming streams, need to completely decode encrypted packets. This requires computational complexity of the security algorithms to be low enough to make real-time processing possible. There is hence a trade-off between providing enhanced security to data flow by adopting higher order code at the source sensor node and permissible delay requirements. [27] [38]

In the previous Section, we mentioned the considerable threat of physical node capture and described the Sybil attack it exposes WSNs. If an authenticated node is captured and replaced with a malicious node using the same key set, an adversary gains a possibility of launching Sybil attacks against WSN routing algorithms. The Sybil nodes can simply be in direct communication with other nodes, in which case the malicious device performing the attack will listen and reply to all the messages sent to Sybil nodes. The communication can also be indirect, where the malicious device claims to be able to reach the Sybil nodes. Messages sent to a Sybil node are routed through malicious device, which pretends to pass on the message to a Sybil node. WSN routing in general is also particularly vulnerable to DoS attacks. A simple form of a DoS attack is to broadcast a high energy signal in an attempt to jam the network’s communication. [12] [39]

4 STANDARDS AND SECURITY SOLUTIONS IN WIRELESS SENSOR NETWORKS

This Chapter will first shortly introduce some well established standards for WSNs from the security standpoint. Then the WSN research projects outside standardization work are introduced to provide solution propositions to challenges introduced in Chapter 3.

4.1 IEEE 802.15.4

IEEE 802.15.4 is the core standard for majority of the wireless sensor networks. The 802.15.4 specifies the physical layer (PHY) and MAC layer definition for low-rate wireless personal area networks (LR-WPANs). Other WSN specifications, like ZigBee define upper layers of the OSI model and are based on 802.15.4. IEEE 802.15.4 can also be used with 6LoWPAN and standard Internet protocols. [40] [41]

First version of IEEE 802.15.4 standard was released on 2003, following with second release in 2006. The latest release was in 2011. The 2011 release added 802.15.11 amendments from a through d to the standard, adding additional frequency ranges and PHY specifications to the standard. [40]

The main focus of the 802.15.4 standard is to offer low-cost, low-power and low-speed ubiquitous communication of nearby devices with very little underlying infrastructure. The basic setting conceives a transfer rate of 250 kbit/s over a 10 meter communications range. Latest 2011 version of 802.15.4 specifies five different frequency bands. These are 779-787 MHz (for China), 868,0-868,6 MHz (for Europe), 902-928 MHz (for North America), 950-956 MHz (for Japan) and 2400-2483,5 MHz (for worldwide use). In addition to these frequencies a few optional ultra-wide bands are defined outside the mentioned frequency range. Physical layer requirements for 802.15.4 devices vary depending on supported frequency bands. MAC scheme in 802.15.4 is either carrier sense multiple access with collision avoidance (CSMA/CA) or ALOHA for lighter networks. [40]

The 802.15.4 defines two different node types. Full-function device (FFD) implements functions to talk to any other device in a PAN area, serving as a network coordinator. A FFD that only relays messages is a dubbed coordinator. The other node type is reduced-function device (RFD). These are basic nodes of the network with limited computation power and energy supply. They can only communicate with FFDs. [40]

Network topology is either peer-to-peer ad-hoc network or a star network centered around a FFD node. A few more structured variations of these also exist. Applications

that typically use star topology include home automation, personal computer peripherals, games and personal health care. A peer-to-peer network also needs at least one FFD working as a network coordinator. Purpose of the peer-to-peer networks is to work as a basis for self-managing and self-organizing ad-hoc networks. Since 802.15.4 defines only PHY and MAC layers, routing algorithms are left for network layer solutions. [40]

The 2011 version of 802.15.4 standard currently has three amendments, which all are either draft standards or approved standards already. These are: 802.15.4e (MAC modifications to better support industrial markets), 802.15f (support for active RFID sensor applications) and 802.15.4g (PHY specifications for smart metering utility networks). We will not go in to more detail on these amendments, as the problems presented in this thesis are mainly related to the higher layers of the protocols stack. [40] [42]

4.2 Standards designed upon IEEE 802.15.4 and example sensor hardware

Next, a few well known WSN standards built upon IEEE 802.15.4 definition are introduced to establish an overview of the current standardization state of WSNs. The example of typical sensor node hardware is also given.

6LowPAN (IPv6 over Low power Wireless Personal Area Networks) is a standard developed by the corresponding working group in the IETF (Internet Engineering Task Force). The group finished its standardization work in 2012. The core idea of 6LowPAN definition is to allow connectivity over IP to even smallest constrained devices. 6LowPAN defines the methods for IPv6 packets to be communicated over IEEE 802.15.4 based network [43]. IEEE 802.15.4 maximum frame size is much smaller than IPv6 frame size, so an adaptation layer is defined. 6LowPAN also redefines packet format and address management. 6LowPAN packets contain compressed header and shortened address to further reduce the IPv6 packet size. 6LowPAN adaptation layer is specified on top of the IEEE 802.15.4 specified physical and data-link layer. The adaptation layer allows the use of TCP/IP-based network layer protocols. From the security point of view, IPv6 offers an opportunity to take advantage of existing IP security architecture. [44] [35] [23]

Another well known standard in the WSN world is ZigBee. First ZigBee standard was made publicly available in June 2005. ZigBee defines the higher layer communication protocols built on the IEEE 802.15.4 standards. ZigBee defines three types of devices. They are: ZigBee coordinator, ZigBee router and ZigBee end device. ZigBee routers and coordinators are IEEE 802.15.4 standard defined FFDs and end device can be either FFD or RDF. ZigBee coordinator is responsible for network formation, storing information and bridging separate ZigBee networks together. ZigBee routers link ZigBee end devices together and form multi-hop connections with other ZigBee routers. ZigBee end devices are sensors, actuators and controllers that transmit data only to ZigBee routers or coordinators. Message encryption in ZigBee networks is commonly

based on 128-bit AES encryption and symmetric keys. These keys are either link based or associated to the whole network. Keys are distributed through pre-installation, agreement or transportation. Transported keys are distributed through dedicated trust center. Initial communication with the trust center is done with a global master key, which is preloaded to the nodes. Master key is also used in key agreement, if link keys are negotiated between ZigBee routers and end devices. Latest versions of ZigBee standard also introduce public key cryptography based on Elliptic Curve Cryptography (ECC). [45] [35]

WirelessHART is a standard specially designed for industrial use. This includes applications like process management and control applications, in addition to more sensor oriented applications. WirelessHART was first released in September 2007. WirelessHART is an extension to the Highway Addressable Remote Transducer Protocol (HART). HART is one of the most popular industrial protocols today, as it can operate over legacy analog industrial wiring. WirelessHART uses 2,4GHz frequency specified in IEEE 802.15.4. The network consists of wireless field devices, gateways, process automation controller, host applications and a network manager. Wireless field devices communicate with host applications through gateways. Network manager configures the network and communication schedule and also handles routing. Network manager does not have to be separate entity and can be integrated to a gateway, host application or process automation controller. [46] [35]

WirelessHART network security relies on additional entity called security manager, which manages network keys and collaborates with network manager. Security manager can be integrated application or a separate device. Like ZigBee, WirelessHART uses AES-128 encryption with different symmetric keys. WirelessHART security manager has many similarities to trust center in ZigBee. On WirelessHART, all wireless devices are preloaded with join keys. The devices send joining requests to Network Manager, which verifies the join key from security manager. Upon successful authentication, all the other keys are distributed to the device. [46] [47]

A representative example of sensor hardware is the Mica mote[2]. The unit is a small, several cubic inch sensor/actuator with central processing unit (CPU), power source and radio. The unit can also be equipped with several optional sensing elements. The processor is a 8-bit 4MHz Atmel ATMEGA103 with 128 KB of instruction memory. The data random-access memory (RAM) size is 4 KB and 512 KB of flash memory is also available. The power consumption of CPU is 5,5 mA when active with 3 volt operating current. Sleep state power consumption is two orders of magnitude less. The radio is 916 MHz low-power radio, delivering up to 40 Kbps bandwidth on a single shared channel with a range of up to few dozen meters. The radio consumes 4,8 mA of power in receive mode at 3 volt operating current and up to 12 mA in transmit mode. Sleep mode power consumption is at 5 µA. Optional sensors are mounted on a sensor board. Sensor board allows mounting of temperature sensor, magnetomer, accelometer or microphone for example. The device is powered by two AA batteries, which provide approximately 2850 mA hours at 3 volts. This results in around 315 days of battery life

with one minute of CPU activity and one minute of radio transmitting and receiving in every hour. [48]

4.3 Authentication and key distribution

In current WSN standards, key management and authentication is loosely defined and available schemes are either insecure or rely heavily on connectivity to trusted base station. Outside standardization work, there is a lot of other research available that define new key management propositions designed for WSNs.

4.3.1 Solutions

The possible key agreement schemes can be categorized to three types: the public-key schemes, the trusted server schemes and key predistribution schemes. We already mentioned that public key cryptography is not ideal for many WSNs, due to very limited processing power, memory and communication bandwidth of the sensor nodes.

The trusted server schemes based on symmetric key cryptography depend on a trusted server for key agreement between the nodes, like Kerberos [49]. We also mentioned that this type of scheme is not particularly good for WSNs, due to high cost of base station nodes in relation to sensor nodes and scalability issues. In a WSN scale, the furthest sensor nodes may be several tens of hops away from the authentication base station, which makes this scheme very inefficient due to high energy cost of communication. The third approach to key agreement is to predistribute key information to all sensor nodes prior to deployment. This scheme can be seen as suitable candidate for WSN context. [50]

At very extreme case, each node would contain a unique symmetric shared key for each other node in the network. This scheme guarantees strong resilience against adversaries taking advantage of compromised nodes. However, this solution is not viable for WSNs due to memory limitations of sensor nodes. Adding new nodes to the network also proves very problematic with this solution as we would need a secure way to deliver the new key to each node in the network to communicate with the newly deployed node.

The basic random key pool based key predistribution scheme was developed by Eschauer and Gligor in 2002 [51]. The basic idea of the scheme is fairly simple. Each node is preloaded with a random subset of keys from a large key pool before deployment. To agree with communications, each pair of nodes needs to find a common key from their respective key pools. This key is used as their shared secret. It is not guaranteed that any given two nodes find a common shared key and thus be able to establish communications. However the key scheme is based on idea that probabilistically enough nodes find common keys to form a secure connected network. Furthermore, this probability can be adjusted by parameters like, key subset size and key pool size.

Another paper further strengthens the random key pool scheme by introduction of q-composite scheme [28]. The difference is that any two nodes now need to find q (q >

1) common keys to derive a shared secret key. This solution prevents adversary eavesdropping a large number of communication channels in the network when a small number of nodes are compromised. This increased resilience comes at the cost of reduced resistance against large scale attacks. The requirement of having q common keys instead of just one reduces the probability of any given two nodes being able to form communications with each other. To achieve same communication probability with basic random key pool scheme, we need to decrease the size of the key pool, which in turn reduces the amount of nodes that attacker has to compromise to completely break the scheme.

The q-composite key distribution scheme was further developed in 2005 in by Authors W. Du, J. Deng, Y. Han et al. [50]. The authors introduce a proposition to enhance the q-composite key scheme by introducing multiple key spaces. The scheme works by formation of a key pool matrix from several separate key pools. Each node then receives a small sub-matrix key set from the key pool matrix. If any given two nodes find a sufficient overlap in their respective key sets, they form a connection. The paper proves that this multi-space key distribution scheme provides the same probability of connection between any two given nodes with no additional memory requirement. The overall probabilistic security is also increased with the cost of additional computation requirements. The computation requirements still remain considerably smaller than in public key cryptographic schemes.

We mentioned the Sybil attack being particularly harmful against WSNs. The Sybil attack is performed by first compromising nodes and extracting key information. This key information is used to generate Sybil nodes that an adversary tries to authenticate to the network. Key agreement scheme's ability to resist passive eavesdropping attacks is at least in some relation to the ability to resist Sybil attacks, as both attacks take advantage of the adversary's pool of compromised keys. There has also been dedicated research by J. Newsome, E. Shi, D. Song et al. on different key agreement schemes' ability to resist Sybil attacks [12]. The authors introduce a key validation phase as an additional defence against Sybil attacks. The validation works by nodes challenging their neighbours for keys they claim to have. As the information of which keys the node has as part of its key set is public, the neighbouring node can challenge nearby node via picking a shared key from its own set and sending an encoded challenge using that key. The challenged node can reply with a correct message if it can successfully decode the challenge message. The full validation, meaning each node challenges all the other nodes in the network, is not practical. It causes unacceptable communication overhead and allows a possibility for DoS attacks. A partial validation means that each node challenges certain amount of its closest neighbours. The degree of validation must be chosen to make it sufficiently improbable for an adversary generated Sybil node to pass the validation.

The research by J. Newsome, E. Shi, D. Song et al. also shows that the basic random key pool scheme is vulnerable to Sybil attacks without addition key validation phase [12]. Validation of 30 neighbouring nodes in a densely populated large WSN gives the scheme some protection, but it still lacks the resistance of q-composite- or multi-space

key distribution scheme. Out of the introduced key schemes, the multi-space key distribution scheme proves to be most resistant to Sybil attacks, requiring an adversary to capture majority of the nodes in the network to achieve even minimal probability of creating a Sybil node. [12]

The radio resource testing method has also been adapted to be more suitable for WSNs to offer protection against Sybil attacks [12]. The resource testing is based on an assumption that each device has only one radio, which is not able to receive or send on more than one channel at the time. When a node wants to verify that none of its neighbours are Sybil identities, it assigns each of its neighbours a different channel to listen. Then the node chooses a random channel on which to broadcast a hello message and then listen for a reply. If the neighbour that was assigned that channel is a legitimate, it should hear the message and send a reply. The test can be repeated in order to achieve sufficient probability to detect Sybil nodes.

The research paper by Y. Zhou, Y. Zhang and Y. Fang introduces a suggestion to strengthen security in authentication situations when individual nodes are added to the operating WSN [33]. The paper suggests introducing time stamps to the trusted third party certificates that nodes use to authenticate and join WSN based on PKI authentication system. The introduced time stamps could only offer a small time window in which a certain newly deployed node could bootstrap itself and join the WSN. After initial authentication, the communication could be encrypted via periodically changing symmetric keys. This makes it hard for an attacker to take advantage of certificates acquired along with captured nodes.

4.3.2 Discussion

The key predistribution schemes are at particular interest in the WSN concept. They have many design advantages that make them well suited for WSNs. However, the concept of providing each node a random key set from a finite key pool makes the key pool generating and key pool providing server a single point of failure in the architecture. Nevertheless, all this communication can be done prior to deploying the sensor in the network. There is no need to connect the key pool server to the actual WSN, which denies an adversary an opportunity to target this weakness with any attack through the WSN. Out of all the introduced predistribution schemes, the random multi-space key distribution scheme is most promising, offering superior security to other schemes with little additional cost in computation and transmission overhead.

Despite obvious advantages, there are many disadvantages to the predistributed key schemes as well. One major disadvantage is that due to probabilistic connection forming, the predistributed key schemes achieve at best a partial mesh network topology. These key schemes are designed for very large sensor networks with over 1000 densely deployed nodes with sizeable communication range resulting each node having over 20 nodes within its communication range [28]. The probabilities dictate, that these conditions will result fully connected and sufficiently redundant network. However, network efficiency is always lost with this scheme. Due to variance in the amount of formed

connections for each node, the traffic load and energy consumption is not well balanced. This can be detrimental to applications that rely on constant data streams that consume most of the node's data transmission capacity. The traffic balancing can be improved by some degree with the use of a specified routing protocol, but it is done at the cost of transmission delay by increased buffering of data on the busy nodes or diverting data streams through longer routes.

The radio resource testing can be used to add another layer of security against Sybil attacks despite what authentication or key distribution scheme is used. The verification is breakable with custom radio hardware, but it makes a larger scale attack increasingly costly and more difficult for an adversary. This compliments the fact that latest random key predistribution schemes are very resilient to smaller scale attacks. However, the radio resource testing increases energy consumption in a form of additional transmission overhead. The increased security level must be weighed against other requirements for the particular WSN application.

Another Sybil attack protection method not previously mentioned in this thesis is position verification [12]. The method relies on the assumption that Sybil nodes should appear exactly at the same position as the malicious node that generates them. The WSN specific problem of this approach is that sensor nodes are physically very small and on many applications, nodes are randomly deployed to the environment. This makes it possible to legitimate nodes to reside on each other as well. We will discuss this method of verification in more detail with the concept of VANETs, as there is much research available on the subject. Some of the methods could be suited for WSNs, but in general, these methods cause relatively high communication overhead, which will greatly affect energy consumption of constrained sensor nodes.

Finally, the introduced timestamping method along with PKI authentication can be considered highly beneficial. This method also increases protection against DoS attacks that are particularly harmful against constrained WSN nodes when using a public key authentication. When timestamps are used, the node receiving the authentication message can decrypt the timestamp part of the certificate first and discard the message right away if the timestamp is not valid, without evaluating rest of the message. This saves processing power and therefore also device's limited energy reserves.

4.4 Secure localization

We introduced the problem of nodes determining their geographical position and relative position in the WSN, known as localization. We already briefly mentioned the possibility of including GPS unit on the nodes or manual location preconfiguration as direct localization approaches. As direct approaches have proven infeasible for many WSN applications, several indirect approaches have been developed.

4.4.1 Solutions

One proposition for indirect localization is called Spotlight [20]. Spotlight relies on external Spotlight device, which performs all the localization related calculation. The Spotlight device is equipped with a laser light source that can be pointed freely to the sensor nodes in the known terrain. The Spotlight device generates controlled events in the area where sensors are deployed. The area of affected sensors is called a lightened sensor area. Using time events perceived by a sensor node and spatio-temporal properties of the generated events, spatial information regarding the sensor node can be constructed.[35] [20]

Another proposed solution is Radio Interferometric Positioning System (RIPS) [52]. The system works by using two external radio transmitters to create an interference signal. The transmitters are placed on different locations and create a signal with slightly different frequencies. At least two sensor nodes need to calculate the phase offset of the observed signals. The relative phase offset is a function of the relative positions between the two transmitters, the receivers and the carrier frequency. This information can be used to calculate the relative locations of two sensor nodes, or the actual location of the sensor nodes, if the location of the radio source is known. [35] [52]

Another possibility for indirect localization is to use Moore's algorithm. The researchers have shown that distributed localization algorithm can work without the use of GPS or any kind of beacon nodes [53]. This method also works robustly with noisy distance measurements. The method is based on the use of robust quadrilateral. A robust quadrilateral is a fully connected quadrilateral, whose four sub-triangles are robust. [35]

The algorithm has three phases. First the cluster localization phase starts by each node becoming the center of the cluster and measuring the distance of its one-hop neighbours. This information is then broadcasted to the neighbours. For each cluster, each node computes the complete set of robust quadrilinears. Position estimations for a local coordinate system are computed for as many nodes as possible. This is done by using the overlap graph formed from broadcasted information of overlapping clusters. The second phase is the cluster optimization phase. This is done by using numerical optimization, like spring relaxation. The last phase is cluster transformation phase. In this phase, nodes compute a transformation between local coordinate system of connected clusters. The transformation computes the rotation, translation and possible reflection that best aligns the nodes of two local coordinate systems. The paper proves that in a case of high measurement noise, the nodes with unreliable measurement data are excluded from the quadrilinear formation process. This results to an algorithm forming a correct network topology with high probability, or not being able to form it all, if the measurement noise is high enough and node connectivity is low. [35] [53]

The several secure indirect localization methods have been also provided. One of them is called SeRloc [54]. It is based on a set of directional antenna equipped locator nodes that provide sensor nodes their location. The main idea of the system is that each locator node transmits a different beacon at each antenna sector. The beacon message

consists of locator coordinates and angles of directional antenna boundary lines. The use of directional antennas also improves localization accuracy and also results in an adversary having to impersonate several beacon nodes to compromise localization process. [35] [36]

Another secure indirect localization method is called secure positioning method in sensor networks (SPINE) [55]. SPINE is based on verifiable multilateration, which we will go into more detail in the context of VANETs. In short, SPINE works by distance bounding each sensor node to at least three reference points to calculate its position. The amount of reference points is relatively high in comparison to other beaconing methods, which is a definite drawback on this method. [35] [36]

Yet another secure indirect localization method is called a robust positioning system in WSNs (ROPE) [56]. ROPE is a hybrid algorithm. First part of the algorithm allows sensors to determine their location without any centralized computation. The second part of the algorithm is a location verification mechanism which verifies the location claims of the sensors prior to any data collection. ROPE defines the WSN node types as sensor and locator nodes. Sensor nodes share a pairwise key with every locator node. As the number of locators in the network is considerably smaller, this will not cause considerable memory requirement to the sensor nodes.

4.4.2 Discussion

Localization in WSNs has three important aspects to consider: energy efficiency, accuracy and security. The first two have been researched for nearly a decade, but the attention of researchers has shifted to security aspect of localization only in the recent years. [36]

The first indirect localization method introduced, Spotlight has certain advantages over the others. The Spotlight device is a single point of failure in the network and definitely a point of interest for any adversary. But because only one Spotlight device is required, it can be tamper-proofed and supervised with considerably less effort. Spotlight system is also proved accurate over long distances and scalable to large WSNs [20].

The second solution, RIPS, requires two fairly simple radio transmitters to create an interference signal, which is not a heavy hardware requirement. As the localization process depends on receiving signals from both transmitters, they also become single point of failure. Another downside of the system is that every node needs to collaborate with at least one other node to calculate its own position. Collaboration can be done with several neighbouring nodes to make it impossible for an adversary to disturb localization process with a small number of captured nodes, which slightly increases communication overhead.

The localization method based on Moore’s algorithm was developed for sensor networks with no additional positioning hardware available, but it is considerably more challenging to secure. The system excludes nodes with very noisy or incomplete distance measurements from quadrilinear formation phase, so proving falsified information

at this phase is not very beneficial for any adversary. However, the next phase of the protocol works by node sending its localization information to neighbour, the neighbour stitching received and its localization information together and sending it to the next node on the line. This allows any compromised node on the line to falsify a large amount of localization information, most likely corrupting the localization for a significant part of the network. These attacks can be resisted to some degree by implementing majority voting and plausibility checks to the later localization steps. This will however increase communication overhead and allows additional DoS attacks.

Majority of the more recent localization methods that have been already much considered from the security aspect, are based on the use of beacon nodes. On most beacon node scenarios, there are two key elements to make localization process secure. If the beacon node sends the location information to the sensor node over the network, this communication needs to be secure. Additionally, network needs to be able to resist attacks based on captured beacon nodes.

The lastly introduced method, ROPE, has a simple idea of securing communication between sensor nodes and beacon nodes via a preshared pairwise key. As we discussed in the context of authentication, the preshared pairwise keys offer the best resistance to node capture with a little computation overhead, but they are not viable option in the direct communication between sensor nodes due to limited memory space for the key storage. However, as the number of beacon nodes is far less than sensor nodes, the memory requirement lowers considerably. Nevertheless, this method still has the downside of destroyed or captured beacon nodes being impossible to replace in the deployed network.

The resistance to captured beacon nodes can be achieved by beacon nodes monitoring each other and reporting misbehaving nodes to sensor nodes in a majority voting principle. The network is also naturally resistant to beacon node capture if sensor nodes are able to receive beacons from several beacon nodes, in which they can choose from which to use for localization information. In this case, the sensor nodes can directly detect the beacon nodes sending suspicious localization information.

There is a wide variety of localization methods available, each having different hardware requirements, strong and weak points in security. Few introduced propositions can be considered strongly secured with relatively inexpensive additional hardware required [20] [52]. Still, the practicality of using any additional hardware depends highly on the WSN application. For example, the introduced Spotlight system might work very well in an environmental monitoring or a military application. The sensor nodes can be deployed from an aerial vehicle. The vehicle could act as a Spotlight device as well, lightening the deployed area and completing sensor node localization process right after deployment. Being an aerial vehicle, the Spotlight device would be harder to target for a potential adversary. Other introduced propositions [52] [56] have similar advantages and disadvantages and work best in a scenario where the additional hardware used is well suited for the application and environment and the weak points in security can be covered by other means.

4.5 Routing and data aggregation

As discussed in Chapter 3, after the initial authentication and localization procedure is completed and routing is initiated, we need to consider attacks against operating WSNs. On many scenarios, adversaries are able to capture authenticated nodes that are already participating WSN communication, which offers adversaries a direct way to disrupt WSN routing protocols. Many routing protocols are designed with very little attention to security and completely securing existing WSN routing protocol is usually not possible [48]. Still, there is some research available on secure routing protocol design, as well as attempts to secure existing WSN routing protocols.

4.5.1 Solutions

An early proposition for secure WSN is called an Intrusions-tolerant routing protocol for wireless sensor networks (INSENS) [57]. INSENS is based on flat network topology, where network consist of sensor nodes and a single base station which also acts as a data sink. The authors of the paper focus on securing routing against sensor node capture and make an assumption that network base station is secured from physical access. Also direct communication between sensor nodes is not supported. The base station communicates with the sensor nodes via one-way sequence number to prevent spoofing attacks. The base station is the only entity in the network that is allowed to use broadcasting. The sensor nodes can only use unicast and only communicate with base station to prevent DoS attacks. The communication between individual sensor nodes and the base station is secured with a unique preshared pairwise key. All control routing information must be authenticated through base station, which makes it harder for an adversary to inject malicious routing information the network. Finally, the routing protocol is designed to form redundant multipath routing tables to increase the amount of nodes an adversary needs to capture to disable parts of the network.

A proposition to secure an existing WSN routing protocol, Implicit Geographic Forwarding (IGF) has been made [58] [59]. IGF is a stateless location based routing protocol, without dependence on knowing the network topology or the presence or absence of any other nodes. It allows receiving nodes to determine a packet's next-hop at transmission time coupling routing and MAC components into a single Network/MAC protocol. [58]

The secure version of the routing protocol is called Secure Implicit Geographic forwarding (SIGF). SIGF consists of three protocols, each adding new security features to the previous. SIGF-0 is a stateless protocol based on probabilistic defences. SIGF-1 uses local history and node reputation evaluation to protect against certain attacks. SIGF-2 uses neighbourhood-shared state to provide stronger security guarantees.

As IGF has no routing tables, it naturally confines attacker's impact to the neighbourhood and prevents spoofing, altering or dropping routing information. Single attacker can still perform a simple blackhole attack in the local neighbourhood by pretending to be best node for next-hop relay. When a legitimate node has data packet to

relay, it sends an Open Ready To Send (ORTS) –request. A malicious node replies immediately with a Clear To Send (CTS) -reply. After the malicious node is chosen as a next-hop relay, it can send a confirmation message of receiving and forwarding the data packets (ACK) and still drop the actual data packets (DATA). [58] [59]

The probabilistic defences included in SIGF-0 consist of configurable receiving angles in which CTS messages are listened from forwarding area, waiting for several CTS replies and different options to choose forwarding candidates. SIGF-1 adds additional layer of protection by nodes keeping statistics about their neighbours. Each node collects following statistics from each of its neighbours: packets sent to a node for forwarding, the number of packets that node has forwarder on this node's behalf, last claimed location of the neighbouring node and average response delay of a node. Other parameters are calculated using these statistics to from a node reputation value. If the value drops below threshold, the node is excluded from forwarding decisions. SIGF-2 assumes that authentication scheme is used that provides pairwise keys between neighbours and offers encryption of up to all the protocol messages (ORTS, CTS, AKC and DATA). This will offer protection from replay based DoS attacks at the cost of increased communication and calculation overhead.

The specific problem of securing multimedia streams in sensor networks is an example of a problem caused by limitations in sensor node hardware. The problem is addressed in a paper consisting of lightweight security principles for multimedia WSNs [38]. The paper introduces novel modifications to existing hardware to for analog-to-digital and digital-to-analog conversions. The modifications allow analog data streams to be encrypted via symmetric key conversion phase, adding very little additional power requirements and transmission overhead. The solution effectively allows sensor nodes to be equipped with symmetric key cryptography capable hardware.

4.5.2 Discussion

Routing in WSNs is a much researched and challenging subject. Due to constrained nature of WSNs, the performance and reliability considerations have left security with a little attention on routing protocol design [48] [37] [4].

The introduced INSENS routing algorithm shows how implementing security features sets limitations to WSNs. The routing protocol can be considered fairly secure, but at heavy cost in communication overhead and network scalability. As each node shares pairwise key with the base station, data decryption is not possible on the intermediate nodes. This prevents data aggregation and results in scalability issues as data streams from all the WSN nodes are directed to the base station. This effect will also be amplified by the fact that all control routing messages are also authenticated through base station.

The SIGF protocol offers a good overview of measures available to secure routing in WSNs. The location based routing is immune to some of the attacks against WSN routing protocols, but few common attacks still remain viable. The simple configuration methods of SIGF-0 offer a significant increase in defence against simple blackhole at-

tacks. The reputation system in SIGF-1 increases the network performance under variety of attacks and offers protection against simple Sybil attacks. More advanced Sybil attacks can still go undetected, as malicious nodes can pretend forwarding messages to non-existent Sybil nodes, which will satisfy the sender's message forwarding check. An adversary can still disrupt the neighbourhood communication by simple DoS attack based on replicating observed legitimate messages. DoS attacks can be prevented using SIGF-2 and adding sequence number to encrypted messages. Advanced Sybil attack protection requires nodes collaborating on detection of malicious and Sybil nodes via trust ratings.

In general, WSN protocol design should take advantage of wide deployment area and multiple routing paths available. Node capture can be resisted by sending packets along multiple paths and checking consistency in the destination. Important routing decisions should also require multiple reports before response is made. A wide area of deployment makes also a typical DoS attack to only affect a fraction of the network. Detection methods and solutions have been developed to avoid routing traffic through jammed area [39]. However, the presented solutions are still far from optimal. [18] [60]

Implementing cryptography always entails a performance cost for extra computation and often increased packet size. Cryptographic hardware support increases efficiency, but also increases the financial cost of the nodes. Therefore, the decision to use dedicated hardware highly depends on the application context. It can be argued that a reasonable level of security can be achieved with software-only cryptographic implementations on most of the WSN applications that do not require large streams of real-time data. Still, the dedicated hardware is well suited on multimedia WSNs with video streaming nodes. [18]

5 SECURITY CHALLENGES IN VEHICULAR COMMUNICATIONS

Vehicular communications is a distinctly separate IoT application field. The topic has been researched for over two decades now and wide availability and low-cost of global-positioning systems (GPS) and wireless local area network (WLAN) transceivers has made it a step closer to reality.

Vehicular communication systems that enable cooperative applications to improve road safety and traffic efficiency are generally called Intelligent Transportation Systems (ITS). Vehicular applications can be roughly classified into either ITS applications or non-ITS applications. Non-ITS applications are driver and passenger oriented applications, which include Internet connections and multimedia services. They are usually commercial and comfort applications. ITS applications include route guidance, traffic control, public transportation management, electronic payment services, onboard safety and security monitoring, collision avoidance and disaster response and evacuations. They present the primary vision of vehicular applications and we mainly focus on them in this work. [61] [62]

In a more recent classification, European Telecommunications Standards Institute (ETSI) has classified vehicular applications into three classes: road safety, traffic efficiency and other applications. Other applications include business and comfort applications and it is similar classification to non-ITS applications. Road safety applications are defined to decrease number of road accidents. They can be further classified into two classes: driver assistance applications and actions on vehicle applications. The purpose of driver assistance applications is to assist driver to avoid road dangers and accidents. Actions on vehicle applications provide necessary information to vehicle systems to avoid and reduce damage of accidents. The main difference is that in the former category, driver is responsible of evaluating the relevance of received data. [62]

5.1 Example use scenario

Imagine a scenario, where an emergency vehicle, like an ambulance approaches a four-way intersection. Vehicle's on-board unit (OBU) could send an alert to the other vehicles and to the road-side unit (RSU) controlling the traffic lights. Traffic lights for the incoming traffic from the other directions would turn red in advance. The drivers would be alerted of an incoming emergency vehicle and if necessary, their cars would be autonomously slowed down.

The presented scenario features several types of ITS applications, including both types of road safety applications. Driver assistance applications and actions on vehicle applications provide multiple layers of road safety assistance. Driver assistance applications typically generate information and sound or light alarms between two and 30 seconds before collision in order to give enough time for driver to take appropriate actions. On actions on vehicle applications, decision and actions are automatically initiated by vehicle systems a few seconds before highly probable event like crash. These are the most sophisticated road safety applications and require a high level of security to be operational. Most of the European and American ITS related standards and projects focus on driver assistance applications as they will be first deployed cooperative road safety applications. Driver assistance applications are also currently defined as primary road safety applications by many OEMs. [62]

5.2 Relevant PHY and MAC layer restrictions

When defining security requirements for road safety applications, we will first shortly examine OSI-models' PHY and MAC layers associated with vehicular communications as they have some special characteristics that affect practicality of possible security solutions. Moving vehicles add special requirements to the network, like: long operation range, nodes moving at high speeds, extreme multipath environments, multiple overlapping ad hoc networks and extremely high quality of service (QoS) in some emergency scenarios [61]. High mobility of nodes and extreme multipath environments present unique challenges to the wideband communication. Vehicle-to-vehicle communication channel is "doubly selective". This means that frequency response varies significantly over signal bandwidth, and its time fluctuations happen in the course of a symbol period [63].

Although current cellular networks enable voice communication and certain informational services to drivers and passengers, they are far from optimal solution for direct vehicle-to-vehicle and vehicle-to-roadside communications, which is the main form of communication in VANETs. VANET applications, like the presented emergency-response vehicle scenario, require extremely reliable and minimal-latency method of message delivery. The main challenge is that on most of the scenarios, communication is decentralized and no control can be assumed. Moreover, because there is no handshaking, many applications will be broadcasting their information to surrounding cars. This may cause channel throughput degeneration in case of sudden emergencies, like collisions. On congested roads, this leads to the requirement of a dedicated control channel. The well known problem of hidden and exposed nodes is also particularly problematic in a vehicle-to-vehicle communication scenario. The distance between the moving nodes varies constantly, which makes the occurrence of the problems unpredictable.

Several different approaches have been proposed to solve these medium access control (MAC) related issues. The main focus today is using the IEEE 802.11 carrier sense

multiple access (CSMA) based MAC for direct vehicle-to-vehicle or vehicle-to-roadside communications. Even though CSMA adds unwanted random elements to MAC, it has an advantage of good availability of supporting hardware and low implementation costs. [64] [65]

Another current challenge is the bandwidth range of the VANET channels, which ranges from 10 to 20 MHz. With a high number of nodes within transmission range from each other, the congestion becomes a significant issue. Use of multiple channels leads to the channel synchronization and co-channel interference problems, which will add more complexity to MAC definition. [64] [65]

5.3 Authentication and data-centric trust

As we continue up to OSI-model's network layer, the first big security related issue is authentication. Providing reliable authentication and authenticity maintaining methods is a different kind of challenge in VANETs in comparison to WSNs. While VANET nodes are lifted from many processing power and energy consumption constraints, the communication channel remains very challenging due to the high mobility of nodes. The constantly changing network topology and public nature of the network also sets different requirements and restrictions to authentication scheme.

The problematic feature of VANETs is that every vehicle on the road has, and also on most situations, should have an ability to access and join the network. When VANETs will be widely deployed, majority of the nodes on the roads will be privately owned cars. Any of these cars can be legitimately registered and owned, along with proper certificates and still belong to an attacker. This presents a problem, as a node with a previously trustworthy communication record still has the potential of turning into a hostile one. These attackers can be classified as malicious insiders as they have joined the network with a proper authentication procedure and can be considered as valid members of the network before the initiation of the attack. It can be argued that relying on traditional authentication procedure as a sole method of providing authenticity is not practical in VANET, as there is a certain trust problem even between two legitimately authenticated nodes. However, VANETs also differ from many other networks by having considerable presence of governmental authorities and other special entities. Many applications, like our emergency-response vehicle scenario can greatly benefit if a certain node can reliably authenticate itself as an emergency vehicle, police car, or a government controlled RSU controlling the traffic lights, for example. Reliable vehicle identities are also useful for liability reasons, which we will introduce in the following Section.

In many other networks, authentication and message encryption can be done with self-organized trust management system, like PGP (Pretty Good Privacy). Self-organized trust management systems rely on using public key pairs for authentication and setting up private keys for further communication. However, as malicious insiders

have easy access to VANETs, there is a need for trusted third party authority, which implies the need of PKI (Public Key Infrastructure). [66]

In addition to trust issues, we need to examine technical limitations of the authentication procedure. Current vehicular communication systems have maximum range of about one kilometre [65]. This combined with the fact that nodes move at relatively high speeds allows only a few seconds of communication time before connectivity is lost. This presents a serious challenge for the authentication procedure. Authentication needs to be completed with as few message transactions as possible to fulfil the low-latency requirements. Public key cryptography introduces additional overhead to the messages, which increases message transmission time and latency. This overhead can be kept on an acceptable level by using a compact cryptosystem. ECC is by far the most viable candidate for VANETs. [66] [67] [68]

Under a PKI solution, safety messages sent by vehicle are signed with its private key and a certificate signed by the CA (Certificate Authority). Receiving vehicle uses the certificate to extract and verify the public key of the sender and then verifies the message's contents by using the public key. This scheme reduces the number of message transactions required between communicating nodes compared to self-organized trust management systems, making it more ideal solution considering latency requirements in VANET communication.[66]

The use of secret information like private keys incurs the need for a Tamper-Proof Device (TPD) in every vehicle. In addition to storing secret information, this device is also responsible for signing outgoing messages. To reduce the risk of being compromised by attackers, this device needs to have its own battery, which can be charged from the vehicle's battery. The device also needs to have a clock, which can be securely synchronized when passing a trusted roadside base station, for example. The access to this device should be restricted to authorized people. TPD's cryptographic keys could be renewed during vehicle's periodic technical checkup. [66]

When a PKI based solution is used, there are a few different candidates for CAs. Considering the involvement of authorities in vehicle registration, governmental transportation authorities are likely candidates. The main problem is that vehicles are certified by a regional authority in a given country, but vehicles from different regions and countries should also be able to authenticate with each other. This problem can be usually solved by including certificate chain leading to a common authority, but in VANETs this would create unacceptable message overhead. This leads to a requirement of registering each vehicle to the local certificate authority to replace the certificate chain with a single certificate of transit or destination region. This requires governmental cooperation. Another candidate for CA could be vehicle manufacturers, given a limited number of trust already endowed in them by government authorities, but most likely governments aren't very inclined to involve non-governmental institutions in law-enforcement mechanisms. The advantage on using PKI in VANETs is also accompanied by other challenging problems, notably certificate revocation. The certificates of a detected attacker or malfunctioning device need to be revoked. [66] [68]

In many vehicular applications, like in our emergency-response vehicle scenario, the trustworthiness of the data is top priority, even over the trustworthiness of the nodes transmitting this data. This combined with strict technical limitations for authentication procedure has led many security solutions to the direction of data-centric trust and verification. If other nodes, namely the traffic light controlling RSU and other cars approaching the intersection can verify the trustworthiness of the emergency message solely by examining message contents and other available data, there is no need to waste time on a complicated authentication procedure between different nodes. The use of PKI can be classified as proactive data-centric trust security concept, but there is a smaller scale of studies on reactive security concepts. Data-centric trust and verification needs to provide security means to ensure that in-transit traffic tampering and impersonation attacks can be detected by the receiver of the message. Solutions are presented in more detail in Section 6.3. [68]

5.4 Geo-addressing and secure localization

After authentication, the next big security issue is how to manage an addressing system used by routing protocol and also by many applications, like the collision avoidance system in our emergency-response vehicle scenario. Routing in VANETs differs from traditional Internet routing as well as from routing in other ad hoc networks, like WSNs.

In traditional Internet, as well as in majority of WSNs, routing is done by using topological prefixes. Due to rapidly changing topology in VANETs, a topology based routing becomes problematic. Additionally, many VANET applications, like the presented emergency-response vehicle scenario require that the messages include the physical position or at least geographic region in which the vehicle is located in. This has lead to the use of position based routing protocols. However, in comparison to WSNs, the public nature and massive scale of VANETs requires specific solutions in managing geographic information associated with vehicles. High mobility of vehicles makes tracking and managing these "geo-addresses" an extremely challenging task. [69]

Integrating physical location information to the current design of Internet can be roughly categorized to three different families of solutions. These are: application layer solutions, GPS-multicast solution and unicast IP routing extended to deal with GPS addresses. GPS-addresses can be represented by using closed polygons, such as circle with center point- and radius attributes. Any node residing in the area of the polygon is able to receive message addressed to that polygon. [70] [71]

Application layer solutions use an extended DNS (Domain Name System) scheme to resolve geographical position. DNS system is extended to include database of geo-addresses, which contains directory of information, down to the level of IP address of each base station and coordinates of a polygon representing base stations' coverage area. [71]

GPS-multicast solution to addressing uses GPS Multicast Routing Scheme (GPSM). GPSM is based on atoms and partitions. Atom represents the smallest geographic area

that can have a multicast address. A partition is a larger geographic area that contains a number of atoms and also has its own geographic multicast address. A partition could represent a country, town or state. The working principle of this protocol is to approximate the addressing polygon of the smallest partition inside current larger partition and use multicast address of the approximated partition as the IP address of the message. GPSM has an advantage of being flexible mix between application level filtering for the geographic address and multicast. [69] [72]

Unicast IP routing solution extended to deal with GPS addresses is used in several promising propositions. Geometric Routing Scheme (GEO) uses polygonal geographic destination to form GPS-cast header used directly for routing. GEO routing is based on virtual network, formed by GPS-address routers. GPS-routers use GPS-cast header for routing overlayed in current IP network. Geographic Positioning Extension for IPv6 (GPIPv6) defines geographical positioning information to be distributed in IPv6 frames. This can be done by introducing two new option types for IPv6. These are GPIPv6 source and GPIPv6 destination, used for signaling sender's and receiver's geographic position. Using unicast prefixes to target multicast group members has also been proposed. This is an extension to the IPv6 architecture that uses unicast prefix for multicast address allocation. These new multicast addresses are used to target multicast group members within certain geographic area. [69] [72]

After the introduction of methods to integrate the geo-addressing information to VANET routing, there is also a need to mention about multihopping requirements in the context of this work. A typical feature of ad hoc networks, like WSNs, is multihopping. However, VANET safety applications, like our example scenario, rely mainly on broadcasted emergency messages. Additionally, dedicated short-range communications (DSRC) specifications used in VANETs require safety messages to be transmitted with a sufficient power to warn vehicles in a range of 10 seconds travel time. Due to these reasons, multihopping is not required when delivering most delay-sensitive safety messages. Nevertheless, some form of multihopping is still required. Vehicles that receive warning messages estimate whether the reported problems can also affect their followers. In this case they will forward message to them. [66]

From the security perspective, the first requirement for geo-addressing solution is to provide a reliable method of associating position information with messages. However, this has to be done in a way that the protocol is able to resist attacks designed to deliberately retrieve and track the location of vehicles. We refer this ability as secure localization in the VANET context. Methods to provide secure localization are similar to methods of resisting Denial of Service attacks. Implementations of secure localization solutions may vary depending on chosen geo-addressing solution. [69]

One proposed solution for secure localization is tamper-proof GPS system [73]. On a concept level, the receiver could register its location at all times and would provide this information to other nodes in the network in an authentic manner. The main problem with this solution is the limited availability in urban environments. Current GPS systems do not provide reliable reception on bridges, or in tunnels etc. GPS-based sys-

tems also offer an attacker a several new ways to attack the system without tampering the system hardware, like blocking or spoofing the signal from GPS satellites. Moreover, these attacks can be performed by fairly unsophisticated adversaries [74]. More viable solutions are in Section 6.4.

5.5 Anonymity, liability and privacy

On our emergency-response vehicle scenario, all the receiving nodes of the safety message sent by the emergency vehicle need to be able to trust that the entity that generated this information really is the emergency vehicle. This is required even if the message has been forwarded by other nodes, like privately owned cars on the way. At the same time the privacy of the drivers of these privately owned cars needs to be protected. In many countries, this is even enforced by laws.

For liability reasons, VANETs also have a requirement to disclose certain communicated information and its origin to governmental authorities, like police. This information is useful in controlling traffic violations and in traffic accident investigation. Attacking VANET communications also offers an imaginative attacker a new way to accomplish crimes. Imagine a chaos that can be caused by compromising the presented emergency-response vehicle scenario. If there is no way to backtrack identities of nodes participating in a security attack, attacks could even be designed to perform a homicide, looking like an accident.

One of the main challenges of VANETs is to provide a solution that is able to support tradeoff between the authentication, liability and privacy. To ensure anonymity and privacy, cryptographically protected messages should not allow their sender to be identified. Furthermore, it should be difficult to link together two or more messages sent by the same node. [69]

Several solutions suggest protecting vehicle's privacy with anonymous vehicle identities. These can be based on electronic identity issued by a government called an Electronic License Plate (ELP) [73], or alternatively an Electronic Chasis Number (ECN) issued by the vehicle manufacturer. These identities need to be unique and cryptographically verifiable in a case the vehicle needs to be identified to the government authority. Cryptographic verification can be done by attaching a certificate issued by CA to the identity. Like physical license plates, ELP should only be changed when the owner of the vehicle changes or vehicle is registered to a different state or country. [66]

Direct authentication between other nodes is done by using public/private key pairs authenticated by CA. These key pairs are authenticated to vehicle's ELP or ECN by CA, but do not contain any information about the connection, so the actual identity of the vehicle cannot be discovered by eavesdropping attacker. These key pairs can also be referred to as pseudonyms. This protects vehicle's anonymity against unauthorized nodes, but preserves conditional liability towards authorized entities, like government authorities. [66]

To prevent vehicle tracking by eavesdropping, each vehicle needs to have a set of authenticated public/private key pairs to be used. Each key pair is only used for a certain time period and when all the keys have been used or their lifetimes have expired, the key set needs to be renewed. This introduces scalability issues as the number of keys each vehicle has to store can be huge on congested roads. The method of periodically renewing the vehicle's key set also needs to be defined. Options to solve these issues are discussed in Section 6.5.

6 STANDARDS AND SECURITY SOLUTIONS IN VEHICULAR COMMUNICATIONS

This Chapter will first introduce some well established VANET standards. Then we will continue to some more recent standardization work and research projects that provide solution propositions to issues introduced in Chapter 5.

6.1 WAVE framework

In 1999, the U.S. Federal Communications Commission (FFC) granted 75 MHz of spectrum in the 5,85-5,925 GHz range for the use the dedicated short-range communications in intelligent transportation systems [61]. The initial effort at standardizing DSRC radio technology took place in ASTM 2313 working group. FCC rules and orders specially referenced this document for DSRC spectrum usage rules. [75]
In 2004, this standardizing effort migrated to the IEEE 802.11 standard group as DSRC radio technology is essentially IEEE 802.11a adjusted to low overheads operations in the DSRC spectrum. IEEE assigned a new task group for DSRC [75]. This task group started working on the amendment to the IEEE 802.11 specification. The amendment is known as IEEE 802.11p WAVE (Wireless Access in Vehicular Environments).
Currently, WAVE framework consists of IEEE 802.11p standard, and IEEE 1609 family of standards. IEEE 802.11p defines PHY and lower parts of MAC layer for vehicular communications with nodes moving up to 200 km/h. IEEE 1609 -family of standards continue to define upper levels of MAC layers and specify certain aspects of 802.11p. Majority of research efforts and projects in USA are based on WAVE standards [69]. WAVE is fully intended to serve as an international standard applicable in other parts of the world as well as in the U.S [75].

IEEE 802.11p is a relatively mature standard in an IoT perspective. The project was accepted as part of the IEEE working group in September 2004. Final approval date was 17th of June 2010 and the standard was added to the part of IEEE 802.11 standard as amendment 6. Operation band for 802.11p devices is 5,85–5,925 GHz in United States and 5,855–5,905 GHz in Europe. [65] [42] [76]

Physical layer specification of the 802.11p is identical to the orthogonal frequency-division multiplexing (OFDM) based old IEEE 802.11a standard, with the addition to operation on reduced 10 MHz channels. Vehicular communication scenarios suffer from increased delay between arrival of the multipath components of the signal, compared to the traditional 802.11a-based WLANs. Halving channel bandwidth from 20 MHz reduces the problem, but also halves the supported physical layer data rate to 27 Mb/s.

802.11p also allows a lot higher maximum radio output power to fill the need of increased communication distance due to nodes moving at high speeds. Maximum output power is increased to 760mW in 802.11p from 40mW in traditional 802.11a indoor antennas. Radios also need to operate on broader temperature range due to harsh outdoor conditions, thus 802.11p extends the range from -40 °C to 85 °C. [65] [42] [76]

The 1609 family of standards consists of 1609.4 (upper MAC layer definition) 1609.3 (networking), 1609.2 (security), 1609.1 (resource management), 1609.5 (communication management) and 1609.0 (overall architecture). As briefly discussed earlier in this work, WAVE frequency bandwidth is divided into multiple channels. This is defined in 1609.4. Frequency channels consist of control channel for safety applications and service channel for non-safety applications. Coordination of multichannel access in vehicular ad hoc networks requires a global synchronization method. 802.11p offers a timing synchronization function to facilitate global synchronization based on external timing source, like GPS. [65] [42]

The 1609.2 security standard outlines an authentication and certification methods used for PKI in VANET communication. The standard also describes message encryption and decryption using ECC. The trusted entity for signing certificates is defined as Security services in the standard. However, the definition does not extend on how this entity is physically integrated to the network topology. One possible candidate would be authentication using existing cellular network, but high latencies and blind spots on network coverage create vulnerability windows. The problems of attacker taking advantage of these vulnerability windows are not addressed in 1609.2. [77]

6.2 Authentication and data-centric trust

Section 5.3 introduced the general problems and limitations involving authentication procedure on VANETs. Most of the derived security questions remain unsolved in the VANET standardization work. The available research on subject introduces solutions to simplify or completely replace the authentication procedure. Following subsections will go into more detail on this research. The proposed solutions can be roughly classified as proactive and reactive security solutions.

6.2.1 Public key infrastructure

The previously introduced PKI can be classified as proactive security solution involving digitally signed messages. Under the PKI solution, messages also include certificates signed by certificate authority. With governmental authorities acting as CAs, there will be several CAs, similarly to current vehicle registration authorities. These CAs will correspond to a given geographical region (e.g., country, state, metropolitan area, etc). In case of vehicle manufacturers acting as CAs, different CAs will also have to be cross-certified so that vehicles from different manufacturers can authenticate each other. This requires each vehicle to store the public keys of all the CAs whose certificates may need to be verified. As explained in Section 5.3, vehicles authenticate a set of public/private

key pairs with CA using ELP or ECN. A single pair of keys has only a lifetime of few minutes to prevent vehicle tracking. In the case of regional CAs, vehicles can request a new set of public/private keys as they enter new region, but in the case of vehicle manufacturers acting as CAs, the stored public/private key set needs to be considerably larger. [68]

One of the challenging problems of using PKI is certificate revocation. System needs to able to revoke certificates of recognized maliciously acting vehicles and malfunctioning devices.

Commonly used method to revoke certificates is distribution of Certificate Revocation Lists (CRLs) that consist of the most recently revoked certificates [66]. CRLs are distributed when infrastructure is available. Keys also expire automatically due to short lifetime of certificates. Both of these methods are described in the IEEE 1609.2 standard [77]. There are still a few drawbacks to using these methods. CRLs can be very long due to the large number of vehicles and their high mobility. A given vehicle can encounter an enormous number of vehicles during its trip through congested region, especially over longer distances. The short lifetime of certificates also creates a vulnerability window. Availability of the CA infrastructure is also a major shortcoming. Infrastructure can't be expected to be always available, especially in the first stages of deployment. [68]

A set of revocation protocols have been suggested to avoid the mentioned shortcomings [68]. First protocol of the set is Revocation Protocol of the Tamper-Proof Device (RPTD). This protocol assumes that each vehicle is equipped with Tamper-Proof Device, which stores all the cryptographic information required for authentication procedure (tamper-proof hardware will be further discussed in Subsection 6.2.2). This protocol also assumes that TPD of the vehicle is not compromised and attacker cannot interfere with its operation. Once the CA has made a decision to revoke all the keys of a given vehicle M, it sends a revocation message encrypted with vehicle's public key. After the vehicle's TPD receives the message, it decrypts it, erases all the keys and stops signing further safety messages. Vehicle confirms the operation by sending a confirmation message to the CA. All the communication between vehicle and the CA takes place via base stations, so the CA has to have information about vehicle's location in order to select the base station through which it will send the revocation message. If vehicle's exact location is not known, the most recent known location of the vehicle is used and paging area is defined with a set of covering base stations. Revocation message is then multicasted through these base stations. In case there is no recent location available, or ACK is not received within timeout period, the CA broadcasts the revocation message, for example, via the low-speed FM radio on a nationwide scale or via satellite broadcast. [68]

The second protocol of the set is Revocation protocol using Compressed Certificate Revocation Lists (RCCRL). This protocol is used when only a subset of a vehicle's keys needs to be revocated or when the TPD of the vehicle is unreachable. TDP can become unreachable for example, in the case of jamming or by tampering of the device. RCCRL

makes use of Bloom filters. Bloom filter is a probabilistic data structure used to test whether an element is a member of a set. Given the large size of CRLs in VANETs, this can reduce its size to a few kilobytes. These reduced CRLs are broadcasted once in every 10 minutes, so this protocol also heavily relies on available infrastructure. RCCRL messages are also received by neighbouring cars. [68]

The last introduced certificate revocation protocol is called Distributed Revocation Protocol (DRP). The DRP is used in the pure ad hoc mode in vehicle-to-vehicle communications. Vehicles accumulate accusations against misbehaving vehicles, evaluate them using reputation systems, and in case a vehicle is deemed untrusted, CA is notified once the connection is available. Unlike the first two protocols, when using DRP, certificate revocation is triggered by neighbouring vehicles when misbehaviour is detected. Detecting malicious information is based on digitally signed messages, that can be leveraged to spot vehicles generating this data via similar methods to position cheating detection methods presented in Subsection 4.2.1 [78]. [68]

6.2.2 Other proactive concepts

To avoid complexity and infrastructure requirements of the PKI, other proactive solutions have been proposed, including the use of digital signatures without certificates [78] [79]. These solutions use the public/private key pair authentication to establish private keys for further communication, similarly to the PKI. Keys are also changed periodically, usually between few minutes. Without third party certification, key pairs can be freely generated by nodes themselves and node may generate new pairs constantly. These solutions offer weak assumption of identification and authenticity.

However, signing messages extends local distinguishability over time and space and adds another way to perform plausibility checks. As long as the node keeps the same public key, it can be authenticated as the same node by the other nodes that have previous records of communication with a given node. This is true regardless of where and when the previous communication took place. Consider a node Alice that has had nodes Bob and Carol at its local neighbourhood. During that time, Alice was also able to establish that Bob and Carol are truly distinct nodes (via other plausibility checks). Though these nodes may have moved out of Alice's neighbourhood of distinguishability, they now remain distinguishable to Alice as long as they sign their messages with the same private keys. [78]

We need to also consider strong adversaries who may collude and exchange private keys. Similarly to using PKI and DRP based certificate revocation, when a node is deemed untrusted, all messages coming from the node are dropped. As node's public key can no longer be trusted, the dropping decision needs to happen based on multiple plausibility checks, including also ones based on vehicle's location.

Another proactive authentication solution is to use proprietary system design. This can be done by using non-public protocols to restrict access from the nodes that are not using these protocols. The same can be achieved with the use of customized hardware or with the combination of both solutions. Due to massive scale of deployment of future

VANETs, it is likely that these solutions will not stop adversaries with considerable expertise. These solutions aim at raising the required financial and time effort an attacker has to spend in order to gain access into the system. [69]

The last proactive solution for authentication is tamper-resistant hardware. Some tamper-resistant hardware is already required by the other authentication solutions. We introduced the requirement of the Tamper-Proof Device when using PKI. As the name implies, the TPD needs to contain a set of sensors that can detect hardware tampering and erase all the stored keys to prevent them from being compromised. This feature makes designing a TPD for VANET conditions a bit problematic. The device cannot be too sensitive to light shocks caused by road imperfections. In some regions, TPD also needs to tolerate extreme heat or cold. All this will affect the cost of the device, which needs to acceptable for non-business consumers. [66]

An alternative to a TPD is to use TPM (Trusted Platform Module) that can resist software attacks, but not sophisticated hardware tampering. Considering the construction of modern cars, TPMs can be designed into car's structure in a way that requires a significant effort to gain physical access to them. This makes replacing malfunctioning units more difficult, but also raises the effort attacker has to spend in order to achieve his or her goals. TPMs are also considerably cheaper to produce than TPDs. [66]

Whether we choose TPD or TPM and manage to secure the external communication part of the application, it is not possible to guarantee that the in-vehicle system is free from the generation of unnecessary accident warnings. Attacker can also directly feed false information to vehicle's sensor systems, like proximity sensor or radar, to generate distress signals that system accepts as true warnings. There are papers written about this, but the methods of guaranteeing the integrity of the whole inter-vehicle system fall outside the scope of this thesis [80] [81]. The optimal solution for VANET would be an internal vehicle-system security solution that does not require additional communication with other nodes.

6.2.3 Reactive security concepts

Reactive security concepts are based on correlation of information that is either already available into the system from observation on normal system operation or which is introduced additionally. Each vehicle collects information from any information source available to its neighbourhood in order to create an independent view of its current status and the current surroundings environment. When data is received, it is compared to vehicle's own estimates related to status and environment data, like position to detect intrusion. Methods of detecting these types of attacks are similar to anonymous sensor solution and plausibility check solution to detect position cheating introduced in Subsection 4.2.1. [69]

Context verification checks can be roughly categorized in three groups. Position information verification aims to prevent an attacker from pretending to be at arbitrary positions. The time verification correlates the vehicle's internal clock, which is syn-

chronized and updated using information provided by GPS, with time and data fields of the received messages, and in particular of the beacon messages. [69]

The last verification method is based on application context. Vehicle compares if application context correlates with a similar application context known to a vehicle. This solution is only possible when there is a set of constraints in a realistic scenario where the application can for example, generate and deliver warning messages. [69]

One application context based security concept introduces a trustworthiness value table [82]. In this concept, the trustworthiness of the warning message is calculated based on the function of the node (e.g. a police car, a road maintenance vehicle or a private vehicle) and the event type (e.g. a junction warning or a revocation list distribution). Same can be easily applied to our introduced emergency-response vehicle scenario. When a private vehicle receives a junction warning message that is signed by the emergency vehicle or an RSU controlling the traffic lights, it can be considered more trustworthy than the same message received from a relaying private vehicle. This is solely based on an event probability. More application context based solutions relying on probability calculations, majority voting and plausibility checks can be found on other papers [78] [83].

Like already mentioned when discussing about proactive security concepts, digital signatures do not provide strong guarantee of trustworthiness, unless they are accompanied with the trustworthy PKI. Yet, digital signatures alone can still be useful in signature-based intrusion detection, where messages with known signatures of attackers are dropped. The distinguishability they offer can often be used in conjunction with other context verification methods to form a more accurate view of the current surroundings environment.

6.2.4 Discussion

Security solutions for authentication and providing data-centric trust on VANETs can be classified as proactive and reactive. The requirement of the PKI authentication as proactive security solution was introduced early in VANET security research [5]. The PKI introduces a requirement of CA infrastructure in some form of RSUs and tamper-proof hardware on the vehicles.

The reliable method of certificate revocation also proves to be very challenging in the PKI based solutions. The three introduced protocols for certificate revocation (RPTD, RCCRL and DRP) each present different dependability on available hardware. RPTD offers fairly reliable method of certificate revocation message reaching the target vehicles, but the size of the vulnerability window depends on coverage of the CA controlled RSUs. The protocol also relies on expectation that malicious vehicle's TPD is not compromised, which is not very realistic. For the protocol to operate correctly, TPD needs to contain all the radio communication hardware as well as to be resistant to external interference signals. Additionally, as the CA has no way of knowing if the vehicle's TPD is compromised or not, the other vehicles still need to be notified via other protocols. RCCRL is a simple and reliable method of revocation, but relying on timed

broadcasts makes it unviable for delay-sensitive scenarios, like our presented emergency-response vehicle scenario. Such scenarios have to rely on DRP for certificate revocation. This protocol relies on similar methods of detecting attackers than verification based reactive security concepts.

When considering PKI based authentication solutions, the advantages and shortcomings of the system needs to be weighted carefully. The PKI presents a significant hardware requirement in a form of external authentication infrastructure. Still, due to latency requirements, the very time sensitive applications, like emergency warning scenarios have to rely purely on vehicle-to-vehicle ad hoc communication. On these situations, certificate revocation of a given vehicle may need to be done at the same time with the decision whether to trust the emergency message sent by the same vehicle.

This problem has lead researchers to a direction of data-centric trust security concepts that do not rely on the PKI [78] [82]. When certificates provided by the CA are not used, the digital signatures on messages can no longer provide strong authenticity and only offer a local node distinquishability. This distinquishability can still be used in conjunction with other plausibility checks to better detect falsified information. In theory, when two privately owned vehicles communicate with each other, digital signatures alone can offer a similar trust level to the PKI solution, as threat of previously trusted node turning into malicious insider is a serious threat in VANETS, even when the trusted node provides keys certified by the CA.

The clear disadvantage of missing the CA is that trust level on government controlled nodes cannot be guaranteed compared to the PKI based solution. Under the PKI solution, the CA's certificate can provide strong authenticity. If we can trust that certain vehicle really is a police car or a certain RSU really is government controlled, we can also trust safety messages signed by these nodes. On our emergency-response vehicle example scenario, most critical security issues can be solved by using the PKI.

Proprietary system design is another direction in proactive solutions for authenticity. Free mobility of vehicles between regions, countries and even continents requires these systems to be interoperable. Over the course of history, public protocols have proven to be more secure over private protocols. This is due to extensive amount of evaluation and testing the public protocols are subjected to. Considering massive scale of VANETs, the likelihood of any protocol remaining private also decreases. Due to these reasons, the chances are that proprietary system design solutions can cause more harm than good.

Tamper-resistant hardware is also suggested as proactive security solution, and PKI solutions already require some level of tamper-resistance from vehicle's on board systems. The initial implementation of VANETs will require the cost of the required hardware to be at acceptable level, which will support the choice of TPM over TPD. The exact composition of vehicle's on-board tamper-resistance systems will have to be compromise between cost and acceptable security.

Most reactive data-centric security concepts are based on plausibility checks. When plausibility checks are done locally, they cause very little extra strain on the system, as

VANET nodes have a little transmission time available, but plenty of computation and battery power.

Consequently, the use of these plausibility checks in addition to any other chosen security solution is advisable. Digital signatures should be used even when PKI solution is not used, as they can be used as additional information source for plausibility checks. The final data-centric trust solution for VANETs is going to be a compromise of both, proactive and reactive security concepts.

6.3 Geo-addressing and secure localization

As discussed in Section 5.4, rapid network topology changes in VANETs require a geo-addressing based routing solution. These routing solutions expose VANETs to specialized attacks designed to deliberately retrieve and track the location of vehicles or otherwise take advantage of sending messages with misguided location information. Secure localization solution is needed to protect the system from these kinds of attacks. We briefly introduced tamper-proof GPS as one possible solution, but GPS-based solutions are pointed to suffer from several vulnerabilities [73].

6.3.1 Solutions

One proposed solution that doesn't rely on GPS is verifiable multilateration. This solution is based on roadside infrastructure and distance bounding. Distance bounding guarantees that the distance is no greater than certain value. Multilateration is the same operation in several dimensions. The working principle of verifiable multilateration is the following: Four base stations with known locations perform distance bounding to the vehicle. The results give them four upper bounds on the distance from vehicle. If verifying base stations can uniquely calculate vehicle's location using three distance bounds and this location can be placed in a triangular pyramid between verifiers, then the location is deemed correct. Similarly, vehicle's location can be calculated in two dimensions with only two base stations. [73]

As distance bounding is based on ultrasound, the location verification can produce erroneous results giving vehicle a longer distance to the verifier than it really is, but the result can never be shorter than the real distance. A location verification protocol that uses distance bounding to verify a node's self-provided location has also been proposed [84]. This allows vehicles to use insecure location determination mechanism, like GPS, without compromising the security of the system. The solution is based on challenge-and-response scheme and also involves verifier nodes. Verifiers are placed between acceptable distances from each other to form overlapping coverage circles with the radius of R. Verifier first requests a node to send its position via radio link and after position message is received, verifier sends challenge message to the node. Upon receiving the challenge message, the node has to reply via ultrasound. If the reply arrives in time, the verifier accepts that node is within the region R. [69]

Another challenge-and-response based secure localization solution relies on the broadcast nature of radio communication and cooperation of sensor nodes [85]. Intuitively, once the location provider produces a radio signal, nodes in its vicinity will receive the signal, while more remote nodes will not. The nodes that received the signal can compare their signal receiving times to determine if the location provider's information can be trusted. Nodes outside the assumed zone of the location provider act as rejectors. If these nodes receive the location signal, it will be rejected. [85]

A few research papers introduce a position verification system based on autonomous sensors that detect nodes sending falsified location data [86] [87]. Despite their name, the described sensors are mostly a set of threshold limits each vehicle monitors from received messages. Sensors only use information provided by routing layer and special hardware is required. One of these sensors is Acceptance Range Threshold (ART), which is a simple method of discarding position beacons from nodes claiming to be at distance larger than maximum communications range. Using a combination of autonomous sensors, vehicles independently calculate trust ratings of neighbouring nodes. Untrusted nodes are excluded from future routing decisions. Vehicles can also act in collaboration, exchanging and comparing sensor information with their neighbours. [86]

There are also suggestions to provide secure localization to certain geo-addressing protocols. Secure Grid Location Service (SGSL), an improvement to original GLS-protocol is designed to prevent position spoofing attack [88]. SGSL uses distance bounding, plausibility checks and ellipse-based location estimation to verify node's claimed position. Secure localization is also developed for Position Based Routing (PBR) [89]. PBR is considered and evaluated by the Car2Car Communication Consortium (C2C-CC) and found to be scalable and efficient unicast forwarding solution for large-scale and highly volatile ad hoc networks. PBR is based on beaconing, multi-hop forwarding and geo-location discovery. Location discovery is used when a node needs to send a message to another node that is not marked in its location table. The originator node sends a location query message with the ID of requested node. Query message also includes sequence number and hop limit values. Query message is forwarded by the neighbouring nodes, until the searched node is reached. Searched node then replies with a message carrying its current position and a time stamp. When originating node receives the reply message, it marks the new entry to its location table. To secure these query and location messages and also other PBR messages, each received messages need to pass plausibility checks. Plausibility checks are done by comparing message's timestamp and location information with expected values. If a message passes the plausibility check, then message's certificate is validated. If certificate is found valid, the digital signature of the message is verified. Failing any of these checks causes message to get discarded. [69] [89]

6.3.2 Discussion

A few promising secure localization solutions have been proposed to secure geo-routing and position-critical safety applications in VANETs. Many solutions have also been found functional on a concept level.

Verifiable multilateration solution can be used in many situations by only two strategically placed base stations. Knowing vehicle's position in two dimensions can be enough when the known road infrastructure is taken into account. Still the system has a distinctive disadvantage of huge infrastructure requirement. Verifiable multilateration can also be improved by time synchronization. If base stations have synchronized clocks, distance bounding can be done with only one base station sending the request message each recording the time they received reply from the vehicle. This reduces overhead of the system, but still distance bounding needs to be done frequently to keep vehicle's position updated. The system does not scale well compared to solutions that rely on vehicle's self-provided location source.

Another distance bounding based solution that uses verifier nodes lessens the number of base stations required, but also limits the location accuracy to a circular region. This solution also requires vehicles to be equipped with ultrasound-capable transmitters. The main disadvantage of this solution is that while knowing that vehicle is on certain region is enough for many geo-routing solutions, most of the safety related applications rely on knowing exact location of the vehicle. Collision avoidance applications, like the emergency-response vehicle scenario presented in Chapter 5 can have at most few meters of error margin in provided position information. This would require application level of more accurate secure localization solution.

A solution based on radio broadcast monitoring achieves similar location accuracy to distance bounding using verifier nodes. The main difference is that no external infrastructure is needed. The solution also has an advantage of accuracy being related to the number of nodes in the area. The problem with this solution is that it is not resilient against collaborating attackers. The protocol assumes that messages from verifiers and rejectors can be trusted, which is not true in the case of VANETs as malicious insiders have very easy access to the network. The protocol also relies in message chains where an acceptor waits message from another acceptor, before sending its own reply. This makes the solution unreliable due to rapidly changing VANET topology.

Solutions that involve autonomous position cheating detecting sensors have advantage of requiring no additional hardware and adding no extra security overhead. VANET nodes have adequate amount of processing and battery power, but limited time for message exchange, which makes this an ideal approach. A sensor that checks claimed position information against known road infrastructure and even known other vehicle locations can prevent several position spoofing attacks. Having vehicles exchanging sensor information with each other exposes network to a new security attacks, but the trust rating system offers a better ways to detect malicious insiders than previous solutions.

A few more recent propositions go a step further and integrate some of the previously introduced secure localization methods to known geo-addressing based protocols, based on unicast IP routing extended to deal with GPS addresses. These solutions seem most promising as providing secure localization directly on a routing level reduces security overhead. However, there is an open problem of position information accuracy. Providing very accurate position information is not optimal for routing purposes. It is likely that collision related safety applications will require more accurate positioning solution.

6.4 Anonymity, liability and privacy

Due to unique nature of VANETs, a certain level of anonymity, liability and privacy is required. Providing optimal tradeoff between these requirements is a challenging task. We introduced ELPs, ECNs and periodically changing public/private key pairs as key elements of protecting driver's anonymity and privacy. However, the introduction of changing anonymous pseudonym does not yet fully protect VANET nodes from movement tracking attacks. If lifetime of the public key is several minutes and different vehicles update their public keys are different times, the situations can be observed where consecutive messages and key pairs can be linked together and thus the whole movement of a vehicle can be traced [69]. Despite the pseudonym update, an attacker can link new and old pseudonyms together using temporal and spatial relocation between the new and old locations of the vehicle. A few solutions exist that can reduce the risk of attacker being able to link subsequent keys together. These solutions are examined in this Chapter.

6.4.1 Solutions

One research paper introduces the use of a random silent period when the vehicle enters VANET network or changes its public key [90]. When a target vehicle enters the network it broadcasts using pseudonym Alice, and then goes to silence. If a neighbouring vehicle updates its pseudonym from Bob to Ben during this silent period, then an attacker could be mislead to consider pseudonym Ben as the new pseudonym for the target vehicle.

Another research paper introduces a concept of creating mix-zones at appropriate predetermined locations in VANETs to protect driver's privacy [91]. All vehicles authenticated in the same mix-zone share the same private key. The private key is provided by an RSU located in the mix-zone. Vehicles use the same public key as long as they are within the mix-zone, but switch to a new public key when exiting the mix-zone and entering a new one.

A few papers by the same authors present the concept of adaptive privacy to protect driver's anonymity [92] [93]. The authors argue, that privacy is a user-specific concept, and a good privacy protection mechanism should allow users to select the degrees of privacy they wish to have. Users may want to use different level of privacy depending

on whether they are communicating with a public or a private server. Offered trust policies are full-trust, partial-trust, and zero-trust. Full-trust policy trusts both types of servers. Partial-trust policy trusts only public servers and zero-trust policy neither types of servers. The higher level of privacy results in more overheads. In computational overheads, the overhead includes encrypting, digitally signing and decrypting messages. In communication overhead, the overhead includes the transportation of authentication messages and encrypted or digitally signed user data.

The protocol also assumes a similar group based authentication to the introduced mix-zone concept that involves vehicles authenticating through RSUs. The key idea in the concept is the adaptive protocol that allows users to choose appropriate compromise between desired anonymity and computational overhead.

Another solution focuses on the practicality of the implementation of pseudonyms that protect drivers' anonymity, namely the periodically changing public/private key pairs [94]. The solution attempts to bring together different aspects of previously introduced concepts like random silent period and mix-zone and address the concept across layers of real VANET protocol stack. The paper provides practical solutions to different aspects, like, cross-layer addressing concept to tie together MAC, position-based routing and IPv6 addresses. The paper also provided extended location service to protect vehicles' identities in a multi-hop forwarding scenario. Pseudonymity-enchanced forwarding scenarios are introduced to deal with difficulties the periodically changing pseudonyms can cause to message forwarding. The paper also mentions the use of IEEE 802.11's positive acknowledgments and MAC level retransmissions to inform upper layer protocols of unsuccessful data frame delivery. These link layer callbacks can reduce the time that expired entries are kept in the forwarding table.

The issue of providing liability in VANETs is not widely researched. The issue is mentioned in several papers, but no specific solutions are provided [68]. Some papers provide solution concepts that can potentially support liability, like the previously introduced paper about the practicality of pseudonym implementation [94]. However, all the potential solutions introduced rely more or less on a PKI authentication system. The PKI offers direct vehicle-to-vehicle or vehicle-to-roadside communication using periodically changing pseudonyms, but still allows tracing vehicle's true identity by authorized party. Vehicle's true identity is based on ELP or ECN, which can only be linked to pseudonym by the information possessed by CA.

If the PKI is not used and the authentication is done by using periodically changing pseudonyms, there is no reliable way to link a certain node to any given pseudonym. We can still provide liability if we give up using pseudonyms and authenticate directly using ELPs or ECNs, but this solution forfeits vehicle's anonymity and allows vehicle tracking.

6.4.2 Discussion

The issue of providing anonymity and privacy on VANETs has been introduced early on VANET research, but many research papers offer similar solutions to the issue [78].

The proposed random silent periods enhance protection against movement tracking attacks, but make the practical implementation of changing pseudonyms increasingly problematic.

When a vehicle switches its pseudonym, other vehicles have to treat it as a new member to the network. If legitimate members of the network can connect the new pseudonym to the previously used one, so can the possible attacker. This also makes all the recorded communication information from the previous pseudonym obsolete. Consequently, this will affect practicality of some of the promising security concepts introduced with secure localization and data-centric trust [78] [82] [83] [86] [87]. These methods use plausibility checks to compare received information from a node with the previous information received from the same node and expected normal values of the information context. Periodical flushing of recorded information cache makes these methods more unreliable and particularly vulnerable right after the pseudonym update. Random silent periods will increase this vulnerability window.

Introduction of mix-zones has positive impact on the vulnerability window, provided that mix-zones are large enough of geographical regions. Providing adaptive privacy and the placement of mix-zones itself offers a good control over how large scale movement tracking attacks can be performed, within the selected pseudonym updating rules.

However, the clear disadvantage is the requirement of additional roadside hardware. Joining a new mix-zone first requires each vehicle to authenticate receive the required private key through RSU, so connection to the RSU is necessary for all the new vehicles entering the mix-zone. Movement tracking between two nodes authenticated on the same mix-zone is possible, but mix-zones should be placed and designed in a way that attacker is not able to gain significant advantage from the attack. This will likely result in mix-zones requiring even better coverage of roadside nodes is comparison the PKI only solution.

The introduced research paper by E. Fonseca, A. Festag, R. Baldessari et al. on implementation of changing pseudonyms provides a few good methods to make the solution more practical and also extends the solution to cover multi-hop routing [94]. However, the paper does not include considerations of periodically changing pseudonyms working in conjunction with plausibility checks. This area requires more research.

In the case of secure localization, authentication and data-centric trust, viable non-PKI solutions are presented. Additionally, the use of the PKI presents additional problems in these areas, like the issue of certificate revocation. However, in the case of liability support in VANETs, all the reliable solutions are based on the PKI. The liability issue also requires additional research. Considering how important providing liability support is for governmental institutions, it can be argued that the current research results favor a PKI based solutions as candidates for VANET implementation.

7 CONCLUSIONS

This thesis introduced the current state of security research and standardization work on two IoT application fields: WSNs and VANETs. Many of the major security challenges are similar in both cases, like authentication and secure localization. However, these challenges still require completely separate solutions due to major differences in communication, network topology and hardware.

Out of the two areas, the WSNs can be considered to be more advanced regarding the standardization work. ZigBee and WirelessHART standards specify authentication and key distribution procedure, leaving some options to the implementation. These standards also set limits to which WSN applications they can be used for. There are many applications that do not fit to the better specified WSN standards. The key issue is that solutions for authentication, key distribution, secure localization, routing and data aggregation each highly depend on the exact WSN application purpose. Certain compromises also need to be made, as security can come with a price of high overhead in aspects like routing. Therefore, prioritizing security against most probable threats in the particular application is advisable. The attacks that are hardest to counter usually involve first compromising a legitimate sensor node. Securing the WSN becomes considerably easier if the node capture can be reliably detected, even with only human supervision.

In the case of VANETs, standardization work leaves many security questions completely open and to be solved in the implementation phase. The big question related not only to authentication, but to other major security challenges as well, is the implementation of the PKI. There is a lot of research available and solutions to solve individual security issues without the use of the PKI. However, none of the non-PKI solutions solve the simultaneous liability and anonymity requirement present on VANETs. Furthermore, most of the non-PKI security measures rely on plausibility checks and possibly on majority voting, which even though has shown promising results, will not be as reliable as trusted third party.

Implementing PKI using cellular network infrastructure requires a lot of effort and international cooperation by the governments. The full potential of many safety applications also requires that majority of the vehicles on the roads can communicate with VANET. The result is a transition phase, where the penetration of VANET communication capable vehicles increases and more VANET applications become gradually available.

The increasing coverage of the 4th generation (4G) cellular networks also requires more research on the VANET context. The new cellular technology allows lower latency times, which could allow even some of the latency-dependent emergency messages to be transmitted over the cellular network, instead of direct vehicle-to-vehicle communication. 4G networks may also offer other advantages, such as more accurate positioning methods over multilateration in comparison to previous generation of cellular networks.

REFERENCES

[1] M. Chui, M. Löffler, and R. Roberts, “The internet of things,” *McKinsey Quarterly*, 2010.

[2] Kevin Ashton, “That ‘Internet of Things’ Thing - RFID Journal,” *RFID Journal*, 2009. [Online]. Available: http://www.rfidjournal.com/articles/view?4986.

[3] D. Kozlov, J. Veijalainen, and Y. Ali, “Security and privacy threats in IoT architectures,” *Proceedings of the 7th International Conference on Body Area Networks*, pp. 256–262, 2012.

[4] C. Li, H. Zhang, B. Hao, and J. Li, “A survey on routing protocols for large-scale wireless sensor networks.,” *Sensors (Basel, Switzerland)*, vol. 11, no. 4, pp. 3498–526, Jan. 2011.

[5] M. Raya and J.-P. Hubaux, “The security of vehicular ad hoc networks,” *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks - SASN ’05*, p. 11, 2005.

[6] J. F. Kurose and K. W. Ross, *Computer Networking, third edition*. Pearson Education, 2005, pp. 654–655.

[7] A. C. Sarma and J. Girão, “Identities in the Future Internet of Things,” *Wireless Personal Communications*, vol. 49, no. 3, pp. 353–363, Mar. 2009.

[8] B. Scheider, “Adversaries,” in *Secrets & Lies: Digital Security in a Networked World*, John Wiley & Sons Inc., 2000, pp. 42–58.

[9] D. Welch and S. Lathrop, “Wireless security threat taxonomy,” *Information Assurance Workshop, IEEE Systems, Man and Cybernetics Society*, pp. 76–83, 2003.

[10] M. Al-Shurman, S.-M. Yoo, and S. Park, “Black hole attack in mobile Ad Hoc networks,” *Proceedings of the 42nd annual Southeast regional conference on - ACM-SE 42*, p. 96, 2004.

[11] J. Douceur, “The sybil attack,” *Peer-to-peer Systems*, pp. 1–6, 2002.

[12] J. Newsome, E. Shi, D. Song, and A. Perrig, “The sybil attack in sensor networks: analysis & defenses,” *Proceedings of the 3rd international symposium on Information processing in sensor networks*, pp. 259–268, 2004.

[13] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, a. Sundaram, and D. Zamboni, “Analysis of a denial of service attack on TCP,” *Proceedings 1997 IEEE Symposium on Security and Privacy (Cat No97CB36097)*, pp. 208–223, 1997.

[14] R. Chang, “Defending against flooding-based distributed denial-of-service attacks: A tutorial,” *Communications Magazine, IEEE*, vol. 40, no. 10, pp. 42–51, 2002.

[15] D. Raymond and S. Midkiff, “Denial-of-service in wireless sensor networks: Attacks and defenses,” *Pervasive Computing, IEEE*, vol. 7, no. 1, pp. 74–81, 2008.

[16] T. Frantti and H. Hietalahti, “A Risk-Driven Security Analysis and Metrics Development for WSN-MCN Router,” *Prceeding of the IEEE International Conference on Information Networking*, pp. 210–215, 2013.

[17] A. Aijaz, B. Bochow, and F. Dötzer, “Attacks on inter vehicle communication systems-an analysis,” *Proceedings of the 3rd, International Workshop on Intelligent Transportation*, pp. 189–194, 2006.

[18] J. Votano, M. Parham, and L. Hall, “Security in Wireless Sensor Networks,” *Chemistry & Biodiversity*, vol. 47, no. 6, pp. 53–57, 2004.

[19] X. Shen, Z. Wang, and Y. Sun, “Wireless sensor networks for industrial applications,” *Intelligent Control and Automation, 2004 WCICA 2004 Fifth World Congress on*, vol. 4, no. 60304018, pp. 3636–3640, 2004.

[20] R. Stoleru, T. He, J. Stankovic, and D. Luebke, “A high-accuracy, low-cost localization system for wireless sensor networks,” *Proceedings of the 3rd international conference on Embedded networked sensor systems*, pp. 13–26, 2005.

[21] G. Simon, M. Maróti, and Á. Lédeczi, “Sensor network-based countersniper system,” *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pp. 1–12, 2004.

[22] J. Khan, R. Katz, and K. Pister, “Emerging Challenges: Mobile Networking for‘ Smart Dust,’” *Journal of Communications and Networks*, vol. 2, no. 3, pp. 188–196, 2000.

[23] V. Gungor and G. Hancke, “Industrial wireless sensor networks: Challenges, design principles, and technical approaches,” *Industrial Electronics, IEEE Transactions*, vol. 56, no. 10, pp. 4258–4265, 2009.

[24] V. C. Gungor, M. C. Vuran, and O. B. Akan, “On the cross-layer interactions between congestion and contention in wireless sensor and actor networks,” *Ad Hoc Networks*, vol. 5, no. 6, pp. 897–909, Aug. 2007.

[25] A. Castellani and M. Gheda, “Web Services for the Internet of Things through CoAP and EXI,” *Communications Workshops (ICC), IEEE International Conference*, pp. 1–6, 2011.

[26] M. Brachmann, O. Garcia-morchon, and M. Kirsche, “Security for practical coap applications: Issues and solution approaches,” *Proceedings of the 10th GI/ITG KuVS Fachgespraech Sensornetze*, pp. 1–4, 2011.

[27] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury, “A survey on wireless multimedia sensor networks,” *Computer Networks*, vol. 51, no. 4, pp. 921–960, Mar. 2007.

[28] H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” *Proceedings 19th International Conference on Data Engineering (Cat No03CH37405)*, pp. 197–213, 2003.

[29] W. Diffie and M. Hellman, “New directions in cryptography,” *Information Theory, IEEE Transactions on*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[30] R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[31] M. Sethi, J. Arkko, and A. Keränen, “End-To-End Security for Sleepy Smart Object Networks,” *IEEE 37th Conference on Local Computer Networks Workshops (LCN Workshops)*, pp. 964 – 972, 2012.

[32] D. Carman, P. Kruus, and B. Matt, “Constraints and approaches for distributed sensor network security (final),” *DARPA Project report*, pp. 1–139, 2000.

[33] Y. Zhou, Y. Zhang, and Y. Fang, “Access control in wireless sensor networks,” *Ad Hoc Networks*, vol. 5, no. 1, pp. 3–13, Jan. 2007.

[34] G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella, “Energy conservation in wireless sensor networks: A survey,” *Ad Hoc Networks*, vol. 7, no. 3, pp. 537–568, May 2009.

[35] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey,” *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, Aug. 2008.

[36] A. Srinivasan and J. Wu, “A survey on secure localization in wireless sensor networks,” *In B. Furht (Ed.), Encyclopedia of Wireless and Mobile Communications*. 2008.

[37] J. N. Al-Karaki and A. E. Kamal, “Routing techniques in wireless sensor networks: a survey,” *Wireless Communications, IEEE*, vol. 11, no. 6, pp. 6–28, Dec. 2004.

[38] D. Kundur, T. Zourntos, and N. J. Mathai, “Lightweight security principles for distributed multimedia based sensor networks,” *Signals, Systems and Computers, 2004 Conference Record of the Thirty-Eighth Asilomar Conference*, vol. 1, pp. 368–372, 2004.

[39] a. D. Wood, J. a. Stankovic, and S. H. Son, “JAM: a jammed-area mapping service for sensor networks,” *Proceedings 2003 International Symposium on System-on-Chip (IEEE Cat No03EX748)*, pp. 286–297, 2003.

[40] “IEEE Standard 802.15.4 - 2011,” *The Institute of Electrical and Electronics Engineers*, 2011.

[41] D. Gascón, “Security in 802.15.4 and ZigBee networks,” 2008. [Online]. Available: http://sensor-networks.org/index.php?page=0823123150. [Accessed: 17-Jun-2013].

[42] G. Hiertz, D. Denteneer, and L. Stibor, “The IEEE 802.11 universe,” *Communications Magazine, IEEE*, vol. 48, no. 1, pp. 62–70, 2010.

[43] G. Mulligan, “The 6LoWPAN architecture,” *Proceedings of the 4th workshop on Embedded networked sensors - EmNets ’07*, p. 78, 2007.

[44] C. P. P. Schumacher, N. Kushalnagar, and G. Montenegro, “IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals,” *RFC 4919, The Internet Engineering Task Force (IETF)*, 2007.

[45] “ZigBee Alliance.” [Online]. Available: http://www.zigbee.org/. [Accessed: 17-Jun-2013].

[46] “HART Communication Foundation.” [Online]. Available: http://www.hartcomm.org/. [Accessed: 23-Oct-2013].

[47] S. Raza, A. Slabbert, T. Voigt, and K. Landernas, “Security considerations for the WirelessHART protocol,” *2009 IEEE Conference on Emerging Technologies & Factory Automation*, pp. 1–8, Sep. 2009.

[48] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures,” *Proceeding of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113–127, 2003.

[49] C. Neuman and T. Tso, “Kerberos: An Authentication Service for Computer Networks,” *Communications Magazine, IEEE*, vol. 32, no. 9, pp. 33–38, 1994.

[50] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, “A pairwise key predistribution scheme for wireless sensor networks,” *ACM Transactions on Information and System Security (TISSEC)*, vol. 8, no. 2, pp. 228–258, 2005.

[51] L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks,” *Proceedings of the 9th ACM conference on Computer and communications security - CCS ’02*, p. 41, 2002.

[52] M. Maróti, P. Völgyesi, S. Dóra, and B. Kusý, “Radio interferometric geolocation,” *Proceedings of the 3rd international conference on Embedded networked sensor systems*, pp. 1–12, 2005.

[53] D. Moore, J. Leonard, D. Rus, and S. Teller, “Robust distributed network localization with noisy range measurements,” *Proceedings of the 2nd international conference on Embedded networked sensor systems - SenSys ’04*, p. 50, 2004.

[54] L. Lazos and R. Poovendran, “SeRLoc: Secure range-independent localization for wireless sensor networks,” *Proceedings of the 3rd ACM workshop on Wireless security*, pp. 21–30, 2004.

[55] S. Capkun and J. Hubaux, “Secure positioning of wireless devices with application to sensor networks,” *24th Annual Joint Conference of the IEEE Computer and Communications Societies Proceedings IEEE*, vol. 3, pp. 1917–1928, 2005.

[56] L. Lazos, R. Poovendran, and S. Čapkun, “ROPE: robust position estimation in wireless sensor networks,” *Proceedings of the 4th international symposium on Information processing in sensor networks*, pp. 324–331, 2005.

[57] J. Deng, R. Han, and S. Mishra, “A performance evaluation of intrusion-tolerant routing in wireless sensor networks,” *Information Processing in Sensor Networks*, pp. 349–364, 2003.

[58] S. Son, B. Blum, T. He, and J. Stankovic, “IGF: A state-free robust communication protocol for wireless sensor networks,” *Technical report CS-2003-11, University of Virginia CS Department*, 2003.

[59] A. Wood, L. Fang, J. Stankovic, and T. He, “SIGF: a family of configurable, secure routing protocols for wireless sensor networks,” *SASN ’06 Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks*, pp. 35–48, 2006.

[60] A. Wood and J. Stankovic, “Denial of service in sensor networks,” *Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[61] R. A. Uzcátegui, U. Nacional, E. Politécnica, and A. José, “WAVE: A Tutorial,” *IEEE Communications Magazine*, vol. 47, no. 5, pp. 126–133, 2009.

[62] R. Moalla and B. Lonc, “How to secure ITS applications?,” *Ad Hoc Networking Workshop (Med-Hoc-Net), The 11th Annual Mediterranean*, pp. 113–118, 2012.

[63] G. Acosta-Marum and M. A. Ingram, “Six Time- and Frequency-Selective Empirical Channel Models for Vehicular Wireless LANs,” *2007 IEEE 66th Vehicular Technology Conference*, pp. 2134–2138, Sep. 2007.

[64] H. Hartenstein and K. Laberteaux, “A tutorial survey on vehicular ad hoc networks,” *Communications Magazine, IEEE*, vol. 46, no. June, pp. 164–171, 2008.

[65] “IEEE Standard 802.11p - 2010,” *The Institute of Electrical and Electronics Engineers*, 2010.

[66] M. Raya and J. Hubaux, “Securing vehicular ad hoc networks,” *Journal of Computer Security*, vol. 15, pp. 39–68, 2007.

[67] Z. J. Haas, “Securing ad hoc networks,” *IEEE Network*, vol. 13, no. 6, pp. 24–30, 1999.

[68] M. Raya, P. Papadimitratos, and J. Hubaux, “Securing Vehicular Communications,” *IEEE Wireless Communications*, vol. 13, no. 5, pp. 8–15, Oct. 2006.

[69] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, “Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions,” *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 584–616, 2011.

[70] J. Navas and T. Imielinski, “GeoCast—geographic addressing and routing,” *Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking*, pp. 66–76, 1997.

[71] T. Imielinski and J. Navas, “GPS-Based Addressing and Routing,” *RFC 2009, The Internet Engineering Task Force (IETF)*, 1996.

[72] Y. Khaled, M. Tsukada, and T. Ernst, “Geographical information extension for IPv6: Application to VANET,” *2009 9th International Conference on Intelligent Transport Systems Telecommunications, (ITST)*, pp. 304–308, Oct. 2009.

[73] J. Hubaux, S. Capkun, and J. Luo, “The security and privacy of smart vehicles,” *Security & Privacy, IEEE*, vol. 2, no. 3, pp. 49–55, 2004.

[74] “UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea | News.” [Online]. Available: http://www.utexas.edu/news/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/. [Accessed: 29-Aug-2013].

[75] D. Jiang and L. Delgrossi, “IEEE 802 .11p: Towards an International Standard for Wireless Access in Vehicular Environments,” *IEEE Vehicular Technology Conference*, pp. 2036–2040, 2008.

[76] “IEEE Standard 802.11 - 2012,” *The Institute of Electrical and Electronics Engineers*, 2012.

[77] I. Transportation, S. Committee, I. Vehicular, and T. Society, *IEEE Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages IEEE Vehicular Technology Society*, vol. 2013, no. April. 2013.

[78] P. Golle, D. Greene, and J. Staddon, “Detecting and correcting malicious data in VANETs,” *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pp. 29–37, 2004.

[79] M. Gerlach, A. Festag, and T. Leinmüller, “Security architecture for vehicular communication,” *Proceedings of the International Workshop on Intelligent Transportation*, 2005.

[80] T. Garfinkel, B. Pfaff, and J. Chow, “Terra: A virtual machine-based platform for trusted computing,” *Proceedings of the nineteenth ACM symposium on Operating systems principles*, pp. 193–206, 2003.

[81] D. Schellekens, B. Wyseur, and B. Preneel, “Remote Attestation on Legacy Operating Systems With Trusted Platform Modules,” *Electronic Notes in Theoretical Computer Science*, vol. 197, no. 1, pp. 59–72, Feb. 2008.

[82] M. Raya and P. Papadimitratos, “On data-centric trust establishment in ephemeral ad hoc networks,” *The 27th Conference on Computer Communications IEEE*, 2008.

[83] B. Ostermaier, “Enhancing the security of local dangerwarnings in vanets-a simulative analysis of voting schemes,” *The Second International Conference on Availability, Reliability and Security*, pp. 422–431, 2007.

[84] N. Sastry, U. Shankar, and D. Wagner, “Secure verification of location claims,” *Proceedings of the 2nd ACM workshop on Wireless security*, pp. 1–10, 2003.

[85] A. Vora and M. Nesterenko, “Secure Location Verification Using Radio Broadcast,” *Dependable and Secure Computing, IEEE Transactions*, vol. 3, no. 4, pp. 377–385, 2006.

[86] T. Leinmuller, E. Schoch, and F. Kargl, “Position verification approaches for vehicular ad hoc networks,” *Wireless Communications, IEEE*, vol. 13, no. October, pp. 16–21, 2006.

[87] T. Leinm, C. Maih, P. O. Box, E. Schoch, F. Kargl, T. Leinmueller, and C. Maihoefer, “Improved Security in Geographic Ad hoc Routing through,” *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, pp. 57–66, 2006.

[88] J.-H. Song, V. W. S. Wong, and V. C. M. Leung, “A framework of secure location service for position-based ad hoc routing,” *Proceedings of the 1st ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks - PE-WASUN ’04*, p. 99, 2004.

[89] C. Harsch, A. Festag, and P. Papadimitratos, “Secure Position-Based Routing for VANETs,” *2007 IEEE 66th Vehicular Technology Conference*, pp. 26–30, Sep. 2007.

[90] K. Sampigethaya, L. Huang, and M. Li, “CARAVAN: Providing location privacy for VANET,” *Proceedings of 3rd Workshop on Embedded Security in Cars (ESCAR2005)*, 2005.

[91] J. Freudiger and M. Raya, “Mix-zones for location privacy in vehicular networks,” *Proceedings of the First International Workshop on Wireless Networking for Intelligent Transportation Systems (Win-ITS)*, 2007.

[92] K. Sha, Y. Xi, and W. Shi, “Adaptive privacy-preserving authentication in vehicular networks,” *First International Conference on Communications and Networking in China*, pp. 1–8, 2006.

[93] Y. Xi, K.-W. Sha, W.-S. Shi, L. Schwiebert, and T. Zhang, “Probabilistic Adaptive Anonymous Authentication in Vehicular Networks,” *Journal of Computer Science and Technology*, vol. 23, no. 6, pp. 916–928, Nov. 2008.

[94] E. Fonseca, A. Festag, R. Baldessari, and R. L. Aguiar, “Support of Anonymity in VANETs - Putting Pseudonymity into Practice,” *2007 IEEE Wireless Communications and Networking Conference*, pp. 3400–3405, 2007.