I. J. Computer Network and Information Security, **2017, 11, 27-35**
Published Online November 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.11.03

Enhancing the QoS of IoT Networks with Lightweight Security Protocol using Contiki OS

Haytham Qushtom
Arab American University, Jenin, Palestine
E-mail: hkalalwah@qou.edu

Dr. Khalid Rabaya'h
Arab American University, Jenin, Palestine
E-mail: Khalid.Rabayah@aauj.edu

Received: 15 July 2017; Accepted: 07 August 2017; Published: 08 November 2017

***Abstract*—**The Internet of Things (IoT) is advancing to prevail the application of the Internet, with the vision to connect everything around us. The deployment of IoT is advancing at a very fast pace, and relying on modified versions of the TCP/IP protocol suits. This rapid growth of the field is leaving a number of critical issues unresolved. Among the most critical issues are the quality of service and security of the delivered data. This research is set to tackle these issues through proposing a data delivery scheme that improves the quality of service (QoS) of classified data. The proposed solution relies on differentiating the priority of the delivered data, and to give preferences to secured and user-defined high priority traffic. The proposed solution denoted as Secured Traffic Priority Differentiation (STPD), is made to support any application, and is implemented at the Medium Access Control (MAC) sub layer. The proposed solution was tested in a virtual environment that simulates real scenarios using the Contiki operating system, using the Cooja simulator. The simulation results demonstrated a significant improvement of the proposed solution over the Carrier Sense Multiple Access Collision Avoidance, (CSMA/CA), by at 20%. The proposed solution worked to improve the channel utilization, data reliability, decreased latency of high priority traffic, and low priority traffic as well.

***Index Terms*—**Wireless sensor networks, Internet of Things, quality of service, medium access control, secure traffic, traffic priority, IPsec, MAC Layer, CSMA/CA, IEEE 802.15.4.

I. Introduction

Next to the World Wide Web and smart devices, a new technological trend is getting through, that is the Internet of Things (IoT). IoT technologies are advancing very rapidly on all fronts and aspects. These technologies continue to be getting smaller, faster, cheaper, more power-efficient, and smarter. IoT is used to monitor and control valued things for humans, society, nature and industry. The technology allows people to perform any action at any time anywhere on the surface of the earth [1]. IoT comprises of a collection of IP-enabled sensors, detectors and actuators, that in principles, able to measure, detect, and actuate any device, via the Internet. Yet, these devices can communicate and interact with each other's using heterogeneous network with different hardware and software platforms. IoT networks are to be designed and operated carefully as they are built in a very constrained-resource environment. IoT networks comprise mainly of distributed smart devices that are in general made very small in size with very limited storage and memory size. They are, in many cases, installed in remote locations where they have to rely on batteries for long time, which creates constraint in power consumption. These devices and the network that connects them are unable to work effectively with standard TCP/IP protocol suits as they need light weight protocols and a special type of operating system such as Contiki. To tackle this issue, the IoT network uses an interfacing protocols like 6LoWPAN that are integrated with the original TCP/IP. 6LoWPAN works very efficiently to solve interfacing problems, enhances the ability to connect constrained devices to the real world Internet [2]. 6LoWPAN allows IEEE 802.15.4 data link layer to utilize IPv6 over resources-constrained networks [2] [3]. IoT networks inherited many vulnerabilities from the original TCP/IP protocol. One major challenge facing the design of the IoT network has to do with security and privacy. Additionally, IoT networks lack efficient data delivery mechanisms, prioritization mechanism, and are not made to satisfy application specific and user defined requirements. Applications like healthcare, security, military, and home automation demand different level of quality of services than for instance, environmental, agricultural, and luxuries applications. This poses a serious challenge to the standard IoT protocols. The challenge even magnifies when these networks operate in heterogeneous environments with constrained resources. To provide a level of service that is required by an application or a user, a new protocol needs to be designed. And there comes the contribution of this research. To our

knowledge, and as reported by related literature, minimum efforts are extended in that domain. As will be details in the related works, substantial research efforts were paid to tackle end to end issues such as end-to-end delay and throughputs. However, the performance of these solutions are not efficient when they are employed for applications that require different level of QoS. In this paper, we are reporting on a proposed protocol that will improve the mechanism which controls the quality of service provisioning for secured data applications.

The proposed solution is implemented at the MAC layer, with IPsec protocol [4] integrated in the solution to provide security for the packets at the network layer level [5]. The reasons behind chosen IPsec from other protocols that provide security, its inherent in IPv6 and provides complete end to end security [6], it does not only provide confidentiality and message integrity but it also includes efficient key exchange mechanism and authentication [6]. Our modified version of the MAC protocol, titled "Secure Traffic Priority Differentiation" (STPD), utilizes the assets of the contention-based medium access technique, and is designed to achieve higher channel utilization. The performance of the proposed solution or protocol is analyzed using the best known simulation environment used by IoT engineers, the Contiki OS, together with the Cooja simulator, which was specifically designed for IoT systems. The rest of this paper is organized as follows: in the following section, briefly came across some related work on QoS provisioning at the MAC layer for IoT networks. Section 3 reports on the details of proposed solutions, the STPD protocol. Section 4 presented the performance evaluation results. Finally, Section 5 concludes the paper.

II. Related Work

Several research efforts have been extended in recent years tried to enhance the QoS of IoT based networks, each of which has tackled the issue from different perspective. Awan in [7] proposed queuing system with pre-emptive resume (PR) service priority with complete buffer sharing scheme by all classes of traffic under a push out mechanism. These approaches do not look into the QoS requirements like throughput, and packets delivery ratio in IoT networks. However, the technique of pushing out low priority traffic is used to avoid data loss of high priority traffic, which reduces the overall throughput, and packet delivery ratio of low priority packets. Other mechanism utilized advertisements, as the one proposed by Adil A Sheikh [8] who suggested a new routing framework for VSN (visual sensor network) to deliver critical imagery information with system's time constraint. The proposed priority-based routing framework makes sure that intermediate nodes forward high priority packets (first pass image layer) faster than low priority packets. The VSN nodes send advertisements to their neighbors declaring identities and the number of hops from sink. These advertisements are sent periodically to allow the intermediate nodes decide the priority of the incoming packets based on the number of hops from the sink, while the intermediate nodes use priority queue mechanism to organize the incoming packets. Few research efforts focused more on modifying the classical access mechanism implemented by the MAC sub-layer in the IoT networks.

Tanmay Chaturvedi, et al. [9] investigated a scalable multimode-based MAC protocol. They proposed a new IoT-MAC sub-layer to reduce contention of the channel resulted from the existence of many IoT devices, which consists of a channel contention period and a data transmission period. The two periods interchange periodically and are synchronized by the base station. The proposed data transmission scheduling algorithm is used to maximize data transmission under the constraints of radio link quality and remaining energy of the IoT node, while ensuring a fair access to the radio channel. This allows the nodes to find their transmission slot within the super frame and only transmit during their scheduled time to prevent collision.

Thien D. Nguyen [10] introduced an adaptive energy efficiency algorithm, known as ABSD (Adaptive Beacon Order, Super-Frame Order and Duty cycle) that changes the MAC parameters of the IEEE 802.15.4 sensor nodes in response to the queue occupancy level of sensor nodes and the offered traffic load conditions. The ABSD algorithm minimizes the network contention which could in turn improve the energy efficiency as well as the throughput of the overall network.

Irfan Al-Anbagi [11] introduced medium-access approach, namely delay-responsive cross-layer (DRX) data transmission. DRX is based on delay-estimation and data-prioritization mechanisms that are performed by the application layer. The delay-estimation is done by the prediction of the end to end delay and the creation of cross-layer measures. In DRX uses the application-layer controls the medium access by performing delay estimation, such that if the estimated delay is higher than the delay requirement set by the application layer, DRX gives higher priority to the node to access the channel by reduces the Clear Channel Assessment (CCA) duration. DRX achieved delay improved responsiveness of the network by modifying the parameters of the physical layer of the IEEE 802.15.4 protocol, as demanded by the application layer.

Muhammad Akbar et al. [12] proposed a protocol which suites the tele-medicine applications, labeled as the tele-medicine protocol (TMP). The proposed protocol was implemented using the IEEE 802.15.4 slotted CSMA/CA with beacon enabled mode. They combined two optimization methods; the MAC layer parameter tuning optimization and duty cycle optimization methods. Their proposed protocol presented good results in terms of delay, reliability, energy consumption, and collision rate as compared to other existing protocols under the constraints of patient monitoring applications.

Sabin Bhandari et al. [13] proposed a priority-based adaptive MAC (PA-MAC) protocol for wireless body area networks (WBANs). They used the beacon channel, which is normally used for transmission and reception of

beacon frames, to exchange control information with coordinating node and leaves the data channel for data communication. PA-MAC classifies Data traffic into four priority levels and allocates time slot dynamically in accordance to the number of nodes in each traffic priority category. In regards to data Prioritization they used priority-guaranteed CSMA/CA in contention access period. The downgrade of PA-MAC occurs when the node wants to reserve the resources for periodic traffic, it has to send the request to the network coordinator.

Saima and Yun [14] proposed message scheduling with service provisioning technique. This technique classifies traffic into high priority and best effort messages. For the selection they used the best QoS algorithm. They used clustering based approach; which categorizes IoT nodes into subgroups, and assigns a broker node to each subgroup. The broker node works to collect the data from other nodes in the subgroup and redirects them as messages to the base station by handling separate queues for best effort and high priority messages.

In conclusion, most of the efforts in this research area aim to improve one aspect of QoS requirements (e.g. latency), and limited support to different traffic types like secure traffics. As a result, the proposed protocols are optimal only for specific use cases. This paper presents QoS designs at MAC layer for traffic differentiation with multiple QoS metrics. Thus, the protocol designs enable heterogeneous IoT applications with varying QoS requirements to operate in the same network.

III. Secure Traffic Priority Differentiation (STPD)

Our proposed solution aims at generating a more efficient MAC protocol for IoT secured applications. In IoT networks traffic generated by nodes with different kind sensors requires different level of security to be delivered. Moreover, different kind of sensors generate data traffic with various characteristics, such as data rate, data type (being secured and not secured), packet size, and transmission delay. These are to be added to the application and end user requirements of IoT networks. All of these specifications require different level of QoS to be supported by the IoT protocols. QoS of networks in general is defined in terms of latency, reliability and data rate. Our proposed model is designed to satisfy these requirements and at the same time achieves efficient performance.

Our proposed solution targets both messages that used for connection setup and data transfer. IPsec protocol in our proposed solution uses at the network layer level, exchanges a collection of parameters needed to establish a secure session (connection setup). These exchanged messages have different characteristics than other secured data traffics. The characteristics of the connection setup for secured session in IoT network is done via exchange of two pair of messages between sender and receiver. The single message size ranges between 3 to 5 packets. The connection starts all over again if any of these packets get lost, when the time is over due to long connection, and after the communicated security key gets expired. Our proposed solution is designed to overcome these issues. Receiving and transmitting packets at the same time cannot be done in IoT devices. Figure1 illustrates the proposed modification on the MAC protocol. As is shown by the figure, we divided traffic into two types; secure and non-secure, and give priority to secure traffic when competes with low priority (non-secure) traffic. The secured traffic is further divided into two distinct classes; high priority and low priority. The classification process provides low latency as well as high throughput as high priority traffic.

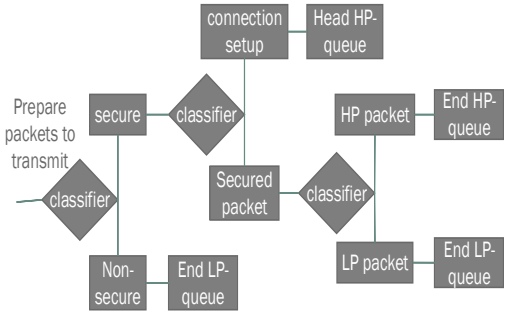

Fig.1. Basic idea for STPD.

Other than that our model gives the highest possible priority to connection setup, which is used to create end-to-end secured connection for IPsec protocol.

Our adaptive STPD-MAC protocol works to enhance the resources utilization, provides reliability in establishing a secure connection for IPsec protocol, and provides a prioritization mechanism to fulfill the needed QoS requirements. Our proposed architecture involves two layers; the adaptation layer, and the data link layer.

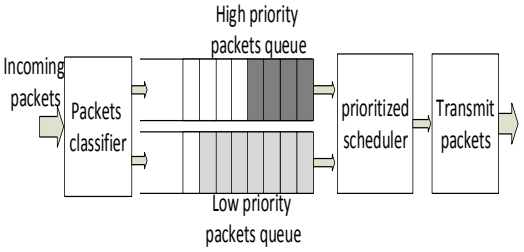

Fig.2. STPD Arbitration Scheme.

When a packet is prepared for transmission, the adaptation layer gets the sender address (an IPv6 Address) from the prepared packet and consults the priority table to find the priority level for that packet. Afterwards, the priority value is passed over to lower layer; the MAC sub-layer, which use this value to set the packet prioritization mechanism that we will describe in more detail in next sub-sections. Please remark that the priority table is distributed among all nodes in the network, and this table contains the priority level and the IPv6 addresses for all sending nodes in the network. The prioritization mechanism implemented by the STPD protocol, consists mainly of two "First Input First Output" (FIFO) queues. Each of these queues uses different mechanism for arranging the incoming packets,

based on the packet priority values, as is depicted in Figure 2. The first step in the prioritization mechanism is packets classification which is performed by the packet classifier, see Figure 2. The classifier checks the priority of the incoming packet and inserts it at the end of the appropriate queue.

However, if the packet is a connection setup one, it is inserted at the start of the high priority (HP) queue. This guarantees that it will be immediately processed. HP queue contains HP packets, in addition to the connection setup packets. Low priority (LP) queue contains LP, routing and control packets. The second step of the prioritization mechanism is priority scheduling. In this step a scheduler decides which packet is to be sent. The scheduler keeps selecting HP packets as long as the HP queue is occupied and it is not in a state of back-off from collision. If this is not the case, the scheduler switches transmitting from LP queue. As a final step, the protocol transmits packets. However, when collision occurs, the protocol offers lower delay for HP packets compared to LP packets. The queues in our model uses dynamic memory management. This is achieved by splitting the allocated memory that is allocated to all queues into halves. The first half is assigned to priority queue, and the second half is set to be shared by both priority queue. The flow diagram of our STPD protocol in depicted in Figure 3.

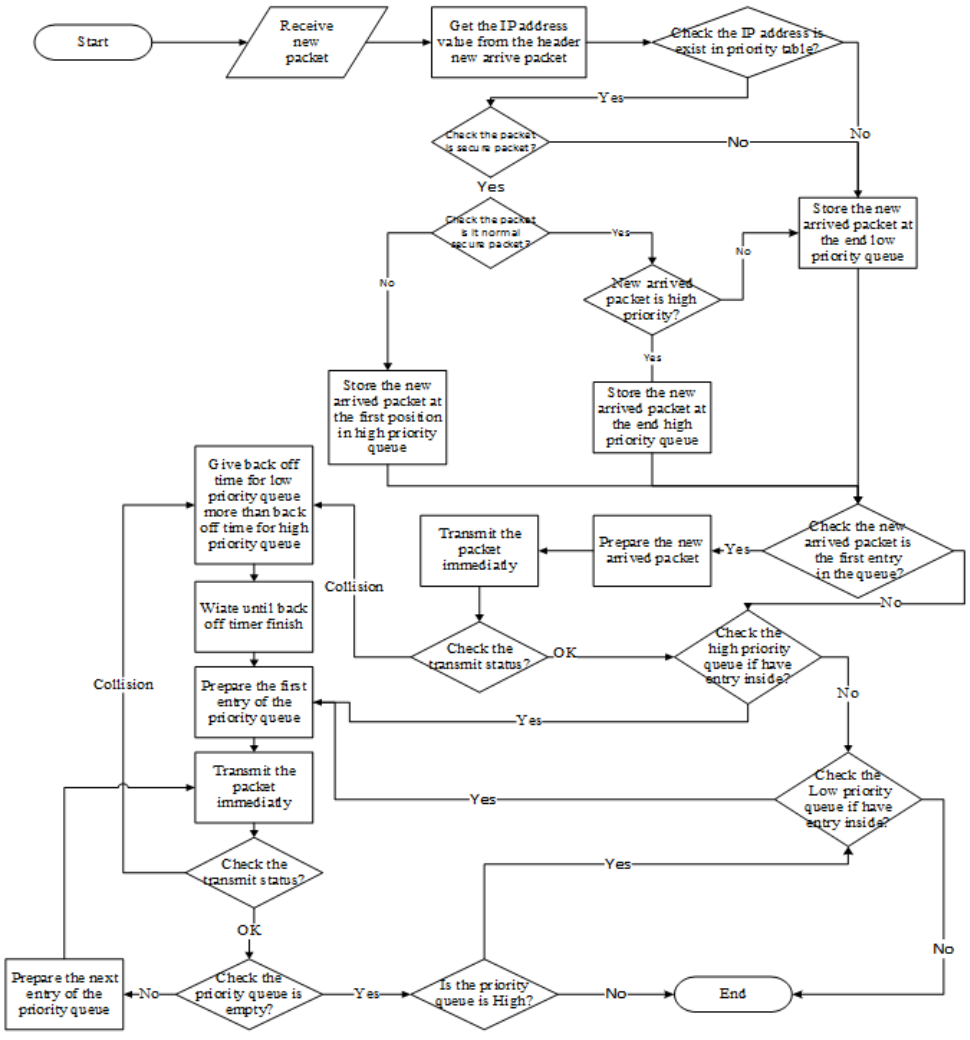

Fig.3. STPD Arbitration Scheme

IV. Performance Evaluation of STPD-MAC Protocol

In this section we report on the efficiency and effectiveness of our proposed protocol (STPD), throughout series of experiments carried out using the Cooja simulator [15] with Contiki as the operating system [16]. The performance enhancement achieved by our protocol is measured against the IEEE 802.15.4 standard, which defines the Carrier Sense Multiple Access/ Collision Avoidance (CSMA/CA) protocol [17] [18]. In all simulated scenarios, our protocol outperformed the standard IEEE 802.15.4 MAC protocol in various performance metrics such as channel utilization, latency, packet delivery ratio, and packet collisions ratio. Figure 4 below depicts the Cooja simulation environment used to carry out the experiments of our study.

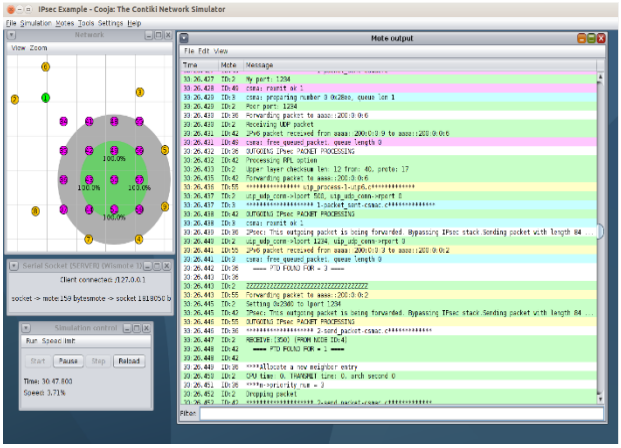

Fig.4. Cooja Simulation Graphical User Interface.

A. Simulation Scenario and Tested Parameters

This section details the simulated scenarios of STPD as well as the variables we used to measure the network performance. A secure end to end IoT network in a wireless environment is setup in the simulation environment. The IoT nodes are equipped with IPsec security protocol as is detailed by Raza et al. in [19]. The system setup guarantees integrity, confidentiality, and authentication of all simulated scenarios. Table 1 details the parameters used in the simulated cases.

Table 1. Simulation Settings

Parameter	Value
Transmission range	60m
Interference range	100m
Number of intermediate nodes	9,16,25 and 36 nodes
Number of sending nodes	6 nodes
Number of receiving nodes	2 nodes
Packets rate	2.5 packets/sec
Channel type	Wireless
Routing protocol	RPL
Security protocol	IPsec
Adaptive layer protocol	6LoWPAN
MAC layer protocol	CSMA/CA, STPD-MAC
Radio duty cycling layer Protocol	Contiki-MAC
Physical layer Protocol	IEEE 802.15.4
Packet size	127 bytes
MAC layer header size	25 bytes
Payload size	102 bytes
MAC layer queue size	8 packets
Ratio of high priority to low priority nodes	50-50%
Queue mechanisms	Default queue, PQ (Priority Queuing)
Service types	Default service (one queues to one transmission line), Priority service (several queues to one transmission line)

B. MAC Layer Parameters (STPD-MAC Protocol)

To distinguish between high and low priority traffic, the back-off time for low priority packets was set to be twice that of the high priority packets. Additionally, in the Contiki environment, and as default state, a static memory was selected, and this memory was set to be equal for all packet queues. The Memory Block Allocator (MEMBA) used in the default library, used a statically declared memory areas to store objects of fixed size. To simulate our STPD-MAC protocol, dynamic memory allocation was set to store packets in the queues. This is needed in all nodes with limited memory and scarcity of resources. STPD implement Managed Memory Allocator (MMEM) library which enables dynamic allocations with automatic defragmentation by using pointer indirection.

C. Simulation Environment

Two main simulation scenarios were setup. One which simulates our proposed STPD protocol, and the other simulates the standard IEEE 802.15.4 MAC (CSMA/CA) protocol. Both scenarios used exactly the same parameters. At the sending side, a network of six sending nodes was used, with all nodes implementing IPsec protocol. To that network, one border router was added to connect the entire IoT network with the Internet. At the receiving side, two IPsec nodes were set. The number of intermediate nodes was set to be a variable to investigate its impact on the overall system performance. To simulate a true and real scenarios, all nodes in the entire IoT network were meshed together. This mesh topology will decide the mode of communication when the packets start to be exchanged. As for transmission range, each node is allowed to transmit within the range of four neighboring nodes. Under these conditions, a fair comparison is guaranteed between out proposed STPD and the standard CSMA/CA protocols. Each simulation experiment was repeated ten times, where different seeds were used every time. The results of the 10 trials were averaged out and used as the final outcome of the experiment. MATLAB simulation environment, was used to further analyze the outcomes of the simulation.

In what follows we shall focus on the results of the simulation experiments in terms of channel utilization, packet latency, and successful packet delivery ratio.

D. Simulation Results: Transmission Channel Utilization

Channel utilization or throughput is measured in terms of packets/sec and is defined as the ratio of the packets successfully delivered to the total number of packets sent out in a fixed period of time. This metric designates the overall effectiveness of the protocol in use by the network. Since secured communication applications always require high level of throughput, achieving high channel utilization is one of the primary goals of our STPD protocol. The simulation results depicting the channel utilization performance metric is shown in Figure 5 and Figure 6.

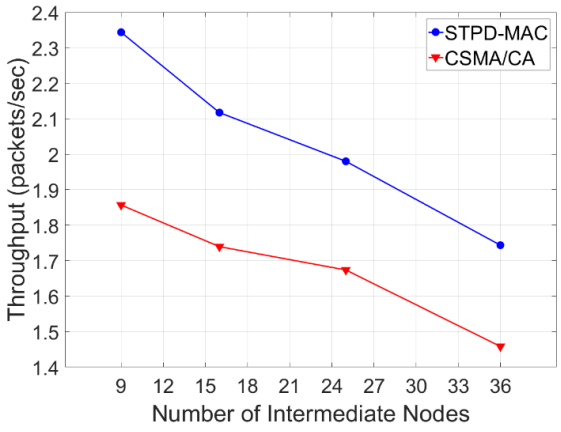

Fig.5. Comparison between STPD and CSMA/CA Performance in Relation Channel Utilization.

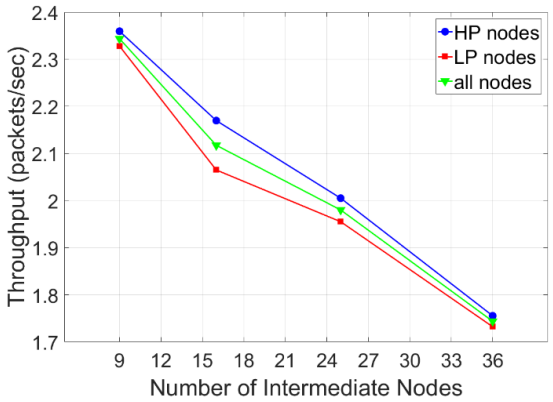

Fig.6. Channel Utilization of STPD for Different Priority Packets.

Figures 5 and 6 compare STPD protocol performance with that of CSMA/CA protocol in terms of channel throughput. As is shown by the Figure5, STPD outperforms CSMA/CA by 25% in all simulated scenarios, regardless of number of intermediate nodes used. The enhancement can be referred to the use of back-off time, which was set to be shorter for high priority (HP) than low priority (LP) packets, which in turn enhances the contention decision. The dynamic memory management likewise plays a role in maximizing the channel utilization. Additionally, storing the control messages such as RTS / CTS and ACK inside the low priority queue contributed to that enhancement.

E. Simulation Results: Delivered Packets Latency

Latency as measured by the average end-to-end delay and expressed in millisecond, comprises of processing time, queuing time, and retransmission delay at the MAC, in addition to propagation and transmission delays. Figure 7 displays the average end-to-end delay time as measured for STPD and CSMA/CA protocols. Once more, STPD exhibited its superiority over the standard CSMA/CA. STPD guarantees an average latency time (≤ 1.3 s) which is significantly lower than that of the CSMA/CA with an average of 2.82 s.

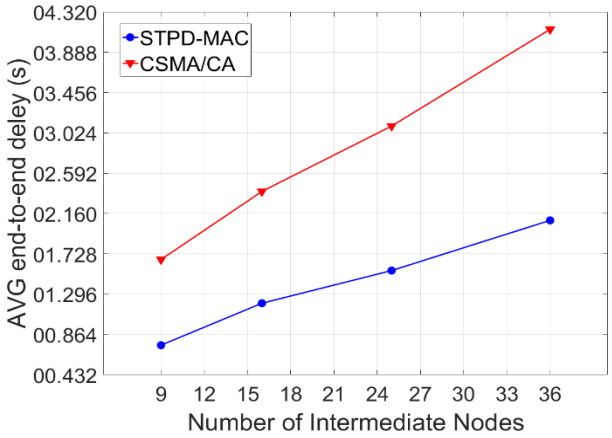

Fig.7. End to end Latency of STPD vs. CSMA/CA.

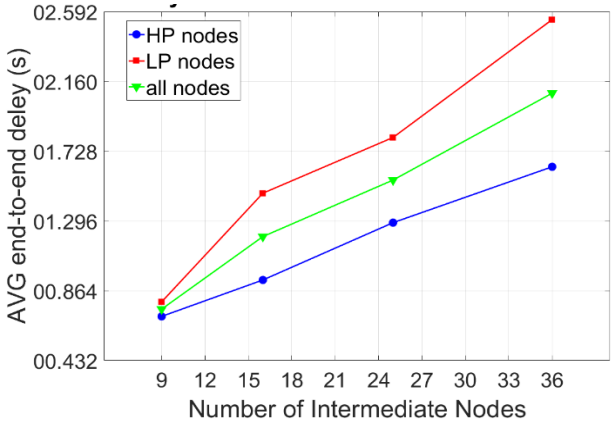

Fig.8. End to end Latency of STPD as Measured for both High and low Priority Packets.

Figure 8, displays the average end-to-end delay of high and low priority traffics for STPD protocol. HP out performs LP, which guarantees that HP packets reach their destinations faster than LP packets. This is an additional advantage of STPD protocol, which demonstrates that the preference mechanism does work in favorite of high priority packets.

F. Simulation Results: Packet Delivery Ratio (PDR)

Packet Delivery Ratio (PDR) is defined as the ratio of packets that are successfully delivered to a destination compared to the total number of packets sent out by the sender. This performance metric signifies the network reliability. Reliable data delivery is very critical for classified and secured network applications. Simulation results depicted in Figure 9 shows both STPD and CSMA/CA Packet Delivery Ratio for all types of tested traffic. Results evidently show that STPD achieves better results. PDR for STPD traffic is recorded at 70% in the worst case scenario, and averaged around 85%. Yet, the PDR for CSMA/CA averaged around 65%, and 57% as the worst case scenario. An improvement of 20% in PDR is recorded for STPD in comparison with the CSMA/CA stander protocol.

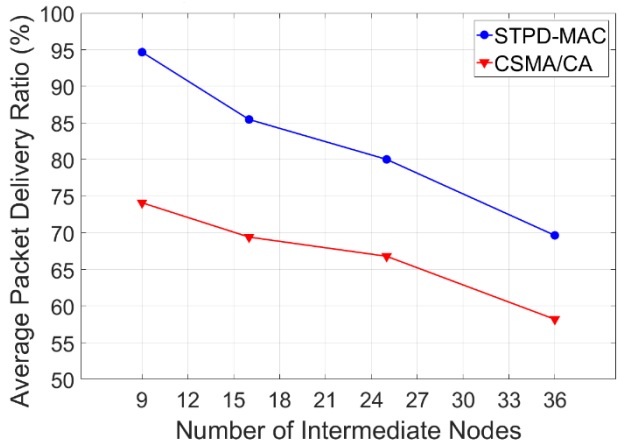

Fig.9. Comparison between STPD and CSMA/CA Performance in Relation PDR.

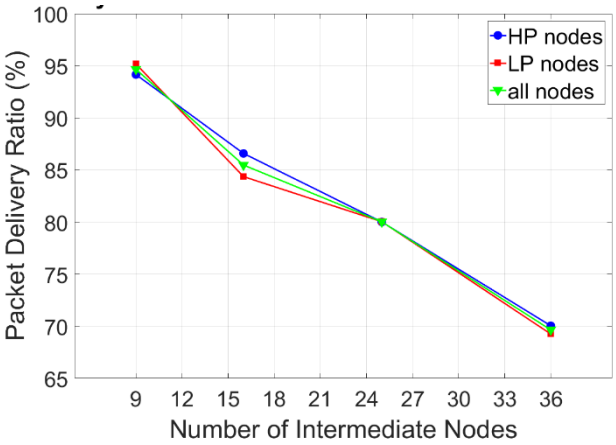

Fig.10. PDR of STPD for Different Priority Packets.

The results further emphasize that the prioritization mechanism implemented by STPD reduces collisions among packets and therefore minimizes packet loss, which resulted in an enhanced successful packet delivery. The dynamic memory management has a role to play in enhancing the PDR, as it allows for better memory utilization, which in turn reduces packet drop out, especially when one queue is full and the another queue is still not full. The PDR gets improved regardless of the priority level of the packets, as is demonstrated by Figure 10. In Figure 10 the simulation results indicated that STPD achieved the same level of PDR both for LP and HP traffic. An average value of 85% is recorded for PDR in both priority cases.

G. Simulation Results: Number of attempts to Make Secured Connection for IPsec Protocol

STPD further improved network performance through reducing the number attempts to establish a secured connection, as presented by Figure 11. The number of attempts to create a secure session for IPsec protocol is significantly lower for our proposed model than it is for the CSMA/CA standard protocol. This enhancement is attributed to the prioritization mechanism implemented by STPD.

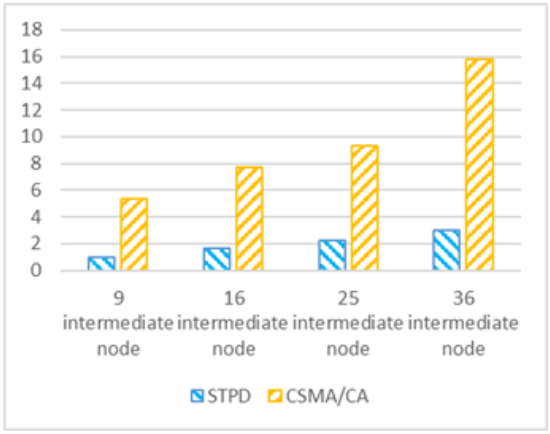

Fig.11. Average Number of Attempts To Create Secure Connection for IPsec Protocol.

Additionally, the dynamic memory management played a role through extending the HP queue when that queue reaches its limit. Which prevent dropping or losing receiving packets that belong to connection setup messages if their specs available in other queue. And give the connection setup the highest priority than other traffic, which guarantee it will be transmit immediately before any other packet types. If the number of attempts increases, More CPU cycles are needed to re-prepare encryption key, and other parameters for the IPsec protocol. As a result, energy consumption got increased. The large number of attempt return to: the characteristic of the connection setup, and the destination node can only deal with one connection at the same time, if any other node attempts to setup a connection it will be drop.

H. DISCUSSION: Comparison with Former Studies

It is quite evident that STPD outperforms CSMA/CA standard protocol in all simulated scenarios. Throughout the implementation of the STPD protocol, channel utilization, latency of packets, successful packet delivery ratio, and number of attempts to establish a secured connection, are all got improved in reference to CSMA/CA standard protocol. As was explained in the above section, these improvements are all attributed to the novel mechanisms, and algorithms incorporated with the STPD proposed protocol. However, the validity of our results will not be substantiated till we contrast our results with similar attempts made by other researchers. To ensure fair comparison, we have to make sure that other studies used almost the same working conditions, as set by the simulation environment. The studies list below do almost have similar conditions.

On the whole, when the results of our study are compared with what is there in literature, STPD achieved superior results in terms of all performance variables; being throughput, latency, packet delivery ratio, and Packet collision ratio. Figure 12 illustrates the percentage enhancement in performance resulted from our protocol as contrasted with other protocols found in literature. Remark that performance enhancement of all proposed protocols including STPD is referenced to the performance of the CSMA/CA protocol.

In relation to latency measure, our protocol (STPD) outperformed both the Priority-based Adaptive (PA-MAC) protocol [13], which achieved 33% improvement, and the Delay Responsive Cross-Layer (DRX) protocol [11], which achieved 10% improvement. However, the Tele-Medicine (TMP) protocol [12], which achieved 60% improvement outperformed STPD by 10%. In terms of throughput, which is measured by the ratio of successfully delivered packet to the total number of transmitted packets, only the priority-based adaptive (PA) protocol did similar measurements to what we have done, and the results of both protocols are almost identical. In terms the delivery ratio improvement, STPD (33% improvement) achieved almost similar results to the Tele-medicine protocol (32% improvement). However, STPD significantly outperformed the delay responsive cross layer (15% improvement). Finally, in regards to collision ratio improvement variable, STPD outperformed all other protocols with improvement ratio of 47%, compared to 30% for priority-based, 40% for tele-medicine, and 10% for delay responsive cross-layer protocol. The high collision ratio in PA-MAC is referred to the issue of using guaranteed timeslots, number is limited, especially in case of heavy and high data rate traffic. The second protocol that we compare with is TMP-MAC protocol which achieve near result to our protocol, but still our model has better performance than TMP-MAC protocol. The last protocol which called DRX-MAC has lower average percentage change than our protocol, which data prioritization depend on the application-layer to control the MAC sub-layer, and the estimated delay mechanism that use is the main reason to hinder the performance.

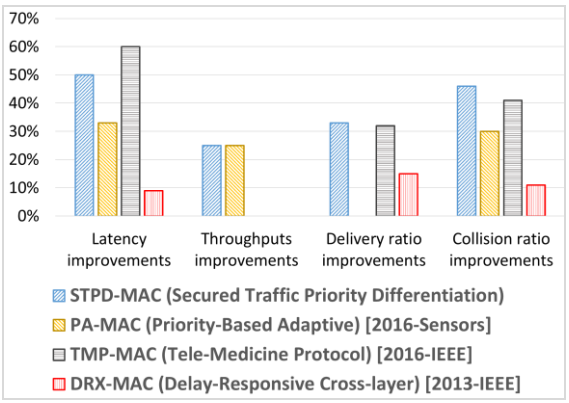

Fig.12. Comparison between the Performance of STPD and other Proposed Protocols.

V. Conclusions

The main purpose of this paper was to test the possibility of improving the quality of services provided by the data link layer to the IoT applications. Towards that end, the research efforts were designed around examining the implementation of a proposed protocol denoted as Secure Traffic Priority Differentiation, (STPD). The proposed solution is implemented into Adaptation layer and the MAC layer, as the MAC layer is counted as the main factor for determining the overall network performance. The enhancements introduced by the proposed solution were assessed using extensive simulation experiments. In the experiments three major network performance metrics were tested; channel utilization, network latency, and packet delivery ratio. As a result, our model successfully achieves the goals of our research by improving packets prioritization, enhancing resources utilization, upgrading quality of service (QoS) support, and improving performance of (IPsec) security protocol. Also outperforms the standard IEEE 802.15.4 MAC protocol regardless of the number of intermediate nodes that exist between sender and receiver. Finally, we are among the first developers who are working towards improving performance of IoT networks that use IPsec protocol written inside Contiki OS.

References

[1] Nik Bessis and Ciprian Dobre, "Big Data and Internet of Things: A Roadmap for Smart Environments," *Springer*, 2014.

[2] J. Hui and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4 Based Networks," *RFC 6282*, Sept. 2011.

[3] Jaideep Kaur, Kamaljit Kaur, "Internet of Things: A Review on Technologies, Architecture,Challenges, Applications, Future Trends," *International Journal of Computer Network and Information Security(IJCNIS)*, vol. Vol.9, no. DOI: 10.5815/ijcnis, pp. pp. 57-70, 2017.04.07.

[4] S. Kent and K. Seo, "Security Architecture for the Internet Protocol," *RFC 4301*, December 2005.

[5] Er. Gurjot Singh, Er. Sandeep Kaur Dhanda, "Quality of Service Enhancement of Wireless Sensor Network Using Symmetric Key Cryptographic Schemes," *Information Technology and Computer Science*, no. DOI: 10.5815/ijitcs, pp. 32-42, 2014.

[6] Azka a, S Revathi b, "Protocols for Secure Internet of Things," *I.J. Education and Management Engineering*, no. DOI: 10.5815/ijeme, pp. 20-29, 2017.02.03.

[7] Awan, I.; Younas, M.; Naveed, W., "Modelling QoS in IoT," *Network-Based Information Systems (NBiS)*, no. 17th International Conference, pp. 99-105, 2014.

[8] Adil A Sheikh ,Emad Felemban, Saleh Basalamah, "Priority-Based Routing Framework for Multimedia Delivery in Surveillance Networks," *MMEDIA 2014 : The Sixth International Conferences on Advances in Multimedia*, 2014.

[9] Tanmay Chaturvedi, Kai Lia, Chau Yuena, Abhishek Sharmab, Linglong Daic, Meng Zhang, "On the Design of MAC Protocol and Transmission Scheduling for Internet of Things," *SUTD-MIT International Design Center*, 2016.

[10] Thien D. Nguyen, Jamil Y. Khan, and Duy T. Ngo, "An Energy and QoS-Aware Packet Transmission Algorithm for IEEE 802.15.4 Networks," *IEEE 26th Annual International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC): MAC and Cross-Layer Design*, 2015.

[11] Irfan Al-Anbagi, Melike Erol-Kantarci, and Hussein T. Mouftah, "Priority- and Delay-Aware Medium Access for Wireless Sensor Networks in the Smart Grid," *IEEE*, no. 1932-8184, 2013.

[12] Muhammad Sajjad Akbar, Hongnian Yu, ShuangCang, "TMP: Tele-Medicine Protocol for Slotted 802.15.4 with Duty-Cycle Optimization in Wireless Body Area Sensor

Networks," *IEEE*, no. 1558-1748, pp. 1-1, 28 December 2016.
[13] Sabin Bhandari and Sangman Moh, "A Priority-Based Adaptive MAC Protocol for Wireless Body Area Networks," *Sensors* , no. 401, 2016.
[14] Saima Abdullah, Kun Yan, "A QoS Aware Message Scheduling Algorithm in Internet of Things Environmen," *IEEE Online Confer-ence on Green Communications (OnlineGreenComm)*, 2013.
[15] Thiemo Voigt, Fredrik Osterlind and Adam Dunkels , "Contiki COOJA Hands-on Crash Course: Session Notes," *Swedish Institute of Computer Science*, July 2009.
[16] "Contiki: The Open Source OS for the Internet of Things.," [Online]. Available: http://www.contiki-os.org/. [Accessed 25 1 2017].
[17] F. A. Tobagi, "Analysis of a two-hop centralized packet radio network–part ii: Carrier sense multiple access," *IEEE Transaction on Communications*, vol. vol. 28, no. no. 2, p. pp. 208–216, Feb. 1980.
[18] C. E. a. F. A. I. Demirkol, "MAC protocols for wireless sensor networks: A survey," *IEEE Communications Magazine*, vol. vol. 44, no. no. 4, p. pp.115–121, Apr. 2006.
[19] S. Raza et al, "Securing communication in 6LoWPAN with compressed IPsec," *IEEE Int. Conf. Distrib. Comput. Sens. Syst.*, no. Proc. 7th, p. pp. 1–8, Jun. 2011.

Authors' Profiles

Haytham Qushtom, born in 1987. Master in Arab American University, Jenin, Palestine. His main research interests include wireless sensor network, Internet of Things, quality of services (QoS), and security protocols.

Dr. Khalid Rabaya'h is an Associate Professor in Computer Science and Information System. He is the founder and the manager of an Information System research center at the Arab American University-Jenin, Palestine. Dr. Rabayah is an active researcher in three IT related areas; Information systems, Wireless Networks and Internet of Things (IoT), and Data Analysis and Mining. His research interest in Information systems includes knowledge management, e-commerce, e-learning, technology adoption modelling and diffusion, especially in the context of developing countries, and cross-cultural issues in the use of IT.

His research interest in Wireless Networks and Internet of Things, started in 2015. Currently he is involved in a project which focuses on enhancing the quality of services (QoS) of Internet of things (IoT), based on light weight security protocols.

His research interest in Data mining and data analysis started back in 2013. His research experience in data mining and analysis focuses on the use of the statistical software package of IBM SPSS and AMOS. He professionally uses these packages in developing predictive models for business processes and discovering hidden patterns in unstructured data and big data.

How to cite this paper: Haytham Qushtom, Khalid Rabaya'h,"Enhancing the QoS of IoT Networks with Lightweight Security Protocol using Contiki OS", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.11, pp.27-35, 2017.DOI: 10.5815/ijcnis.2017.11.03

