IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

An Analysis for Security Enhancement in Internet of Things using Proposed ECSM Model

Mr. Kapil, Research Scholar, Department of Computer Science, BMU, Rohtak.

Dr.Preeti, Professsor, Department of Computer Science, BMU, Rohtak.

ABSTRACT:

IoT extends the interconnection among the information equipment's, such as computer and mobile phone, to the interconnection of all intelligent or non-intelligent physical objects. In this research paper we have compared and introduced standard based security architecture of the IoT. Our proposed architecture provides message registration, confidentiality & authenticity generating a valid certificate for a valid session key with their identity.

KEYWORDS:

Internet of Things, Security, Privacy, Encryption and Authentication.

INTRODUCTION

Internet of Things (IoT) is a fast-growing technology and prevalent in day-to- day life due to their improved use in ubiquity of smart mobile devices such as smart phones, tablets, notebooks, personal digital assistants (PDA), etc. These devices have become a part of everyone's life in this digital world and have been utilized in various contexts. With reference to this context of research, the currently available huge range of challenges must be focused in depth to create a smart world.WSNs and Internet are integrated as a new application area called Internet of Things (IoT), covering almost every area in current daily life. Wireless sensor network(WSN) is a group of large number of sensor nodes organized or dispersed that combine to form a network which is used to sense data such as pressure, temperature, sound, vibration, motion etc. after collecting data through sensor nodes the data is collectively send to a sink node where data can be observed and analyzed. The data which is required can be rectifying by asking queries and gathering result from the

sink node. The data measured by sensor nodes is in its accurate form. These sensors are implanted at a cheaper cost then traditional wired system. Each sensor node consists of a battery enabled chip, a radio trans receiver, a memory chip and a position finding system [1]. Sensor nodes are constrained devices consist of less efficient battery backup, a small memory chip in terms of storage and other limited resources due to the small size of sensor node.

The main issue with the wireless sensor network is the nodes are abandoned for a long period of time or forever, have a short duration of lifetime and the topology used for implementation is generally unknown. The main challenges in wireless sensor network emerge due to restricted resources they have and deployment of sensor nodes in adverse conditions, where almost insuperable or invincible for humans to attend or observe the sensor nodes. Due to the negligence it may affects the efficiency of many applications in the field of military or civil applications such as security, tactical surveillance, inventory control, distributed computing, intrusion detection, disaster management and detection ambient conditions. Many applications request the sensor nodes to be small in size and limit the transmission range to minimize the chances of detection. This results in additional constraints on other resources such as speed, size of memory, RF bandwidth and lifetime of sensor node. Therefore, efficient techniques of communication are required for enhancing the time period of existence of a sensor node and increasing the rate of acquiring data and reducing the communication latency of such wireless devices [2]. Inspite of having limited communication and computation capabilities a wireless sensor network that consists of thousands or millions of sensor nodes enhances the different ways through which data can be collected from physical environment with highly precise knowledge about the data that is to be sensed. But when it comes to integration of wireless sensor network with the existing Internet it comes with several number of challenges. This dissertation discusses the challenges and the best method to interface WSN with the IoT to monitor the environmental parameters is analyzed.

Objectives of IoT

Compared with the traditional information net- works, IoT has three new goals, i.e., more extensive interconnection, more intensive information perception, and more comprehensive intelligent service. IoT extends the interconnection among the information equipment's, such as computer and mobile phone, to the interconnection of all intelligent or non-intelligent physical objects. It has the following outstanding characteristics:

- Extensiveness in the quantity of devices. The amount of the connected devices will sharply rise from several billions to over hundreds of billions, including a multitude of equipment's, sensors, actuators, vehicles, and devices attached with

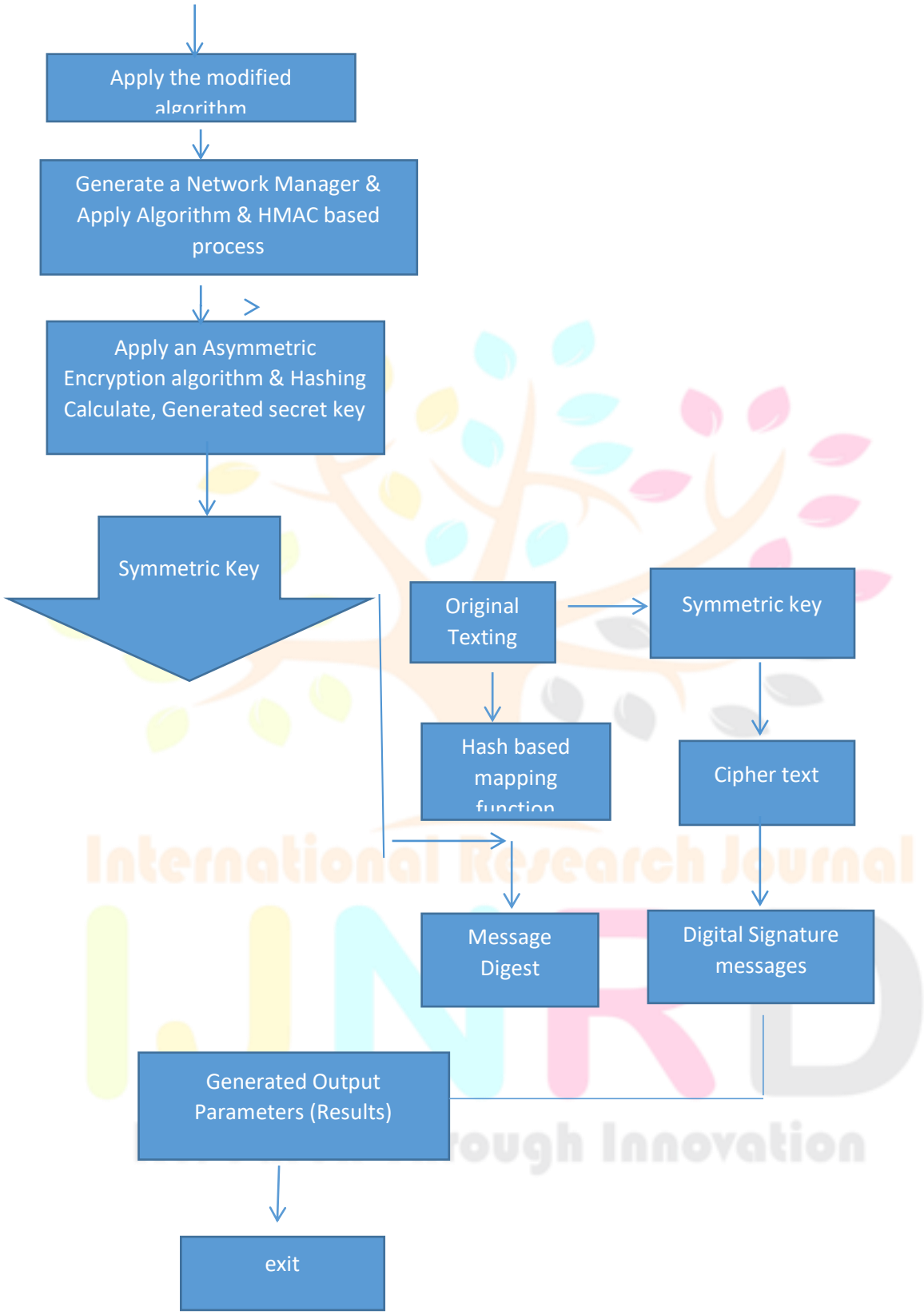
- Extensiveness in the type of networking devices (networking elements) may be powered by the electronic power directly or by batteries; the computation and communication capacity may be greatly different, e.g., some devices even may not have any computational ability.
- Extensiveness in the connection the devices may be connected in a wired or wireless mode; the communication could be a single hop or multiple hops; the connection can be strong state routing or statistical weak state routing.

Thus, in such a large-scale heterogeneous network, we must meet the challenge of highly-efficient interconnection of network elements.

METHODOLOGY

We are implementing the ECSM in NS-2.35 for security of internet, generating valid key id, authentication process, and Registration process and generating the certificate for entering in a network. The Implementation of security on NS-2.35 is a necessary in network simulation. However, currently, NS-2 does not support these features. In this thesis we aim to solve this issue. The information security using cryptographic algorithms which comprises (symmetric and asymmetric) and hash function is to encrypt and send data securely between no. of nodes. The system must encrypt the data or systematically scramble information so that it cannot be read without knowing the coding key. This operation determines to a certain level the strength of the security system; the harder it is to break the encrypted message the more secure the system is to be. In this dissertation we have used ECSM cipher, HASH function and encryption algorithm for encryption/decryption of messages. Results are compared. The proposed scheme is tested using ordinarily image processing. ECSM Handshake CoAP, with its support for reliable message transmission and block wise-transfer [7], could be used to transfer ECSM handshake messages, instead of the complex ECSM handshake protocol. With this, the need for ECSM to support retransmission, fragmentation and handling of reordering could be omitted and just the handshake logic needed to be implemented. CoAP is designed for applications following the ECSM architectural style. So, the ECSM connection is modeled as a CoAP resource which is created when a client wants to initiate a connection and updated to modify the state and parameters of the connection. Figure 4.1 illustrates this idea: The client POSTs to the well-known URI requesting the server to create a new session resource. The server responds with the Verify response code (not yet defined) and Hello Verify Request message in the payload to which the client responds with the same POST containing the cookie. After the server having created the resource, the client requests the server to change session parameters by applying the PATCH method to the resource. The DELETE method can be used to close a current connection and free all resources related to the session.

FLOW DIAGRAM OF WORKING PROCEDURE



We have now seen the different aspects of a secured Internet of Things (IoT) in combination with Constrained Application Protocol (CoAP), we present the first step towards such a secured environment:

We implemented European Cyber Security Month (ECSM) model to secure CoAP during the operational phase.

RESULT

We have simulated directed diffusion with European Cyber Security Month (ECSM) on the framework in exactly the same setup as implemented in NS2 to compare the performance of the simulator with respect to NS2.

PERFORMANCE PARAMETERS

Performance parameters that are been used as a comparative study between the base paper and the proposed work**.**

- Average Throughput
- Average energy
- End to End Delay
- Packet Delivery Ratio

Table 1:Simulation parameters in NS2

Simulation Tool	NS-2.35
Operating System	Ubuntu 12.04
No. of Nodes	15,20,25,30
Technology	DTLS, ECSM
MAC/PHY layer	IEEE 802.11
Antenna model	Omni directional
Interface queue size	50 packets
Data payload	512 bytes
Pause time	20 seconds
Channel bandwidth (data)	12Mbps
Transmission range	250m
Examined protocol	AODV
Interface Queue Type	Queue/Drop Tail/PriQueue

Mobility model	Random way point
Simulation area	917M*500M
Link Layer Type	LL
Rx Power	0.6
Tx Power	0.6
Data Rate	200k
Simulation Time	20 secs

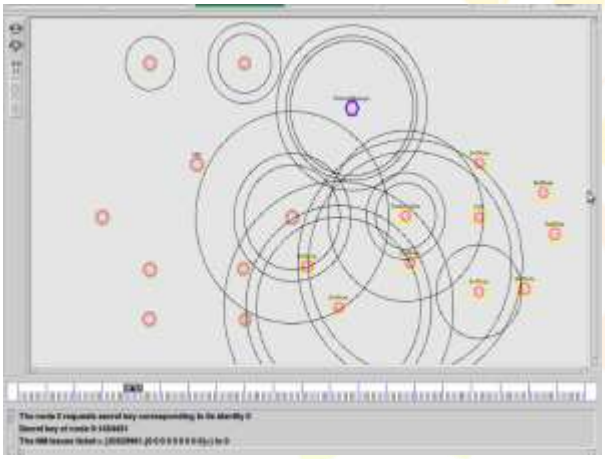


Figure: Checking Authentication of node 0

Figure shows the Authentication process of a node and checking its corresponding identity node and if authentication process is completed then network manager generates a secret key of a node 0.

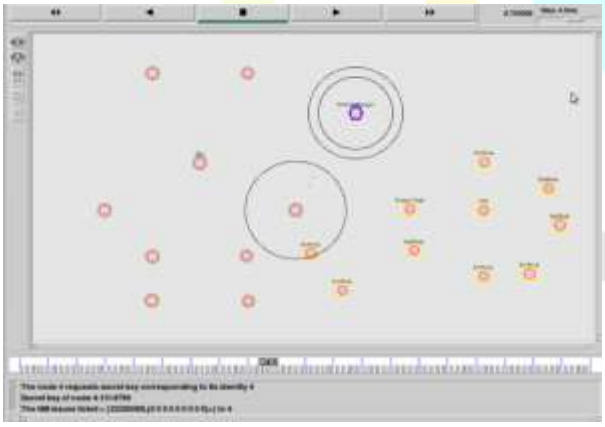


Figure: Starting Registration Process

Figure shows that after the authentication process is completed after then generates a request message to issuing the ticket or certificate authentication. Node 4 request secret key to generate a request of a valid CA or ticket

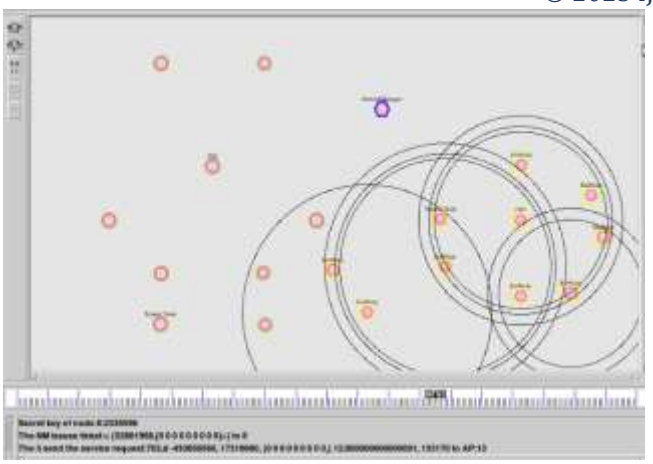


Figure: Issuing Ticket Process of a Node to Authenticate Node

Figure shows the After completion the network manager issue a ticket, node 3 send the service request for a valid session key.

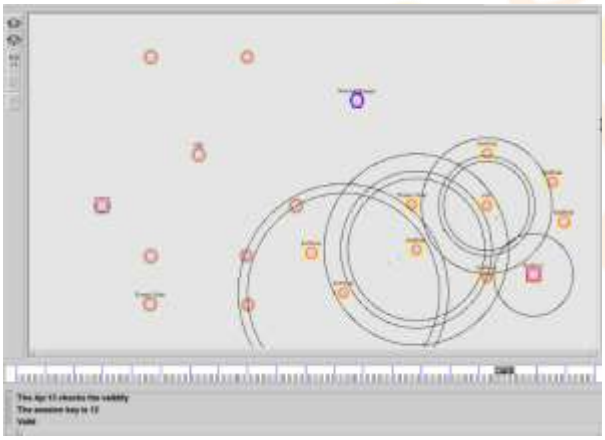


Figure: complete valid processes

In Figure shows the process of Registration, Authentication, Validation, trusted node all process is completed then generates a valid key session. So valid session key is 12

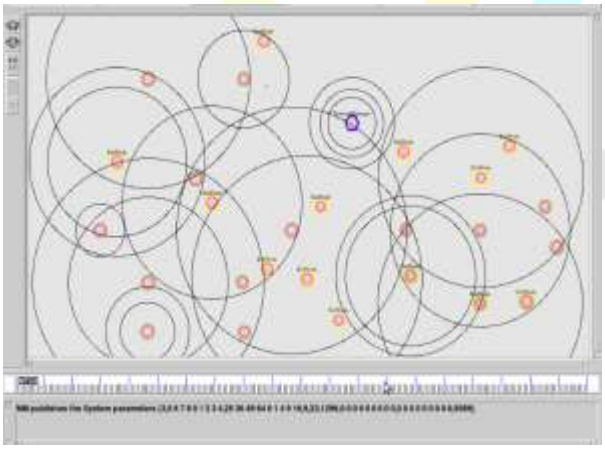


Figure: Communication started between nodes

Figure shows the starting of communication process between 2 nodes. Client send the request to the server side and server send the acknowledge . Transmission will be done between Network Manager and 0. node 1 is a intermediate node between trasnmission process.

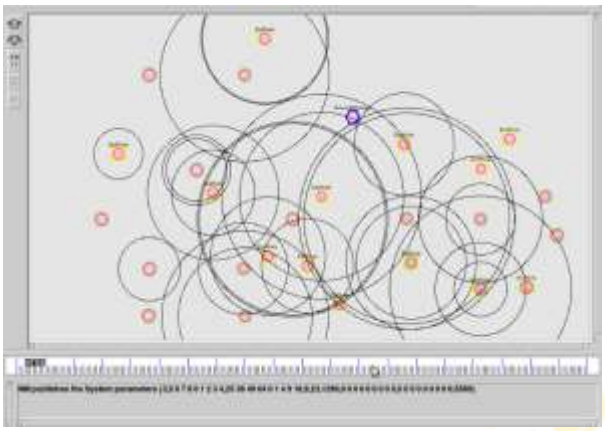


Figure: Communication started between nodes, transmission started

Figure shows that the communication between 2 networks one is an Access Point network and another one is WSN in both network starting to send and receive the Data.

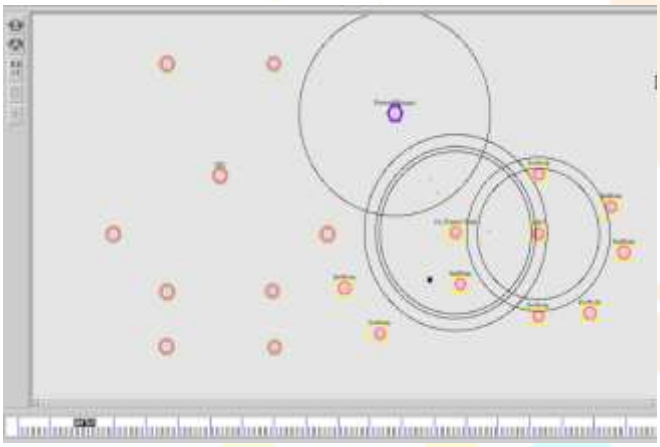


Figure: Packet drop

Figure shows the packet dropping during communication process between network manager and a WSN node. When client generate the request message to server then server generate the reply message within same window size. If that time client drops the packet that means, it's a suspicious node.

CONCLUSIONS

In this paper we have compared and introduced standard based security architecture of the IoT (ECSM). ECSM integrate and modified some internal files in ns-2.35. The authentication is performed during a fully authenticated ECSM handshake and based on exchange certificates containing hash function which we have implemented in ns-2.35. Our extensive evaluation based on network simulation tool in WSN our proposed architecture provides message registration, confidentiality & authenticity generating a valid certificate for a

valid session key with their identity. Previous works have demonstrated techniques to minimize packet headers for similar protocols and generating a certificate for every node. With the help of Hash function, we plan to apply these techniques to ECSM in real time implementation in future work.

FUTURE SCOPE

In future work this system can be deployed in real world IoT environment containing smart sensors, constrained devices and smart phones with real time application. Such deployment helps to deeply study the ECSM and evaluate significance of this system with confidential applications.

REFERENCES

[1] ANSI X9.62-2005. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). American National Standards Institute, Nov. 2015.

[2] F. Aslam, C. Schindelhauer, G. Ernst, D. Spyra, J. Meyer, and M. Zalloom. Introducing TakaTuka – A Java Virtual Machine for Motes. In Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems (SenSys 2008), New York, USA, Nov. 2018.

[3] S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk, and B. Moeller. Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS). RFC 4492 (Informational), May 2016. Updated by RFC 5246.

[4] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280 (Proposed Standard), May 2018.

[5] JAIN, A., KANT, K. and TRIPATHY, M. R. Security solutions for wireless sensor networks[C]. Proceedings of the 2012 Second International Conference on Advanced Computing and Communication Technologies (ACCT '12). IEEE Computer Society, 2012, pp. 430433.

[6] A. Becher, Z. Benenson, and M. Dornseif. Tampering with Motes: Real-World Physical Attacks on Wireless Sensor Networks, volume 3934 of Lecture Notes in Computer Science, pages 104–118. Springer Berlin / Heidelberg, 2016.

[7] K. Hartke and O. Bergmann. Datagram Transport Layer Security in Constrained Environments. draft-hartke-core-codtls-02, July 2012.

[8] Z. Shelby, K. Hartke, C. Bormann, and B. Frank. Constrained Application Protocol (CoAP). draft-ietf-core-coap-12, Oct. 2012.

[9] T. Aura. Cryptographically Generated Addresses (CGA). RFC 3972 (Proposed Standard), Mar. 2015.

[10] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (Proposed Standard), Aug. 2018.

[11] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944 (Proposed Standard), Sept. 2017.

[12] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944, IETF, Sept. 2017.

[13] L. Huai, X. Zou, Z. Liu, and Y. Han. An Energy-Efficient AES-CCM Implementation for IEEE802.15.4 Wireless Sensor Networks. In Proceedings of the International Conference on Networks Security, Wireless Communications and Trusted Computing (NSWCTC 2009), Wuhan, Hubei China, Apr. 2009.

[14] S. F. Pileggi, C. E. Palau, and M. Esteve, "On the convergence between wireless sensor network and rfid: Industrial environment," in 8th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, pp. 430–436, May 2010.

[15] B. Zhang, K. Hu, and Y. Zhu, "Network architecture and energy analysis of the integration of RFID and Wireless Sensor Network," pp. 1379–1382, IEEE, May 2010.

[16] D. McGrew and D. Bailey. AES-CCM Cipher Suites for Transport Layer Security (TLS). RFC 6655 (Proposed Standard), July 2012.