2011 Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing

# A Resource Perspective To Wireless Sensor Network Security

Venkatesh Kannan
*Assistant Professor,*
*Department of Information Technology, SRM University, Chennai, India.*
*Email: venkateshkannan@gmail.com*

Sahena Ahmed
*M.Tech. Student,*
*Department of Information Technology, SRM University, Chennai, India.*
*Email: ahmed.shaina@gmail.com*

***Abstract*—The challenges thrown by wireless sensor networks (WSNs) are unique given their delicate architecture and scant resources. Even though security for wireless networks has been a widely researched area for many decades, security for WSNs is still a major roadblock for their efficiency and performance. This is due to the tussle of how much resources can be expended for security in proportion to the sensor application. The current security perspective for WSNs is on a per-attack basis, which creates an inflexible model resulting in poor efficiency and scalability. The work presented in this paper is the first step in creating a security framework offering high flexibility, good scalability and a redundancy-free security layer for the WSN protocol stack. The proposed framework is based on a resource perspective when deciding security solutions, where solutions are designed to secure each resource in the WSN environment, rather than defend against attacks. Also discussed in this paper are the advantages and preliminary implementation ideas for the proposed framework.**

***Keywords*-Security framework; wireless sensor network; resource perspective; holistic approach.**

## I. Introduction

Over the years, wireless sensor networks (WSNs) have gained access into a variety of fields. Even though they were primarily envisioned for military and observational purposes in the wild, they are widely used in fields such as health-care, traffic monitoring and many other day-to-day applications. The data that wireless sensor nodes collect, process and aggregate, depending on the application, may be sensitive or otherwise, and hence needs to be secured. Security is not just limited to data protection but also deals with securing the sensor node itself and the WSN as a whole, to ensure information protection, node and network performance and efficiency. In this context, some key ideas have to be summarised.

### A. Limited Resources

The key aspect that necessitates special design and operation considerations for WSNs is the limited availability of resources: *memory, energy, processing power and transmission channel*. The sensor, being a tiny device, has only a small amount of memory and storage space for data and code. Hence it is necessary to limit the code size used for both the sensor operation and security. One of the biggest constraints in a sensor node is the power source. Thus, it is mandatory for applications to be energy efficient, which will extend the life of the sensor node and hence the entire sensor network. Thirdly, despite many advances in processor technology, the processor on a wireless node is an equally big roadblock since it is tied to energy availability in a sensor. Thus limited energy often limits the processor speed and capability on a sensor node. Finally, the wireless transmission medium is more prone to higher error rates, dropped packets, channel access conflicts, and security attacks as compared to wired networks. Thus unreliable communication requires protocols and algorithms to cater to the needs of both network reliability and resource efficiency. [1]

### B. Security Requirements in WSN

Given that in addition to information, the sensor nodes are also valuable, it is essential to have security solutions to protect both commodities in a WSN. Given this, the foremost essential security features for a sensor network are data confidentiality, data integrity, data freshness, availability of sensor nodes, authentication and authorisation. [1]

### C. Need for Efficient Security

These security requirements not only ensure protection of sensitive data but also secure the limited resources in each sensor node that keep the sensor network alive. On the other hand, this needs algorithms to be implemented for the proposed security solutions. Every line of code executed by the sensor, be it for application or security, consumes different degrees of the limited resources available. This drives the need for efficient security solutions that use less resource for providing the required security and make more available for the actual sensor application.

### D. Taxonomy of Security Attacks

A comprehensive listing of layer-wise security attacks is available in [1]. The types of attacks in a WSN can be broadly categorised as follows.

- Physical attacks.
- Privacy attacks.
- Traffic-analysis attacks.

978-0-7695-4372-7/11 $26.00 © 2011 IEEE
DOI 10.1109/IMIS.2011.96

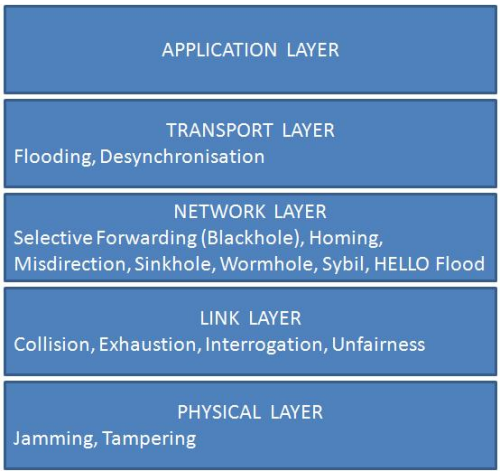


Figure 1. Taxonomy of Attacks

- Routing attacks.
- Denial-of-Service (DoS) attacks.

Attacks from one or more of these types are launched at each protocol layer of a sensor node. For instance, tampering, interference and jamming are attacks on the sensor and signal respectively, at the physical layer. Suggested solutions to these are tamper-proof packaging of the node, and spread-spectrum communication or priority messages or low duty cycle. Attacks at the link-layer include collision, exhaustion, unfairness, and Sybil attack in the form of data aggregation. Solutions in literature for these include error-correction codes, randomised back-off time for retransmission, authentication of client requests, and rate-limitation [1].

A sensor node is prone to attacks at the network layer from misdirection, selective forwarding, flooding, sinkholes, Sybil attack, homing and HELLO flood attack. Authentication of routing updates and nodes, dynamic routing decisions, encryption, authorisation and egress filtering are the security solutions that defend against these attacks [7]. At the transport layer, flooding and desynchronisation aim at launching DoS attacks on sensor nodes. Though limited, the suggested solutions for these attacks are state-less connections, client puzzles and authentication of packets [7] [9].

Given the myriad of attacks, they can however be listed under one of the five categories listed above: tampering being a physical attack on a sensor node; collision, interference, unfairness, exhaustion are attacks on privacy of the control and data messages; attacks on the network layer are achieved mainly by analysing the network traffic and exploiting vulnerable routing protocols. The ultimate aim of these attacks is most often to drain the sensor off its limited resources, which brings down the node and possibly the entire WSN a.k.a. DoS.

### *E. Issue*

From summarising the literature, it is evident that security solutions and defenses against attacks have been primarily based on a protocol layer-wise attack-based approach. This, in ideal conditions, succeeds in preventing and/or detecting intrusions. But the question in the context of a wireless sensor network is *"Is this the efficient solution against security attacks?"*.

More and more literature [2], [3], [6] are generated everyday identifying the reason behind the different attacks and devising solutions. Each proposed solution is based on the protocol layer where the attack is targeted and the vulnerability that allows the attack. This only results in a long list of attacks and an even longer list of proposed solutions, with each solution translated into a security algorithm in a sensor node, consuming precious processor power, memory and energy.

### *F. Goal*

Given the poor scalability of the layer-wise attack-based approach, this paper aims to reevaluate the perspective when designing security solutions: *"Are we fighting attacks?"* or *"Are we securing assets?"*. The latter is the driving question behind the work presented here. The goal here is to analyse the wireless sensor environment and the different attacks possible to identify the key resources (transmission frequency, frame content, memory, MAC parameters, routing information, connection requests are some examples of resources) and extract security objectives (such as encryption, authentication, authorisation and so on) to protect and verify these resources. Solutions for many of these objectives are widely available in the literature. Having done this, it is possible to observe which attacks are prevented by protecting a certain resource. The final aim is to have a single security layer spanning across all the layers of a WSN protocol stack in a sensor node. This security layer will contain a concise set of security algorithms to defend against attacks across multiple layers. Note that this paper focuses on the physical, data-link, network and transport layers of a WSN protocol stack. Application layer security is not currently in the scope of this work.

### *G. Rest of the Paper*

§2 summarises some of the important work related to providing generic security solutions through holistic approaches and security frameworks. §3 presents details of the proposed ideas including identification and analysis of key WSN resources, and building of the security layer. §4 analyses the proposed security layer, its advantages, lackings and future direction of this work. The conclusion in §5 summarises the significance and reason behind this article and work.

## II. Related Work

Recent literature on security framework for wireless sensor networks has a variety of approaches with two goals: separate security component in a sensor node, and flexible security solutions in the component. In relation to these goals some of the recent work are discussed here.

[15] proposes a three-tier security framework by listing the security issues of interest in sensor networks. The levels of security are divided into three classes, small, medium and high level based on the security requirements listed for the type of network. However, this proposal falls short in that each class of sensor network is characterised using security requirements, where assumptions about expected attacks are suggested. This does not discount the vulnerabilities of these networks to the different attacks.

[16] presents an extensible distributed security framework for heterogeneous WSN. In this idea, as new attacks are discovered, security solutions are added to the framework. For the set of attacks possible, the authors suggest a mechanism to choose a subset of solutions that defend against these attacks depending on the weights attached to the attacks. Here again the main drawback is that the approach is clearly described as a one solution per attack framework.

[14] precisely states the problem with the traditional layer-wise attack-based security approach where redundant security solutions use the limited resources inefficiently. As a solution to this, the authors propose a separate security component (Intelligent Security Agent) that communicates with all protocol layers in a sensor node. However, there are two types of problems in this literature. First, the solution depends on clustering the sensor nodes and electing a group head. This creates significant administrative overhead, which includes group head transfer and maintenance. Especially in the case of WSN, this overhead could result in degradation of performance and efficiency. Second, despite modularising the security component, there is no improvement to how security solutions should be designed to reduce redundancy in layer-wise attack-based solutions. The solutions provided here are still on a per attack perspective, where a new attack would result in addition of a solution to the framework.

The formal framework suggested in [17] summarises the characteristics and security requirements of a WSN. However, here again the authors use an ISO/OSI reference model to develop a formal framework to identify security risks and suggest possible countermeasures. The literature also suggests extension of the taxonomy to include missing weaknesses using the layer-wise approach.

To summarise, there are three main issues in the current approaches to designing security for WSN. One, new security components tend to add significant overhead due to administrative and moderation functionalities. This is a serious drawback given the limited resources of a WSN. Two, the security frameworks or modularisation still provides security solutions largely based on a layer-wise attack-based perspective. This does not solve the problem of redundant security solutions. And third, all of the proposed frameworks neglect flexibility by tightly coupling the security solutions with the attacks. Every addition or variation of security risk will need modification to the framework itself, which makes such a design rigid. Rather, a plug-in based approach, where security requirements are listed for each resource leaving the implementation to the user, is a more flexible, scalable and universal design.

## III. Proposed Framework

The work starts by identifying the ***key resources*** in a wireless sensor network. Key resources can be defined as objects that can be exploited actively or passively to launch security attacks on either a sensor node or the network. The key resources identified in this article at the physical, datalink, network and transport layers of the protocol stack are listed in Table I.

### A. Key Resources in WSN

At the physical layer, each *sensor node* itself is resource prone to direct attack by an adversary, apart from the specific *transmission frequency* used by the nodes to communicate information. At the datalink layer, information organised as frames makes the control and data fields (*frame fields*) a valuable source for the attacker. Modification of bits during transmission or by an attacker leads to error in the frame (*frame bits*) rendering it useless. The *channel* used by nodes for communication is critical and can be exploited by an attacker to deteriorate the performance of frame transmission. Nodes at datalink layer *buffer* frames to be sent and those received in their local buffers. Causing an overflow of these buffers could stall the node from further sending or receiving any frames. Finally, the *MAC protocols* used to co-ordinate the channel access and synchronise the sensor nodes can be exploited by the attackers as they are merely protocols suggested for a seamless communication. The attacker can choose to ignore these protocols sending the entire sensor network into chaos at the datalink layer. At the network layer, similar to datalink layer, the *packet fields* (with control and data fields) are valuable sources of information for the attacker. Apart from the packets, an adversary can exploit the *routing updates, algorithms and decisions* of a sensor network to redirect the network traffic aiming at degradation of network performance. *Memory buffers* and the *network links* can be overrun by an attacker who passively or actively floods them with unauthenticated packets. Finally at the transport layer, the *segment fields* are key resources. Also, *connection requests* and *connection state information* can be used to launch attacks such as flooding and desynchronisation at the transport layer.

Table I
SECURITY SOLUTIONS FROM RESOURCE PERSPECTIVE

| | Resources | How to Protect | How to Verify | Attacks Defended |
|---|---|---|---|---|
| PH-L | Communication Frequency | Spread-spectrum, Low-duty Cycle | Jamming Report | Jamming |
| | Sensor Node | Tamper-free Packaging, Hiding | | Tampering |
| DL-L | Frame Bits | MAC, Error-correction Code | Error-detection Code | Collision, Exhaustion, Interrogation, Unfairness |
| | Frame Fields | Encryption, Error-correction Code | Error-detection Code, Authenticate | Collision, Exhaustion, Interrogation, Unfairness |
| | MAC Protocol | Randomise MAC parameters, Small Frames | | Collision, Exhaustion, Unfairness |
| | Channel/Link | Rate-limit Response, Notify Upper Layers | | Interrogation, Unfairness |
| | Memory/Buffer | Rate-limit Response | | Interrogation, Unfairness |
| NW-L | Routing Updates | | Authenticate, Check Freshness, End-to-end Verification, Packet Leashes, Location Verification, Check Bi-directionality | Selective Forwarding, Misdirection, Sinkholes, Wormholes, Sybil Attack, HELLO Flood |
| | Routing Decisions (including Traffic Analysis) | Algorithms resistant to arbitrary configuration, Geographic Forwarding, Dynamic Routing | | Selective Forwarding, Sinkholes, Wormholes, Homing |
| | Routes | Egress Filtering, Multiple Disjoint Paths | | Misdirection, Sinkholes, Flooding, HELLO Flood |
| | Packet Fields | | Authenticate, Check Frames | Homing, Misdirection, Flooding |
| | Memory/Buffer | Limit number of packets accepted, Authentication | | Misdirection, Sinkholes, Flooding |
| TR-L | Segment Fields (connection requests) | | Authenticate, Client Puzzles | Flooding, Desynchronisation |
| | Memory/Buffer | Stateless Connections, Authenticate | | Flooding, Desynchronisation |

### B. Security Solutions for Resources

Having enlisted the valuable resources in a wireless sensor environment, the next step is to secure each resource. The approach is to analyse *"what information does each resource offer that can be exploited by the adversary?"*, *"how can the resource be modified or tampered with?"*, and *"how can the resource be forged?"*. Thus there are at least two methods to secure every resource: *protection* and *verification*. Protecting a resource addresses the security requirements of confidentiality, privacy, unpredictability, fairness and such. Verification of a resource mainly aims at identifying integrity, freshness and authenticity. Thus, securing each resource in a WSN involves providing efficient protection and verification solutions. In existing literature, there are numerous methods available for protection and verification of resources including spread-spectrum, encryption, error detection and correction, authorisation, authentication, dynamic multipath routing, client puzzles, stateless connections and the likes. Table 1 gives a detailed list of protection and verification methods analysed for each resource in this work.

### C. Reducing Redundancy in Security Solutions

The goal and advantage of looking at security requirements from a resource perspective described here is that it is possible to identify redundancies in security solutions. Providing security for a *resource X* could automatically secure *resource Y*. For example protecting the frequency used for communication at the physical layer would inherently move towards preventing collision of frames at the data-link layer. As a result, the number of security solutions required and implemented in WSNs can reduce considerably. This finally boils down to reduced algorithms for the security module, less processing, and efficient use of the limited resources available in a sensor network. Analysing the list of security solutions compiled in Table 1, Fig. 2 shows a list of reduced number of security solutions suggested on a layer-wise basis, which can be implemented to defend against the attacks. Which of these suggested security solutions are implemented is left to the network designer and implementer according to the application type, security requirement and threats. This provides high flexibility to the framework where security

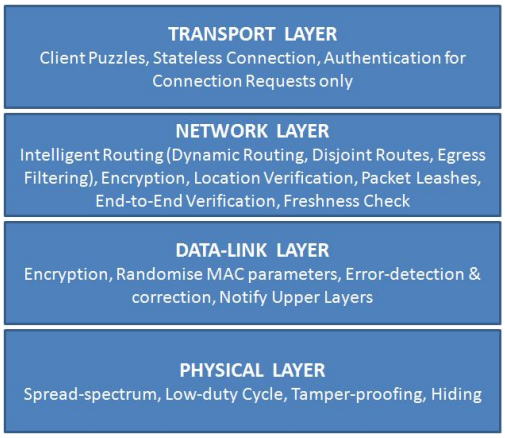


Figure 2. Redundancy-free Layer-wise Security Solutions

solutions are aimed at securing the resources rather than attacks.

### D. Framework for Implementation

The objective of this design is not just to reduce redundancy in security solutions, but also to provide a flexible and scalable framework to support implementation of the security solutions. Fig. 3 shows a protocol stack with the typical physical, data-link, network and transport layers of the ISO/OSI model, supported by a vertical security layer. The proposed security layer will contain implementations of the security solutions listed in Fig. 2. During development, these solutions are implemented to provide the suggested functionalities (for example, encryption algorithms, authentication methods, and so on). This choice gives maximum flexibility to the implementer and supports a plug-in based approach, where different algorithms can be substituted for the same security function required.

## IV. Lessons Learnt and Future Work

The framework proposed allows security solutions to be implemented using proprietary solutions (which could be the choice for corporate or defense applications), or using well known solutions for protection and verification from the literature (such as existing encryption mechanisms, error correction, client puzzles, dynamic routing), which can be provided as library functions in the security framework. The choice is lift to the designer or implementor w.r.t. implementation of security solutions, with the framework providing a list of basic security requirements for each resource.

This proposed idea is also applicable to an application-driven security framework where different levels of security are suggested for different domains (home, office, defense / low-level, medium, high-level). All that is needed is to implement the required security solutions of choice depending on the application domain.

These two major features of the proposed framework from a resource perspective accounts to providing much higher flexibility during implementation and deployment, and improved scalability of the security layer. Scalability is improved because with a comprehensive list of resources in a WSN, the requirement is to provide solutions to secure the resources than defend against the numerous possible attacks of the present and future.

The future course of action from this paper is the development of a software framework implementing the security layer to secure each resource. This framework package will be deployed by users who will insert their own security code into the functions for the security layer. Also, existing security solutions will be implemented and provided as library functions for easy inclusion by the users.

## V. Conclusion

To summarise, this paper is a first step in designing a security framework for wireless sensor networks that is highly flexible, scalable and redundancy-free. Rather than design security solutions through a protocol layer-wise attack-based approach, this work identifies key resources in the wireless sensor network environment, which can be exploited by an adversary to pose different classes of security risks to the network. Thereafter, methods to secure these resources, that is protect and verify, are identified through analysis of literature following which a set of redundancy-free security solutions are proposed for a separate security layer. This builds a framework that allow flexible choices to the implementer to include implementations of security solutions based on application domain, security requirements and threats. Since the solutions are bases on securing resources, a long list of attacks and defenses are avoided. Finally, the directions for continuing this work towards further development and deployment of the proposed framework are also briefly described.

## References

[1] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, *Wireless Sensor Network Security: A Survey*, Security in Distributed, Grid, and Pervasive Computing, Auerbach Publications, CRC Press, 2006.

[2] Chonggang Wang, Mahmoud Daneshmand, Bo Li, and Kazem Sohraby, *A Survey of Transport Protocols for Wireless Sensor Networks*, IEEE Network Magazine Special Issue on Wireless Sensor Networking, 2008.

[3] Levente Buttayán, and László Csik, *Security Analysis of Reliable Transport Layer Protocols for Wireless Sensor Networks*, IEEE Workshop on Sensor Networks and Systems for Pervasive Computing (PerSeNS), Mannheim, Germany, 2010.

[4] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, *Security in Wireless Sensor Networks: Issues and Challenges*, International Conference on Advanced Communication Technology (ICACT), 2006.

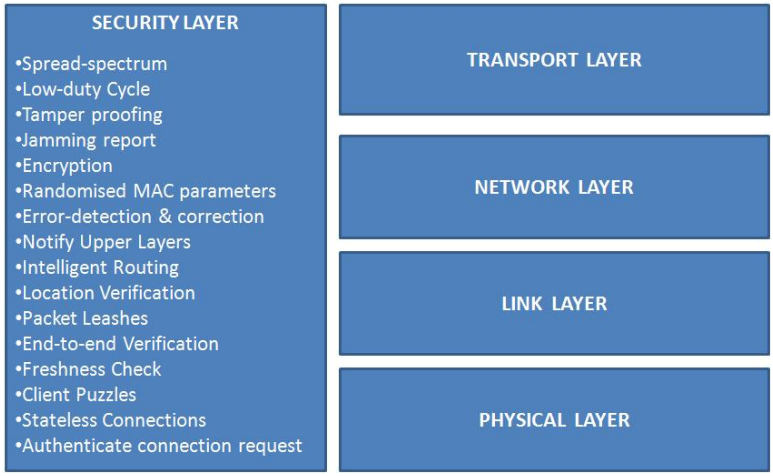


Figure 3. Proposed Security Layer

[5] Hemanta Kumar Kalita, and Avijit Kar, *Wireless Sensor Network Security Analysis*, International Journal of Next-Generation Networks (IJNGN), Vol.1, No.1, December 2009.

[6] David Boyle, and Thomas Newe, *Securing Wireless Sensor Networks: Security Architectures*, Journal of Networks, Vol. 3, No. 1, January 2008.

[7] Anthony D. Wood, and John A. Stankovic, *A Taxonomy of Denial-of-Service Attacks in Wireless Sensor Networks*, Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, 2004.

[8] Tanya Roosta, Shiuhpyng Shieh, and Shankar Sastry, *Taxonomy of Security Attacks in Sensor Networks and Countermeasures*, IEEE International Conference on System Integration and Reliability Improvements, 2006.

[9] Anthony D. Woods, and John A. Stankovic, *Denial of Service in Sensor Networks*, IEEE Computer Magazine, October 2002.

[10] Sasikanth Avancha, *A Holistic Approach to Secure Sensor Networks*, Doctor of Philosophy Dissertation, Department of Computer Science, University of Maryland, USA, 2005.

[11] Adrian Perrig, John Stankovic, and David Wagner, *Security in Wireless Sensor Networks*, Communications of the ACM, Vol. 47, No. 6, June 2004.

[12] Siebe Datema, *A Case Study of Wireless Sensor Network Attacks*, Master's Thesis in Computer Science, TU Delft, The Netherlands, 2005.

[13] Tanveer Ahmad Zia, *A Security Framework for Wireless Sensor Networks*, Doctor of Philosophy Dissertation, School of Information Technologies, University of Sydney, 2008.

[14] Kalpana Sharma, M. K. Ghose, and Kuldeep, *Complete Security Framework for Wireless Sensor Networks*, International Journal of Computer Science and Information Security, Vol. 3, No. 1, 2009.

[15] Neeli R. Prasad, and Mahbubul Alam, *Security Framework for Wireless Sensor Networks*, Wireless Personal Communications (2006), Springer 2006.

[16] Himali Saxena, Chunyu Ai, Marco Valero, Yingshu Li, and Raheem Beyah, *DSF - A Distributed Security Framework for Heterogenous Wireless Sensor Networks*, Proceedings of IEEE Military Communications Conference (MILCOM), 2010.

[17] A. A. E. Kalam, A. Atzeni, A. Cappadonia, E. Cesena, S. F.-Hübner, S. Kindskog, L. A. Martucci, and C. Pastrone, *Toward a Formal Framework to Evaluate Wireless Sensor Networks Security*, NEWCOM++, ACoRN Joint Workshop, 2009.

[18] Kalpana Sharma, and M. K. Ghose, *Cross Layer Security Framework for Wireless Sensor Networks*, International Journal of Security and Its Applications, Vol. 5, No. 1, 2011.

[19] Kui Ren, *Communication Security in Wireless Sensor Networks*, Doctor of Philisop