Security Aspects of IPv6-based Wireless Sensor Networks

Review

Krešimir Grgić
Josip Juraj Strossmayer University of Osijek,
Faculty of Electrical Engineering, Department of Communications
KnezaTrpimira 2b, Osijek, Croatia
kresimir.grgic@etfos.hr

Višnja Križanović Čik
Josip Juraj Strossmayer University of Osijek,
Faculty of Electrical Engineering, Department of Communications
KnezaTrpimira 2b, Osijek, Croatia
visnja.krizanovic@etfos.hr

Vanja Mandrić Radivojević
Josip Juraj Strossmayer University of Osijek,
Faculty of Electrical Engineering, Department of Communications
KnezaTrpimira 2b, Osijek, Croatia
vanja.mandric@etfos.hr

Abstract *– Seamless integration of wireless sensor networks (WSN) with conventional IP-based networks is a very important basis for the Internet of Things (IoT) concept. To realize this goal, it is important to implement the IP protocol stack into a WSN. A global IP-based network is currently going through a transition from IPv4 to IPv6. Therefore, IPv6 should have priority in the implementation of the IP protocol into WSN. The paper analyses the existing security threats and possible countermeasures in IPv6-based WSNs. It also analyzes the implementation of a unique security framework for IPv6-based WSNs. The paper also analyzes a possible intrusion detection system for IPv6-based WSNs.*

Keywords *– security, IPv6, wireless sensor network.*

1. INTRODUCTION

Wireless sensor networks (WSN) are currently going through their intensive development and worldwide spreading. Intelligent sensor nodes tend to vastly outnumber other networking enabled devices in future [1-3]. Further development of WSNs naturally leads to their interconnection and integration with conventional networks, mostly based on TCP/IP protocol architecture. The implementation of IP protocol into WSNs was previously considered inappropriate due to their strict resource limitations, which resulted in numerous non-interoperable solutions. Currently, there are significant efforts to implement the IP protocol into a WSN, since it leads to their seamless integration into the global IP network.

Simultaneously, the global IP network started with gradual transition to the IPv6 protocol that should entirely replace the IPv4 protocol in future [4-5]. Consequently, regarding the implementation of the IP protocol into the WSN, the focus is on version 6 (IPv6) prior to version 4 (IPv4). The IPv6 protocol provides enormous address space, auto-configuration mechanisms and extensibility, what is very suitable for networks with a large number of nodes (such as WSNs). The implementation of the IPv6 protocol into WSNs enables their simple integration and convergence with the global Internet, what extends their application possibilities. Such integrated network that satisfies demands on flexibility, scalability and robustness represents an important foundation for the Internet of Things (IoT) concept [6].

Security aspects of the IPv6-based WSN are very important. Adequate solutions of security issues are decisive for their wider acceptance and further integration with other IP networks. IPv6-based WSNs have certain specificities that disable direct implementation and utilization of the existing security solutions known from IPv6 networks and conventional sensor networks. Therefore, thorough adaptation of the existing security solutions and development of novel ones with full support for IPv6 are required. These solutions must fit into a unique security framework for the IPv6-based WSN in order to achieve their synergy and common effect.

This paper reviews important aspects of the IPv6 protocol implementation into WSNs. Further, it analyzes security aspects of IPv6-based WSNs (types of attack and possible countermeasures). It also analyzes a possible implementation of a unique security framework for IPv6-based WSNs. A short overview of an intrusion detection system for IPv6-based WSNs is given. Finally, some conclusions and directions for future development are given.

2. IPV6 PROTOCOL IN WSN

During the nineties it became obvious that some problems with the IPv4 protocol (e.g., address space exhaustion, security issues, complex configuration, and routing table enlargement) will even increase in the future. This fact initiated development of the IPv6 protocol that brings some important improvements (e.g., 128-bit address space, a fixed-length simplified header, auto-configuration mechanisms and security improvements). Currently, the transition from IPv4 to IPv6 is a long-lasting ongoing process.

A WSN consists of a large number of inexpensive sensor nodes capable of sensing, basic data processing and wireless communication with other nodes. Although it is a special subtype of mobile ad hoc networks (MANET), most of the existing technical and algorithmic solutions known from MANETs are inapplicable directly into WSNs because of their resource limitations. Thus, a WSN usually implements some alternative solutions (different from a MANET) and avoids the IP protocol.

Since the implementation of the IP protocol stack into a WSN is an important prerequisite for their easier integration with other networks, IETF established certain working groups to contribute to this goal. The 6LoWPAN working group (IPv6 over Low-power Wireless Personal Area Network) defined a necessary adaptation layer that enables implementation of the IPv6 protocol into the WSN protocol stack [7]. Frame size used at the WSN physical layer is usually much smaller than in conventional IP networks. The 6LoWPAN adaptation layer enables adaptation of the IPv6 datagram for transmission within IEEE 802.15.4 frame. The 6LoWPAN standard defines the frame format, address auto-configuration methods and the forming of link-local addresses in networks based on the IEEE 802.15.4 standard, since it is currently the most common standard used for physical and MAC layers in the WSN. IPv6 header compression methods are specified for resource savings and easier transfer over IEEE 802.15.4 links [8]. The use of acknowledgements for received packets can be used as an option. The IEEE 802.15.4 frame has only 127 bytes at the physical layer. It is quite small for a full IPv6 packet, since without any compression methods and with AES encryption used, it leaves only 33 bytes available for the application layer data. Consequently, for larger data, fragmentation would be unavoidable, and additional resources would also be consumed. The 6LoWPAN adaptation layer defines header compression methods, both for IPv6 and UDP headers. In a best-case scenario (local unicast communication), the IPv6 and the UDP header can be compressed to 6 bytes.

The implementation of the IPv6 protocol into a WSN also requires an adequate solution for a routing protocol. The IETF working group ROLL (Routing Over Low-power and Lossy networks) specified a novel Routing Protocol for Low-Power and Lossy Networks (RPL) suitable for WSNs and other types of low-power lossy networks [9]. It is the first routing protocol suitable for WSNs that implements full IPv6 support. RPL is a modular protocol, with the mandatory core part and optional features that depend on a particular application. Currently, it is a routing protocol recommended for use in the IPv6-based WSN.

3. SECURITY ISSUES IN IPv6-BASED WSN

The open nature of the communication medium makes security issues in wireless networks even more challenging than in wired ones. Thus, securing mobile ad hoc networks is often a more complex task than securing a wired network. Although WSNs are a special subtype of MANETs, there are some significant differences that prevent direct implementation of MANET security mechanisms into a WSN. Compared to a typical MANET, a WSN may have a significantly larger number of nodes that are prone to failures and strong resource limitations. A WSN is usually based on broadcasting, while point-to-point links still predominate in MANETs. These differences make WSNs more vulnerable to denial-of-service attacks. Weak WSN computational resources also inhibit the wider use of cryptographic techniques based on a public key (asymmetric cryptography). Therefore, in most cases, the implementations are constrained to the use of symmetric cryptographic techniques (based on private keys) for the application in WSNs [10-11].

Ensuring physical security for every sensor node in a WSN would be very expensive and in opposition to the basic premise of a WSN as a network of cheap intelligent nodes. Therefore, research focus is on different detection and prevention methods for attacks that do not involve attacker's physical contact with sensor nodes or the base station. Possible attacks on WSNs can be categorized according to different criterions. The attacks originating from nodes that are not members of the targeted network are outsider attacks, while insider attacks are initiated by former legitimate nodes that became compromised by the intruder and begun to behave maliciously [12-13]. Also, attacks can be classified as passive (eavesdropping and data tracking) and active (include data modification). The attacks in a WSN can be focused on different security premises: confidentiality, authenticity, network availability (denial-of-service attacks) and data (or service) integrity. The attacks can also be observed according to a specific layer of the layered networking model they focus on

[14]. Most of the security aspects of WSNs are not directly related to the network layer and do not depend on the network layer protocol version. Therefore, both IPv6-based and conventional WSNs are vulnerable to attacks focused on other layers with no significant difference. Nevertheless, the implementation of the IPv6 protocol as the network layer protocol has an indirect impact on security aspects of other network layers. It is manifested through the fact that currently the choice of IPv6 as the network layer protocol in WSNs narrows a possible set of protocols and technologies which can be used on other layers. Fortunately, proper adaptations and support for the IPv6 protocol are being intensively developed and therefore most protocols and technologies used in WSNs will certainly support IPv6 as a network layer protocol in near future.

3.1. ATTACKS ON PHYSICAL LAYER

The attacks targeted to the physical layer are jamming and tampering. In a jamming attack, the attacker uses his own transmitter to cause interference on WSN's operational frequencies intentionally. Since in most WSNs only one channel is used for communication, they are very vulnerable to jamming attacks. The implementation of advanced methods for interference avoidance would significantly increase sensor node complexity, price and energy consumption, which is mostly unacceptable. A jamming attack is not related to the protocol stack, so both conventional and IPv6-based WSNs are equally vulnerable to this type of attack. It is also the case for a tampering attack. In most WSNs, nodes are exposed to tampering since they principally do not have physical protection. Therefore, security mechanisms for WSNs have to predict a possible compromise of certain nodes, and implement a mechanism for their exclusion from the network.

3.2. ATTACKS ON DATA LINK LAYER

The data link layer in WSN network architecture is responsible for dataflow multiplexing, data framing, medium access and error control. It enables reliable point-to-point and point-to-multipoint connections within a WSN. Possible attacks on the data link layer are primarily focused on intentional collision causing and resource exhaustion.

If two or more nodes within a transceiver range try to simultaneously transmit at the same frequency, collision occurs and causes packet loss. Unfortunately, the attacker may cause collisions intentionally during transmissions of data or acknowledgements. Such attack is not difficult to detect, but it is very difficult to prevent it. If collision occurs, nodes repeatedly try to retransmit lost packets, what may lead to power resource exhaustion. Resource exhaustion by retransmission can be reduced by limiting the allowed frequency of medium access and by using time-division multiplexing [15]. Both IPv6-based and conventional WSNs are vulnerable to these attacks with no significant difference since they are not related to higher level protocols.

3.3. ATTACKS ON NETWORK LAYER

The network layer in WSNs must satisfy some important principles (e.g., energy efficiency) that have a significant impact on design of networking mechanisms (e.g., a routing mechanism). Some complex networking mechanisms important for proper network operation (e.g., routing or addressing) are running at the network layer. Therefore, the network layer is mostly exposed to various types of possible attacks.

A large number of network layer attacks target on the routing mechanism. They are oriented towards routing information exchanged between sensor nodes. The attacker may spoof or alter routing data, such as repeat sending of data captured earlier in order to disrupt the normal network dataflow. In this way, the attacker can intentionally create routing loops, attract or repel network traffic, change original routes, generate false alerts or intentionally increase delay. A message authentication code may be used as a possible countermeasure against spoofing and unauthorized modification of routing messages. In that case, the receiver may verify message integrity and sender authenticity. The use of counters and timestamps may prevent unauthorized repetition of older messages by the attacker.

Most WSNs use the multihop communication paradigm, assuming that all intermediate nodes will fairly forward received messages toward their destination. This assumption is often misused by the attacker, where in most cases the attacker selectively forwards packets. The simplest case of a selective forwarding attack is the situation where a malicious node refuses to forward any packet (all packets are dropped). This variant of a selective forwarding attack is usually called black hole attack. However, a black hole attack is easier to detect than other types of selective forwarding. This kind of malicious behavior can usually be detected by neighboring nodes if an adequate intrusion detection mechanism is implemented into the WSN. If a black hole attack is detected, routes should be reconfigured in order to exclude malicious nodes.

A more sophisticated attack is the case where a malicious node selectively forwards some packets (while some are dropped). The attacker discards or modifies packets from certain nodes. Simultaneously, the attacker regularly forwards packets from some other legitimate nodes. Such behavior makes a selective forwarding attack difficult to detect, since neighboring nodes will hardly be suspected of malicious behavior. In most cases of selective forwarding attacks, the attacker is one of the intermediate nodes on the route to the destination (i.e., a base station). Also, it is possible that the malicious node is not directly on the route, but in the neighborhood of the intermediary node. In that case, the malicious node monitors the neighboring

dataflow and uses its transmitter to cause intentional collision with packets that it tends to drop. A possible countermeasure against selective forwarding attacks is the use of multiple routes between source and destination nodes.

The attack where a malicious node attempts to attract all traffic from the network (or at least one part of the network) is usually called the sinkhole attack. It is usually achieved by falsifying routing data (e.g., the attacker advertises quality routes to the base station, and encourages neighboring nodes to send their packets to the malicious node). Therefore, the malicious node acts like a sinkhole for all traffic from its surrounding. A sinkhole attack most frequently occurs in combination with a selective forwarding attack. Good practice in the prevention of sinkhole attacks is the use of exact information about the node's geographical location in the routing mechanism. Unfortunately, obtaining exact node positions usually implies the implementation of some positioning system (e.g., the GPS), which increases the complexity and costs of sensor nodes. Therefore, most routing protocols reckon on the exchange of routing data between sensor nodes instead on precise location data. Afterwards, an additional problem in the IPv6-based WSN is a lack of a geographical routing protocol with support for the IPv6 protocol.

In most attack scenarios, the attacker utilizes one or more devices with significantly larger resources than the average sensor node (usually laptop computers). These devices enable him to perform even more complex attacks. The attacker most frequently uses two devices to establish a fast low-latency link (tunnel) between two distant parts of the network (usually called a wormhole). By virtue of that tunnel, the attacker can convince distant nodes that they are close to the base station and in this way disrupt the network routing mechanism. The attacker creates the sinkhole in a distant area of the WSN, which attracts complete traffic from legitimate nodes since the attacker advertises a quality route to the base station (better than alternative legitimate routes). Since the wormhole attack is usually combined with other types of attacks (e.g., eavesdropping, selective forwarding), it can be very hard to detect it. Special additional markings can be used for every packet as a possible countermeasure against the wormhole attack. Geographical data can be used to limit the maximum distance allowed between the sender and the receiver, while temporal data can be used to limit the maximum packet lifetime [16]. Unfortunately, a positioning system is necessary for ensuring geographical data, and the application of temporal markings requires strict time synchronization between sensor nodes, which leads to a more complex and expensive WSN.

The attacker can also steal the identity from a legitimate node and misrepresent itself to other nodes. It is possible that the attacker uses several different identities at the same time, while he can present itself as several new nodes or steal the identity of the existing nodes. This type of attack is called a Sybil attack and it is already known from peer-to-peer and mobile ad hoc networks [17]. Therefore, it is good security practice to forbid addition of new sensor nodes into a WSN after setup (except if it is really necessary, depending on particular WSN applications). The Sybil attack has the largest impact on routing distributed data storage. The attacker can achieve that ostensibly multiple routes actually pass through a single malicious node (with multiple identities). The Sybil attack can seriously harm the data aggregation mechanism (frequently used in a WSN due to resource savings) by inserting fake data. Actually, the Sybil attack may affect all WSN mechanisms based on distributed algorithms and collaboration between nodes (e.g., some types of intrusion detection systems). Possible countermeasures for the Sybil attack must include a mechanism for node identity verification. It usually connotes the use of cryptographic methods. In that case, it is necessary to use proper mechanisms and techniques for cryptographic key distribution and management. A frequently used method is key pre-distribution during network setup. Therefore, every node gets a certain number of keys deployed so that neighboring nodes can find (or calculate) a common shared key. It is desirable to implement a key management mechanism that supports additional key exchange and key revocation in case of node compromise.

Most routing protocols for WSNs use broadcasting of control messages for routing data exchange between nodes (e.g., nodes inform their neighbors about their status by broadcasting HELLO messages). Such mechanism can be easily misused by the attacker. The attacker can use a laptop computer for broadcasting control messages with transmission signal power much higher than legitimate nodes. In this way, the attacker can easily cover the whole network area and persuade legitimate nodes that he is their neighbor. However, the malicious node is not in range of legitimate nodes, so they try vainly to send their packets. This type of attack is usually designated as a flooding attack, and may have a serious impact on all networking mechanisms that reckon on data exchange between neighboring nodes. A possible countermeasure can be to obligatorily check for link bidirectionality before data exchange. Also, a possible solution can be implementation of a neighbor authentication mechanism, usually based on cryptographic techniques.

3.4. ATTACKS ON TRANSPORT LAYER

Similarly to conventional networks, the transport layer in a WSN is responsible for handling end-to-end connections. There are some security threats that directly affect the transport layer. Since the transport protocol has to maintain a connection, a typical method for connection disruption is resource exhausting by flooding. For every connection, a destination node has to allocate certain re-

sources. If the attacker floods his target with connection requests, all resources will be exhausted and unavailable for legitimate connection requests. It is extremely difficult to prevent this attack. A possible measure that can slow down the attacker in exhausting resources is to define a specific task (a computational problem) that the node has to solve (calculate) before the connection is established. Unfortunately, such approach additionally consumes resources of legitimate nodes, and is not effective if the attacker has significantly larger resources than the average sensor node. The attacker can also disrupt the established connection by sending false error messages and demands for retransmission, forcing legitimate nodes to spend their resources on unnecessary transmissions. As a possible solution, it is recommended to implement authentication mechanisms that could authenticate every single packet.

3.5. ATTACKS ON APPLICATION LAYER

Some existing attacks in WSNs are targeted directly towards the networking model application layer. Overwhelm attack connotes the attacker's attempt to excessively stimulate a sensor on network nodes. In this way, the attacker increases the amount of transferred data causing also an increase in consumed power and networking resources. The impact of this attack can be reduced by implementing efficient data aggregation algorithms and limiting the frequency of sending data to the base station.

Most sensor nodes used in sensor networks support remote reprogramming (over the network), without the need for direct physical access. It makes network management and administration much easier and comfortable (especially in large networks), but it could be a serious security problem. If the attacker successfully reprograms the nodes, he can take control over the whole network. Therefore, security practice is recommended to disable the possibility of remote programming if it is not really indispensable.

The attacks and security threats analyzed, including possible countermeasures, are summarized in Table 1.

4. SECURITY FRAMEWORK FOR IPv6-BASED WSN

A large variety of possible application scenarios for wireless sensor networks (e.g., military, industrial, agricultural and environmental applications) makes their security aspects extremely complex. It is primarily because different applications have different security requirements and demands. Therefore, it is difficult to develop a general security solution suitable for all applications. Consequently, it is desirable to develop and implement solutions that are adaptive and modular, in order to be able to suit application security demands. On the other hand, implementation of quality security mechanisms into a WSN improves their overall security and opens possibilities for their wider acceptance and use. Most security mechanisms proposed for WSNs are focused on a single threat on a certain layer of the layered networking model. Therefore, such independent mechanism cannot provide a desired security level to the end user. The desired security level could be reached by implementing several different security mechanisms that should operate cooperatively. However, it would make network installation and maintenance very complicated. Thus, some research focus on development of integrated cross-layer security frameworks for WSNs. Such framework integrates several security mechanisms and provides the end user with necessary security services [18-19].

Due to certain specificities of the IPv6 protocol, security frameworks intended for conventional WSNs cannot be directly applied to the IPv6-based WSN. Therefore, IPv6-based WSNs require adaptation of the existing security frameworks and proposal of novel ones. In [20], the authors propose an integrated security framework intended for the IPv6-based WSN. The proposed security framework includes security mechanisms required to provide basic security premises i.e., authenticity, reliability, integrity and availability. The security framework is modular and enables the use of required security services and functions according to the current application. The security framework consists of four security modules, i.e., cryptographic module, secure routing module, secure data aggregation module and intrusion detection module (Figure 1).

Table 1. Attacks and possible countermeasures in the IPv6-based WSN

Attack Type	Possible Countermeasures	IPv6 influence
Physical layer		
Jamming	Multiple channels	no
Tampering	Physical protection	no
Data link layer		
Intentional collision	Error correction codes	no
Resource exhaustion	Time division multiplexing, Medium access frequency limitation	no
Network layer		
Routing attack	Message authentication code, Counters and timestamps	yes
Selective forwarding	Multiple routes	yes
Sinkhole attack	Routing based on location data	yes
Wormhole attack	Limiting packet lifetime, Use of location data	yes
Sybil attack	Cryptographic methods	yes
Flooding attack	Cryptographic methods	yes
Transport layer		
Flooding with connection requests	Computational task before accepting connection	no
Application layer		
Overwhelm attack	Secure data aggregation	no
Reprogramming attack	Disable remote reprogramming	no

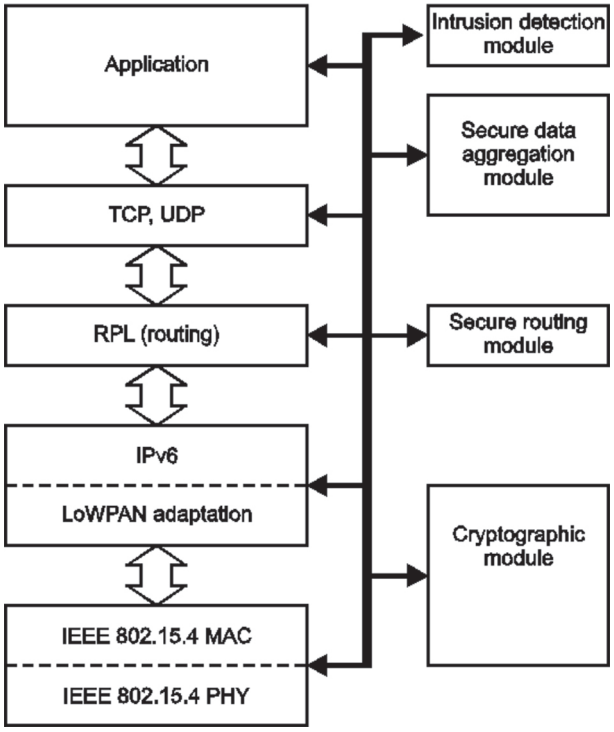

Fig. 1. Structure of the security framework for the IPv6-based WSN [20]

The security framework follows a cross-layer approach and pervades all layers of the protocol stack. Security modules are interconnected in order to use each other's services. The proposed security framework is flexible (i.e., it allows the user to choose desired security services depending on application requirements) and scalable (i.e., it supports node addition or removal). It is also economical in resource consumption and resistant to node compromise.

The cryptographic module includes two submodules: the encryption submodule (provides data confidentiality, authentication and integrity) and the cryptographic key management submodule (responsible for secure key distribution, setup and revocation). Data confidentiality is ensured by the use of data encryption methods, predominantly based on secret keys (symmetric cryptography) due to lower resource demands. A message authentication code (MAC) is used for the purpose of authentication. In the IPv6-based WSN, the most common standard for the physical layer is IEEE 802.15.4. This standard implements the AES (Advanced Encryption Standard) with 128-bit keys that can be used for securing messages on single links (in case of multihop communication, security mechanisms have to be applied on higher layers). The key management submodule deals with problems of secure initial key distribution, discovery of shared keys (for mutual communication between pairs of nodes), path key establishment (for communication between nodes without a common shared key) and key revocation (in case of a compromise). Cryptographic techniques are usually resource demanding, which can be a problem in a resource-constrained WSN. Further development of crypto-processors and their integration within sensor nodes will significantly improve WSN security in future, since hardware implementation of cryptography mechanisms will enable the use of more advanced cryptographic techniques in resource-limited sensor nodes [21].

The secure routing module for the IPv6-based WSN is based on the RPL routing protocol, as the first routing protocol for WSNs with IPv6 support. This module consists of three blocks that perform operations of secure route discovery, secure route maintenance and secure data forwarding. The block for secure route discovery initially establishes multiple routes between sensor nodes, such as routes to the base station. The block for secure route maintenance performs route reconfiguration in case of a topology change due to different possible reasons (e.g., node failure or node compromise). The block for secure data forwarding takes care of message sending and receiving. For assuring data integrity, confidentiality and authentication, the secure routing module uses services of the cryptographic module. Currently, the RPL routing protocol is most suitable for integration into the security framework for the IPv6-based WSN because of IPv6 support. Accordingly, it represents the core of the secure routing module. It is necessary to preserve authentication and integrity of its routing control message (DIO, DIS and DAO messages) and prevent their unauthorized retransmission. The secure routing module receives data about detected malicious nodes from the intrusion detection module in order to exclude compromised nodes from secure routes.

Data aggregation is a very important procedure in large sensor networks, since it reduces necessary communication and in this way saves resources and extends network lifetime. Attacks on data aggregation usually try to insert false data or modify aggregated data. Therefore, the secure data aggregation module is also an important part of the integrated security framework. It uses services of the cryptographic module (for data encryption and decryption if partial aggregation is required on intermediary nodes). According to data obtained from the intrusion detection system, the data aggregation module can exclude data from malicious nodes and prevent disrupting of the final data aggregation result. The secure data aggregation module obtains data about the network structure and topology from the secure routing module. It is good security practice to choose an aggregation function that closely follows expected sensor readings and to limit sensor reading intervals. It is also recommended to discard minimum and maximum values before aggregation, such as to use the median function instead of average. The secure data aggregation module uses services of the cryptographic module to preserve data confidentiality and integrity.

A very important part of the complete security framework for IPv6-based WSNs is the system for detection of intrusions and malicious node behavior. Therefore, it is

implemented through the intrusion detection module that is analyzed in the next section.

5. INTRUSION DETECTION IN THE IPv6-BASED WSN

A system for detecting intrusions and malicious node behavior represents a very important security component of every complete security framework. Implementation of the intrusion detection system (IDS) into WSN represents a great challenge due to numerous problems and limitations. Some typical problems are as follows: resource limitations (causes the need for reduced communication and disables the possibility of using the IPsec protocol and public key cryptography), various possible security threats and attack types (denial of service, routing attacks, sinkhole, Sybil, wormhole, etc.), and key management problems.

The intrusion detection system for the IPv6-based WSN has to fulfil some general demands equally as in a conventional WSN. It should provide an automated mechanism for attack source identification (a malicious network node), generate proper alert for the rest of the network and take proper preventive measures. Every action targeted against data, communication or computing resources can be considered as an attack. The IDS system has to distinguish legitimate network activities from abnormal (malicious) ones, which could be a serious problem, especially in larger networks. For that purpose, one of three different approaches is usually used: misuse detection, anomaly detection and specification-based detection.

A misuse detection technique compares current network activities with known attack signatures (behavior patterns of known malicious activities). An anomaly detection approach includes a learning phase, where the IDS learns a pattern of normal network behavior (after a learning phase, statistical deviations from normal behavior are characterized as malicious behavior). Specification-based detection combines properties of these two methods, and is chosen as most appropriate for the proposed IDS for the IPv6-based WSN in [22]. Like the anomaly detection technique, it also detects deviations from normal behavior, but it has predefined specifications that describe normal network behavior. Such approach is less resource demanding, and at the same time it also enables detection of novel attack types.

There are certain proposals of intrusion detection systems for WSNs. These proposals are very heterogeneous, but they can be roughly categorized into few categories [23] as follows: the IDS using routing protocols, the IDS based on neighbor monitoring, the IDS based on innovative techniques and the IDS based on fault tolerance. Unfortunately, most of them are inapplicable in the IPv6-based WSN without necessary modifications and adaptations. The IDS for the IPv6-based WSN should be integrated into a unique security framework as the intrusion detection module (intended for detection of intrusions and malicious node detection). The intrusion detection module for the IPv6-based WSN consists of two main submodules, i.e., the local detection submodule and the cooperative detection submodule (Figure 2).

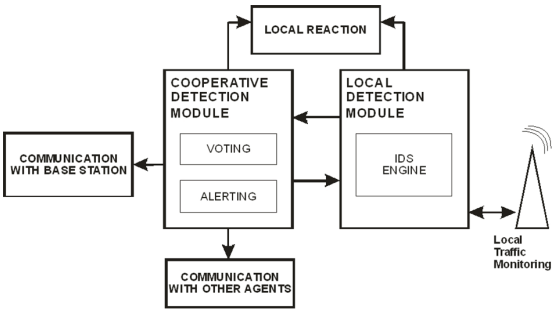

Fig. 2. Intrusion detection agent

Identical IDS modules (agents) are implemented on every wireless sensor node, executing cooperative algorithms and communicating with other modules. Since the system is fully distributed, every network node monitors network traffic by using a watchdog technique. It is assumed that every network node has several neighboring nodes within the range of its transceiver. Accordingly, every IDS module listens to their neighbor's traffic and collects data that represent input parameters into the collective decision-making process. At first sight, it seems that traffic monitoring by watchdog nodes will significantly increase power consumption. Fortunately, it is not true, since in most radio communication systems implemented in WSNs sensor nodes already receive packets broadcast from their neighbors. Therefore, additional power is used only for additional data processing and for communication between IDS modules.

The local detection submodule analyzes neighbor activities, and according to predefined rules, creates a list of possibly malicious neighboring nodes with estimated malevolence probabilities. All distributed IDS modules exchange lists of suspect nodes. The cooperative detection submodule makes the final decision about behavior character of suspected nodes. The final decision is a result of the cooperative algorithm that takes into consideration all malevolence estimations from all network nodes. If the final estimated malevolence probability for a certain node exceeds the predefined threshold value, the node will be declared as malicious and excluded from the network.

6. CONCLUSION

Intensive development of wireless sensor networks with their numerous application possibilities naturally requires their seamless integration with other types of networks. A very important step toward that goal is the implementation of the IP protocol stack into the WSN, where the focus should be on the implementation of the IPv6 protocol because it provides huge address

space enabling addressing of each individual node in very large networks. IPv6 should also replace IPv4 in other IP-based networks in the foreseeable future.

Adequate solutions of WSN security aspects are very important for numerous applications. All security solutions for the IPv6-based WSN must have full support for the IPv6 protocol. IPv6-based WSNs are exposed to many different attack types, similarly to conventional WSNs. Since there are differences between protocol stacks in IPv6-based WSNs and other types of WSNs, the implementation of the IPv6 protocol has an impact on certain attack types (depending on the targeted layer). Since these differences primarily refer to adaptation and network layers, IPv6 protocol implementation mostly affects the attacks targeted towards the network layer. The attacks on the network layer are similar, but the attacker also has to adapt his techniques for networking mechanisms used in the IPv6-based WSN (IPv6 addressing and RPL-based routing).

Security solutions used in conventional WSNs have to be modified and adapted with full IPv6 support implemented in order to use in IPv6-based WSNs. There is also a requisite for new security mechanisms, developed primarily for the IPv6-based WSN. All proposed security solutions should fit into a unique modular cross-layer security framework. Only in this way their synergy and common effect can be achieved, and at the same time the user can adapt the desired security level to the current application requirements.

The IPv6-based network may possibly have a very large number of nodes. Therefore, it is important to ensure proper network functioning in case of some node failures or compromise. Accordingly, the system for detection of intrusions and malicious node behavior with full support for the IPv6 protocol is crucial for successful integration of the IPv6-based WSN into the global network in the context of the Internet of Things (IoT) concept.

7. REFERENCES

[1] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Computer Networks, Vol. 52, No. 12, 2008, pp. 2292-2330.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, Vol. 40, No. 8, 2002, pp. 102-114.

[3] K. Grgic, D. Zagar, "Wireless sensor networks – applications and development," Proceedings of the 2nd IFAC International Conference on Modeling and Design of Control Systems in Agriculture (AgriControl), Osijek, Croatia, 3-5 September 2007, pp. 217-222.

[4] RFC 2460: "Internet Protocol, version 6 (IPv6) Specification," December, 1998, http://www.ietf.org/rfc/rfc2460.txt (accessed: 2016)

[5] D. Zagar, K. Grgic, S. Rimac-Drlje, "Security aspects in IPv6 networks – implementation and testing," Computers and Electrical Engineering, Vol. 33, No. 5-6, 2007, pp. 425-437.

[6] L. Atzori, A. Iera, G. Morabito, "The Internet of Things: A survey," Computer Networks, Vol. 54, No. 15, 2010, pp. 2787-2805.

[7] RFC 4944: "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," September, 2007, http://www.ietf.org/rfc/rfc4944.txt (accessed: 2016)

[8] RFC 6282: "Compression Format for IPv6 Datagrams over IEEE 802.15.4-based Networks," September, 2011, http://www.ietf.org/rfc/rfc6282.txt (accessed: 2016)

[9] RFC 6550: "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," March, 2012, http://www.ietf.org/rfc/rfc6550.txt (accessed: 2016)

[10] Y. Zhou, Y. Fang, Y. Zhang, "Securing Wireless Sensor Networks: A Survey," IEEE Communications Surveys & Tutorials, Vol. 10, No. 3, 2008, pp. 6-28.

[11] Y. Wang, G. Attebury, B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Communications Surveys & Tutorials, Vol. 8, No. 2, 2006, pp. 2-23.

[12] T. Kavitha, D. Sridharan, "Security Vulnerabilities in Wireless Sensor Networks: A Survey," Journal of Information Assurance and Security, Vol. 5, No. 1, 2010, pp. 31-44.

[13] C. Krauss, M. Schneider, C. Eckert, "On handling insider attacks in wireless sensor networks," Information Security Technical Report, Vol. 13, No. 3, 2008, pp. 165-172.

[14] M. Saxena, "Security in Wireless Sensor Networks – A Layer-based Classification," Purdue University, Indiana, USA, Technical Report CERIAS TR 2007-04, 2007.

[15] A.D. Wood, J.A. Stankovic, "Denial of Service in Sensor Networks," IEEE Computer, Vol. 35, No. 10, 2002, pp. 54-62.

[16] Y.C. Hu, A. Perrig, D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless

Networks," Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communication Societies (INFOCOM), San Francisco, USA, 30 March – 3 April 2003, pp. 1976-1986.

[17] K-F. Ssu, W-T. Wang, W-C. Chang, "Detecting Sybil attacks in wireless sensor networks using neighbouring information," Computer Networks, Vol. 53, No. 18, 2009, pp. 3042-3056.

[18] K. Sharma, M.K. Ghose, "Cross layer security framework for wireless sensor networks," International Journal of Security and Its Applications, Vol. 5, No. 1, 2011, pp. 39-52.

[19] N.R. Prasad, M. Alam, "Security framework for wireless sensor networks," Wireless Personal Communications, Vol. 37, No. 3, 2006, pp. 455-469.

[20] K. Grgic, D. Zagar, V. Krizanovic, "Security in IPv6-based Wireless Sensor Network – Precision Agriculture Example", Proceedings of the 12th International Conference on Telecommunications (ConTEL), Zagreb, Croatia, 26-28 June 2013, pp. 79-86.

[21] N. Sklavos, "On the hardware implementation cost of crypto-processors architectures", Information Systems Security, Vol. 19, No. 2, 2010, pp. 53-60.

[22] K. Grgic, "System for malicious node detection in IPv6-based wireless sensor networks", Josip Juraj Strossmayer University of Osijek, Faculty of Electrical Engineering, Osijek, Croatia, PhD Thesis, 2011. (in Croatian)

[23] A. Mitrokotsa, A. Karygiannis, "Intrusion Detection Techniques in Sensor Networks," Wireless Sensor Network Security, pp. 251-272, IOS Press, Amsterdam, 2008.