World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:12, No:1, 2018

The Security Trade-Offs in Resource Constrained Nodes for IoT Application

Sultan Alharby, Nick Harris, Alex Weddell, Jeff Reeve

***Abstract*—**The concept of the Internet of Things (IoT) has received much attention over the last five years. It is predicted that the IoT will influence every aspect of our lifestyles in the near future. Wireless Sensor Networks are one of the key enablers of the operation of IoTs, allowing data to be collected from the surrounding environment. However, due to limited resources, nature of deployment and unattended operation, a WSN is vulnerable to various types of attack. Security is paramount for reliable and safe communication between IoT embedded devices, but it does, however, come at a cost to resources. Nodes are usually equipped with small batteries, which makes energy conservation crucial to IoT devices. Nevertheless, security cost in terms of energy consumption has not been studied sufficiently. Previous research has used a security specification of 802.15.4 for IoT applications, but the energy cost of each security level and the impact on quality of services (QoS) parameters remain unknown. This research focuses on the cost of security at the IoT media access control (MAC) layer. It begins by studying the energy consumption of IEEE 802.15.4 security levels, which is followed by an evaluation for the impact of security on data latency and throughput, and then presents the impact of transmission power on security overhead, and finally shows the effects of security on memory footprint. The results show that security overhead in terms of energy consumption with a payload of 24 bytes fluctuates between 31.5% at minimum level over non-secure packets and 60.4% at the top security level of 802.15.4 security specification. Also, it shows that security cost has less impact at longer packet lengths, and more with smaller packet size. In addition, the results depicts a significant impact on data latency and throughput. Overall, maximum authentication length decreases throughput by almost 53%, and encryption and authentication together by almost 62%.

***Keywords*—**Internet of Things, IEEE 802.15.4, security cost evaluation, wireless sensor network, energy consumption.

I. Introduction

THE concept of IoT has recently grabbed the attention of the academic and industrial communities [1]. The IoT is not associated with a particular technology, and can be used in different applications. However, the Wireless Sensor Network (WSN) is a foundational technology for IoT [2], [3]. Sensors are the main tools for reporting events in *things* such as cars, home appliances, and any object to which a sensor can be attached. However, IoT devices do suffer from major issues involving limited resources [4], particularly energy, and a vulnerability to various types of attack. Protecting the communication between IoT devices with limited resources is a complex task. Nodes are usually equipped with small batteries, which makes energy conservation crucial to WSNs. Every bit consumes energy [5], so conventional security mechanisms which introduce more overheads for both computation and communication are unsuitable for such limited devices [6]–[9]. It is clear that security and power consumption are opposite parameters. One of the main obstacles facing security solutions for IoT devices is energy consumption. Batteries are the main source of power in these devices, and the indicator of IoT device lifetime. Usually these devices are implemented in remote area or harsh environment which make changing a battery difficult. Thus, the energy limitation of these small devices necessitates a trade-off between security mechanism and energy consumption. Security has become essential to many IoT applications [10], [11], especially when dealing with sensitive data such as medical and military applications, but it does, however, come at a cost to resources. Nevertheless, security cost has not been studied sufficiently. Many research have used security specification of 802.15.4 for IoT MAC layer, but the cost of each security level is unknown. Basic security services include encryption to guarantee confidentiality, authentication to ensure packets are sent from a legitimate party, integrity to guarantee packets have not changed through transmission, and freshness of data to ensure that packet is recent and old packets are not being re-played. This paper investigates the overhead introduced by IEEE 802.15.4 security levels at MAC layer and their effect on the QoS parameters. To obtain accurate results, the effects of MAC and Radio Duty Cycle(RDC) protocols on the security cost has been excluded, since the purpose of this evaluation is only to get the extra overhead of security on sensor networks. However, the mechanism used ContikiMAC and the methods employed to avoid its effects are discussed, as it is the RDC protocol employed in this emulation. The obtained results assume a perfect communication environment, therefore packet delivery is 100% successful as long as the two nodes involved are within the same transmission coverage area. The results represent the minimum security overhead, and the actual overhead could be greater, depending on the mechanism employed for the Radio Duty Cycle. For example, re-transmitting packets increases security services' impact on performance. The overhead considered in this scenario is that introduced by the transmission mode of each security level. The evaluation focuses on the following performance parameters:

1) Per-packet energy Consumption E: The total energy needed for delivering one packet from source to destination at each security level. This includes the

S. Alharby is with the Department of Electronics and Computer Science, University of Southampton, UK (corresponding author, e-mail: sa1c15,@soton.ac.uk).

N. Harris, A. Weddell and J. Reeve are with the Department of Electronics and Computer Science, University of Southampton, UK (e-mail: nrh@ecs.soton.ac.uk, asw@ecs.soton.ac.uk, jsr@ecs.soton.ac.uk).

energy consumed by transmission mode E_{tx} and receiving mode E_{rx}, and the energy required by a relay nodes to forward a packet E_{fwd}. Hence, the total energy consumption of transmitting one packet E can be represented as follows:

$$E = E_{tx} + E_{rx} + n * E_{fwd} \quad (1)$$

2) Latency (L): This measures the time needed for a node to transmit a packet until it received by the destination.
3) Throughput (Thr): This is the number of packets received at the destination per unit time (one second in this research).

At the end of this paper, the most significant security levels will be identified based on their impact on sensor network performance, particularly in terms of energy consumption.

II. Related Work

Several studies have evaluated the cost of security at the IoT MAC layer, but the cost of each security level in IEEE 802.15.4 is unknown. For instance, [12] have analysed the energy consumption of AES, RC5 and RC6. They have evaluated the energy cost and memory requirements of these cipher algorithms.

Similar study [13] has evaluated the cost of AES, RC5 and RC6. This study also investigates the impact of key size on energy cost and concludes that RC5 is the most energy-efficient for limited resource devices. Also, [14] provides a method of optimising encryption hardware implementation. The study investigates the energy consumption and performance of AES in both software and hardware implementations. The results indicate that hardware is more efficient than software implementation. However, none of these studies discuss authentication cost, which is crucial to security services in WSNs. In addition, a network engineer cannot identify the cost of security over non-secure transmission, as these studies present only the cost of encryption.

Reference [15] have analysed the cost of using different encryption block ciphers such as AES and RC5 on two popular hardware platforms: MicaZ, and TelosB. The study evaluates the effects of different key sizes on energy cost, and also presents the energy cost of different MAC protocols. However, the study does not evaluate IEEE 802.15.4 and its implications on communication cost. Also, the cost of security over non-secure transmissions is undefined, as the study focuses on the comparison of cipher algorithms rather than security over non-secure transmission.

In contrast, the present study focuses on the security levels of IEEE 802.15.4. It identifies the impact of different security levels on energy consumption and QoS parameters such as latency and throughput, and illustrates how transmission power affects the security cost. In addition, the study clarifies the relationship between security cost and the packet data length. Furthermore, it covers aspects which have been neglected by previous studies, such as how security affects energy consumption indirectly by causing multiple transmissions. Finally, this study provides a methodology for evaluating the security overhead of the IoT MAC layer.

III. Simulation Setup and Parameters

There are many lightweight operating systems (OSs) which could be used in wireless sensor nodes. These operating systems provide similar services, but certain characteristics of these operating systems might affect the choice of the developers. Examples of these operating systems are Contiki, RIOT and TinyOS. However, Contiki operating system was selected in this experiment for its suitable features. The Cooja simulator, which comes with Contiki OS, is used to obtain the results in this paper. Also, Powertrace tool [16], which is supported in Contiki, is used to provide detailed information about where the energy is consumed (transmission, receiving, etc). It calculates the time each component takes in particular mode. This tool is claimed to be 94% accurate in measuring the energy consumed by a real device [16]. Table I shows the parameters which used in the simulator.

TABLE I
Simulation Parameters

Parameter	Value
Platform	Tmote Sky
MAC protocol	CSMA
Radio Duty Cycle	ContikiMAC
Payload	24 and 80 byte
Transmission range	50 Meters
TX/RX success ratio	100%
Radio	CC2420
Microcontroller unit (MCU)	MSP430

The simulation uses single hop communication to deliver packets from source to destination.

IV. IEEE 802.15.4 Security Specifications

This experiment uses a MAC layer security protocol which supports eight levels, as defined by the IEEE 802.15.4 security specifications (as shown in Table II). The minimum security level is 0, whereby no security mechanism is used, and the highest level is 7, which includes encryption,replay protection, integrity and authentication with AES-128.

TABLE II
Security Suites, Reproduced from [17]

Security Suites				
SuiteID	*Description*	*Services*	*Replay detection*	*MIC size (Byte)*
0	No Security	Null	-	0
1	AES-CBC-MAC-32		ON	4
2	AES-CBC-MAC-64	Authentication	ON	8
3	AES-CBC-MAC-128		ON	16
4	AES-CTR	Encryption only	ON	0
5	AES-CCM-32	Authentication	ON	4
6	AES-CCM-64	and	ON	8
7	AES-CCM-128	encryption	ON	16

The security services added at each security level are shown in Fig. 1. AES-CTR mode only provides encryption for the payload, hence it supports confidentiality. The length of the key used is 128 bits, as recommended by the IEEE 802.15.4 security specifications. This length will be fixed at all levels which support confidentiality in this experiment. Authentication can be achieved by appending a message authentication code in every packet. Message authentication

code is also named message integrity code (MIC). This research will use MIC to indicate to message authentication code, so we can differentiate between media access control (MAC) and message authentication code. Authentication can be of various lengths based on the required security strength [4, 8 or 16 byte].

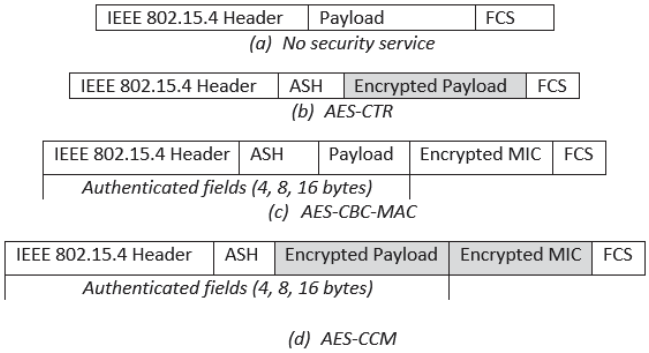

Fig. 1 Security services frame format

Auxiliary Security Header(ASH)(as shown in Table III) consists of three fields: security control, frame counter, and key identifier. ASH is added to the frame only when frame control bit field is set to one [18]. Security control specifies the security level employed for a frame, frame counter is used to provide replay protection against replay attack, and key identifier provides information about the key identifier mode.

TABLE III
AUXILIARY SECURITY HEADER

1 byte	4 byte	0 -9 byte
Security Control	Frame Counter	Key Identifier

V. ACCURACY OF THE SECURITY OVERHEAD RESULTS

There are many factors which affect the accuracy of the results obtained from the emulator, such as the padding mechanism and MAC protocol. The ContikiMAC protocol is used as a RDC protocol. Energy consumption is significantly affected by the employed RDC protocol. Under the ContikiMAC protocol, the sender checks the medium channel before transmitting, and if there is no radio activity, it sends a full data packet and continues to transmit until the receiver wakes up and acknowledges the message. This can affect the result of assessing the overhead of security, as the number of AES invocation varies. At the receiver side, a node checks the medium channel periodically for any activity [19]. Fig. 2 shows the work mechanism of ContikiMAC through unicast transmission. Node 2 represents the transmitter, and node 1 represents the receiver. ContikiMAC requires a minimum length packet size. This is to guarantee that the packet doese not fall down between two Clear Channel Assessment (CCA) [19]. This becomes more important in broadcast communication, as there is no acknowledgement returned to the sender. If the packet size is lower than the minimum size, then a padding mechanism is used to increase the packet size to the minimum. In order to avoid the impact of the padding mechanism on the experiment results, the packet size will always be larger than the minimum packet size.

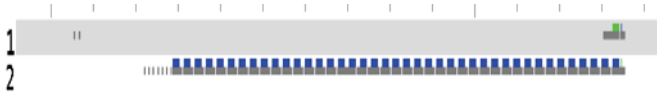

Fig. 2 ContikiMAC mechanism

It can be observed that the radio is turned on and off on regular basis to save power. This is determined by a parameter known as Channel Check Rate. There is an optimisation phase for ContikiMAC which reduces the number of re-transmissions by keeping a track of the receiver wake up period. This could help in making the sender transmit just before the receiver wakes up. Retransmission can significantly affect the energy consumption and assessment of security overhead. In order to avoid the impact of re-transmitting the packet and obtain an accurate result for transmitting one packet, the receiver node is kept on at all times (as shown in Fig. 3). Node number 1 is the transmitter and node number 2 is the receiver.

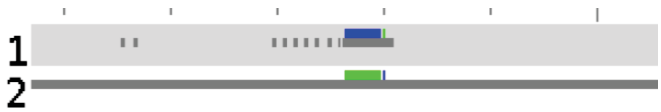

Fig. 3 The radio state for both sender and receiver

Fig. 3 depicts the CCA mechanism, at every transmission the radio checks the channel to make sure it is clear. To eliminate the impact of CCA on the obtained results for energy consumption, CCA is disabled before transmission (as it shown in Fig. 4).

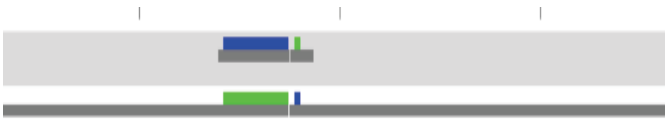

Fig. 4 CCA is disabled before transmission

VI. SIMULATION RESULTS

A. Energy Consumption Evaluation

In order to obtain the total security related energy consumption, all components which affects security cost should be investigated. There are two factors that contribute to the energy consumed by security processes: computation, and communication overhead. Security computation related energy consumption is caused by adding/removing security services such as cryptography. Computation processes makes the MCU run longer to compute complex algorithm. The communication cost is can be obtained by the energy consumed by the radio to transmit the extra byte for authentication. Hence, the total security energy consumption for single packet transmission can be represented as follows:

$$E_{sec-total} = \sum_{k=1}^{n} (E_{sec-compu} + E_{sec-comm}) \quad (2)$$

where, n indicates the number of nodes involved in the transmission, $E_{sec-total}$ the total security energy consumption, $E_{sec-compu}$ computes the energy required for computation overhead, which includes processing the actual transmission and cryptography algorithm, and $E_{sec-comm}$ the energy required for transmitting a packet, which includes transmitting the actual frame and the extra bytes needed for MIC authentication. In the following sections, energy cost is investigated for each security level of the IEEE 802.15.4 security standard. This will include both computation and communication energy cost. The obtained result is an energy cost for delivery of a single packet and expressed in μJoule units. Cost per packet delivery includes the generation of the packet by the MCU and transmission by the radio at the source. This will be acquired for each security level. Required security services are added/removed for each plaintext block according to the security level. The cost of transmission without security services will be taken as a *baseline* for comparison, since security overhead increases by selecting higher security level. In this evaluation, the powertrace tool is used to measure energy consumption. Powertrace records the time that a component (Radio or MCU) enters a specific mode, hence, the time that the MCU and Radio spend in each mode (active, low power mode, etc.) is recorded. The current drawn by the MCU and Radio in different modes should be known in order to estimate the energy consumption. Tmote sky uses CC2420 as a radio driver and MSP430 as a microcontroller. According to Sky mote datasheet [20], the current drawn by the radio and the micro-controller is shown in Table IV

TABLE IV
TYPICAL CURRENT CONSUMPTION FOR TMOTE SKY

Component	Current drawn
MCU- active state	2400μA
Radio - Transmitting mode	17.4mA
Radio - Receiving mode	19.7mA

The objectives of this experiment are as follows:

1) Measure the energy consumption in delivering a single packet at each security level for transmit mode.
2) Investigate the impact of frame length on the security cost.
3) Explore the most significant security level based on energy and also according to security services.
4) Investigate the impact of the power of transmission on performance in terms of energy consumption.

Scenario 1: Evaluation with a payload length of 24 byte in transmit mode The two components of sensor node which affected by security are the MCU and the radio. Hence, the energy consumption associated with these components will be studied. First, the energy consumption of transmitting single packet with 24 byte without security is measured. This will serve as a baseline for comparison with other levels which include different security services. The following formula is used to calculate the energy consumption of every node components:

$$E = Energest\_Value * Voltage * Current \\ / RTIMER\_SECOND * runtime \quad (3)$$

where, E is the energy consumption of a node's component at a specific mode, $Energest\_Value$ is the difference between two interval times, and $RTIMER\_SECOND$ is the number of ticks per second, which in the current simulation is 32768 ticks/second.

Table V shows the energy consumed by the MCU and radio transmitting a single packet with a 24 byte payload. As can be seen from Table V, the radio is the main contributor to energy consumption. MCU consumption at level 0 constitutes 11.5% of the total energy consumption, and it grows as the code increases in complexity with higher security services. However, at the top security level it constitutes only 22% of the total cost of energy. This extra consumption by the MCU at higher security levels is due to AES operation and the processing of extra bytes added by progressive levels of authentication. On the contrary, the radio is responsible for the majority of energy consumption during transmission (as shown in Fig. 5). It can be noticed that radio energy consumption at all levels fluctuates between 73.7% and 88.5% of overall packet consumption, which is a very high percentage. The Radio is responsible for transmitting packets, and it remains in use longer with a greater number of bits. This explains the high energy consumption when enabling authentication, as authentication adds more bytes to the packets.

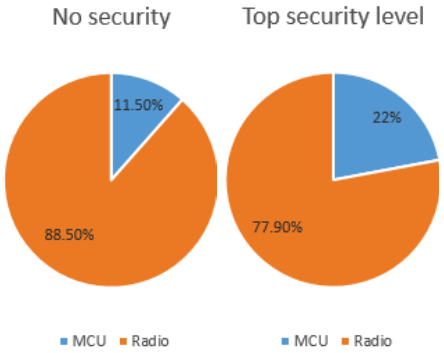

Fig. 5 Radio consumption vs MCU consumption for level 0 and 7

Also, it can be noticed that, total energy consumption increases gradually from security level 0 to level 3, and from 5 to level 7. This is due to the length of MIC, as every level employs a different MIC length. Security level 4 employs encryption only, therefore the radio consumes less energy comparing to authentication security levels. There is a slight difference in MCU energy consumption between security levels 1, 2 and 3. This also applies for security levels 4, 5, 6 and 7, which see only minor changes in MCU energy consumption. However, the increased energy consumption for the MCU at levels 5, 6 and 7 is almost 4 times of the energy consumed by level 0. According to Table V, the percentage

TABLE V
ENERGY CONSUMPTION OF TRANSMITTING ONE PACKET WITH A PAYLOAD OF 24 BYTE IN DIFFERENT SECURITY LEVELS

Security level	MCU energy consumption (μJ)	Radio energy consumption (μJ)	Total energy consumption (μJ)	Percentage of increased security overhead over non-secure packet (%)
0	9.53	73.28	82.81	-
1	24.01	84.91	108.926	31.54%
2	24.15	92.39	116.54	40.72%
3	24.32	103.546	127.87	54.4%
4	28.95	81.24	110.19	33%
5	28.5	83.8	112.3	35.6%
6	29.11	90.80	119.91	44.8%
7	29.33	103.55	132.88	60.46%

increase in security overhead over non-secure communication is high. It can be observed that the minimum security level, level 1, adds a 31.54% overhead, and the highest security level adds 60.46%. This significant overhead affects the network lifetime, and may shorten it significantly depending on the employed security level.

Scenario 2: Evaluation with a payload length of 80 byte in transmit mode The previous experiment was conducted a second time but with longer payload, to investigate the effects of frame length on security overhead. Table VI depicts the security overhead on a frame with an 80 byte payload. Obviously, the security overhead is less with a longer frame. The overall security overhead decreases at all security levels compared to the previous scenario which uses a 24 byte payload. This is because the security cost is the same in both scenarios at all security levels, but the security cost becomes more obvious when the overall energy consumption is small, and less obvious when the overall energy consumption is large. However, in both scenarios, the security cost is significant and makes difference in terms of the network lifetime. Sensor node hardware is limited in terms of payload size, therefore the extra byte added by authentication may lead to multiple packet transmissions if the message exceeds the maximum packet length. For instances, TinyOS uses 36 byte as a default packet length.

The most significant security levels are 0, 4, 6 and 7. The reason for selecting these levels is that the energy consumption at level 2 and 3, which provide authentication only, is similar to 5 and 6, which provide encryption, integrity and authentication. Hence, the latter are chosen since they provide more security with the same energy consumption. Level 4 has been chosen as it provides encryption only at an acceptable cost in case authentication is not required.

Scenario 3: Evaluating the effect of transmission power on security cost

It can be observed in Table VII and Fig. 7 that transmission power does affect security overhead in terms of energy consumption. This due to that MCU run independently and not affected by transmission power change. This makes MCU overhead more visible, in comparison to the radio cost, when the transmission power is reduced, and affects overall energy consumption. The overall security cost will be higher with low transmission power.

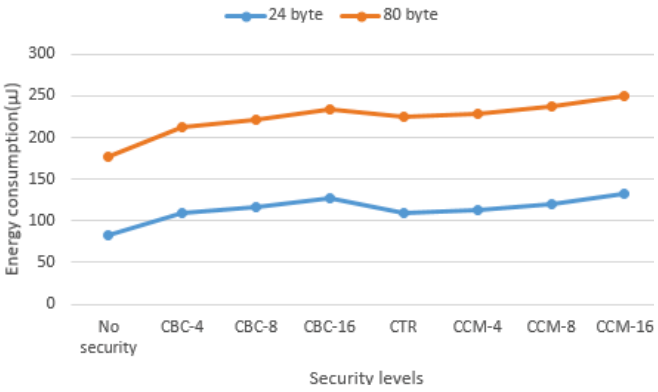

Fig. 6 Energy consumption for different payload size

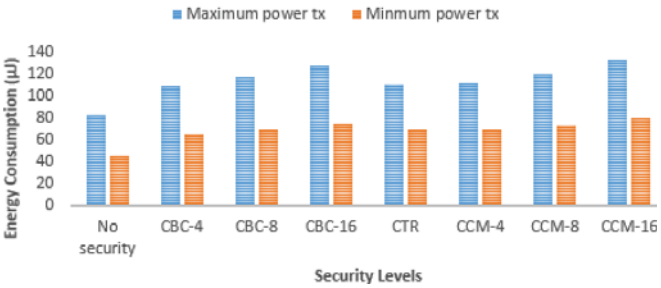

Fig. 7 Energy consumption of different security levels with minimum and maximum transmission power-24 bytes payload

B. Latency Evaluation

In this section, the trade-off between security level and latency is studied and evaluated. It is assumed that cryptography will increase the computation time when adding/removing security services. This also applies for communication overhead, as MIC adds an extra byte to the frame, consequently, a longer frame requires more time for transmission. There are many factors which affect the time required for delivering a single packet. Note that CCA is disabled here to prevent its impacting the results. Fig. 8 depicts the process for transmitting a frame with and without security services. It is demonstrated based on the functionality of ContikiMac. ContikiMac waits for an acknowledgement after each transmission to guarantee that a transmission has been received at the next hop.

Latency without security services can be calculated analytically as follows:

TABLE VI
ENERGY CONSUMPTION OF TRANSMITTING ONE PACKET WITH A PAYLOAD OF 80 BYTE IN DIFFERENT SECURITY LEVELS

Security level	MCU energy consumption (μJ)	Radio energy consumption (μJ)	Total energy consumption (μJ)	Percentage of increased security overhead over non-secure packet (%)
0	11.93	165.67	177.6	-
1	35.92	176.82	212.74	20%
2	36.2	184.79	220.99	24%
3	36.49	197.5	233.99	31.7%
4	51.26	173.63	224.89	26.62%
5	51.35	176.82	228.17	28.47%
6	51.65	184.8	236.45	33%
7	51.68	197.53	249.21	40.32%

TABLE VII
PERCENTAGE OF SECURITY COST OVER NON-SECURE PACKET TRANSMISSION WITH MINIMUM AND MAXIMUM TRANSMISSION POWER

Sec_LVL\TX Power	With maximum transmission power	With minimum transmission power
No Security	-	-
CBC-4	31.54%	44.47%
CBC-8	40.72%	52.77%
CBC-16	54.40%	65.05%
CTR	33%	51.40%
CCM-4	35.60%	53.32%
CCM-8	44.80%	62.05%
CCM-16	60.46%	76.10%

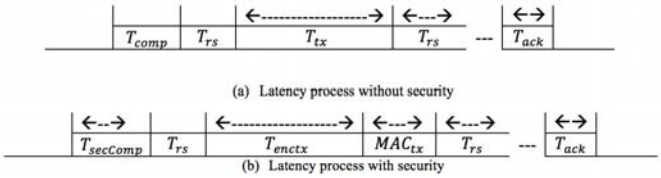

Fig. 8 Latency process

$$Latency = T_{comp} + T_{tx} + T_{rs} + T_{wait} + T_{ack} \quad (4)$$

where, T_{comp} is the time required to process a frame format by MCU, T_{tx} is the time required to transmit the actual frame, T_{rs} is the time required for a radio to switch from transmit mode to receive mode or from idle to transmission mode, T_{wait} the time needed to receive an acknowledgement from the destination, and T_{ack} the time required to process an acknowledgement frame. Fig. 8 (b), shows the required overhead when security services are added to the communication. It is assumed that Cryptography, Integrity and Authentication are enabled. This is demonstrated mathematically in the following formula:

$$Latency_{sec\_enabled} = T_{seccomp} + T_{enctx} + MIC_{tx} + T_{rs} + T_{wait} + T_{ack} \quad (5)$$

where, $T_{seccomp}$ is similar toT_{comp} but with one or more security services such as cryptography, T_{enctx} is the required time to transmit an encrypted actual frame. MIC_{tx} is the time it takes to transmit the extra bytes needed for authentication. The time needed for the extra bytes depends on the length of MIC, it can be 4, 8 or 16 byte.

Scenario 1: Latency evaluation with different payload lengths Network performance may be affected by security services in terms of latency. This might be due to the extra overhead incurred by processing and transmitting. Fig. 10 shows the simulation layout of this experiment. The latency is obtained by calculating the time it takes to transmit a packet from node 3 to node 1 passing through node 2. This includes the time needed to add data to buffer, add security services, transmitting time, receiving time and finally removing security services at the destination. The extra time added by security services for transmitting one packet with two different payload length has been measured. The first with 24 byte, and the second with the same setting but with an 80 byte payload length. In the simulation, to obtain an accurate result for latency added by security services at each level, the radio is kept on for all nodes to avoid latency caused by RDC protocol. The experiment is run without security services, at security level 0, then again for each progressive security level. The receiver in this experiment located in two hops distance, hence, the layer two acknowledgement cannot be received at the sender. Consequently, the extra time over level 0 is recorded as follows, where n is the number of received packets:

$$TotalLatency = \sum_{k=1}^{n} (rx_{time} - tx_{time}) \quad (6)$$

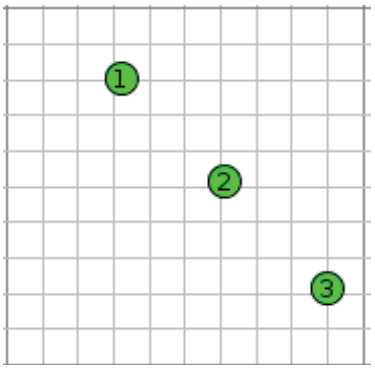

Fig. 9 Experiment layout for latency with three nodes

Fig. 10 shows the latency performance in ms for each security level of the IEEE 802.15.4 security standard. As can be seen, latency increases sharply when security services are enabled. For example, the latency is almost $42ms$ without

security, and with an 80 $byte$ payload, this rises dramatically by almost 328% when authentication is enabled (Level 1).

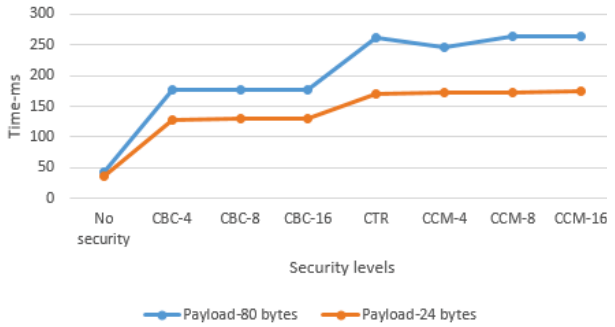

Fig. 10 Latency time per-packet with different payload length

The result shows that all authentication levels [*CBC-4, 8 and 16*] have similar latency performance once authentication is enabled. This may indicate that MIC length of [4, 8 and16] has similar effects on latency in the two payload experiments. CTR encryption increases the latency by almost 526% over level 0. This includes the latency of encryption at the source, decryption and encryption at the relay node, and decryption at the destination node. Overall, latency performance increases sharply with authentication by more than three times of the original packet cost, but it increases with encryption by almost 46% over authentication cost. This indicates that latency is affected more by processing overhead than with transmission overhead. In fact, the processing effects can be noticed clearly by observing the latency at different payload lengths. As can be depicted in Fig. 10, the greater the payload length, the greater the resulting latency, due to the need for more resources being required to encrypt or decrypt a packet.

C. Throughput Evaluation

The objective of this experiment is to assess whether security services have obvious impact on the throughput of packets. In this experiment, throughput refers to the number of packets received at the destination node over a certain time. Throughput has been calculated between two nodes with different security levels for 300 $seconds$. A payload of 24 $byte$ is used in all levels. To obtain an accurate result, the radio of the receiving node is kept 'on' to achieve the maximum throughput. Theoretically, security services are expected to affect the number of received packets, because the radio keeps on longer to transmit longer packet length with authentication, and the MCU computation takes longer to process security operations. As shown in Fig. 11, the percentage of received packets at $securitylevel1$ decreases by 53.5% when compared to a state of no security level throughput. This percentage is similar for levels 2 and 3, with only small variations. Levels 4, 5, 6 and 7 have a greater effect on throughput by reducing the percentage of received packets to almost 62%. At higher levels, cryptography and authentication are enabled, and this cause the drop in throughput. Overall, authentication decreases throughput by almost 53%, and encryption and authentication by almost 62%.

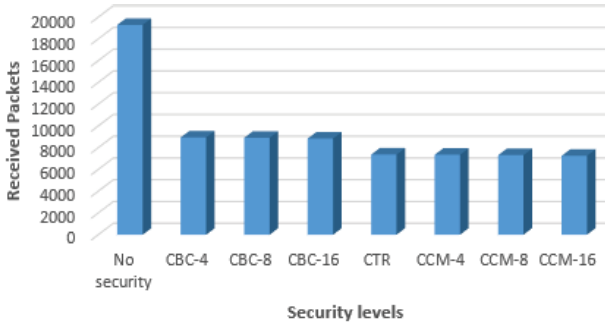

Fig. 11 Throughput of different security levels-300 seconds

TABLE VIII
MEMORY EVALUATION ON TTMOTE SKY HARDWARE

Scheme	text (B)	data (B)	bss (B)	RAM (KB)	ROM (KB)
Contiki OS	22415	142	5136	∼5.2 KB	∼22 KB
Contiki OS + Security	25449	182	5558	∼5.6 KB	∼25KB

VII. MEMORY FOOTPRINT EVALUATION

The memory required by the security modules might become an issue, especially with such constrained devices as WSN nodes. Evaluating memory usage is crucial, as it provides information on whether a security algorithm could run on constrained devices. This information can be obtained by determining the size of the compiled file with and without security modules. Memory size can be known by using the command ' $size$' followed by the compiled file name on Linux OS. Memory is divided into flash memory (ROM) and dynamic memory (RAM). Table VIII, Figs. 12 and 13 show the memory used by security processes on Contiki OS for different segments on tmote sky hardware. 'text' represents the read-only part of memory, 'data' represents the read-write part of memory, and 'bss' contains uninitialized data, global and static variables which are initialised to zero would be included in this part. RAM size can be determined by the sum of data+bss, and ROM size by text+data. Out of $48k$ in sky mote ROM size, Contiki OS with maximum security services consumes in total $\sim$ $25k$, with only $3k$ used for security, while RAM consumes $\sim$ $5.6k$ out of $10k$ available in sky mote. These results, as depicted in Figs. 12 and 13, show that the hardware could accommodate the security specification of IEEE 802.15.4, leaving 44% of RAM, and 48% of ROM free for application usage.

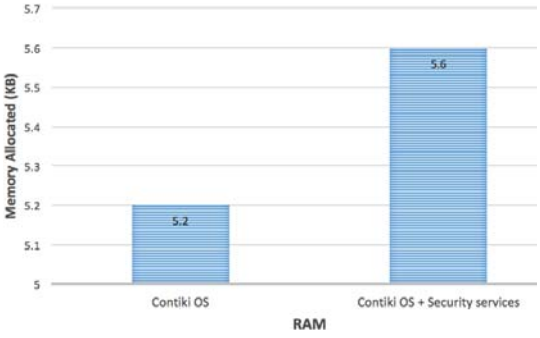

Fig. 12 RAM memory usage

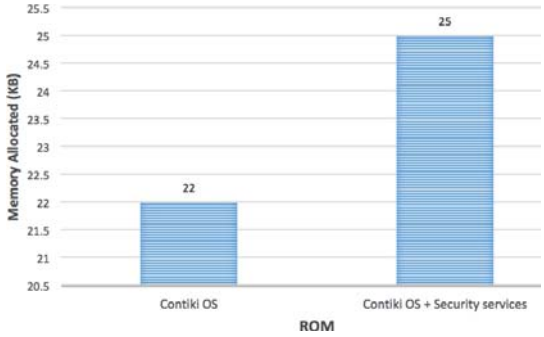

Fig. 13 ROM memory usage

VIII. Conclusion

Security has become essential in IoT devices, but it does, however, come at a cost to resources. Security costs are associated with two main components: the radio for transmission/receiving, and the MCU for processing security operations. The cost of security at several levels has been studied at the IoT MAC layer. The results show that security processes contribute a significant overhead, particularly, in terms of energy consumption, which is quite high. The energy consumed at high security levels may shorten network lifetime significantly. The results also reveal that high security levels increase latency by almost five times over that of the non-secure level when used with an 80 byte payload. It is also observed that latency increases with encryption at a higher rate than it does with authentication due to the greater number of security operations performed by the MCU. In addition, the results have shown that security cost is higher with low transmission power, as the cost of the MCU is not affected by transmission power. Experimental measurements show a significant impact on data throughput. It is reduced by 53% over non-secure packets when authentication is enabled, and 62% when both encryption and authentication are enabled. It is not easy to gather accurate data on security cost, as many factors such as packet length, power transmission, and the type of security service employed can affect the results. However, it is clear that security processes reduce the performance of IoT devices significantly, and energy consumption increases in line with ascending security levels. The results of this paper are aimed to benefit network designers and researchers in terms of security cost, and allow them to choose the level which suits their application requirements. In the future work, a calibration will be made, between emulation results and real-hardware results to check the credibility of the emulation. Also, A mechanism to trade-off security with QoS, and energy consumption will be proposed.

References

[1] Y. Zhong, L. Cheng, L. Zhang, Y. Song, and H. R. Karimi, "Energy-efficient routing control algorithm in large-scale wsn for water environment monitoring with application to three gorges reservoir area," *The Scientific World Journal*, vol. 2014, 2014.

[2] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," *Ad Hoc Networks*, vol. 20, pp. 96–112, sep 2014. (Online). Available: http://linkinghub.elsevier.com/retrieve/pii/S157087051400064X

[3] L. D. Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[4] M. Elshrkawey, S. M. Elsherif, and M. E. Wahed, "An enhancement approach for reducing the energy consumption in wireless sensor networks," *Journal of King Saud University-Computer and Information Sciences*, 2017.

[5] Z. Jiang and Y. Pan, *From Problem to Solution: Wireless Sensor Networks Security*. Commack, NY, USA: Nova Science Publishers, Inc., 2009.

[6] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[7] M. K. Jain, "Wireless sensor networks: Security issues and challenges," *International Journal of Computer and Information Technology*, vol. 2, no. 1, pp. 62–67, 2011.

[8] D. K. G., M. K. Singh, and M. Jayanthi, Eds., *Network Security Attacks and Countermeasures*. IGI Global, 2016. (Online). Available: http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-4666-8761-5

[9] S. B. Othman, A. A. Bahattab, A. Trad, and H. Youssef, "Confidentiality and integrity for data aggregation in wsn using homomorphic encryption," *Wireless Personal Communications*, vol. 80, no. 2, pp. 867–889, 2015.

[10] H. Modares, R. Salleh, and A. Moravejosharieh, "Overview of security issues in wireless sensor networks," in *Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on*. IEEE, 2011, pp. 308–311.

[11] S. Sciancalepore, G. Piro, E. Vogli, G. Boggia, and L. A. Grieco, "On securing ieee 802.15. 4 networks through a standard compliant framework," in *Euro Med Telco Conference (EMTC), 2014*. IEEE, 2014, pp. 1–6.

[12] S. B. Othman, A. Trad, and H. Youssef, "Performance evaluation of encryption algorithm for wireless sensor networks," in *Information Technology and e-Services (ICITeS), 2012 International Conference on*. IEEE, 2012, pp. 1–8.

[13] A. Trad, A. A. Bahattab, and S. B. Othman, "Performance trade-offs of encryption algorithms for wireless sensor networks," in *Computer Applications and Information Systems (WCCAIS), 2014 World Congress on*. IEEE, 2014, pp. 1–6.

[14] C. Panait and D. Dragomir, "Measuring the performance and energy consumption of aes in wireless sensor networks," in *Computer Science and Information Systems (FedCSIS), 2015 Federated Conference on*. IEEE, 2015, pp. 1261–1266.

[15] J. Lee, K. Kapitanova, and S. H. Son, "The price of security in wireless sensor networks," *Computer Networks*, vol. 54, no. 17, pp. 2967–2978, 2010.

[16] A. Dunkels, J. Eriksson, N. Finne, and N. Tsiftes, "Powertrace: Network-level power profiling for low-power wireless networks," 2011.

[17] A. V. Taddeo, M. Mura, and A. Ferrante, "Qos and security in energy-harvesting wireless sensor networks," in *Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on*. IEEE, 2010, pp. 1–10.

[18] J. Misic and V. Misic, *Wireless personal area networks: Performance, interconnection, and security with IEEE 802.15. 4*. John Wiley & Sons, 2008, vol. 1.

[19] A. Dunkels, "The ContikiMAC Radio Duty Cycling Protocol," SICS, Tech. Rep., 2011. (Online). Available: http://soda.swedish-ict.se/5128/1/contikimac-report.pdf

[20] "Moteiv Corporation. SkyTmote Datasheet," 2006, (Online Document) Available: http://www.eecs.harvard.edu/ konrad/projects/shimmer/references/tmote-sky-datasheet.pdf.