Computer Systems Science & Engineering
DOI: 10.32604/csse.2022.024018
Article

Tech Science Press

Cyber Secure Framework for Smart Containers Based on Novel Hybrid DTLS Protocol

Waseem Ullah Khan*, Safdar Nawaz Khan Marwat and Salman Ahmed

Department of Computer Systems Engineering, University of Engineering and Technology Peshawar, Peshawar, 25120, Pakistan
*Corresponding Author: Waseem Ullah Khan. Email: waseem@uetpeshawar.edu.pk
Received: 30 September 2021; Accepted: 15 December 2021

Abstract: The Internet of Things (IoTs) is apace growing, billions of IoT devices are connected to the Internet which communicate and exchange data among each other. Applications of IoT can be found in many fields of engineering and sciences such as healthcare, traffic, agriculture, oil and gas industries, and logistics. In logistics, the products which are to be transported may be sensitive and perishable, and require controlled environment. Most of the commercially available logistic containers are not integrated with IoT devices to provide controlled environment parameters inside the container and to transmit data to a remote server. This necessitates the need for designing and fabricating IoT based smart containers. Due to constrained nature of IoT devices, these are prone to different cyber security attacks such as Denial of Service (DoS), Man in Middle (MITM) and Replay. Therefore, designing efficient cyber security framework are required for smart container. The Datagram Transport Layer Security (DTLS) Protocol has emerged as the de facto standard for securing communication in IoT devices. However, it is unable to minimize cyber security attacks such as Denial of Service and Distributed Denial of Service (DDoS) during the handshake process. The main contribution of this paper is to design a cyber secure framework by implementing novel hybrid DTLS protocol in smart container which can efficiently minimize the effects of cyber attacks during handshake process. The performance of our proposed framework is evaluated in terms of energy efficiency, handshake time, throughput and packet delivery ratio. Moreover, the proposed framework is tested in IoT based smart containers. The proposed framework decreases handshake time more than 9% and saves 11% of energy efficiency for transmission in compare of the standard DTLS, while increases packet delivery ratio and throughput by 83% and 87% respectively.

Keywords: Logistic container; logistics security; cyber security; perishable products monitoring

1 Introduction

With the recent advancements in communication and physical sciences, it is now possible to connect physical objects to the Internet from any place any time. This advancement is referred to as the Internet

of Things (IoT) [1]. One of this century's key technological development has been the IoT, which is still in its fancy stages. In the coming years, this development is expected to hit a big figure. By the end of 2023, 51 billion IoT devices are expected to exist [2]. According to Statista report, it is predicted that this number will rise to 75.4 billion by 2025. The significance of the IoT system has been acknowledged by major international standards bodies, thereby ensuring development towards the proper functionality, flexibility and compatibility of this system. Due to which IoT is making an impact in the majority of the fields i.e., healthcare, agriculture, logistics, oil and gas industries and traffic [3]. In logistics many products such as foods, vegetables, fruits, medicine, cosmetics and especially perishable products which are sensitive to humidity, temperature and pressure etc. and require controlled environment. Commercially available logistic containers are not integrated with IoT devices due to which the perishable products are handled abnormally and give huge food loss. The IoT devices, however can genuinely make an impact on the growing problem of food loss.

Food consciousness has grown amongst the people lately with the exponential increase of the food industries and radical improvements in individuals' dietary behaviors and ways of life [4]. People nowadays are more worried about the quality and safety of the food they consume. Food safety is perceived to include food that is liberated from contaminants and chemicals that may cause the development of microscopic organisms destructive to individuals' safety and lives [5]. According to [6], approximately 33% of food delivered for human consumption is being wasted worldwide, which amounts to 1.3 billion metric tons. A huge extent of this is because of loss in quality of foods during transportation. As many as 40% of food perishes in developing countries while it is being shipped. A significant portion of waste happens in the transportation, changing in environmental conditions i.e., temperature and humidity etc., inadequate cooling and even in post-harvest storage and handling [7].

Logistic container plays a significance role in the economic growth of country. Logistics means to deliver the product to legitimate carrier in the right state, in accurate quantities, at the right time, at the right place. However, according to Food and Agriculture Organization, 33% of perishable products do not reach in accurate quantity at the consumer's location [8]. The primary source of this loss is variations in environmental conditions such as temperature, humidity and heat etc. To address these challenges, proper monitoring of environmental conditions from farm to fork is essential. However, the monitoring mechanism and the supervision system in logistics container is not yet implemented appropriately. The use of telematics technology is documented in the literature; however, it measures the temperature of the entire unit rather than the temperature of the perishable product. Also, radio frequency identification (RFID) and barcode scanners can only identify direction, not product quality [9]. Smart container concept has been proposed to overcome this issue and is based on the integration of IoT with commercially available logistic container. Smart container is a shipping container which are integrated with Internet of Things (IoT) technologies and sensor nodes to keep the perishable food fresh till it reaches the final destination [10]. The IoT devices inside the smart container continuously measure environmental parameters which are pertinent for the quality of perishable foods. Undoubtedly, IoT has a significant impact in the implementation of smart container. However, there exists many challenges, but one of the critical aspects, which need special attention, is the adoption of state of the art security mechanisms. Since IoT devices are resource constrained having limited computing power and memory, due to which they are prone to different cyber security attacks. Thus, if the IoT devices monitoring these products are handled improperly due to security attacks or product sensitive information is lost, then it will give huge economic loss. In terms of security implementation in smart container, no concrete framework for secure monitoring of smart container in IoT environment has been deployed to date. Development of secure monitoring system for smart container with the help of IoT devices is an essential requirement of this era. The Datagram Transport Layer Security Protocol has emerged as the de facto standard for communication security in the IoT and standardized by Internet Engineering Task Force (IETF) [11]. However, DTLS

was initially designed for comparably powerful devices [12]. It is still expensive to implement DTLS on constrained IoT devices due to the computational overhead. The DTLS first establish a secure session between two communicating parties before transmitting data and negotiate same cipher suites. This is known as session negotiation and is achieved through process called handshake. However, DTLS is vulnerable to the Denial of Service (DoS) attacks. Also, the DTLS's cookie exchange scheme during the handshake session fails to handle DoS attacks. DoS attack is the act of complete elimination or disrupt of network communication. It targets the network availability by preventing the desired services to the intended user. Also, these attacks are very crucial for IoT devices in terms of memory, power and energy consumption. Though some frameworks exist related to smart container and IoT, security of IoT, use of CoAP and DTLS in constrained environment [13–15]. However, no work has been done on the security of smart container to mitigate the chances of DoS attacks yet. Therefore, the main contribution of this paper is to design a cyber secure framework by implementing novel hybrid DTLS protocol in smart container which can efficiently minimize the effects of cyber attacks during handshake process. The proposed framework used the Trusted Entity (TE) mechanism which is responsible for the authentication of client and for the exchange of secret key by using the message authentication code (MAC) algorithm. The TE authenticates only the trusted client for starting secure handshake session with the server and rejects malicious handshake session. The significance of proposed framework is to improve the efficiency of energy transmission and utilization and to minimize the chances of cyber security attacks.

The remaining part of this paper is structured as follows. The literature review related to smart container, IoT and cyber security is discussed in Section II. Section III presented the system architecture of smart container and DTLS protocol, and the proposed system architecture based on novel hybrid DTLS protocol. The proposed novel hybrid DTLS algorithm is discussed in detailed in Section IV. Simulation and evaluation of results is presented in Section V. Concluding remarks are given in Section VI.

2 Background and Related Work

This section gives a comprehensive review of the previous work that has been done in the field of smart containers, smart logistics, IoT and security of IoT.

In [16], the authors discussed a cognitive sensor net for fruit logistics. The authors explained that the intelligent container is a sensor network for the controlling and monitoring of perishable food items such as vegetables, fruits or meat. This paper presented the paradigm of dynamic FEFO (First Expire First Out) the remaining life time estimated shelf life of the transported fruits in the logistic process. In [17], the authors addressed challenges and opportunities in remote container monitoring (RCM) of perishable food items by designing a prototype of an intelligent container based on a case study of banana transport and prediction of hotspots that are a critical risk for item loss. However, development of mathematical models for shelf life prediction for new types of products is of high importance. A smart grain container for tracking food consumption have developed in [18]. In this prototype, the ultrasonic sensor is used to detect the level of container and transmits the information to the remote mobile or personal computer via bluetooth. However, this prototype does not utilize any mechanisms for expiry detection of items stored in the container. In [19], the authors elaborated that the new technique of RFID's based WSN in intelligent container has decreased wastes and improve quality in food logistic. This paper focused on tracking and monitoring of intelligent packaging and logistics for the fresh food. However, the future trend of RFID design will be heavily focused on increasing functionality while lowering costs in order to develop a smart coupling of heterogeneous technologies that leads to a better system solution.

The layered architecture of IoT is discussed in detail in [20] and also provided an overview of security attacks in each layer. They presented an overview of communication technologies along with characteristics and limitations which are used by IoT applications. They discussed existing security mechanisms with their

limitations and restrictions to secure the IoT environment. This paper suggested a new six-layered IoT architecture to secure IoT infrastructure. In [21], a security testbed framework to secure IoT environment has been proposed. The paper presented implementation of a security module for authentication and monitoring of IoT devices. The proposed system strengthens the IoT security by providing information about IoT devices such as device location, IoT device user at the time of incidence, total number of IoT devices in the network etc. In [22], authors presented an architecture to secure data communication in medical devices with limited resources by deploying an IoT security gateway as an intermediary between device and destination. This solution solves the issues with communication of data over the Internet. However, it leaves gaps in security from the device to the gateway. Data may be intercepted before it reaches the gateway or after if the gateway has been compromised. While this solution focuses on communication between gateway and Internet other solutions attempt secure data from the device.

In [23], authors discussed in detailed the CoAP implementation and its application in transport logistics. CoAP is used for machine to machine (M2M) communication in logistic applications for supervision of the environmental conditions during transport. The embedded system architectures used for the implementation and evaluation are TinyOS and Contiki. The results showed that the CoAP performed better as compare to HTTP in constrained environment. In [24], authors proposed DTLS group handshake involving a group of CoAP servers and client where first handshake needs a ECDH public key operation. On the other hand, the subsequent handshakes are performed based on preshared key mode. In this scheme, a trusted third party will assist the client and servers to negotiate a key. However, this approach needs cooperation between the group members as session key established with one group member has to be shared with all the group members to avoid further DTLS handshake. Lightweight version of the Datagram Transport Layer Security protocol for securing CoAP communication was presented in [25]. This paper provided a secure framework for IoT by implementing lightweight DTLS. It has also enlightened the standardization activities going on in security domain. IoT home automation has been presented as an application scenario.

3 System Architecture

This section enlightens the brief overview of smart container architecture. Also, an overview of the standard DTLS protocol is presented in detailed. At last, the proposed system architecture is presented which is based on hybrid DTLS protocol. The above proposed architecture is used for the smart container application scenario.

3.1 Smart Container

A smart container is a shipping container which uses latest technologies to provide the missing information in the food supply chain. Smart container is equipped with the IoT devices that can be used to control and monitor environmental conditions related to temperature, humidity, pressure, light exposure etc. It is also used for the management of logistic processes, especially for perishable products such as fruit and vegetables [26]. The smart container is able to precisely monitor the condition of perishable products, as well as track its geographical position. Thus, the transport losses can be reduced due to better climate control and enhanced distribution strategies. Wireless sensor nodes are arranged between the perishable products. The sensor nodes continuously measure environmental parameters that are relevant for the quality of the perishable products. The sensor nodes send this information to a central processing unit (computer) inside the container. The processing unit calculates the shelf life of the goods and in case the perishables expire unexpectedly fast, it informs the logistics department via telematics [27]. In this way FEFO can be established and losses of perishables during transportation and storage can be reduced [28]. Fig. 1 shows the smart logistic concept where IoT devices are connected in an intelligent way and there exists real time monitoring and tracking.

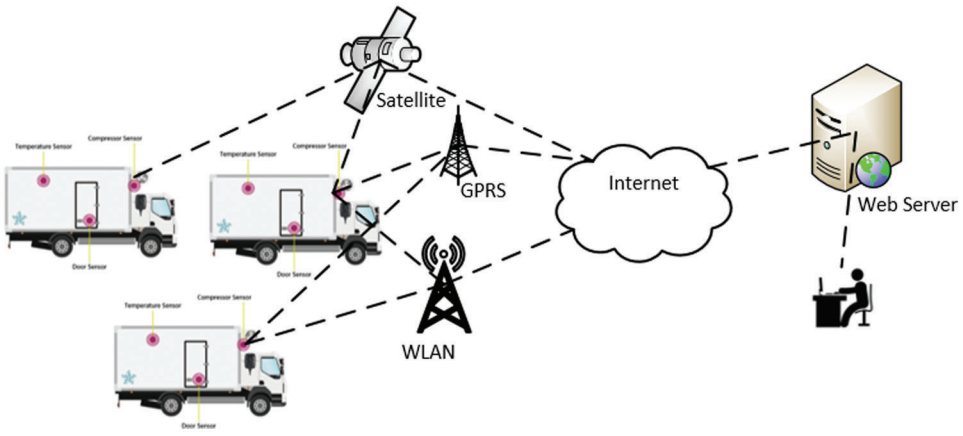

Figure 1: Smart logistics and transportation

The IoT connects these objects via sensors, actuators and other devices to collect and transmit real time data about network activities. The smart container can use different communication channels to send this information via Internet to the logistics department. During shipping by sea, the smart container can use satellite communication. While during shipping by road it can use UMTS/GSM. The overall system of the smart container consists of: A network of wireless sensors, installed inside the container to monitor deviations of temperature and other parameters. A freight supervision unit, installed inside the container, to evaluate the measured data and to calculate a shelf-life prediction for the transported commodities. A telematics unit for external communication by the global system for mobile communications (GSM) or satellite networks [29]. A remote server for web access and integration into company databases.

3.2 Datagram Transport Layer Security

The DTLS is derived from, and designed according to the Transport Layer Security (TLS) infrastructure with some modifications to operate over User Datagram Protocol (UDP). With the emergence of Constrained Application Protocol (CoAP) as a specialized web transfer protocol for constrained devices, DTLS is the preferred security protocol in IoT. DTLS establishes secure session between two communicating parties and ensures the security of data exchange between them.

The DTLS specification lists a set of recommended cryptographic algorithms, also known as cipher suites, to be used for performing the handshake and encrypting data.

The DTLS has record protocol and four sub-protocols such as Handshake, Alert, Change Cipher Spec and Application protocols [30]. To set up a new connection and negotiate security parameters, like cipher suite, hash algorithms or compression, the Handshake protocol is used During handshaking process, both the parties are allowed to negotiate the cipher suite, choose same algorithm, same version, and verify other parameters and certificates necessary for secure communication [31]. Failure of handshaking process results in unsuccessful communication. Fig. 2 shows DTLS Handshake message flow.

The client initiates the handshake by sending a Client Hello (CH) message to the server. The CH message consists of supported protocol version, the supported cipher suites, supported algorithms and a random number [32]. The Hello Verify Request (HVR) message is sent to client by server in order to verify that the message was sent from authentic client. The “Hello Verify Request” message consists of new cookie by generating the request connection for client. After receiving the “Hello Verify Request” message from server, the client sends the “Client Hello” message which contains the cookie received from server.

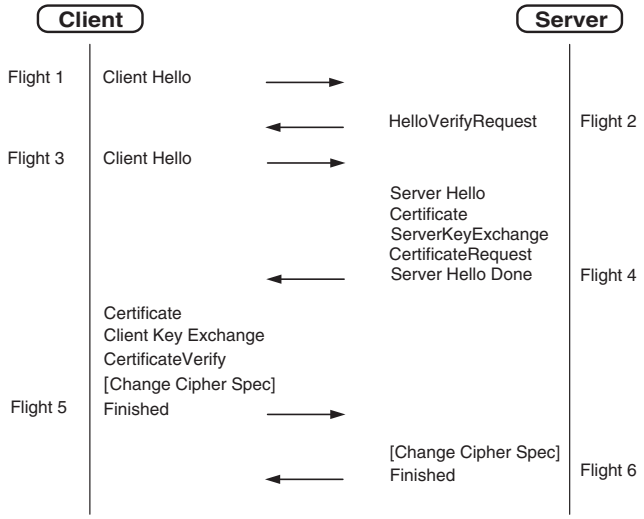

Figure 2: DTLS handshake message flow

Upon successful message receiving, the server verifies the cookie and sends the "Server Hello" message to the client. After sending the "Server Hello" message, the server also sends a message which contains "Server Certificate", Server Key Exchange (SKE), "Certificate Request". At last, the server sends the "Server Hello Done" message to end the flight. The client sends the "Certificate Message" and "Certificate Verify Message" in order to authenticate itself, proving that the public key (client) and private key (server) both are matched. The "ChangeCipherSpec" message is sent by the client, showing that the messages are encrypted successfully with keys and cipher suites. Finally, the "Finished" message is sent containing encrypted previous messages. The server then sends the "ChangeCipherSpec" and "Finished" messages which ends with handshake process. The messages are then fragmented, compressed and encrypted on the Record layer. The Record protocol is used to apply security parameters and to protect data during handshake.

Thus, DTLS is used to handle the unreliable nature of UDP [33]. But DTLS is vulnerable to the cyber security attacks. During the handshake process in DTLS, the cookie exchange scheme is unable to minimize the security attacks.

3.3 Proposed System Architecture

Considering the smart container network, our proposed system architecture is as shown in Fig. 3. The proposed system architecture composed of three modules such as internal network, communication gateway and external network. The internal network consists of logistic container having IoT devices or sensor nodes for monitoring and controlling and Routing Protocol for Low Power and Lossy Networks (RPL) border router/gateway for connectivity with external network i.e., Internet and a web server that provides access through graphical user interface (GUI) to the data. The novel hybrid DTLS protocol is implemented over the CoAP to secure the entire communication. The proposed architecture is developed and emulated in Contiki operating system and Cooja simulator. The VMWare is installed for Contiki operating system where Cooja simulator and Wireshark is used for development and analysis of result.

The pseudocode implementation of proposed architecture is presented in Fig. 4. In Fig. 4, the steps are explained in detailed. First step is to open simulation, then radio propagation model is selected i.e., Unit Disk Graph Medium-distance loss (UDGM-Distance Loss). The Unit Disk Graph Radio Medium abstracts radio transmission range as circles. Two different range parameters are used i.e., one for transmissions, and one for

interfering with other radios and transmissions. In the next step, wismote is selected. Wismote is used having 16 KB of RAM. On one wismote, CoAP server is compiled for communication within container and communication is secured by implementing novel hybrid DTLS. Similarly, on another wismote, Routing Protocol for Low-Power and Lossy Networks (RPL) border router is compiled for connectivity with external network. The next step is the creation of bridge between the border router and external network. To enable the bridge, need to open serial socket server on border router through "Listening on port 60001". In this way, RPL network is created. Now to connect this RPL network to the external network in the scenario, tunslip utility is used which is provided in Contiki. In this way tunslip creates a bridge between the RPL network and the local machine by using command:

- sudo. /tunslip6-a 127.0.0.1 aaaa:1/64

In order to initiate the RPL border router connection, open a new terminal in Contiki and type the following commands:

- cd Contiki/examples/ipv6/rpl-border-router/
- make connect-router-cooja

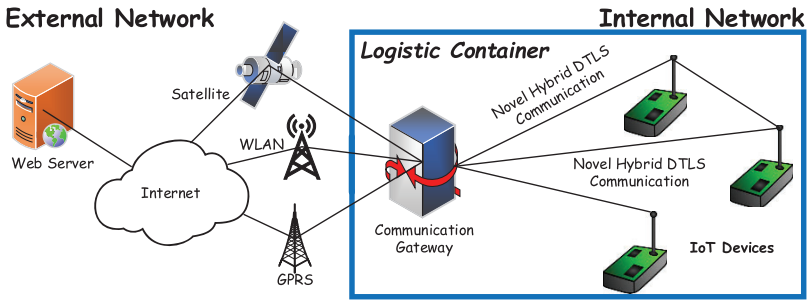

Figure 3: Proposed architecture

Pseudocode Implementation of proposed algorithm

While: Launch Cooja
Initialize: UDGM-Distance Loss
Initialize mote: Wismote
Generate: Mote for Compilation of RPL Border Router
Initialization of wismote for
Compilation of CoAP servers
Assemble novel hybrid DTLS server for secure communication
Initialize: serial socket server on RPL on listening port 60001
Create loopback connection at 127.0.0.1
Installing CoAP user agent in browser
Define path directories
Restart browser

Figure 4: Pseudocode implementation of proposed algorithm

Finally, Copper (Cu) based CoAP user agent is installed for communication with web server which is then opened in browser for control and monitoring of IoT devices in smart container. The Copper CoAP user agent is an add-on for the Firefox web browser, used for browsing and direct interaction with CoAP resources. The proposed architecture in this paper is modeled on the IoT framework, in which the

Internet is supposed to be linked via IPv6 while certain part of it run on 6LoWPAN. The proposed protocol's stack is presented in Fig. 5. The transport layer in 6LoWPAN is User Datagram Protocol (UDP), which is unreliable normally. UDP provides datagram based transport, which is suitable for use in IoT. Flores et al. [34] implemented the routing layer in our proposed protocol architecture, while the IEEE 802.15.4 was used to incorporate the MAC and physical layers. Based on this protocol stack, DTLS was considered as the security protocol. The DTLS was just above the UDP transport layer in the application layer. Similarly, CoAP provided the application layer functionality.

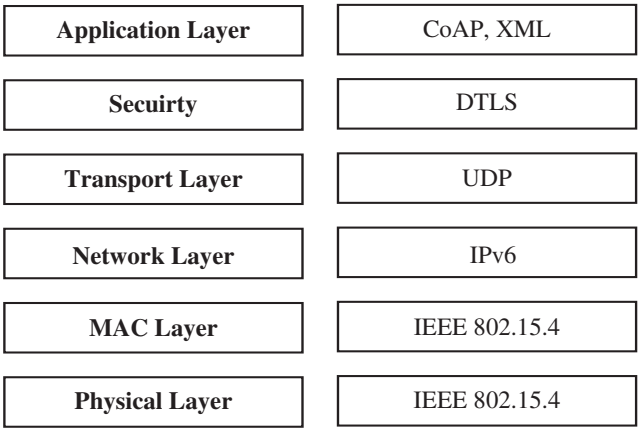

Figure 5: Protocol stack

4 Proposed Novel Hybrid DTLS Algorithm

The proposed algorithm mitigates the chances of cyber security attacks and reduce the DTLS computation overhead. This work detects the cyber security attacks i.e., DoS and DDoS before it reaches to IoT devices. This proposed algorithm uses the concept of Trusted Entity (TE). The TE will be responsible for the exchange of pre-shared secret key by using the message authentication code (MAC) algorithm.

Fig. 6 shows the novel hybrid DTLS algorithm. The server and TE first agree on the pre-shared secret key K before the starting of handshake session. Now the TE and the client both share the key in order to secure the communication between them. Whenever the client wants to start the handshake session with the server, it will send request to the TE first, after receiving request from the client, the TE will provide the sequence number and secret key to the client.

The client will authenticate the Client Hello Message by deriving a message authentication C_auth using the MAC algorithm. Here the MAC size is 16 bytes (128 bits). The authentication message code C_{auth} is generated as,

$$C_{auth} = MAC\ (K,\ SN) \tag{1}$$

where C_{auth} is the client authentication code, K is the shared secret key and SN is the sequence number. After generating the authentication code, the client appends the MAC with the Client Hello Message and sends it to the server through TE to start the handshake session. On the server side, while receiving the Client Hello Message along with authentication code from the client, the server checks the message authenticity. Initially, the server generates its own authentication code as,

$$S_{auth} = MAC\ (K,\ SN) \tag{2}$$

where S_auth is the server authentication code, K is the shared secret key and SN is the sequence number.

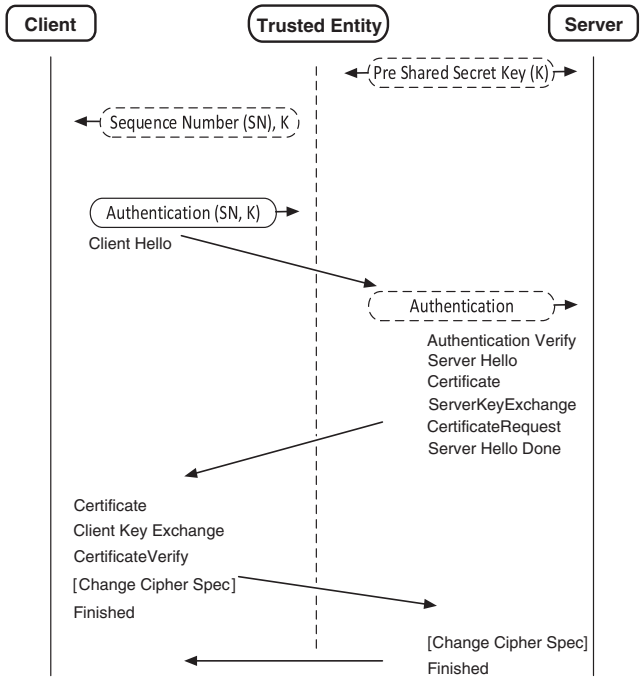

Figure 6: Novel hybrid DTLS algorithm

The server then compares the client authentication code received from the client with its own generated code, if both the codes are same, then it authenticates the client for the services. The server then sends the Server Hello Message by proceedings with the Handshake. Or, if the codes are not the same, the server then rejects the request of the client.

The novel hybrid DTLS used the concept of TE to minimize the chances of security attacks. The server and TE pre-share and agreed on the secret key. Whenever the client wants to start a connection request with server, the TE first authenticates the client for server. Thus, server only further process and provide service if the client is an authentic. The client only sends message through TE that ultimately reduce the overhead of authentication of client on server and minimize the chance to leading the scenario where burden of service processing imposed by attackers.

5 Implementation and Results

To evaluate the performance of our proposed novel hybrid DTLS algorithm, proposed algorithm implemented in Cooja simulator and Contiki OS. Contiki is an open source operating system which is designed for IoT constrained devices. Cooja is an open source network simulator used by Contiki OS.

5.1 Simulation Parameters

The parameters used for simulations are as shown in Tab. 1. These simulation parameters are used in Contiki operating system. The mote used is Wismote having 16 KB of RAM. The DTLS used the TinyDTLS library in this simulation. The DTLS cipher suite used is TLS_PSK_WITH_AES_128_CCM_8.

Table 1: Simulation parameters

Environment	Parameters
Simulator	Cooja
Number of motes	5
Sensor motes	Wismote
Compiler	Msp430-gcc (in Ubuntu)
DTLS library	TinyDTLS 0.8.2
DTLS cipher suite	TLS_PSK_WITH_AES_128_CCM_8
Application layer protocol	CoAP
Network layer protocol	6LoWPAN
Link layer protocol	IEEE 802.15.4
Radio propagation model	Unit disk graph medium (UDGM): distance loss
Operating system	Contiki 3.0

5.2 Scenario Development

The framework proposed in this paper is divided into two scenarios i.e., implementation of standard DTLS with DoS attack and implementation of proposed novel hybrid DTLS scenarios. Scenario 1 consists of 5 wismote which running CoAP servers, 1 border router and 2 malicious nodes. Similarly, scenario 2 composed of 5 wismote running CoAP servers and 1 border router. In scenario 1, mote 1 is the border router while remaining 5 motes are CoAP servers with 2 malicious nodes (in purple), and all motes are placed in transmission range of border router as shown in Fig. 7. The border router is used as gateway for connection of external network with CoAP servers. The simulation environment for scenario 2 is as shown in Fig. 8 containing mote 1 as border router while remaining 5 motes are CoAP servers.

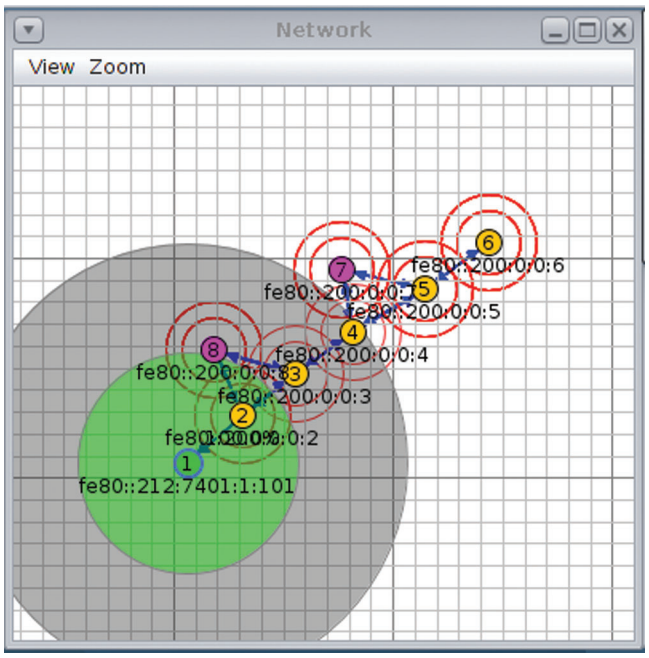

Figure 7: Standard DTLS implementation on cooja with DoS attack

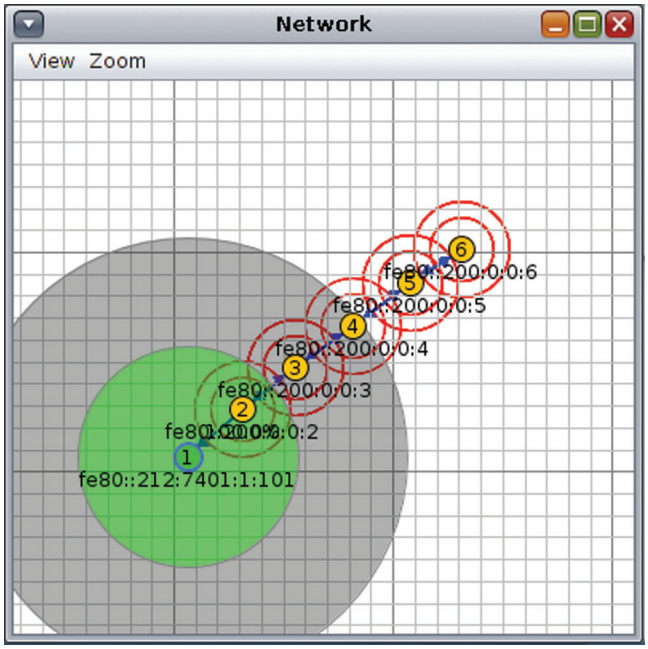

Figure 8: Proposed novel hybrid DTLS implementation on cooja

5.3 Results

This section describes the simulation results obtained. We considered the impact of handshake processing time, energy efficiency, throughput and packet delivery ratio of our novel hybrid DTLS. This implemented algorithm was then compared with the standard DTLS in terms of handshake processing time, energy efficiency, throughput and packet delivery ratio.

5.3.1 Handshake Time Duration

Both the scenarios are simulated and have been compared in terms of Handshake Time. Firstly, the simulation results obtained for the client are presented. Due to the presence of MAC algorithm the Client Hello preparation message takes more time in the processing of Client Hello message. The Hello Verify Request (HVR) message and Client Hello (CH) only belongs to the standard DTLS. Also the authentication process in novel hybrid DTLS takes less time as compared to the verification method used by the standard DTLS as shown in Fig. 9. Also due to the computation of pre-shared key in the standard DTLS, the CKE message processing takes more time as compared to the novel hybrid DTLS. Fig. 10 shows the total Handshake duration time on the client side.

At the client side, its clearly states that the total handshake time duration spent by the client is less in the novel hybrid DTLS than the total handshake time duration spent by the client in the standard DTLS.

The handshake processing time on the server side also less by the delegation of few handshake steps due to the existence of the trusted entity. Fig. 11 shows the DTLS Handshake time per flight on the server side. However, the Client Hello processing message which is received from client spent more time in the novel hybrid DTLS as compared to standard DTLS due to the addition of few lightweight operations. The HVR message and CH only belongs to the standard DTLS. The Client Key Exchange (CKE) processing time is more as compared to standard DTLS due to the computation of pre shared key. The Client Finished (CF) and Server Finished (SF) both also having the same processing time. The total handshake duration time on the server side is as shown in Fig. 12.

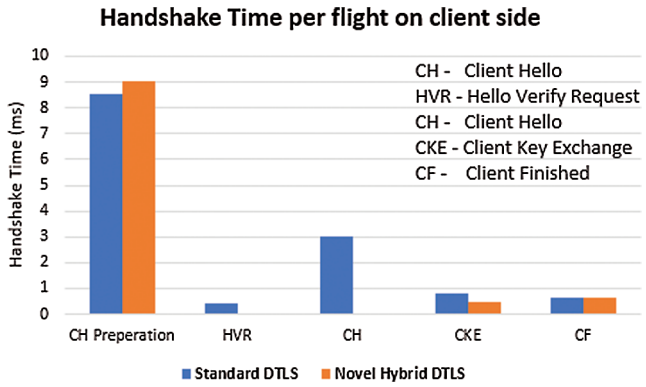

Figure 9: DTLS handshake processing time per flight on the client side

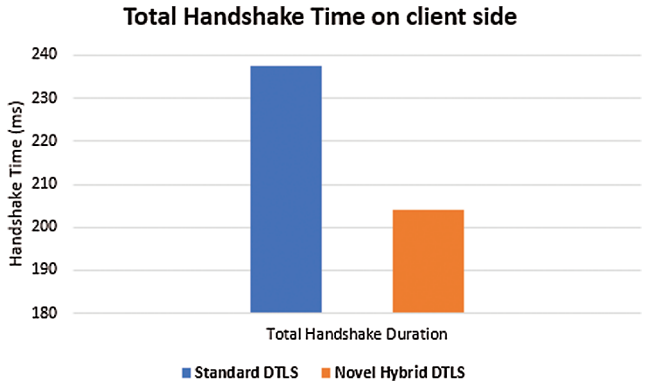

Figure 10: Total DTLS handshake processing time on the client side

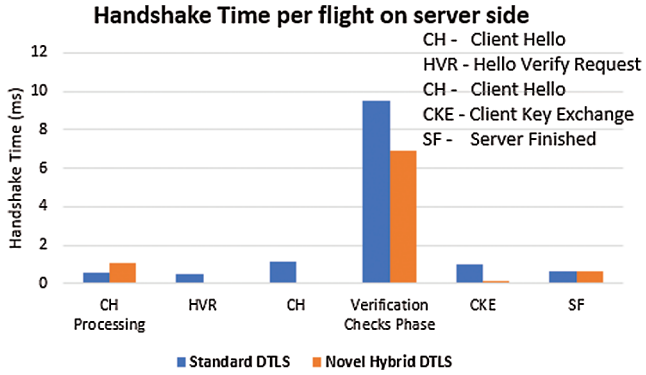

Figure 11: DTLS handshake processing time per flight on the server side

Also, at the server side, the total handshake time duration spent by the server is shorter in the novel hybrid DTLS than the total handshake time duration spent by the server in the standard DTLS. In overall, the handshake processing time decrease by an average of 9% during the handshake session in the novel hybrid DTLS compared to the standard DTLS.

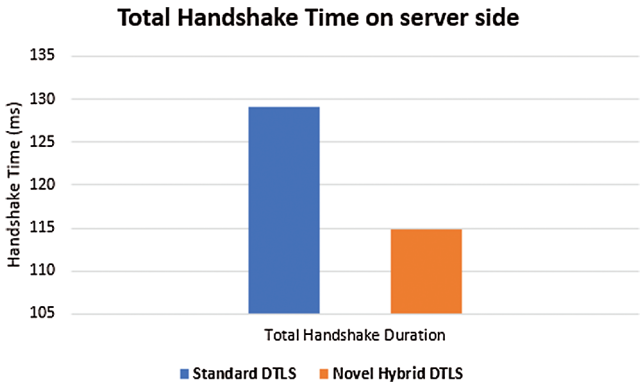

Figure 12: Total DTLS handshake processing time on the server side

5.3.2 Energy Efficiency

Energy efficiency is the most important metric, as it directly impacts on lifetime of the IoT devices. The Contiki OS comes with a built in GUI tools called as Cooja and is used in simulators. The energy efficiency of sensor device is measured by the energest_type_time () function which is built into the Contiki. The function energest_type_time () outputs the clock ticks obtained from the time when the device is booted. Fig. 13 shows the energy efficiency for both the novel hybrid DTLS and standard DTLS during handshake duration.

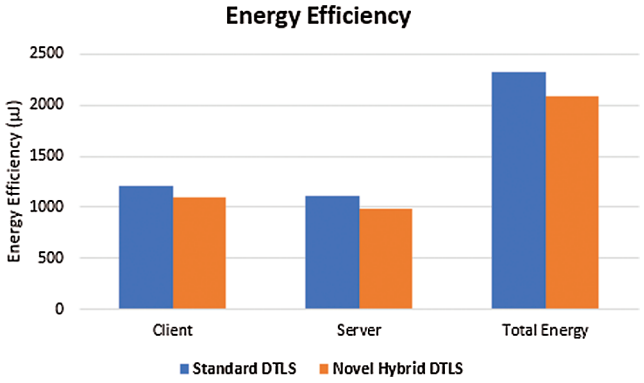

Figure 13: Energy efficiency

The novel hybrid DTLS protocol requires 2080.92 µJ to establish a DTLS handshake session, while the standard DTLS needs 2331.33 µJ to initiates the DTLS handshake session. Thus, an average of 11% of energy efficiency for transmission is being achieved while using the novel hybrid DTLS compare to the standard DTLS.

5.3.3 Throughput

Throughput is defined as the number of packets transmitted successfully from source node to destination node per second. For the good designed network, the throughput value should be high. The throughput value should be decreased if it is attacked by any intruders. Fig. 14 shows the throughput of the network. We calculated the throughput of the network with and without DoS attacks. It has been observed that throughput value is high in our proposed algorithm as compare to the ratio during DoS attack scenario. Its means that our proposed algorithm performs better and maximum number of packets are transmitted successfully by blocking malicious packets.

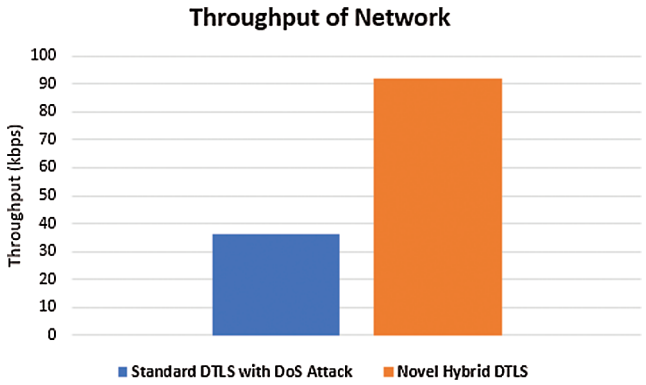

Figure 14: Throughput of network

5.3.4 Packet Delivery Ratio

Packet delivery ratio (PDR) is termed as the ratio of total number of packets delivered to the destination node to the total number of packets sent from the source node in the network. Fig. 15 illustrates the packet delivery ratio of network.

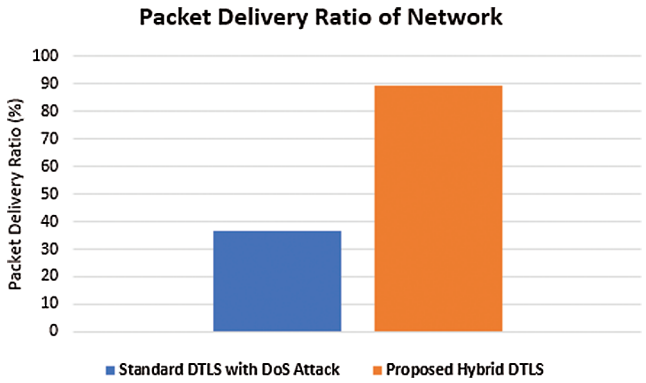

Figure 15: Packet delivery ratio of network

From the figure, it is clear that the PDR value obtained for our proposed algorithm is higher than that of PDR value obtained during DoS attack which illustrates that maximum number of packets has been reached to the destination node.

It has been clearly seen that during DoS attack less packets are reached to the source node which greatly affect the throughput and packet delivery ratio of IoT constrained network. From the above results, it is observed that the proposed novel hybrid DTLS increased the throughput and packet delivery ratio by 87% and 83% respectively. Hence our proposed algorithm minimizes the DoS attack for better efficiency of transmission in IoT constrained network.

6 Conclusion

Logistics plays a significance role in the economic growth of country. In logistics, the products which are to be transported may be sensitive and perishable, and require controlled environment. Most of the commercially available logistic containers are not integrated with IoT devices to provide controlled environment parameters inside the container. This necessitates the need for designing and fabricating IoT

based smart containers. Undoubtedly, IoT has a significant impact in the implementation of smart container. However, there exists many challenges, but one of the critical aspects, which need special attention, is the adoption of state of the art security mechanism. Due to constrained nature of IoT devices, these are prone to different cyber security attacks such as Denial of Service, Man in Middle and Replay. Therefore, designing efficient cyber security framework are required for smart container and is the main objective of this research.

In this paper, a cyber secure framework is designed by implementing novel hybrid DTLS protocol in smart container. The significance of the proposed framework is to minimize the chances of cyber security attacks and to improve the efficiency of energy transmission and utilization. Furthermore, the handshake time, throughput and packet delivery ratio are also computed to evaluate the efficiency of novel hybrid DTLS. From experimental results, it is shown that novel hybrid DTLS performed better compared to the standard DTLS.

In the future, we are planning to extend the existing proposed framework to other IoT applications and to validate the proposed framework on more real life case studies. Hence, it is stated that secure smart containers can generate a valuable contribution to the subject of food waste as well as its security nowadays and it will be profitable in the future.

Acknowledgement: The authors thank UET Peshawar to give the opportunity for this research work.

Funding Statement: This research is funded by the Higher Education Commission (HEC), Pakistan through its initiative of National Center for Cyber Security for the affiliated Innovative Secured Systems Lab (ISSL) University of Engineering & Technology (UET) Peshawar, Grant No: 2(1078)/HEC/M&E/2018/70.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[2] Statista, 2016. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

[3] C. Greer, M. Burns, D. Wollman and E. Griffor, "Cyber-physical systems and Internet of Things," *NIST Special Publication 1900-202*, vol. 1, pp. 52, 2019.

[4] J. Parfitt, M. Barthel and S. Macnaughton, "Food waste within food supply chains: Quantification and potential for change to 2050," *Philosophical Transactions of the Royal Society Biological Sciences*, vol. 365, no. 1554, pp. 3065–3081, 2010.

[5] M. A. Abdulkadyrova, A. H. Dikinov, H. E. Tajmashanov, L. A. Shidaev and E. A. Shidaeva, "Global food security problems in the modern world economy," *International Journal of Environmental & Science Education*, vol. 11, no. 12, pp. 5320–5330, 2016.

[6] J. Gustavsson, C. Cederberg, U. Sonesson, R. V. Otterdijk and A. Meybeck, "Global food losses and food waste: Extent, causes and prevention," *Food & Agriculture Organization of the United Nations Rome*, 2011. [Online]. Available: https://www.fao.org/3/i2697e/i2697e.pdf.

[7] M. Hülsmann and V. Brenner, "Causes and effects of cold chain ruptures: Performance of fragmented *vs.* integrated cold chains," *School of Engineering and Science, International Logistics, Systems Management*, vol. 28, 2011.

[8] M. Rezaei and B. Liu, "Food loss and waste in the food supply chain," International Nut and Dried Fruit Council: Reus, Spain, pp. 26–27, 2017. [Online]. Available: https://www.fao.org/documents/card/en/c/30245942-5cdb-42b6-bb1a-98243f108446/.

[9] W. Lang, R. Jedermann, D. Mrugala, A. Jabbari, B. Krieg-Brückner *et al.*, "The intelligent container-a cognitive sensor network for transport management," *IEEE Sensors Journal Special Issue on Cognitive Sensor Networks*, vol. 11, no. 3, pp. 688–698, 2011.

[10] H. Tschofenig and T. Fossati, "TLS/DTLS profiles for the Internet of Things," *Internet Engineering Task Force*, 2016. [Online]. Available: https://tools.ietf.org/html/rfc7925.

[11] Z. Shelby, K. Hartke and C. Bormann, "The constrained application protocol," *Internet Engineering Task Force*, 2014. [Online]. Available: https://tools.ietf.org/html/rfc7252.

[12] U. Banerjee, A. Wright, C. Juvekar, M. Waller, Arvind, Anantha P. Chandrakasan, "An energy-efficient reconfigurable DTLS cryptographic engine for securing internet of things applications," *IEEE Journal of Solid-State Circuits*, vol. 54, no. 8, pp. 2339–2352, 2019.

[13] J. Jin, J. Gubbi, S. Marusic and M. Palaniswami, "An information framework for creating a smart city through internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 112–121, 2014.

[14] Z. Bi, L. D. Xu and C. Wang, "Internet of things for enterprise systems of modern manufacturing," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1537–1546, 2014.

[15] F. Hecklau, M. Galeitzka, S. Flachs and H. Kohl, "Holistic approach for human resource management in industry 4.0," *Elsevier*, vol. 54, pp. 1–6, 2016.

[16] W. Lang, S. Janßen and R. Jedermann, "The intelligent container-a cognitive sensor net for fruit logistics," in *3rd Int. Conf. on Sensor Networks*, Lisbon Portugal, pp. 351–359, 2014.

[17] R. Jedermann, U. Praeger and W. Lang, "Challenges and opportunities in remote monitoring of perishable products," *Food Packaging and Shelf Life*, vol. 14, no. 1, pp. 18–25, 2017.

[18] R. Pila, S. Rawat and I. P. Singhal, "eZaar, the smart container," in *IEEE 2nd Int. Conf. on Telecommunication and Networks*, Noida, India, pp. 1–5, 2017.

[19] R. Torres, M. T. Zafra, N. Castillejo, A. G. Frutos and F. A. Hernandez, "Real time monitoring system for shelf-life estimation of fruit and vegetables," *Sensors (Basel)*, vol. 20, no. 7, pp. 1860–1880, 2020.

[20] M. Burhan, R. A. Rehman, B. Khan and B. S. Kim, "IoT elements, layered architectures and security issues: A comprehensive survey," *IEEE Sensors Journal*, vol. 18, no. 9, pp. 2796, 2018.

[21] S. Siboni, V. Sachidananda, Y. Meidan, M. Bohadana, S. Bhairav *et al.*, "Security testbed for internet of things devices," *IEEE Transactions on Reliability*, vol. 68, no. 1, pp. 23–44, 2019.

[22] S. Raza, H. Shafagh, K. Hewage, R. Hummen and T. Voigt, "Lithe: Lightweight secure coap for the internet of things," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3711–3720, 2013.

[23] M. Tiloca, K. Nikitin and S. Raza, "DTLS-Based secure IoT group communication," *ACM Transactions on Embedded Computing Systems*, vol. 16, no. 3, pp. 6602–6629, 2017.

[24] C. S. Park and W. S. Park, "A Group-oriented DTLS handshake for secure IoT applications," *IEEE Transactions on Automation Science & Engineering*, vol. 15, no. 4, pp. 1920–1929, 2018.

[25] S. Raza, L. Seitz, D. Sitenkov and G. Selander, "S3K: Scalable security with symmetric keys DTLS key establishment for the Internet of Things," *IEEE Transactions on Automation Science and Engineering*, vol. 13, no. 3, pp. 1270–1280, 2016.

[26] W. Lang and R. Jedermann, "What can mems do for logistics of food? intelligent container technologies: A review," *IEEE Sensors Journal*, vol. 16, no. 18, pp. 6810–6818, 2016.

[27] G. A. Tejedor, G. B. Hernandez, A. Garre, J. Egea, P. Fernandez *et al.*, "Quality changes and shelf-life prediction of a fresh fruit and vegetables purple smoothie," *Food Bioprocess Technol.*, vol. 10, pp. 1892–1904, 2017.

[28] Z. Zou, Q. Chen, I. Uysal and L. Zheng, "Radio frequency identification enabled wireless sensing for intelligent food logistics," *Philosophical Transactions of the Royal Society A*, vol. 372, pp. 1–16, 2014.

[29] P. Dittmer, M. Veigt, B. S. Reiter, N. Heidmann and S. Paul, "The intelligent container as a part of the Internet of Things," in *IEEE Int. Conf. on Cyber Technology in Automation, Control and Intelligent Systems*, Bangkok, Thailand, pp. 209–214, 2012.

[30] K. L. Keung, C. K. M. Lee, P. Ji and K. K. H. Ng, "Cloud-based cyber-physical robotic mobile fulfillment systems: A case study of collision avoidance," *IEEE Access*, vol. 8, pp. 89318–89336, 2020.

[31] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig and G. Carle, "DTLS based security and two-way authentication for the internet of things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2710–2723, 2013.

[32] Y. Ma, L. Yan, X. Huang, M. Ma and D. Li, "DTLShps: Sdn-based DTLS handshake protocol simplification for IoT," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3349–3362, 2020.

[33] C. Park, "Security architecture for secure multicast CoAP applications," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3441–3452, 2020.

[34] J. Flores, V. La, A. Cavalli, R. Velarde and R. Samaniego, "A Monitoring-based approach for WSN security using IEEE-802.15.4/6LowPAN and DTLS communication," *International Journal of Autonomous & Adaptive Communications Systems*, vol. 12, no. 3, pp. 218, 2019.