Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Security in Sensor Networks

- Towards a Secure RPL -

Martin Landsmann

AW1 - Report

Fakultät Technik und Informatik
Studiendepartment Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Martin Landsmann

AW1 - Report

Eingereicht am: February 15, 2013

Martin Landsmann

Thema der Arbeit
AW1 - Report

Stichworte
LLN, RPL, 6LowPAN, Routing, Internet of Things, IPv6, Sensorknoten, IT-Sicherheit

Kurzzusammenfassung
Die Ausarbeitung diskutiert Sicherheitsaspekte des *IPv6 Routing Protocol for Low-Power and Lossy Networks* (RPL). Sensorknoten und andere Geräte mit geringer Leistungsfähigkeit werden zunehmend in einer Vielzahl von Anwendungsszenarien verwendet. Diese Geräte sind oft dafür konzipiert, batteriebetrieben mit ihren Nachbargeräten kabellos zu kommunizieren und dabei sowohl langlebig als auch wartungsfrei zu sein. Die Verwaltung ihrer Kommunikation und ein strukturiertes Routen verlangt es, zwischen Energieverbrauch, Funktionsfähigkeit und Belegung des Übertragungsmediums abzuwägen. RPL steckt in den letzten Entwicklungs- und Standardisierungsphasen um die Herausforderungen für *Low-Power and Lossy Networks* (LLNs) abzudecken. Zudem muß RPL, genau wie andere LLN Protokolle, Sicherheitskriterien berücksichtigen und versuchen sie zu erfüllen. Diese Aspekte sollen in einer Masterarbeit untersucht und evaluiert werden.

Martin Landsmann

Title of the paper
AW1 - Report

Keywords
LLN, RPL, 6LowPAN, Routing, Internet of Things, IPv6, Sensor-nodes, IT-Security

Abstract
This document discusses security aspects of the *IPv6 Routing Protocol for Low-Power and Lossy Networks* (RPL). Sensor nodes and Low-Power devices are used in a growing field of applications. These devices are commonly designed to be battery driven and to interact with their neighbours over the wireless, but with the constraint to be long-lasting and maintenance free. Organizing their communication with a structured routing is always a trade-off between power consumption, operability and occupation of the used communication medium. RPL is in the final stage of elaboration and standardization, to deal with the requirements for *Low-Power and Lossy Networks* (LLNs). Moreover, RPL has to deal with security aspects and threats just as other LLN protocols. These aspects and threats shall be researched and evaluated in the Master Thesis.

Contents

1 Introduction

Wireless sensor-networks consist of a large number of smallest intercommunicating low-power sensing devices. These are often battery driven and developed to be long lasting, self organizing and immune to environmental conditions. Sensor-networks are used in different scenarios where distributed capabilities of sensing, computing and communicating are required, e.g. in automation or surveillance systems. Sensor-networks are build up from a number of collaborating nodes with sensing properties. These are often smallest and low-powered devices communicating over the wireless with neighbour nodes and providing routing abilities. Mostly nodes fall in the category of a 8 bit micro-controller with a few KB of RAM. These properties grant a cheap production, and allows the deployment of countless nodes in a sensor-network. Hence, it is a major trade-off between hardware capabilities and price at the same time. Each individual node has to deal with its low computational and energy capabilities to provide a long lasting life cycle of the overall sensor-network. Additionally the goal of the network has to be achieved despite these limitations [1]. The last decade's development of sensor-nodes and sensor-networks leads to the often named *Internet of Things* (IoT) where countless smallest smart objects are operating with each other [2]. Organizing the communication and cooperation of the individual nodes in a network is always a trade-off between power consumption, operability and occupation of the used communication medium. Additionally the often wireless, noisy and unavailable medium is affected by environmental conditions. To grant a long lifetime of individual nodes and their quantity in a network forces the nodes to operate ad-hoc and independent from interventions and adjustments of maintenance personal. A sensor-network has to organize the communication structure, react on and handle errors, cope with misbehaving nodes and even attacks. It is well known that wireless communication is unreliable compared to a wired one. Links between communicating entities can have variable signal strength or even fail during transmission. The same applies to wireless sensor-networks and is even worse, considering the limited energy amount of nodes. Acknowledging or retransmission of data and information has to be carefully chosen by a node to prevent draining its power unnecessary, which requires tailored strategies for networks and nodes. These fundamental problems cause an ongoing research of sensor-networks and their optimization.

In 2003 the IEEE 802.15 working group[1], which elaborates standards for Wireless Personal Area Networks (WPANs), specified the *IEEE 802.15.4* link-layer protocol [3] for low-rate WPANs (LR-WPANs). This standard is a foundation for higher layer protocols for low-power wireless networks.

Several protocols have been built up on top of *IEEE 802.15.4* either using its full capabilities, such as *ZigBee* [4], or a subset, such as TinyOS[2].

Most proprietary protocols based on *IEEE 802.15.4*, implemented and developed their own upper layers without general standardization or with an industrial standard such as the *ZigBee* protocol. It derived from the situation, that no common standard has been developed for the upper layers in low-power wireless networks. The separated and closed development prevents nodes and networks to interoperate with each other, or with non sensor-network protocols such as the *IPv6* protocol [5].

This results in stand-alone and foreclosed proprietary protocols, only providing connectivity and interoperability through border gateways which causes a poor scaling behaviour, and no real integration of different systems.

This circumstances have risen the need of a standard for the layers above the link-layer to enable an internet for all kind of smallest devices and networks.

In 2007 the *Internet Engineering Task Force* (IETF)[3] specified *IPv6 over Low power Wireless Personal Area Network* (6LoWPAN) [6], a communication protocol for small(est) smart devices. This standard allows to receive and submit IPv6 packets over *IEEE 802.15.4* based networks.

The routing in 6LoWPAN, the topology maintenance and a communication behaviour of nodes have not been addressed by the standard. Existing protocols and approaches designed to provide scalable and reliable routing, such as *Ad-hoc On Demand Vector Routing* (AODV) [7] or *Optimized Link State Routing* (OLSR) [8], do not fit the constraints of sensor-networks. The limitations of low power nodes require different approaches to classical wireless networks. Routing, the topology and the communication behaviour in these *Low-power and Lossy Networks* (LLNs) have taken the limitations of sensor-nodes into account. Particularly the constraints of energy, computational and memory capabilities [9].

The *IPv6 Routing Protocol for LLNs* (RPL) [10], which is in the final stages of standardization, is designed to account for these limitations. It is developed by the IETF's *Routing Over LLNs* (ROLL) working group[4]. The major properties of RPL are to provide a scalable, reliable and efficient routing for LLNs on top of a link-layer protocol such as 6LoWPAN.

[1] http://www.ieee802.org/15/
[2] http://www.tinyos.net/
[3] http://www.ietf.org/
[4] http://datatracker.ietf.org/wg/roll/

1.1 Motivation and Problem Statement

LLNs are applied for various applications, like surveillance or for automation purposes. Individual nodes collect information and have routing abilities to provide a data flow topology towards a collecting point, e.g. a server. Sometimes the nodes even have to operate and use actuators, dependant on sensed and computed condition results, or have to perform the operations remote triggered by other entities, e.g. a server or other nodes.

A sensor-network can be deployed in a static way by placing nodes on fixed well known points or dynamic providing and supporting moveability of individual nodes. This includes allowing the nodes to join and leave the network at will.

Different kinds of operation scenarios in LLNs, where data traffic has to be secured, make it necessary to protect the sensed and forwarded data and control information from eavesdropping and manipulation. As an example, a Brewery would not voluntarily expose their brewing conditions to outsiders and it would not want that a manipulation of the sensed and forwarded data could harm the brewing process or even the employees. Another scenario could be, that the sensor-nodes are spread in an unavailable environment with harsh conditions where no physical maintenance and adjustment is possible, such as quake surveillance on the seabed. The nodes would have to organize themselves and save as much energy as possible to assure a preferably long lasting life cycle. Distributed computing could be applied in the network to lower the communication, computational and memory load for the individual nodes, e.g. relieve the requirement contacting a distant remote station.

In a scenario, where a sensor-network has to operate independently, nodes are responsible for their own health and the overall topology maintenance. In such scenarios often no possibility exists to provide exhausting monitoring or human intervention for adjustments. The nodes and the whole network would have to organize themselves to provide their target goal and to perform protective measures against attacks.

With the ongoing IoT progression countless smallest smart devices appear in all kind of situations. Using RPL and 6LoWPAN these countless smart objects have a standardized foundation to communicate and interact unbound from the limits of foreclosed solutions.

This development has moved sensor-networks from classical automation and surveillance scenarios.

They now provide home automation, entertainment and numerous helpful tasks by interacting and interconnecting with each other, such as in health monitoring and medical aid systems.

Communication, availability, and disturbance of the shared medium are highly dependant on transmission ranges and the energy level of the participants. Just as availability and disturbance

of the shared communication medium. These restrictions also count for LLNs, which have to deal with even smaller energy levels and transmission ranges. Assuming to be battery driven, the nodes have to carefully decide if and when to communicate for power-saving purposes. Data and control traffic have to be balanced out in LLNs to provide a preferably long lasting and working sensor-network. Topology organization and rearrangement of sensor-nodes and routing paths oppose this goal. Wireless networks and LLNs have the characteristic that nodes and links churn with the changing distance between the communicating nodes. Statically placed nodes minimize possible rearrangements and maintenance during lifetime. Constantly moving nodes require to reorganize the topology and spread control traffic to keep it healthy and working.

The decision to use a specific routing protocol for LLNs can have a massive impact on the reliability and the overall lifetime.

Beside the named exemplary scenarios, sensor-networks have to deal with different kinds of security related situations, depending on the operation scenario of the sensor-network and which goal an attacker or adversary tracks against it, e.g. disturbing, manipulating or eavesdropping. One of the core principles of information security, *Confidentially, Integrity and Availability* (CIA-principle) [11] has grown even more important where the sensed and transmitted data is high-grade private or confidential.

Different approaches have been proposed to cope with the possible attack scenarios depending on the topological and environmental conditions the sensor-networks have to deal with. The current standardization of the RPL protocol creates a ground for IoT and sensor-networks together with the number of possible and rewarding attacks against them.

Identifying and preventing attacks in the context of RPL, 6LoWPAN and sensor-networks is a promising field for research. The RPL specification currently provides only basic security approaches against attacks. Additionally enhancing the mobility of nodes in RPL, optimizing the routing and targeting energy efficiency extends the research area of the forthcoming master thesis.

2 Related Topics Regarding Sensor-Networks

There are many contributions in the research area of general sensor-networks as well as in the ad-hoc wireless networks context. Most of the contributions cope with the IoT development and the resulting use cases emerged for a countless number of interoperating smallest smart objects. The use cases for IoT address a wide area of applications. They cope with traditional routing difficulties, computation capabilities of single devices, distributed computing, security and energy efficiency in operation scenarios.

This chapter introduces exemplary relevant scenarios and approached difficulties in sensor-networks.

2.1 Resource Optimization

Optimizing the use of the limited resources of a sensor-network and its participating nodes is an important task. It has to be accomplished to provide a long lifetime and a reliable function of the individual nodes and the whole network. Nodes have to handle their limited hardware and energy resources, providing them to achieve the common goals of the sensor-network. Assumed that nodes have a limited lifetime due to their power consumption, it is required to reduce unnecessary communication and computation.

2.1.1 Mobility of Nodes in Sensor-Networks

To enable nodes to forward and route traffic, a topology has to be established. Routing protocols provides the ability to form and maintain routes between communicating entities. These protocols can be distinguished in two major classes, the link-state and the distance-vector routing protocols.

Link-State protocols perform a controlled flooding mechanism to distribute the presence and the knowledge of present links to neighbouring nodes through the network. Eventually all nodes can achieve a global topology overview, enabling them to compute shortest paths to any destination. This global propagation has to be applied in beacons or when topology changes occur.

Distance-Vector protocols exchange the routing table of a node with its neighbours. The received table is aggregated and combined with each nodes own one. Eventually every node in the network has a routing table that enables it to route packets towards a specific direction. Updates and changes in the topology can be locally announced and resolved.

In any of the both classes, a static topology provides less control message exchanges than a scenario with moving nodes. An expected movement of nodes most likely causes changes in the topology. A moving node affects the quality of the physical links to its neighbouring nodes. These links can even disappear if the distance exceeds the transmission range, or new links can be established if the node enters a transmission range of new neighbours. Both situations causes the exchange of control messages [12].

2.1.2 Distributed Operating

Providing a longest possible lifetime of a sensor-network and its individual nodes, it is required to optimize the organization of the topology, the computation and sensing behaviour, as well as idle states. To take each node's limited power, its computational and memory abilities into account, requires to organize a cooperation of nodes to gain the productivity or lower the power consumption. Distributed computation, as well as sensing and storing of the sensed information can be applied. Exemplary, a surveillance system can possibly achieve to monitor an area using just a subset of nodes in sensing and observation range. Alternating the nodes between idle- and sensing-mode can extend the lifetime of the sensor-network [13, 14]. Transmitting packets over the wireless is expensive to a node's energy resources. To reduce the number of forwarded traffic, nodes can compute results or aggregate information distributed in-network. The reduced number of exchanged messages and relieve the communication and occupation of the shared medium. The sensed and collected data can be stored distributed among neighbouring nodes to provide redundancy, availability, or even security, by not having the whole sensed and computed information kept in one single node.

2.2 Security in Sensor-Networks

Security in sensor-networks is a major objective and fundamental requirement, if personal and confidential data has to be sensed and forwarded through the network. The advantages of RPL and 6LoWPAN enabling an integration of different sensor-networks into a larger internet, opens the ground for attacks from outside. Transmitted data and control messages have to be protected against eavesdropping and manipulation.

Using wireless communication an attacker can listen to all packets exchanged between nodes in transmission range. Not interfering or disturbing the communication, there is no possibility to detect the eavesdropper. Therefore forwarded messages have to be protected in such way, that the value of the message is preferably low for the attacker, or the expense to gain profit preferably high.

Contrary an active attacker tries to intrude into the network or actively manipulate and forge data and control messages. Capturing and manipulating a node enables the attacker to extract encryption and verification keys as well as shared secrets placed on the nodes. Using the containing and extracted information, an attacker can join the topology and pretend being a legitimate participant. Breaking into the sensor-network can be applied if the security level is satisfactory low, e.g. when weak and breakable keys were used, or if the attacker can extract authentication and verification information to enter the network.

2.2.1 Intrusion Detection

Assuming attackers to be able to successfully join the network, mechanisms have to be applied to recognize such an intrusion and prevent causing damage. An intruder, just listening and reporting is hard to identify as it does not behave obviously malicious. The chances of recognition rises if an attack has certain notable effects, that can be identified by honest nodes of the topology. Even though, it has to be carefully distinguished between attacks and possibly occurring errors. In wireless scenarios transmissions fail, packet collisions and inconsistencies appear with a high probability. This situations can be mistakenly lead to the assumption of an attack, or of an occurring error. Successfully identifying an intruder is dependant on the goals of an attacker and if its malicious behaviour can be identified. To detect a constructive attacker, nodes have to distinguish individually, or in composite with other nodes, if they are being attacked, or just facing errors. This can be done passively, by constantly observing and analysing the behaviour of their neighbours. If a node observes an irregularity, it computes and decides if this observation is sane. This approach has the trade-off to sacrifice resources constantly observing a node's behaviour and compute sanity decisions. On the other hand an active approach triggers an inspection of nodes only if an error has been detected. If one node receives messages and recognizes irregularities, say wrong or suspicious control messages, it can trigger a challenge testing the suspicious node. Contrary to the passive approach, no history and constant observation is necessary. Hence, its trade-off is that it can only detect attack if the sanity of received messages is below a certain level [15].

2.2.2 Attack Detection

Detecting attacks and successfully distinguishing them from errors can become a difficult task. If the aim of an attack is to degrade the productivity of the sensor-network, an attacker can just hold back or drop traffic producing a sink-hole [16], or forwarding it to an adversary server using an out of band channel performing a worm hole attack. It is also possible to invoke unnecessary control traffic in the topology, to keep the nodes and the medium occupied. Such attacks drain the spare energy of all affected nodes [17]. In another constructive attack, the attacker could try to pull a major amount of traffic. This would enable the attacker to perform further attacks on a lot of passing messages, say eavesdropping or manipulation.

To enable a node to successfully detect constructive attacks, it must have knowledge about boundaries in which the parameters in control messages can move. Additionally a node has to be aware about the topological situation surrounding it. Such minimum knowledge enables a single node to have a ground for sanity checks on control messages. However, it does only provide a soft criterion considering that unusual seeming control messages can appear in certain situations and be absolutely sane. For instance, if a node is the only one providing a physical route towards a server, being in a physical and topological bottleneck, it automatically pulls all traffic to provide transit. A single node cannot be aware of such a situation, if not consulting neighbour nodes, or even more distant ones. In the collective, a number of nodes have the chance to detect the true situation and determinate sanity of it. This collaborative approach stresses the communication overhead, occupying the involved nodes and draining their resources due to the required exchange of information. Such collaborative approach rises the chance detecting and locating an attack, thus it can be misused by an attacker to occupy and disturb the operation of the sensor-network [18].

Apart of these exemplary constructive degrading attacks, an attacker can simply constantly disturb the communication medium. This would maximize the packet loss rates and the retransmission attempts of the affected nodes. Assuming the attacker has only comparable resources to the attacked nodes, this attack is rather unrewarding. The constant disturbance exhausts the attackers energy resources in a short period of time, compared to the lifetime of the attacked nodes. Hence, it blinds the sensor-network in the disturbed area. The recognition of such attacks is not mandatory in many scenarios. Most topology approaches and routing protocols would handle such attacks similar to handling failing nodes. The topology would be reconstructed to avoid routes to and through the unavailable nodes, if possible. Even though, surrounding nodes have the chance to recognize this kind of attack. If a sufficient number of nodes exchange information about the failed nodes and disappeared links, composing the individual views into a larger overview would reveal an anomaly in a certain area.

2.2.3 Attack Prevention

Due to the limited resources of nodes in sensor-networks, a comprehensive monitoring, or a mature and strong cryptography of transmitted data is not a realistic option. However, the CIA-principle has to be applied to the sensed and forwarded data in many scenarios, e.g. where sensors monitor a person's health conditions or where the sensed data is used to operate actuators. It has to be accomplished providing safe transit of information from a sensing node to a collecting server. Additionally, mechanisms and approaches have to be applied to keep the data unharmed on the way.

Using *Private-Public-Key* (PPK) cryptography is not an option. The computational and memory requirements using PPK would cause the nodes to rapidly exhaust, or just go beyond their limits. Only symmetric cryptography schemes are applicable without exhausting a node's resources.

Individual nodes can encrypt the sensed data with a pre-shared key, or enrich it using a shared secret, which have to be pre-installed on the nodes just before deployment. The collecting server has also these keys and secrets to be able extracting the information of the received packets. If all nodes share a single key, capturing and manipulating one node would break the whole security. To enhance this issue individual or group-wise keys can be applied to the nodes. This has a server-side impact, as it has to establish a key-management system. Additionally every node added to the topology would have to be introduced to the server to exchange such key and secret.

Distributed approaches and aggregation schemes can be also applied to keep the principles active. Sensed information can be divided into parts and distributed to different nodes. This prevents an individual node to have access to all collected information routed, which is only true if a topology does not contain bottlenecks or nodes arranged in a chain. Aggregating sensed data with received parts of other nodes and enriching the resulting packets cryptographically, e.g. using shared secrets, can provide a sufficient security level for the transit of the created packets. An attacker has little chance to reconstruct any of the original information from such build packages. Only with a sufficient number of captured packages and the knowledge of the used shared secrets, parts of information can be extracted successfully [19].

The exemplary approaches have to prevent an attacker to successfully have malicious influence on individual nodes, the overall topology and its goals.

3 The Upcoming and Ongoing Research

RPL spans a Destination-Oriented Directed Acyclic Graph (DODAG) for routing, which prevents loops, dynamically handles topological changes, and self-repairs unwanted loops, either locally or globally. A DODAG has an unique id and is constructed ranked such that the root node, e.g. the server, has the lowest rank. Each descendant node in this topology has a higher rank than its parent(s). A node elects one or a set of parents when participating a DODAG. All communication in RPL is directed upwards to the root node. A common ancestor of communicating nodes or the root node, depending on the mode of operation, routes an incoming message downward to the right destination, using link-local addresses. These characteristics lower and optimize the routing information traffic and the overall power consumption.

The RPL specification currently provides only basic security approaches against attacks. Due attacks against the topology can be applied, a malicious node can deliberately invoke a reconstruction of the whole topology degrading it. To prevent any node from invoking a reconstruction, which causes the topology version to rise monotonic, this initiation of the process can be secured using a shared and distributed approach. The *Version Number and Rank Authentication in RPL* (VeRA) [20] approaches this issue by distributing signed version number hash-chains through the topology, enabling any node to verify if a global reorganization has been invoked by the root. Additionally, this approach enables nodes to verify if a parent node announces its true topological distance to the root using rank hash-chains. However, using the VeRA approach, RPL is still vulnerable to a malicious node improving its topological position. Through a clever withholding of control messages regarding on reconstruction of the topology, a malicious node can still deliberately pretend any rank. This issue has been approached by *Topology Authentication in RPL* [21]. The proposed enhancement is linking a version number hash-chain with an associated rank hash-chain. This successfully prevents a malicious node pretend arbitrary forged ranks. Hence, this approach does not prevent using a replay attack to advance the own rank by one step.

The open question, and the ongoing inquiry, shows that investigating and advancing security related topics in context of RPL and 6LoWPAN constitute a promising area for upcoming researches.

Bibliography

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *Communications Magazine, IEEE*, vol. 40, no. 8, pp. 102 – 114, aug 2002.

[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1389128610001568

[3] IEEE, "Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)," IEEE, IEEE Standard, May 2003. [Online]. Available: http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=8762

[4] Z. allience, "ZIGBEE SPECIFICATION," ZigBee Alliance, Specification 053474r17, January 2008. [Online]. Available: http://www.zigbee.org/Standards/Overview.aspx

[5] S. E. Deering and R. M. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," IETF, RFC 2460, December 1998.

[6] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," IETF, RFC 4944, September 2007.

[7] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF, RFC 3561, July 2003.

[8] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," IETF, RFC 3626, October 2003.

[9] S. D.-H. P. Levis, A. Tavakoli, "Overview of Existing Routing Protocols for Low Power and Lossy Networks," IETF, Internet-Draft draft-ietf-roll-protocols-survey-07, April 2009. [Online]. Available: http://tools.ietf.org/html/draft-ietf-roll-protocols-survey-07

[10] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," IETF, RFC 6550, March 2012.

[11] A. F. Gary Stoneburner, Clark Hayden, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)," NIST - National Institute of Standards and Technology, Recommendations of the NIST Special Publication 800-27 Rev A, June 2004. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

[12] Y. Shi and Y. T. Hou, "Some fundamental results on base station movement problem for wireless sensor networks," *Networking, IEEE/ACM Transactions on*, vol. 20, no. 4, pp. 1054 –1067, aug. 2012.

[13] X. Chu and H. Sethu, "Cooperative topology control with adaptation for improved lifetime in wireless ad hoc networks," in *INFOCOM, 2012 Proceedings IEEE*, march 2012, pp. 262 –270.

[14] W. Choi, G. Ghidini, and S. K. Das, "A novel framework for energy-efficient data gathering with random coverage in wireless sensor networks," *ACM Trans. Sen. Netw.*, vol. 8, no. 4, pp. 36:1–36:30, Sep. 2012. [Online]. Available: http://doi.acm.org/10.1145/2240116.2240125

[15] G. Y. Keung, B. Li, and Q. Zhang, "The intrusion detection in mobile sensor network," *Networking, IEEE/ACM Transactions on*, vol. 20, no. 4, pp. 1152 –1161, aug. 2012.

[16] T. Shu and M. Krunz, "Detection of malicious packet dropping in wireless ad hoc networks based on privacy-preserving public auditing," in *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, ser. WISEC '12. New York, NY, USA: ACM, 2012, pp. 87–98. [Online]. Available: http://doi.acm.org/10.1145/2185448.2185460

[17] A. J. Newell, R. Curtmola, and C. Nita-Rotaru, "Entropy attacks and countermeasures in wireless network coding," in *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, ser. WISEC '12. New York, NY, USA: ACM, 2012, pp. 185–196. [Online]. Available: http://doi.acm.org/10.1145/2185448.2185473

[18] M. Valero, S. S. Jung, A. Uluagac, Y. Li, and R. Beyah, "Di-sec: A distributed security framework for heterogeneous wireless sensor networks," in *INFOCOM, 2012 Proceedings IEEE*, march 2012, pp. 585 –593.

[19] E. Ayday, F. Delgosha, and F. Fekri, "Data authenticity and availability in multihop wireless sensor networks," *ACM Trans. Sen. Netw.*, vol. 8, no. 2, pp. 10:1–10:26, Mar. 2012. [Online]. Available: http://doi.acm.org/10.1145/2140522.2140523

[20] A. Dvir and T. Holczer and L. Buttyan, "VeRA - Version Number and Rank Authentication in RPL," in *Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on*, oct. 2011, pp. 709 –714.

[21] M. Landsmann, H. Perrey, O. Ugus, M. Wählisch, and T. C. Schmidt, "Topology Authentication in RPL," in *Proc. of the 32nd IEEE INFOCOM. Poster*. Turin, Italy: IEEE Press, 2013, accepted for publication.

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, February 15, 2013 Martin Landsmann