SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TNC TRANSACTIONS ON NETWORKS AND COMMUNICATIONS

VOLUME 6, NO. 5
ISSN: 2054 -7420

Secured Communication through Wireless Sensor Network

[1]Talal Alkharoubi, [2]Abdullatif Albaseer, [3]Gamil Ahmed
[1,2,3]King Fahd University of Petroleum & Minerals
Computer engineering department
Dhahran, 31261, Saudi Arabia
talalkh@kfupm.edu.sa; Abdullatif2009@gmail.com; g201302310@kfupm.edu.sa

ABSTRACT

Nowadays, life seems to be deficient without Internet. The Internet of Things (IoT) is heavily affecting our daily lives in many domains, ranging from tiny wearable devices to large industrial systems. In face of this rapid improvements, security threats and privacy issues also have brought critical challenges in designing and implementing such applications. In this work, we aim to find a way to protect the data from the WSNs devices to the cloud server or control unit. Also, the task of data management in WSNs is a vital issue that can be performed with limited resources such as processing, memory and energy. So, we have proposed a light implementation for AES 128 key in order to be used to encrypt the data sent by these sensors. We have adopted three different platforms which are Sky and Z1 motes to test this algorithm. Applying such algorithm leads to consume more power but guarantees a secure communication against malicious nodes.

Keywords: IoT, Threat, Attack, WSNs, AES, TelosB, Z1, Contiki, Cooja.

1 Introduction

Internet of Things (IoT) is a concept that enables various physical objects and methods of communication to achieve a certain task by exchanging information. IoT exploits underlying technologies to make these objects much smarter such as wireless sensor networks (WSNs), applications, Internet protocols and ubiquitous and, embedded devices. (Al-Fuqaha et al. 2015).

Nowadays, the IoT has brought the opportunities to have a smart home and business applications which contribute to increase the quality of our life and grow the world's economy. From a functionality viewpoint, IoT technology promises to improve our life style and make our lives easy and comfortable. IoT depends on the internet infrastructure in order to reach its goals. Consequently, it opens itself into all the known conventional cyber-security threats as well as it opens doors for new threats. Cybersecurity attacks towards IoT not only endanger the IoT functionality but also it may expose human lives to risks in its environments due to security breaches. Even though a plenty of security defense and countermeasures have been developed since the early stage of the internet era, these solutions cannot be applied directly into IoT infrastructure due to a major difference in computation capability between conventional computing devices and IoT devices. Not only that, but there is no a comprehensive study that presents the panoramic picture of the IoT security threats(Abdur et al. 2017).

According to Sharma and(Sharma and Bhadana 2010), sensor nodes are low power, have limited functionality, and are not individually capable of multi-hop routing. These nodes tend to be application

DOI: 10.14738/tnc.65.5101
Publication Date: 14th September 2018
URL: http://dx.doi.org/10.14738/tnc.65.5101

specific to monitor temperature, video, or pressure. Most often, sensor nodes are grouped in clusters and sited at strategic locations. Sensor nodes monitor applications or provide surveillance to send back to the local forwarding nodes (FN). For each sensor node cluster, there is an individual forwarding node (FN). Forwarding nodes receive the sensor node cluster information and then process the information to obtain aggregate results. These nodes also verify the information received from the SN cluster. This "middleman" node consists of two wireless interfaces between the lower level sensor nodes and the next higher level of the node, the access points (AP).

Possessing both wired and wireless interfaces, access points (AP) utilize its multi-hop routing capabilities to send SN and FN packets to wired networks within a designated radio range as well as to forward control information between SNs and FNs and wired networks. APs also can re-verify the information previously verified at the FN node level. At each of these node points, protected and authenticated communication between the various sensor nodes are key security concerns. WSN sensor node vulnerabilities arise from four separate areas: the open nature of wireless channels, the absence of infrastructure, its rapid speed of deployment, and hostile deployment environments (Maw. 2008).

Due to these four vulnerabilities, security protocols centered solely around physical security cannot be successfully used. Security only becomes more critical against security attacks because sensor nodes are heavily constrained and limited in terms of its internal energy, memory, computational and communication abilities. Because it's routing paths and relative neighborhood are subject to constant change, networks frequently cannot provide adequate security measures against posed threats such as breaches in confidentiality, integrity, authentication, and authorization(Banković et al. 2012).

There is little or no capability to identify new threats or impending attacks and to react proactively to prevent damage. Security, then, becomes a paramount concern because roaming nodes must constantly be authenticated within neighboring nodes through secure communication keys. Attacks on WSNs can be categorized as passive or active and internally-sourced versus externally-sourced attacks. More specifically, there are two view levels of attacks: security mechanism attacks and basic mechanism attacks. Major attacks can consist of wormhole attacks, spoofing, selective forwarding, black-holes or sinkholes, Sybil attacks, HELLO flooding, and denial of service of these attack sources, wormhole attacks, the focus of this paper, constitute one of the highest continuing threats to WSNs (Ronghui et al. 2009). Wormhole attacks are malicious, passive, external laptop-class threats.

In a wormhole attack, at least two colluding nodes maliciously "create a higher-level virtual tunnel (wormhole) in the network and transport message packets between the tunnel endpoints" (K. E. N. Kumar, Waheed, and Basappa 2010) by offering shorter network links. Unsuspecting nodes are deceived into selecting the shorter routes and replaying the message in a separate part of the network and corrupting data or disabling networks through faulty information. Wormhole tunnels can be established through wired infrastructure links or hidden within out-of-band channels, through high powered transmission lines, or through packet encapsulation above network layers.

1.1 WSNs security challenges

WSNs design model has been divided into three layers: Application level, Communication level, and Perception level. Each layer is a potential target for several designated attacks. Figure 1.1 describes these three layers.

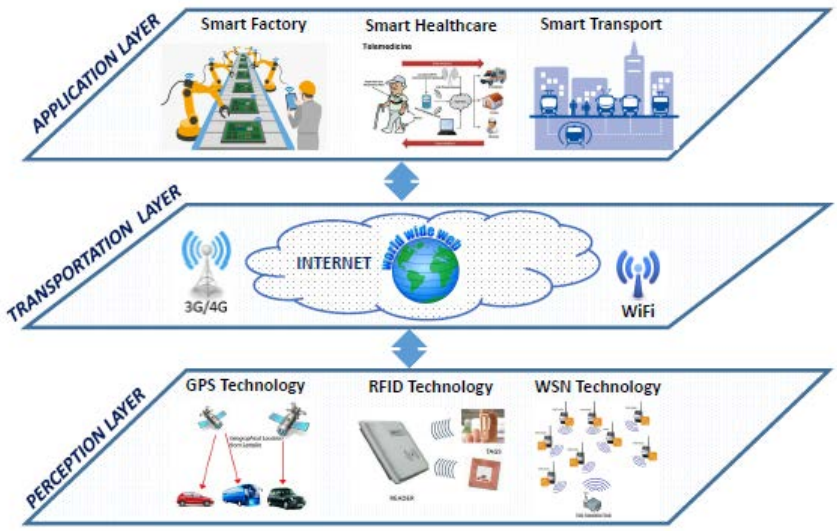

Figure 1: IoT as a Layered Approach [2].

1.2 Application layer attacks

The application layer is a place where specific application business situated such as Smart City, Smart Factories, Health Care etc(Abdur et al. 2017). Each business environment might have its own security and privacy challenge since there is no security standard for IoT for the application layer. Furthermore, at, this layer, some security threats at this layer cannot be avoided at the other layer such as privacy and protection. Even though this layer may have regularly a complex logical business at the different environment with a different purpose, it suffers from various common security threats:

- Data Leak: An adversary could steel client's confidential information such passwords due to an existence of vulnerability on for example in either application authentication implementation or session management.
- DoS attack: Due to this attack, application service availability could be targeted with thousands of fake requests in order to block or shout down the service from other legitimate customers.
- Malicious code injection: an attacker could utilize a vulnerable application for example with maliciously crafted input to push it to action that it's not intended to do.

1.3 Perception Layer

Perception Layer of IoT basically involves gathering and processing data over RFID (Radio-Frequency Identification), WSN (Wireless Sensor Network), RSN (RFID Sensor Network) and GPS(Mendez, Papapanagiotou, and Yang 2017). It consists of sensors and actuators that aim to either query the location or measure for example temperature, acceleration, humidity, etc.)

This layer is a potential target to each of the following attacks:

- Physical attacks: The aim of the attackers her is either to cause the damage to the sensor node or physically insert a malicious code into the targeted node.
- Impersonation: attackers utilize the vulnerabilities in the authentication to insert a fake node for malicious or collusion attacks.

- Data Transit Attacks: unsecured communication at this layer opens doors for several potential attacks such as Eavesdropping, Man-in-the-Middle etc.
- Routing Attacks: an intermediate fake node may modify the routing paths.

1.4 Transport Layer

Communication layer is responsible for delivering all kind of communication traffics between the applications and their related outsourced peripherals such as sensors, actuators, networking devices and so on connected through either wireless or wired mediums. Communication Layer is a potential target to one of the following attack(Zhou, Zhang, and Liu 2018):

- Routing Attacks: an intermediate fake node may modify the routing paths 4
- DoS Attacks: due to the heterogeneous nature of IoT, makes the Communication layer a potential target to DoS Attacks.
- Data Transit Attacks: unsecured communication at this layer opens doors for several potential attacks such as Eavesdropping, Man-in-the-Middle etc.

2 Related Work

Due to the advancement in IoT and their applications, the security threats in these fields have received a good attention from some researchers in the last few years.

In (Yang et al. 2017), Yang et al have published an article survey regarding the privacy and security issues in IoT. Their work studied the security issues from four different perspectives. They initially highlighted on the limitations of applying security in IoT devices (e.g., computation power, the battery lifetime etc.) and the suggested solutions for these problems (e.g. lightweight encryption scheme designed for embedded systems). Then, they introduced a classifications summary of different IoT attacks (e.g. local, remote, physical etc). After that, they paid much attention to the mechanisms and architectures of designing and implementing for authorization and authentication purposes. Finally, they did analyze the security issues at different layers (e.g. Application, Transport, etc.) composed of Application, Network, and Perception layers. The Perception layer belongs to the physical devices that identify and sense analog data and then digitize it for transportation purposes. Infrastructure protocols such as ZigBee, Z-Wave, Bluetooth Low Energy (BLE)(Gomez, Oller, and Paradells 2012), Wi-Fi, and LTE-A run in the Network layer(Ghosh et al. 2010). The Application layer is the interface for end-users to access data and talk to their IoT devices. It supports standard protocols such as HyperText Transfer Protocol (HTTP), Constrained Application Protocol (Yang et al. 2017). (CoAP) (Shelby, Hartke, and Bormann 2014).

Also, the security and privacy issues in IoT have been addressed by (J. S. Kumar and Patel 2014) & (Vikas 2015). They studied the security issues at each layer characterized by the three-layer architecture(Vikas 2015) surveyed most of the security threats in IoT, resulted from the various communication technologies used in wireless sensor networks.

The authors in (Vikas 2015) have proposed an authorization access model. They recommended using this model as a security framework for the IoT to assure access control and legitimate authority for users only.

Authors in (Fremantle and Scott 2017) reviewed the challenges and approach proposed to overcome the security issues of the IoT middleware, where a large number of existing systems inherit security properties from the middleware frameworks. Depending on the well-known security and privacy threats, the authors

analyze and evaluate the available middleware approaches and show how security is handled by each approach. The work concludes by illustrating a set of requirements to have a secure IoT middleware.

3 System Model and problem statement

Let us consider the proposed wireless networks (WSNs) is comprised of multiple sensor nodes. The nodes are deployed to monitor a certain phenomenon, collect an information and report to the base station through multi-hope forwarding scheme. The forwarded data can be read by any intermediate node consequently this node could corrupt this packet and retransmit it again until reaching the base station. In some application, the collected data is crucial and very sensitive such as poison gas detection, fire detection, and health care. The data resulting from these applications should be protected in order to provide confidentiality to make the right decision. Corrupted data may lead to a disaster. As a result, designing and implementing a secure path for this data is essential to prevent such actions. However, most existing encryption solutions cannot be applied in WSNs due to limited capabilities in processing, transmission, and energy.

As pointed out, we propose to implement a lightweight algorithm such as AES light version which is appropriate for such limited resources devices.

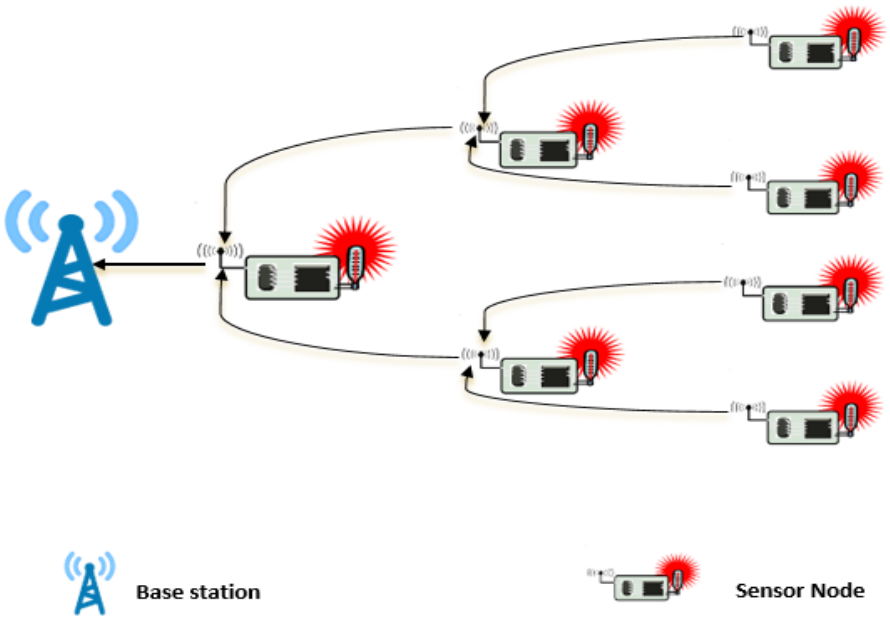

Figure 2: System Model of the proposed application

4 AES light Algorithm

AES Encryption is a method for scrambling data. A key is utilized to mix up data such that it can be securely stored or transferred over the network and the only person with the key can unscramble the data. Algorithm implementation is highly depending on microcontroller technology.

Due to the limited resources of IoT devices, a lightweight algorithm version of AES is developed to be used with these limited resources devices. The lightweight version of AES has small block size, small key size, simple round, and simple key scheduling.

5 Sensors Specification

5.1 TelosB (Sky mote)

TelosB is a platform designed for low power sensor network applications. It uses CC2420 radio chip with a transmission speed of 250 kbps and works on 2.4 GHz radio frequency. Figure illustrates TelosB mote specifications(Memsic 2003).

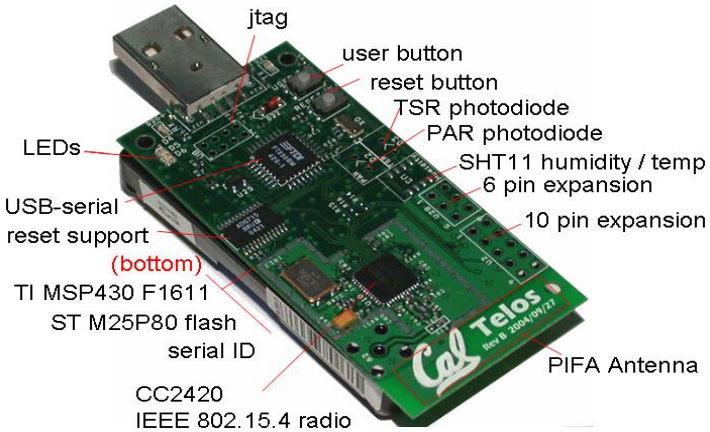

Figure 3: TelosB mote Specification

5.2 Z1 mote

Z1 mote is a low power sensor equipped with a second generation MSP430F2617 microcontroller, which features a powerful 16-bit RISC CPU @16MHz clock speed, built-in clock factory calibration, 8KB RAM and a 92KB Flash memory. Also includes the well-known CC2420 transceiver, IEEE 802.15.4 compliant, which operates at 2.4GHz with an effective data rate of 250Kbps(Zolertia 2010).

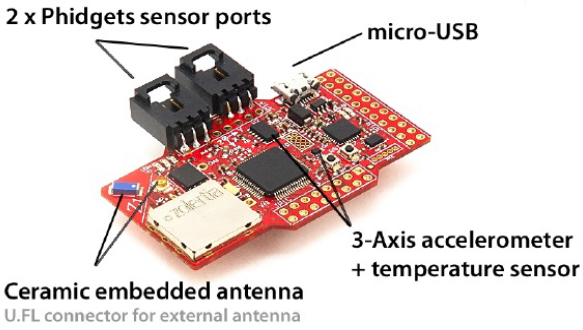

Figure 4: Z1 mote specification

5.3 Experimental Setup

In order to conduct the proposed solution, we have implemented the AES light algorithm on different platforms (mentioned in section) each experiment has been conducted using the following components:

5.3.1 Simulation Scenarios

Initially, TelosB motes have been adopted with different solution scenarios to trace the behavior of this algorithm in different network size. Table 1 summarizes the components of this experiment

Table 1: simulation parameters

Parameter	Value
Tool	Cooja
Network size	Variable (5, 10, 15)
Battery capacity	2600 mAh
Voltage	3 V
Time of sending a packet	10 seconds
Transmission power	0.052 watts
Receiving power	0.069 watts
Active mode	0.0018 watts
Sleep mode	0.0000153 watts

Secondly, the same simulation parameters described in Table also are implemented with Zolertia mote.

5.3.2 Results and Analysis

The analyzed performance metrics that have been used in this study are:

1. Total power consumption: this metric measures the total energy of each sensor nodes as in the following equation. This metric also shows how the effects of the proposed solution are in term of how much of the energy is consumed compared to the unsecured model.

$$Energest_{value}\ per\ cycle = current\ Energest_{value} - previous\ Energest_{value}$$

Where $Energest_{value}$ is the times that the mote spends in this state.

$$Energy\ consumption(mW) = \frac{Energest_{value} * current * Voltage}{RTIMER_{SECOND} * Runtime}$$

Where the $RTIMER_{SECOND}$ is the number of ticks per second.

2. Network lifetime: this metric measures the estimated lifetime of each sensor nodes based on the equation. This metric also determines the lifetime of the whole network. In addition, this metric shows how the ability of the proposed AES encryption in term of how much of the network lifetime is reduced due to security measures.

$$P_{total} = P_{Tx} + P_{RX} + P_{LPM} + P_{CPU}$$

The performance of the two approaches has been investigated using different setups to explore the effect of using different size of sensor nodes in simulation environments. First, we show the effects of applying such algorithm to total energy consumption.

To start with, Figure illustrates the cumulative power consumption for both scenarios (by applying an encryption algorithm and without applying it) when the network size is 10 sensor nodes. It can be noticed that, applying the security measurements require more power due to the complex processing operation

used by the AES algorithm for encryption when the packet is sent. Also, as depicted in Figure , the power consumption increases by 39% as a maximum.

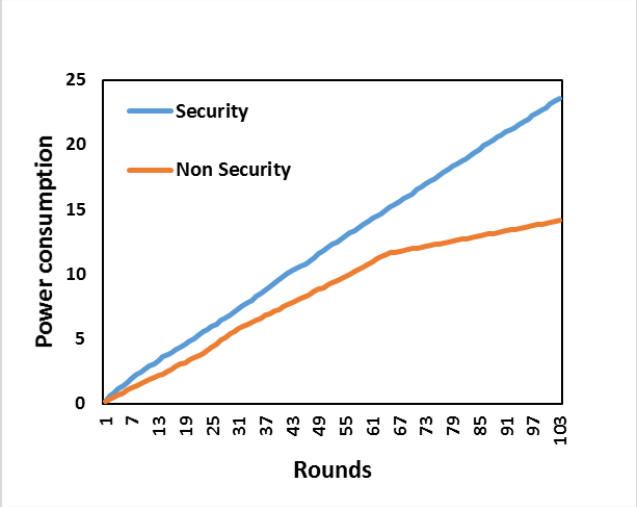

Figure 5: Power consumption (TelosB mote) when the network size is 10 nodes for both security and none security scenarios

For the second scenario when the network size is 15 sensor nodes, as shown in Figure , applying security measurements requires more power compared to the first scenario due to increasing the traffic loads in this scenario. The power consumption increases approximately by 65% compared to none security scenario.

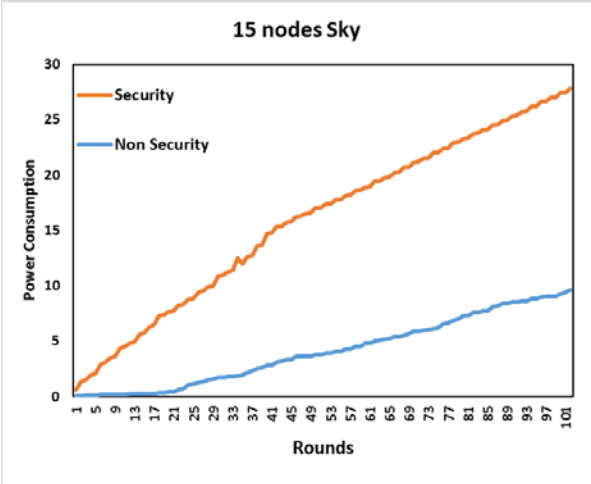

Figure 6: Power consumption (TelosB mote) when the network size is 15 nodes for both security and none security scenarios

In addition, Figure shows the lifetime of both scenarios for with security measurements and without security measurements. It could be seen that the lifetime decreased when the encryption algorithm is applied either when the network size is 10 nodes or when the network size is 15 nodes. This results from the heavier traffic as the network size increases.

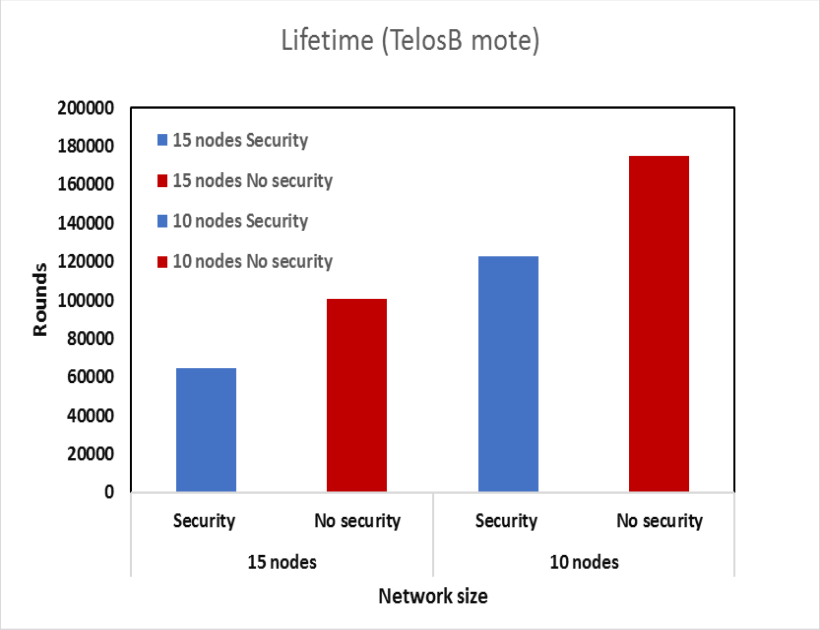

Figure 7: The average network Lifetime when the network size is 10 and 15 nodes for both security and none security scenarios

To see the behavior of this algorithm among different sensor platforms, we have adopted Z1 mote to evaluate the performance of this algorithm. The same simulation setup and performance metrics mentioned in the previous section have been considered in these experiments.

Initially, the first experiment has been conducted when the network size is 10 and 15 sensor nodes and similar to the same scenario in the TelosB motes, applying security algorithm requires more power compared to traditional transmission operation as shown in Figure and Figure .

In contrast, Z1 mote is outperforming TelosB motes in both scenarios either for security or without security measurements.

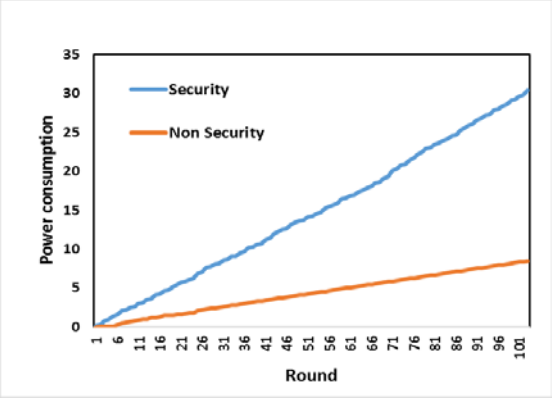

Figure 8: Power consumption (Z1 mote) when the network size is 10 nodes for both security and none security scenarios

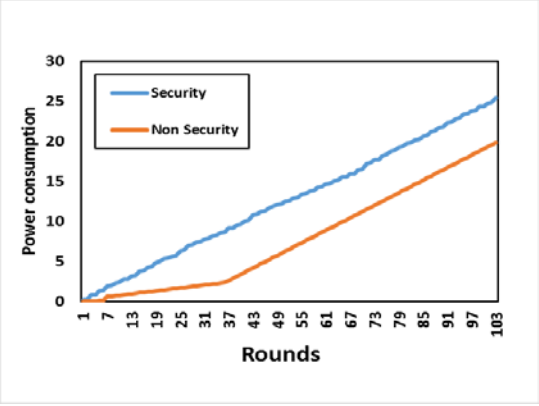

Figure 9: Power consumption (Z1 mote) when the network size is 15 nodes for both security and none security scenarios

6 Conclusion

With its spatially distributed nodes used to monitor physical and environmental conditions in hostile or unattended sites, Wireless Sensor Networks represent a major means of sensing, processing, and communicating data results for military and civilian purposes and applications. Because data is being transmitted and shared, basic security issues such as authentication, integrity, confidentiality, and availability arise. While a variety of threats can be mounted against WSNs, different types of attacks represent one of the major threats to a wireless sensor network's security. Wormhole attacks result from the compromising of two or more sensor nodes. Applying a light version of advanced encryption security algorithm to tackle the gap between the complex computation of encryption algorithm and resource limitation in WSNs. Different experiments with different network sizes have been conducted and the results show that applying such algorithm requires more power but provides a secure communication through multi-hops forwarding schemes. Also, different platforms have been adopted to evaluate the behavior of this algorithm among different sensor manufacturing architecture.

REFERENCES

[1] Abdur, Mirza, Sajid Habib, Muhammad Ali, and Saleem Ullah. 2017. "Security Issues in the Internet of Things (IoT): A Comprehensive Study." *International Journal of Advanced Computer Science and Applications* 8(6). http://thesai.org/Publications/ViewPaper?Volume=8&Issue=6&Code=ijacsa&SerialNo=50.

[2] Al-Fuqaha, Ala et al. 2015. "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications." *IEEE Communications Surveys & Tutorials* 17(4): 2347–76.

[3] Banković, Zorana, David Fraga, José M. Moya, and Juan Carlos Vallejo. 2012. "Detecting Unknown Attacks in Wireless Sensor Networks That Contain Mobile Nodes." *Sensors (Switzerland)* 12(8): 10834–50.

[4] Fremantle, Paul, and Philip Scott. 2017. "A Survey of Secure Middleware for the Internet of Things." *PeerJ Computer Science* 3: e114. https://doi.org/10.7717/peerj-cs.114.

[5] Ghosh, Amitava et al. 2010. "LTE-Advanced: Next-Generation Wireless Broadband Technology [Invited Paper." *IEEE Wireless Communications* 17(3): 10–22. http://ieeexplore.ieee.org/document/5490974/ (December 24, 2017).

[6] Gomez, Carles, Joaquim Oller, and Josep Paradells. 2012. "Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology." *Sensors* 12(9): 11734–53. http://www.mdpi.com/1424-8220/12/9/11734.

[7] Kumar, J Sathish, and Dhiren R Patel. 2014. "A Survey on Internet of Things: Security and Privacy Issues." *International Journal of Computer Applications* 90(11).

[8] Kumar, K E Naresh, Mohd Abdul Waheed, and K Kari Basappa. 2010. "TCPL: A Defense against Wormhole Attacks in Wireless Sensor Networks." In *AIP Conference Proceedings*, , 633–38.

[9] Maw., Z. Tun and A.H. 2008. "Wormhole Attack Detection in Wireless Sensor Networks." *Proceedings of World Academy of Science Engineering and TechnologyEngineering and Technology* 46(3): 545–50.

[10] Memsic. 2003. "MICAz Datasheet: 6020-0065-05 Rev." *San Jose, CA, California* Revision 6: 1–2.

[11] Mendez, Diego M., Ioannis Papapanagiotou, and Baijian Yang. 2017. "Internet of Things: Survey on Security and Privacy." : 1–16. http://arxiv.org/abs/1707.01879%0Ahttp://dx.doi.org/10.1080/19393555.2018.1458258.

[12] Ronghui, He, Ma Guoqing, Wang Chunlei, and Fang Lan. 2009. "Detecting and Locating Wormhole Attacks in Wireless Sensor Networks Using Beacon Nodes." *Engineering and Technology* 3(7): 286–90.

[13] Sharma, Pooja, and Pawan Bhadana. 2010. "An Effective Approach for Providing Anonymity in Wireless Sensor Network: Detecting Attacks and Security Measures." *International Journal on Computer Science and Engineering* 02(05): 1830–35.

[14] Shelby, Zach, Klaus Hartke, and Carsten Bormann. 2014. "The Constrained Application Protocol (CoAP)."

[15] Vikas, B O. 2015. "Internet of Things (IoT): A Survey on Privacy Issues and Security."

[16] Yang, Yuchen et al. 2017. "A Survey on Security and Privacy Issues in Internet-of-Things." *IEEE Internet of Things Journal*.

[17] Zhou, Wei, Yuqing Zhang, and Peng Liu. 2018. "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved." : 1–11. http://arxiv.org/abs/1802.03110.

[18] Zolertia. 2010. "Z1 Datasheet." s: 1–20.