
Ethiopia Nigussie, Antti Hakkala, Seppo Virtanen and Jouni Isoaho
Department of Information Technology
University of Turku
20014 Turku, Finland
email: {ethnig,ajahak,seppo,virtanen,jisoaho}@utu.fi

Abstract—We present a work in progress of an adaptive security management scheme for wireless sensor networks. The unique characteristics of these networks place great demands on their design and operation in terms of resource and security management. Resource and security adaptability achieved through self- and context-awareness will take the feasibility of the networks to a new level. The scheme has self- and context-awareness in addition to a holistic view of security services at each layer of the communication stack. It uses distributed agents and intrusion detection systems to monitor the security threats and then dynamically adapts its security level by jointly considering several dimensions. This translates into optimal security-energy under a given resource and context. The key dimensions are energy budget, computing power and memory size of nodes, location-based security threat levels, data coherence, and data lifetime. Trust management is used to test the integrity of untrusted nodes which further assist the adaptation decision.

I. INTRODUCTION

Wireless sensor networks (WSNs) are proliferating into our everyday life in the form of different applications, such as eHealth [1] [2], home automation [3], and agriculture [4]. In the future, WSNs will be deployed on large scale globally. Millions of wireless nodes will cooperate to gather crucial data and many of those tiny nodes will have a connection with the Internet to establish the future internet-of-things (IoT). In such an environment, providing efficient security and privacy is crucial. Existing security mechanisms are still in their early stages and the level of security they provide is not satisfactory for many applications. In addition, most of the approaches are designed to defend against a specific attack or to provide security for a specific layer, such as routing attack [5], denial of service attack [6], data link [7], and network [8] layer security. The problem with this approach is that the solution for one specific attack does not defend against another type of attack and one cannot know a priori what type of attack one encounters. In addition, these specific defense schemes cannot be simply combined on the node to provide a complete solution because of resource constraints. WSNs differ in many aspects from traditional fixed networks and standard cryptographic solutions cannot be used in this environment due to their requirement of powerful processing capacity. Due to the role of low-power wireless networks as sensing and actuating systems, any disturbances in such a network may have consequences in the real world. Achieving security in such networks is challenging since they face multiple threats that may easily hinder their functionality and nullify the benefits. Depending on application types the required security level varies considerably. For instance, in body area sensor networks the highest possible security is required because tampering with the body sensors may lead to fatality. Home automation sensor networks, which improve the quality of life for individuals through the automation of household devices, require a high level of security so that users are able to have secure remote access and privacy. The nodes in such networks are highly constrained in terms of computational power, memory, bandwidth and energy resources. Thus, security mechanisms should have awareness to the available resources.

WSNs often operate unattended and due to this they are exposed to attacks and failures. A satisfactory level of security must be ensured for such networks and many issues should be considered while designing security solutions. The level of security required for the network depends on security threats, application characteristics, runtime conditions, environment and available resources. Some of these factors change over time which creates a need for adaptive security. Therefore, in this work we present the preliminary system level design of an adaptive security management scheme which has a holistic view of available resources, network state and application requirements. The proposed security scheme relies on monitoring of resource usage and security threats, and uses detection components along with its self- and context- awareness capabilities to make reconfiguration decisions that ultimately make the security solution self-adaptive and optimal.

II. ASWiN: MULTIDIMENSIONAL ADAPTIVE SECURITY

The level of security required for WSN depends on security threats, application requirements, runtime conditions, environment and available resources. Some of these factors change over time which creates a need for adaptive security. An increase in the security level leads to stronger security but also causes an increase in resource depletion. Due to resource constraints, security solutions should balance security and resource usages and to do so, monitoring of resource usage and security threats are necessary. In the proposed adaptive security management, ASWiN, resource usage and security threats are monitored through self- and context-aware implementations, and based on the monitored results reconfiguration of protocols and components are carried out, ultimately leading to self-adaptation (see Figure 1). The main motivation for this is to achieve optimal security-energy balance which extends the lifetime of WSN.

Static security strategies may result in unnecessary waste of resources, especially energy because they are designed for
worst-case security breach scenarios. The optimal security level at a given point in time depends on several parameters, which we will call *security dimensions* in the remainder of this paper. In ASWiN, we determine all possible security dimensions and formulate the relationships between dimensions and security levels so that we can model the adaptability.

A. Dimensions in Autonomous Decision-Making

We can identify the following metrics as dimensions that must be taken into account when making decisions about the general security level of a WSN. All of these dimensions form a complex decision space, which defines the ultimate behavior of a node in a network.

Energy as a decision dimension concerns the amount of power left in a sensor node. It affects the node’s capability to function, its choices of cryptographic algorithms for a particular operating environment, and its ability to transmit messages to other nodes. If a node has sufficient energy reserves, it can use more robust methods of encryption, can transmit security related messages more often, and in general can operate normally. If a node has low energy reserves, it must be able to use them for maximum impact on the situation. If energy is scarce, the node must fall back on more lightweight encryption settings, and must conserve power by minimizing message exchanges as transmission/reception is the major source of power consumption. Energy is generally the most important dimension in WSNs, as it affects all functions in a network.

Processing capacity is the dimension of actual processing capability available to the network and to a single node. As WSN nodes are limited in computation capacity, this is one of the critical dimensions regarding security, as it has ramifications on cryptography algorithm selection. Memory capacity describes the physical RAM and ROM capacities of a network node. As the memory capacity of nodes is usually limited, this dimension has a significant impact on security, as security features require memory in addition to processing capacity.

Data coherence is the situational impact of the processed data. High coherence data has an immediate impact on the present situation, signifying that it is time-critical for handling. Low coherence data can be processed or transmitted later, if other circumstances warrant saving energy or other resources. 

Data lifetime - All data has an effective lifetime. Within its lifetime, the data has relevance and meaning, but when it expires, it has no value, is outdated or incorrect and generally of low priority. Assessing the effective lifetime of a particular piece of data is a complex task, so for a self-aware system, this must be streamlined and simplified for it to be feasible. Data lifetime is related to data coherence, but is still a separate dimension.

Location security level defines the security rating of a network or node location. A straightforward division of security levels can be achieved by defining three different security ratings for an environment: friendly, neutral and hostile. In a friendly environment, the presence of unauthorized or hostile nodes is negligible, and the physical space is assumed to be in the control of known actors. A neutral environment can be likened to a public space where there are unknown actors present, the space is not controlled by known parties, and the presence of hostile parties is possible but unlikely. In a hostile environment, we must assume that there are active malicious entities operating in the environment and the environment itself is under the control of hostile parties. If a particular location is classified as hostile environment, then the node must adjust its encryption settings and power consumption accordingly. This sets the baseline security level for a certain environment. It can be modified by active observations from an IDS/IPS and trust management systems. Mobility becomes a factor if nodes have the capability to physically change locations. It has an impact on network topology, routing and location security levels.

B. Monitoring and Reconfiguration

Monitoring of dimensions, environment changes and security attacks are the first step towards developing an adaptive security strategy. In ASWiN, monitoring is performed using distributed agents which cooperate each other. There are three types of agents: application, intermediary and physical layer agents as can be seen in Figure 2. The application layer agent monitors data lifetime, data coherence, node location and mobility. It also communicates with intermediary agents to share relevant detected events. The intermediary agents monitor transport, network and data link layer activities to provide better security for core protocols and network services. The monitoring agents at transport layer help to prevent the forgery of transport control packets, for example, acknowledgments (ACK) and negative acknowledgments (NACK). The prevention of ACK forgery ensures that the attacker cannot generate a valid ACK for a valid packet that has not been received by the destination, and hence, the loss of a valid packet can be detected by not receiving an ACK for it. The prevention of NACK forgery ensures that the attacker cannot inject NACKs that would trigger the unnecessary retransmission of the corresponding valid data packets. Repetitive retransmissions deplete nodes energy. The intermediary agents also monitor the network layer to prevent security attacks on time synchronization, routing and data aggregation protocols. The physical layer agent monitors the power consumption rate and the remaining energy. This helps to decide which security level is most appropriate from the energy saving point of view.

Fig. 1. Monitoring, decision-making and reconfiguration process in ASWiN
in order to function well until the end of the network’s intended lifetime.

ASWiN has an Intrusion Detection System (IDS) to monitor security attacks. If an IDS detects misbehaving or malicious nodes, it informs the neighboring nodes and decision-making components so that proper countermeasures are taken. We assumed a reconfigurable IDS architecture which is able to detect many attacks at a time and integrate different detection and control modules. ASWiN also has a Key Management System (KMS), which provides cryptographic keys in a secure manner. When IDS detects a compromised node, it informs the KMS. The KMS then revokes the secret key of the compromised node and generates and distributes new keys to the associated nodes except the compromised one. The KMS maintains not only forward and backward secrecy, but also collusion resistance between the newly joined nodes and the compromised ones. In addition, the KMS manages key length based on the command it gets from the decision-making component. Another management component of ASWiN is the Trust management system (TMS), which is useful in assisting the decision-making process. The TMS is used for integrity testing of an untrusted node. It also gives feedback to KMS in the key revoking process. The IDS also uses the TMS output in order to make a better decision. The interaction between these three systems, monitoring agents and decision-making component is shown in Figure 3. Security level reconfiguration decisions are performed based on monitored events of distributed agents and the IDS along with feedback from TMS.

C. Security Level

The security level of a network defines what security features are used on the network, and which settings are used for these features. A simple implementation of security levels is to use a five step security classification with escalating security features. On the lowest level, encryption and authentication are turned off for the network, as they are not required in a friendly operating environment. On the highest level, strong encryption and authentication is used for maximum security. The intermediary layers use lightweight and fast algorithms to provide an optimal trade-off between performance and security. Defining the actual algorithms and their versions is an essential part of analyzing the potential application and its requirements. Applications can range from simple monitoring of a peaceful environment to time-critical monitoring functions in a hospital and military applications with hostile activity directed against the WSN. The initial requirements are derived from the assessment of the target application, but they can be dynamically changed when necessary.

III. MODELING AND ADAPTATION IN ASWiN

The aim of ASWiN is to reconfigure and adapt the provided security level based on the monitored information so that optimal security-energy balance is achieved. In order to make the security level decision, the relationship between a security dimension and decision thresholds has to be formulated. The reconfiguration and adaptation steps are also discussed in this section.

A. Modeling Security Dimensions and Decision Thresholds

First we must find a way to represent the dimensions defined in Section II-A formally, so that we can make decisions in the defined decision space. We can treat the dimensions as a 7-dimensional space, but in this case it is more prudent to demonstrate the concept with a smaller number of dimensions. The problem of modeling and defining exact relationships between the dimensions is left as future work and is out of the scope of this paper. We first reduce the amount of decision dimensions from 7 to 4 with logically grouping related dimensions together. Energy, being the most important dimension regarding WSNs, is left as a single dimension. All possible interactions between these compound dimensions are shown in Fig. 4. Depending on the application characteristics, network type and state, one interaction has more importance than the others. For example, in application where WSN is static and operate in safe indoor environment, the security level adaptability decision relies on interaction “8” than “15”. The security management scheme has awareness of the interactions priority on variety of situations and based on this awareness it carries out appropriate adaptation measures.

All dimensions have a base score representing the significance of that dimension \((d_j)\), and a weight factor \((w_j)\), where \(j\) represents dimension type. The scores are initially set according to the needs of the application, forming the baseline metric for the dimension relevance. The overall security rating is thus described by the 4-tuple

\[
(\alpha, \beta, \gamma, \delta) = \left( d_\text{me} w_\text{e} + d_\text{proc} w_\text{proc}, \frac{w_\text{me} + w_\text{proc}}{w_\text{me} + w_\text{proc}}, \frac{d_\text{co} w_\text{co} + d_\text{li} w_\text{li}}{w_\text{co} + w_\text{li}} \right)
\]

where \((\alpha, \beta, \gamma, \delta) \in [0,100]\). The compound dimensions are represented by weighted averages of the original dimensions.

Now, we can define for each dimension a set of \(i\) thresholds \(T_{\text{dim}}\), which partition the decision space according to the specifications from the application. The dimension score is

Fig. 2. Formulation of security level and dimensions relationship

Fig. 3. Interaction of monitoring, detection and management components
matched against these thresholds, and when a threshold is crossed, the self-aware system changes the security parameters of the system to adapt to the detected change in the operating environment. We set the thresholds for all dimensions as $T^i_{dim} \in \{10, 30, 50, 70, 90\}$, where $i$ corresponds to security levels 1 through 5. The base dimension score is assigned by the administrator as a starting point, and the system adapts to changes in its environment by adjusting the weights of dimensions. If any of the threshold values for dimensions is crossed, the system then analyzes whether changes in the security level are required.

B. Reconfiguration and Adaptation Process

The decision-making subsystem receives feedbacks from monitoring agents and IDS/TMS whenever they detect events which require adjustment of the dimension space and/or reconfiguration of current security level. To avoid unnecessary power draining communication, the monitoring agents and IDS/TMS communicate with the decision making component only vital events since they are designed to have intelligence to identify and categorize events. Upon receiving feedback, the decision-making component sends commands to adjust weights of the dimensions depending on the detected event, the importance of the current dimensions interaction space, application parameters and state of the network. After adjustment, checking of whether the dimension threshold is crossed is performed and if it is crossed, security level reconfiguration is carried out. At each security level, different security mechanisms and cryptographic primitives are integrated with a possibility of modifying parameters (such as key length and authentication code length) for fine-grained adaptability. As discussed in III-A, ASWiN has five security levels and the higher the security level is the stronger the provided protection. The reconfiguration of security levels continues until optimal security-energy balance is achieved. The overall process is shown in Fig. 5.

IV. CONCLUSION

We presented the preliminary system level design of an adaptive security management scheme for WSNs. Static security services cause unnecessary overhead since they are designed for worst-case security violation scenarios. Through continuous monitoring of the environment, the available resources, changes in application parameters and security threats, the security levels are adjusted in order to save energy without compromising the provided security. The presented adaptive security management scheme uses distributed agents and intrusion detection systems for monitoring and based on the monitored information it reconfigured the security components and protocols to dynamically adapt the security level by jointly considering several security dimensions. It also uses a trust management system to further improve the accuracy of its adaptation decisions. The tasks of monitoring agents at each communication layer stacks were presented along with interaction between monitoring agents, intrusion detection, key management and trust management systems. In addition, the relationships between security dimensions and decision thresholds were formulated by using compound dimension metrics. The steps of reconfiguration and adaptation processes were also discussed.

REFERENCES


