A Policy based Security Management Architecture for Sensor Networks

Sérgio de Oliveira, Thiago Rodrigues de Oliveira, José Marcos Nogueira
{sergiool, thiagool, jmarcos}@dcc.ufmg.br
Computer Science Department, Federal University of Minas Gerais
Av. Antônio Carlos, 6627, Belo Horizonte, MG Brazil

Abstract—Wireless sensor networks are subjected to several types of attacks specially attacks of denial of service types (DoS). Several mechanisms and techniques were proposed to provide security to wireless sensor networks, like cryptographic process, key management protocols, intrusion detection systems, node revocation schemas, secure routing, and secure data fusion. A recent work proposes a security management framework to dynamically configure and reconfigure security components in sensor networks according to management information collected by sensor nodes and sent to decision-maker management entities. It turns on or off security components only when they are necessary. Turning off security components save power and extend network lifetime. The architecture is policy based, what enable rules configuration specific for each application. We evaluate that security management framework, showing possibilities to save power and how that work can contribute to extend network lifetime. We propose some scenarios to evaluate the performance of the security management framework and estimate the cost of security components, security management.

Index Terms—Sensor networks, security management, policy based management

I. INTRODUCTION

Wireless sensor networks (WSN) can become target of security attacks, and a few factors make them more vulnerable to enemy action than conventional networks, such as limited computer resources, hostile operational environments, and wireless communication. Several types of attacks can happen to WSNs, such as eavesdropping, false packet injection, and denial of service, among others.

Several works in literature propose security approaches to sensor networks to avoid effects of the presence of enemies in the network. However, each security solution adds a cost to the operation of the network. Operations or activities like processing and communications dispense energy and time and wireless sensor networks must save energy to extend its lifetime because it is unfeasible to recharge the battery, at least in the kind of sensor networks we are dealing with.

A common requirement of most solutions for sensor network is the increasing of network availability. Energy saving is one main target to extend availability by extending network lifetime. However, security problems can be found, especially denial of service attacks, which limit the services provided by the network before the exhaustion of the batteries of the sensor nodes.

Network management techniques, which aim to make possible efficient and optimized operation of networks, can be applied to sensor networks to improve the usage of resources in general. Extending the lifetime of a sensor network is a common requirement that can take profit of network management techniques. Density control is an example of such a network management service used to extend lifetime in Manna, a network management framework for sensor networks [12]. As management run in autonomic way, it is called self-management, and is performed without human intervention. In sensor networks, network management is essential to guarantee rational use of all resources. Network management functions can setup and turn on or off all components to keep better energy consumption.

A security management system can act in a network in the same way, for example, turning on or off security services and functions just when the network presents such a demand. Thus, network can save energy when there is no indication or suspicion of intruder presence. Intrusion detection systems can alert the network about intruder by generating and reporting events. In autonomic management mode, the management system can automatically activate or deactivate security systems in network.

Our recent work [17] proposes a security management model for wireless sensor networks, including security components selection, management information description, messages description, and security events definition. In autonomic mode, security component are grouped into levels, which can be set up in answer to intruder detection events. The objective is to extend the network lifetime by avoiding the effect of attacks and saving energy by the activation of security services only when necessary. The main goal was to protect the network against DoS attacks to maintain network availability. The second goal is to maintain the low energy consumption. Security components protect the network. Security management control energy consumption, turning on security components only when is necessary.

The main contribution of this work is the proposition of architecture for security management that provides dynamic activation and deactivation of security components in response to situation of security attacks. The objective of such architecture is two-fold: for one side, to protect the sensor network from diversity of attacks; for other side, to consume the minimum possible resources given a certain situation of attacks.

Just to enable specific configuration to each application, the architecture is policy based set up. Thus, conditions based in event, and action, like security level changing can be specified.

This proposed management architecture is evaluated in
terms of its functionality, efficacy and energy saving. We
detail the consumption of each security component added to
network and verify the consequences of activation or
deactivation of each solution over the energy consumption.
The rest of this paper is organized as follows. Section 2
presents related works. Section 3 presents the management
and network model used. Section 4 presents the evaluation in
terms of energy consumption. Section 5 presents results of
simulation for integrated levels. Finally, section 6 presents
conclusion and future works.

II. RELATED WORKS

There are few works about management of sensor networks.
Savola and Uusitalo [14] present security management
principles to ad hoc networks, which poses different
challenges for security than sensor networks do. The main
problem in ad hoc networks is the lack of a central trust
administration. Sensor networks, by this turn, don’t have this
kind of problem, although they present more energy and
hardware constraints.

Dimitriou and Krontiris present [19] an overview of current
research challenges on sensor networks security, highlighting
their autonomic communication aspects. They present issues
in sensor network security research: key establishment and
initial trust setup, resilience to denial of service attacks,
resilience to node compromises, routing security, location
aware security, data fusion security, and efficient
cryptography primitives. From the discussion, they show how
autonomic communication behavior offers opportunities to
increase security in sensor networks. This work summarizes
these autonomic characteristics: self-configuration, self-
awareness, self-healing, self-organization and self-
optimization, and discusses what is needed in order to provide
an integrated and complete solution for sensor networks
security.

Song et al [11] propose an element that acts as a mediator
between Universal Plug and Play (UPnP) networks and sensor
networks. This element, called BOSS (Bridge of the sensors),
is an UPnP agent implemented in base station and lies
between the UPnP controllers and non-UPnP sensor nodes to
be managed. The objective is accomplishing easy deployment
of sensor network services and provides zero-configuration
sensor networking.

In Manna [12], policies describe desired behavior of
management components, like agent and manager. Manna
framework considers a three-dimensional management
architecture, which consists of functional areas, management
levels and WSN functionalities. These dimensions are
specified for the management of a WSN and are the basis for a
list of management functions. Manna includes a management
protocol called MannaNMP that describes the services
provided and the format of the messages, as well as a
management information base.

This work extends Manna network management framework
for sensor network, which is based on the paradigm of self-
management, which are the automatic functions and services
of management using a minimum of human interference.

In a previous paper [17], we propose the base of this work
with security model and components. This work differs of that
by results and conclusions.

III. NETWORK MANAGEMENT MODEL

The reference network in this work is a flat homogeneous
network, meaning that all nodes present the same hardware
characteristics and execute the same functions, especially
routing and forwarding functions. A typical network is
composed by a few tens up to hundreds nodes, which are
uniformly distributed over the network area, like a beehive.
Each node has exactly six equidistant neighbors reachable by
its radio. Nodes in low density networks spend less energy
than the ones in high density networks, because the radio
spend energy to receive and a node need to keep its radio
turned on more time to receive more packets if it has more
neighbors. As more neighbors, more time is needed to receive
all their packages. The reference node is Mica2 Motes [6].
This kind of node spends few miliamperes to send and receive
data for distances about tens of meters, which is enough for a
node to reach the neighbors in our model.

The behavior of the network is defined considering the
requirement of minimum energy consumption as possible. The
operation cycle consists of phases sensing, transmission,
reception, data forwarding, and sleeping. Periodically, a node
sense its environment, transmits, receives, and forward data; to
save power, it goes to sleep between sensing operations. The
time spent in sensing, transmitting, receiving and forwarding
data is too short comparing to the whole cycle time that a node
can enter in a sleeping state in idle interval, thus saving power.
The nodes must be synchronized to sleep and wake up
together. Following this behavior model, for the kind of nodes
above mentioned and for a class of application in which the
time distance between two consecutive sense operations is
large compared to the busy time of the node, a single battery
can be used up to one year without recharges or replacements,
attending sensor networks requirements [7].

A. Management Architecture

Our previous work defines security components, security
levels grouping some components, MIB, messages and events.
The management model of this work follows the general
guidelines of the Manna framework [12]. In our work, we
propose extensions to MannaNMP to include security. The
management model, presented in the following, is composed of
a management information base, exchanged messages, and
events. Figure 1 shows networks elements and components.
The base station runs the manager that communicates with
node’s agent. Both, manager and agent must know the MIB.

The model considers that the security components above
described can be part of instances of the management. In this
way, configuration of security components is dynamic, what
means that they can be included, excluded, activated, and
deactivated in operation time.
B. Security Components

There are many techniques, algorithms or strategies to deal with security problems reported in the literature and applied to wireless networks in general and to wireless sensor networks in particular. To support the proposal and validation of the management architecture, a set of security resources was chosen. This set is not complete, but represents well the security resources that can usually be used. So, for data security and integrity, cryptographic services are considered, including both hop-by-hop and end-to-end cryptography, as well the necessary key management techniques. To increase network availability, we chosen intruder detection mechanism to find security problems sources and a revocation schema to avoid them; secure routing mechanisms, and secure data fusion to guarantee data delivery to base station.

- **Cryptographic primitives**: Encryption and signature are used to give privacy, integrity and authentication. These processes can be done hop-by-hop or end-to-end modes. TinySec [4], a cryptography implementation for sensor networks were chose for this work. TinySec is a fully implemented link layer security architecture based on Tiny OS, an operational system for wireless sensor networks. TinySec specifies cryptographic methods to sign and encrypt link layer messages, providing authentication and privacy properties to sensor networks.

- **Key management**: As solution to key establishment, we chose SPINS for end-to-end cryptography and NEKAP for hop-by-hop cryptography. These approaches are chosen because they have lower energy consumption to established and are deterministic approaches, allowing all link communications.

- **Intrusion detection systems and revocation schemas**: Intrusion detection in WSN must have much more different approaches than those for conventional networks, due to differences in models, attacks and resources. Two types of approaches are used for intrusion detection in this: a centralized [16] and a decentralized [1][9]. In the centralized approach, the base station is responsible for detecting intruders, starting the process from the information collected from the network. In the decentralized approach, some

C. Security Levels

In case of networks with low energy consumption requirement, as is the case for the sensor network considered in this work, the devised strategy for the operation of the network is to use each security component only when it is needed. The criteria to conclude about the necessity to use a specific component are based on evidence of intruders. If, for instance, a certain amount of intruders is detected in the network, some of the components are made active (or turn on) for all nodes. If there is a change in the amount of intruders, the set of active components can be changed. Certain functions or services of the network can make difficult or even impede the operation of some kind of security components. In such a case, these services must be changed or deactivated to allow the proper operation of security functions.

<table>
<thead>
<tr>
<th>Level</th>
<th>Security components used</th>
</tr>
</thead>
</table>
| Low     | - No intruder detection in nodes  
|         | - No cryptography  
|         | - Data fusion enabled                                                                     |
| Medium  | - 17% of nodes execute intruders detection  
|         | - Routing update authenticated end-to-end  
|         | - Hop-by-hop cryptography enabled  
|         | - Data fusion enabled                                                                     |
| High    | - 33% of nodes execute intruders detection  
|         | - End-to-end cryptography enabled  
|         | - Routing update authenticated hop-by-hop  
|         | - Alternative routes                                                                      |
| Critical| - 50% of nodes execute intruders detection  
|         | - No data fusion                                                                         |
|         | - End-to-end and hop-by-hop cryptography enabled  
|         | - Routing update authenticated hop-by-hop  
|         | - Alternative routes                                                                      |

In a first approach, in this work, security components are grouped to be activated or deactivated together after the occurrence of specific events. This leads to different modes of operation of the network, called security levels, which make easier autonomic decisions by the manager based on received events from the nodes. In each security level, a subset of the security components is turned on to protect the network against detected intruders. The network can switch to a higher security level in case of intruder’s evidence and, conversely
can switch to a lower security level in case of disappearance or reduction of the thread or even in cases of critical energy levels; to save power, security components, like intruder detection systems, can be turned off.

Security components were grouped according their power consumption. In the first or lowest level, no security component is enabled and data fusion is enabled to reduce network energy consumption.

In the medium level, components were chosen to allow in-networking processing functions, especially data fusion. Data Fusion reduce network communication and represents a great power saving. Thus, security components chosen don’t interfere in network operation. Other components turned on in this level, intrusion detection in nodes and alternative routes, are solutions to increase intruder resiliency and intrusion detection. Intrusion detection in nodes is turned on in 17% of nodes. As all neighborhoods have six nodes, with 17% of nodes with intrusion detection, it has a node with IDS in each neighborhood. Route update messages are authenticated end-to-end. These messages are broadcasted and its authentication enable avoid presence of a false base station.

In the high level, end-to-end cryptography prevents in-network processing. Thus, data fusion can’t be used. Energy consumption increases without data fusion due to increasing of network communication. In-network processing is vulnerability because intermediate nodes, not trusted, have access to data processed and they can adulterate or drop them. Moreover, intruder detection mechanisms, like watchdog, work better without data fusion.

Intrusion detection in nodes increases to 34% of nodes. Thus, there are two IDS nodes in each neighborhood. Just to decide if an intruder detection event is true, base station can evaluate if it was detected by two IDS nodes.

In critical level all security components presented here are activated, including hop-by-hop and end-to-end cryptography. In this level, it is considered that intruder nodes know some network keys. Thus, redundant cryptography, end-to-end, and hop-by-hop are used. In this level, an intruder must know several keys to access network messages. Cryptography includes encryption and signature. Intrusion detection in nodes increases to 50% of nodes. Thus, all neighborhoods have three IDS nodes.

D. Policies Definition

Several distinct applications are proposed to sensor network. Each application has specific security requirements and power limitations. Just to enable specific configuration of conditions and actions in security management, we propose a policy based management architecture. A policy based management system allows definition of rules in the form “condition-action”.

Several conditions can start levels transition, based in production map, intruder detection event, in energy map or other signal of irregular presence in network. Each application must be able to specify conditions important for it. We propose the use of policies to specify these conditions for each application.

Security management policies rules can define:

- Conditions to level transition;
- Network groups, just to enable different security levels in groups of nodes;
- What nodes must run IDS;
- Actions took in each event.

The rules must be defined in base station, where manager run. Manager read rules and take actions based in events receive by node agents.

The most important rules must specify conditions to level transition. They can include:

- Significant lost in production map;
- Intruder detection in a node;
- Reinforcement of a intruder detection by other node;
- Intruder detection by base station;
- Energy down in some nodes or region;
- Nodes without production.

Each application must specify its policies attending its requirements. Some examples of policies:

- Security level must increase when X intruders’ events are received;
- Security level must decrease after X seconds without intruders detection events;
- Security level must decrease to 4, if upper, when battery is lower than X%;
- Security level must decrease to 3, if upper, when battery is lower than X%;
- Security level must decrease to 2, if upper, when battery is lower than X%;
- Security level must decrease to 1, if upper, when battery is lower than X%;

There are some policy languages in literature, like Ponder [20], CIM-SPL[22], and Rei [21], a specific language for pervasive computing. A subset of Ponder can be used to specify our policies.

E. Management Operations

Following MANNA model, this work use messages GET, SET and TRAP.

During installation phase, nodes must send a ROUTING TRAP, with information about routing tree. This information is important to intruder detection in base station. Base station sends a SET message to change network security level, when this operation is demanded. This message can be send in broadcast or multicast, to change security level in a group of nodes.

Nodes use IDS TRAP messages to inform base station about intruder detection. It can use a TRAP to inform other abnormal conditions, like low battery. The traps are received in the base station manager and it takes decisions about turn on or off security components based in defined policies.

IV. Evaluation

There are three strategies about security solutions in WSN: Without security solutions, with some security solution all the time, even if there is no intruder in network, or use a security management framework to balance security solutions and power consumption, as proposed in this work. The first strategy, without security solutions, can be good for closed networks, avoided enemy presence in any way. But, in most
common applications, an enemy presence must be considered. Thus, we have to evaluate differences between power consumption of other strategies, with security solutions all the time or with security management.

The objective of this evaluation is compare power consumption of two other strategies, showing how much energy can be saved with security management.

A. Simulation Model

We realized a set of simulations to validate the management model presented here. In these simulations, we are interested in verify energy consumption by each security component. We used a simulator based in discrete events, developed at DCC-UFGM by Martins et al [13].

Each simulation operates 1890 sec, about 30 min. In this period, 135 sensing operations are realized by each node. Three route update phase are executed, one in the starting and others after each 45 sensing operations. Theses value was chose due to several causes: it presents significant energy consumption, it allows node revocation and route update, it can be executed in real nodes in a short time.

As packet format we considered: 10 bytes for data, 7 bytes for TinyOS header and 16 bytes for preamble, with 33 bytes in total. The radio in transmit mode spend 12 mA and 8 mA in receive mode. Using 38400 baud, the time for a bit is 26 µsec. These values correspond to Mica2 Motes [6].

Sensor node also spent energy with sensing, 5mA, and processing, 6 mA, in full operation mode. Following a model available at Crossbow [7], we consider sensor board and processor turned on during time to send and receive all messages in a cycle operation. Thus, total energy consumption during transmission is 12 mA (radio) + 5mA (sensor) + 6 mA (processor) = 23 mA; and 8 mA (radio) + 5mA (sensor) + 6 mA (processor) = 19 mA during receiving. Thus, for transmit one packet with 33 bytes, using 38400 baud, the node spend about 43.9 x 10-6 mAh, and to receive one packet, about 36.3 x 10-6 mAh.

TABLE 2 - Energy consumption in network without security components

<table>
<thead>
<tr>
<th>Number of nodes</th>
<th>Total transmitted packets</th>
<th>Total received packets</th>
<th>Average spent energy per node (mAh x 10^-5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>16229</td>
<td>112170</td>
<td>110.27</td>
</tr>
<tr>
<td>100</td>
<td>42379</td>
<td>298276</td>
<td>146.33</td>
</tr>
<tr>
<td>200</td>
<td>112592</td>
<td>798710</td>
<td>195.75</td>
</tr>
<tr>
<td>400</td>
<td>308612</td>
<td>2186616</td>
<td>267.99</td>
</tr>
<tr>
<td>600</td>
<td>566560</td>
<td>4022888</td>
<td>328.74</td>
</tr>
<tr>
<td>800</td>
<td>817687</td>
<td>5802845</td>
<td>355.53</td>
</tr>
<tr>
<td>1000</td>
<td>1162417</td>
<td>8238595</td>
<td>403.87</td>
</tr>
</tbody>
</table>

The base case has data fusion enabled in the first hop to decrease energy consumption. The TABLE 2 show average energy consumption in basic reference network without any security components.

This paper evaluates the energy consumption increasing by security components, used in the management security model.

B. Evaluation of Components

Security components spend energy in their configuration and operation. We will list the security components and their power consumption got in our evaluation.

C. Cryptography

The choice for cryptography was TinySec solution [4]. Normally, a network cryptography process evaluation must consider network and processing overhead. But, in motes sensor, as time to transmit is much bigger than time to process cryptography algorithms, the processing energy consumption can be disregard. The processor use the idle time to run cryptography algorithms. Thus, we will consider only network overhead.

TinySec enable authentication in TinySec-Auth mode and authentication and encryption in TinySec-AE mode. TinySec-Auth increase 1 byte in network packet size. TinySec-AE increase 5 bytes in network packet size.

The packet consider in this work has 33 bytes, including preamble, header and data. In TinySec-Auth mode, it increases to 34 bytes. Thus, the energy consumption increases 3%. In TinySec-AE mode, the packet increase from 33 to 38 bytes, about 15%.

D. Key Management

The key management protocols chose, SPINS and NEKAP, establish their keys during network configuration phase. SPINS include two protocols: SNEP and µTesla. SNEP use predistributed keys and don’t spend power to establish the keys. µTesla announce a key after its validity period. This key is used to authenticate broadcast messages from base station.

To evaluate µTesla we need to consider broadcast messages. In you model, the base station only broadcast to network the beacon, for route update and the management messages. As management messages are sent occasionally, we must consider only route update messages now. As update route messages are urgent, it is necessary announce a key after all update route phase. As key announce message is broadcast like route update, the cost of both are similar. Then, we will consider the cost of µTesla distribution key equal to route update. In TABLE 2, the cost of route update is presented, about 80 x 10^-5 mAh in any configuration, with any number of nodes.

NEKAP [15] has some power consumption to establish keys. The keys are established in configuration phase. Each node sends 3 and receives 18 messages to establish necessary keys. This phase increases power consumption in 78.5 x 10^-5 mAh.

E. Intrusion detection systems and revocation schemas

IDS mechanisms can run in base station or in nodes. In base station, IDS has advantages: doesn‘t spend network resources, it is trusted and has access to all network data. In a node, IDS has as advantage the proximity of intruder. A monitor node [2] can heard in a local neighborhood to identify a suspect behavior of an intruder node.

We will consider only a increasing in time to receive packets in monitor nodes. In our model, the nodes maintain radio turned on only to receive necessary packets from their neighbors. After that, they sleep some time. Due to intruder detection, the monitor node has to receive the packets from all neighbors, including that forwarded to base station. We consider six neighbors from each node. Only one of these neighbors has to forward packets to base station. To hear its packets too, we consider the monitor node has to hear 16.7% more, corresponding to one sixth of its neighbors.
In security levels, monitor nodes varies from 0 to 30% of all nodes, increasing 10% in each level. Just to evaluate IDS solution, we calculate the increasing of 16.7% of receiving cost in 10% of nodes. Results are shown in Table 3. The average cost per node is shown too. 10% of monitor nodes are used in medium level security.

<table>
<thead>
<tr>
<th>Number of nodes</th>
<th>Total sent packets</th>
<th>Total received packets</th>
<th>Average extra spent energy per node with IDS (mAh x 10⁻³)</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>16229</td>
<td>112170</td>
<td>1.84</td>
</tr>
<tr>
<td>100</td>
<td>42379</td>
<td>298276</td>
<td>2.44</td>
</tr>
<tr>
<td>200</td>
<td>112592</td>
<td>798710</td>
<td>3.27</td>
</tr>
<tr>
<td>400</td>
<td>308612</td>
<td>2186616</td>
<td>4.48</td>
</tr>
<tr>
<td>600</td>
<td>568560</td>
<td>4022888</td>
<td>5.49</td>
</tr>
<tr>
<td>800</td>
<td>817687</td>
<td>5802845</td>
<td>5.94</td>
</tr>
<tr>
<td>1000</td>
<td>1162417</td>
<td>8238595</td>
<td>6.74</td>
</tr>
</tbody>
</table>

F. Secure routing

Alternative routes were chose to increase security in routing in this work. To evaluate alternative routes we do some simulations in network scenarios presented. Table 4 present results of our simulations.

Other solution to increase security in routing is to authenticate beacon. This solution is cheap because authentication increases the packet in only one byte. And routing packets represents less than 1% of total packets. We don’t consider it.

<table>
<thead>
<tr>
<th>Number of nodes</th>
<th>Without alternative routes (mAh x 10⁻³)</th>
<th>With alternative routes (mAh x 10⁻³)</th>
<th>Increase</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>110.27</td>
<td>117.95</td>
<td>6.96%</td>
</tr>
<tr>
<td>100</td>
<td>146.33</td>
<td>155.67</td>
<td>6.38%</td>
</tr>
<tr>
<td>200</td>
<td>195.75</td>
<td>203.72</td>
<td>4.07%</td>
</tr>
<tr>
<td>400</td>
<td>267.99</td>
<td>283.36</td>
<td>5.74%</td>
</tr>
<tr>
<td>600</td>
<td>328.74</td>
<td>348.61</td>
<td>6.04%</td>
</tr>
<tr>
<td>800</td>
<td>355.53</td>
<td>380.97</td>
<td>7.16%</td>
</tr>
<tr>
<td>1000</td>
<td>403.87</td>
<td>425.42</td>
<td>5.34%</td>
</tr>
</tbody>
</table>

G. Data Fusion

We evaluate how data fusion contributes to decrease energy consumption in sensor network. In upper security levels, data fusion must be turned off to avoid intruder’s effect.

In our simulation, we consider alternative routes too, because data fusion is turned off after alternative routes are turned on. Table 5 shows the results. Data fusion saves up to 40% of power consumption.

<table>
<thead>
<tr>
<th>Number of nodes</th>
<th>With data fusion (mAh x 10⁻³)</th>
<th>Without data fusion (mAh x 10⁻³)</th>
<th>Increase</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>117.95</td>
<td>146.66</td>
<td>24.34%</td>
</tr>
<tr>
<td>100</td>
<td>155.67</td>
<td>200.95</td>
<td>29.09%</td>
</tr>
<tr>
<td>200</td>
<td>203.72</td>
<td>265.88</td>
<td>30.51%</td>
</tr>
<tr>
<td>400</td>
<td>283.36</td>
<td>388.11</td>
<td>36.97%</td>
</tr>
<tr>
<td>600</td>
<td>348.61</td>
<td>472.68</td>
<td>35.59%</td>
</tr>
<tr>
<td>800</td>
<td>380.97</td>
<td>526.62</td>
<td>38.23%</td>
</tr>
<tr>
<td>1000</td>
<td>425.42</td>
<td>595.82</td>
<td>40.05%</td>
</tr>
</tbody>
</table>

H. Security Management Energy Consumption

Two types of management messages are transmitted in this work: messages broadcasted to network by base station; and intruder detected messages, sent from nodes to base station.

Messages broadcasted from base station are forward by all nodes. The total cost is a message by node. These messages are send to revoke intruder nodes and change security level.

Intruder detected messages are sent from nodes to base station. The cost of these messages depends of distance from monitor node to base station and it is equal to a cost to send a sensing data from the node to base station.

About management messages, an important consideration is that the messages are transmitted only in intruder presence. If there is no intruder, no message is send. In intruder presence, the transmission of some messages is a cheap price to pay to avoid the intruder effect.

V. Final Results

We plot the average energy consumption in security levels to see graphically the results obtained. Figure 2 shows the result. The average energy consumption can hit up to 100% in critical level. The levels contain security components according Table 1. We consider cryptography, data fusion, alternative routes and intruder detection.

VI. Conclusion and Future Works

This paper presents an evaluation of security management framework for sensor networks. The objective is to extend network availability and lifetime through the setting up of security services only when it is necessary.

DoS attacks can majority block services in sensor networks. Due to avoid effect of these attacks, security components are necessary. Security solutions can increase energy consumption
up to 100%. Thus, continuous use of all security components can reduce network lifetime. The security management proposed in this work can reduce energy consumption and ensure protection against DoS attacks.

In terms of self-managed or autonomic operation, a manager at the base station can automatically determine changes in security levels of the sensor nodes, turning on or off security components to avoid intruders’ effect or save energy. Intruder detection events start autonomic set up of security levels.

Our simulations and analysis show that the security management can guarantee protection against the main attacks without spend a lot of additional energy. Only under attack the network need to turn on security solutions, increasing the energy spent. Thus, we guarantee the availability, extending the network lifetime and protecting network against the mainly DoS attacks.

Each security component has energy consumption. The data fusion has the biggest difference in total consumption. Data fusion doesn’t can be used with end-to-end cryptography, because the intermediary nodes don’t have access to sensing data.

Policy based languages can allow dynamic set up of different network applications. In WSN, customization is a very important approach.

REFERENCES


