Dipartimento di Ingegneria e Scienze dell'Informazione e Matematica

Università degli Studi dell'Aquila

Università degli Studi dell'Aquila
Dipartimento di Ingegneria e Scienze dell'Informazione e Matematica

Seminario Professionalizzante
" Sicurezza nelle Reti Radio di Sensori e Veicolari / Wireless Sensor and Vehicular Networks Security", ed. 5

A.A. 2020/21

PROPOSTA

Ing. Marco PUGLIESE, Ph.D.

10 Marzo 2021 - rel. 1.0

Course objective

Wireless sensor networks (Wireless Sensor Network, WSN) and wireless vehicular networks (Vehicular Ad-hoc Networks, VANET) are special cases of wireless ad-hoc networks.

A wireless ad hoc network is a decentralized type of wireless network: the network is ad-hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity and the routing algorithm in use.

The course deals with security principles and techniques applicable to WSN and VANET through theoretical lectures and experimental demonstration sessions.

WSNs are a class of ad hoc wireless networks where nodes are smart TX/RX sensor devices that sample measurements of specific environment parameters and transmit data to the base station through multi hop convergecast radio-communications. WSN are energy constrained (in terms of computing power and storage) and infrastructureless networks (the base station can be considered as the ultimate edge device or access point to an external network infrastructure), and WSN nodes are typically deployed in unprotected environments. Measurements can be sensitive data: therefore securing data transmissions over WSNs is a primary issue. WSN can be nomadic.

VANETs are another class of ad hoc wireless networks where nodes are TX/RX mobile devices but their mobility is constrained by the urban layout (are mounted into vehicles). Data are exchanged among vehicles, or between vehicles and the infrastructure, or within the same vehicle. Securing these data transmissions as well as the preservation of privacy are primary issues in VANET (consider the transmission of drivers' identity and their location information).

According to the ISO 31000 standard, we can refer to "security application" as the ultimate step of the iterated process - once a security vulnerabilities have been assessed - of risk mitigation from cyber attacks and the related assessment of the results until a residual risk, assumed as acceptable, has been reached: in

other words "security application" corresponds to a rebalancing process where security vulnerabilities (in this case WSN weaknesses against cyber attacks) get reduced when the proper countermeasures (in this case specific security functions) are applied. Therefore the "Required Security Level" for the system (in this case a WSN) can be determined from the analysis of its security vulnerabilities. On the other side, the security performance offered by a security function (that can quantitatively estimated) determines the "Offered Security Level" (or "Expected Security Level"). The condition for the "security application" to a specific network function is given by its "Required Security Level" balanced by the "Offered Security Level" of some security function.

ISO 31000 defines passive and active countermeasures: from a security point of view, passive functions typically include cryptographic techniques, hashing, message authentication codes, secure routing, while active functions include estimation techniques of system behavior or misbehavior able to detect cyber attacks (intrusion / attack detection and classification) through the issue of an alarm. ISO 31000 principles inspire the operative procedures for the specific technical standards in engineering domains: e.g. ISO 27000 family for the ICT domain, ISO 26262 and the future ISO 21434 for the automotive domain.

Mathematical methods to compute the security performance of a cryptographic technique are set by the "information theoretic security" - or information theory applied to security - introduced by C. E. Shannon in 1949 with its masterwork "Communication Theory of Secrecy Systems".

Passive security functions for WSNs and VANETs are still based on the ordinary cryptographic mechanisms (symmetric, asymmetric, hybrid schemes) but the technical constrains of the microprocessors embedded into WSN and VANET nodes push to innovative and raffinate techniques such as elliptic curve cryptography (ECC) and identity-based cryptography (useful for privacy preserving in VANETs). Active security functions are based on behavior estimators and classifiers derived from the theory of Discrete Event Dynamic Systems and Machine Learning algorithms.

The course introduces specific set of security techniques applicable to WSN and VANET systems that usually result in hybrid approaches trying to optimize benefits of the ordinary schemes with network constrains.

In this sense the family of cryptographic schemes denoted as TAKS (*Topology Authenticated Key Scheme*) and the intrusion detection system denoted as WIDS (*WPM-based Intrusion Detection System*) are introduced. TAKS (and its ECC-based version denoted as ECTAKS) and WIDS techniques have been designed at DEWS within the WINSOME Project (*Wireless Sensor Network Secure System for Structural Integrity Monitoring and Alerting*). WINSOME is an experimental platform where security functions, like TAKS or WIDS, have been developed and tested on various WSN technologies by students as demonstrators ready for customizations in other projects. As an example TAKS and WIDS have been successfully implemented over a clustered IRIS-based WSN in PNRM SEAMLESS Project and currently into operation to collect and monitor parameters related to the agricoltural sector in ECSEL AFarCloud Project.

The general program of the course consists of n. 7 lectures lasting 4 hours each one for a total of 28 hours. The course is split into two parts as follows.

WSN AND VANET SECURITY COURSE PROGRAM (tot. 28 hours)

Part I. Generalities on WSN and VANET Security (12 hours)

Day 1. Lecture I.1 WSN Architectures and Application Scenarios (4h): the position of WSN within wireless networks: ad-hoc networks (MANET, VANET) vs. WSN. Characterization of WSN, design constraints, application scenarios and current standard architectures. WSN security requirements are introduced and defined per application class.

TOPICS*: Wireless ad-hoc networks. WSN vs. mobile ad-hoc networks (MANET). MANET vs. vehicular ad-hoc networks (VANET). Design constraints for WSN. WSN Architecture: MAC and routing functions for WSN. WSN standardization roadmap: IEEE 802.15.4, ZigBee. The operating system for WSN: TinyOS. Security Requirements for WSN layer functions and applications. Security Management Plane.*

Day. 2 Lecture I.2 VANET Architectures and Application Scenarios (4h): the position of VANET within wireless networks, characterization of VANET, communication models (V2V, V2I), smart vehicles, application scenarios and current standard architectures are introduced.

TOPICS*: Definition of VANET, VANET vs. MANET, VANET applications, vehicular communications system, Communication models (V2V, V2I), inter-vehicle and intra-vehicle communications, broadcast techniques.*

Day 3. Lecture I.3 The Framework of Security Management (1h): the standard ISO 31000 Risk Management framework is briefly introduced. The path from risk to security management is delineated and the Reference Security Model is produced. Security levels and criteria for metrics definition are introduced. The concepts of "Required Security Level" and Offered Security Level" are introduced and defined per class of application.

TOPICS*:. The framework of Security Management. From Risk to Security Management. Reference Security Model: Security Metrics, Timing constraints, the "Required Security Level" vs. the "Offered Security Level". Reference technical standards.*

Day 3. Lecture I.4 Cyber Attacks (3h): the classification of cyber attackers and review of the most significant cyber attacks against WSNs and VANETs, the correspondent strategies of countermeasures are presented.

TOPICS*: Classification of Cyber Attackers and Cyber Attacks. Attacks to physical layer, data link layer, network layer, transport layer and application layer. Review of attacks against WSN. Review of attacks against VANET.*

Part II. Techniques for WSN and VANET Security (16 hours)

Day 4. Lecture II.1 Passive Security Functions (4h): passive security functions, i.e. purely defensive techniques without feedbacks for countermeasures, are introduced (cryptographic functions such data encryption and authentication). Key metrics and quantitative criteria to measure the "Offered Security Level" from information theory are represented. A brief mathematical introduction is presented. The main techniques are introduced.

TOPICS*: The Shannon's lessons. Hints on Modular Arithmetic, Generating Prime Numbers, Generating Pseudo-Random Numbers, Factoring Problem, Elliptic Curve Algebra, Pairings on Elliptic Curves. Passive Security Functions: Ciphering, Hash Functions, Message Authentication Codes, Digital Signatures. Key Establishment Protocols (KEP): Symmetric KEP, Asymmetric KEP, Id-based Encryption and Signature schemes, Hybrid KEP. Key Management Protocols (KMP): TinySEC, TinyECC. Passive security techniques for: IEEE 802.15.4 MAC, Routing, ZigBee.*

Day. 5 Lecture II.2 Active Security Functions (4h): active security functions, i.e. security techniques with feedbacks for countermeasures, are introduced (system behavior estimators and anomaly detectors). Key metrics and quantitative criteria to measure the "Offered Security Level" are represented. A brief mathematical introduction is presented. The main techniques are introduced.

TOPICS*: Dynamic Systems. Discrete Event Dynamic Systems (DEDS). The Canonical Problems of Dynamic Systems. The Intrusion Detection Problem: System Modeling (Petri Nets), Mapping into a Finite State Machine (Finite Automata, Stochastic Finite Automata or Discrete Time Markov Chains, Weighted Finite Automata), Identification of the Hidden State Machine (Hidden Markov Models, Weak Process Models), Hidden State Sequence Estimation (Viterbi Algorithm, Highest Score Method). Behavior Classifier. Information Theoretic Model of an Intrusion Detection System. Anomaly Detection System: Audit data, Classification Model, Representation Model. Representation Techniques: Supervised vs. Unsupervised Approach, Parametric vs. Non-parametric Techniques.*

Day 6. Lecture II.3 WSN Security. TAKS/ECTAKS scheme (2h): the cryptographic encryption/decryption and signature scheme TAKS (Topology Authenticated Key Scheme) and its ECC (Elliptic Curve Cryptography) extension is presented. TAKS has been embedded into WINSOME platform: WINSOME Project (Wireless Sensor Network Secure System for Structural Integrity Monitoring and Alerting) is briefly introduced.

***TOPICS**: The TAKS / ECTAKS Scheme. TAKS driving ideas & main features, Authenticated Network Topology, TAKS definition, EC-based TAKS (ECTAKS) pwECTAKS, cwECTAKS and xwECTAKS, ECTAKS Encryption / Decryption Scheme, ECTAKS Signature Scheme, ECTAKS SignEncryption Scheme, NIST Standard ECC. xTAKS in WINSOME Project.*

Day 6. Lecture II.4 WSN Security. WIDS/MVET scheme (2h): the intrusion detection system WIDS (WPM-based Intrusion Detection Scheme) and the behaviour estimator MVET (Mean-Variance Estimation Technique) are presented. WIDS has been implemented over embedded into WINSOME platform.

***TOPICS**: Weak process model IDS (WIDS) Reference Architecture: WIDS Technique, Basic Network Threats, Examples of Anomaly Rules, WPM-based Threats Models, Aggregated Threats Models, Security Analysis. WIDS in WINSOME Project. MVET driving ideas & main features, Reference Architecture, the estimation technique and performance analysis.*

Day 7. Lecture II.5 VANET Security and Privacy (4h): security and privacy requirements, adversary model, specific threat classification, security architectures and techniques are introduced.

***TOPICS**: Security and privacy requirements, security analysis, security architecture, guidelines to secure a VANET, privacy preserving solutions for inter-vehicle communications. Security techniques for intra-vehicle communications.*