International Journal of Computer Information Systems and Industrial Management Applications.
ISSN 2150-7988 Volume 8 (2016) pp. 275-283

A New Security Layer for Improving the security of internet of things (IoT)

Hamoud M. Aldosari, Vaclav Snasel, Ajith Abraham
VŠB-Technical University of Ostrava
17. listopadu 15/2172, 708 33 Ostrava - Poruba, Czech Republic
mub0002@vsb.cz, vaclav.snasel@vsb.cz, ajith.abraham@ieee.org

Abstract: **Recently, various improvements were conducted in the field of both Wireless Sensor Network (WSN) and Mobile Ad Hoc Networks (MANETs) technologies. This results in creating various efficient concepts to enhance the daily life, such as the deployment of the Internet of Things (IoT) concept in unconventional applications. However, this IoT is subject to some restrictions, such as the use of specific communication models and the complexity due to the exchange of information among various heterogeneous devices that located in several contexts. Thus, the implementation of scalable, interoperable and effective security mechanisms is a real challenge. In this paper, an independent single security layer is proposed to meet and manage the majority of security mechanisms distributed over other network layers. This layer could be used to verify the identity of both receiver and sender to assist in avoiding attacks. In addition, it assists other communication reference model layers of the IoT to carry out their functions regardless of security problems. The Network Simulator (NS2) was used to evaluate the suggested layer in terms of end-to-end delay, throughput, packet dropped, Normalized Routing Load (NRL) and Packet Delivery Ratio (PDR). The simulated results showed that adding the new security layer could either improve the performance of the traditional communication models or in other cases offered the same performance.**

Keywords**:** MANETs; TCP/IP Model; routing protocols; Internet of things; Encryption; Decryption.

I. Introduction

Recently, various efforts have been conducted to enhance the sensing process of both WSN and MANET technologies. This process permits measuring and recognizing various environmental conditions, such as urban regions and natural resources. In practice, these continuous improvements result in a new concept in this field, which known as the IoT. The IoT represents the interconnection of a large number of heterogeneous devices to offer alternative applications in order to enhance the quality of life. This is due to its ability to allow incorporating actuators and sensors effortlessly with the surrounding environment and sharing information across several stages to implement efficient operating structures [1].

The first presented project using this concept was the IoT-A Project (IoT-A). It was used to propose an efficient Architectural Reference Model (ARM) design based on deploying various guidelines and approaches [2]. The presented design was able to enhance the interoperability among separated IoT applications. But, this project has ignored both the privacy and security services, which are two main factors that must be considered in the IoT to prevent accessing it by illegal users and attacks. This in turn increases the need for designing efficient security mechanisms. In practice, this is considered as a difficult stage due to the complexity of IoT in which numerous devices exchange their data with each other. One suggested solution was incorporating the IoT with cloud computing techniques, but this makes the security issue more vital. Thus, a modification was performed on the TCP/IP communication model based on adding a new security layer for the model to ensure enhancing the security [3].

II. Background and Related Work

In practice, the IoT includes several features about the Internet and web extension into real world, where this is based on using several distributed devices concerning sensing capabilities and embedded recognition [4]. Although the IoT can sustain various applications, few applications depend on using this concept. This in turn increases the need to conduct more efforts to offer IoT dependent applications in various smart fields, as environment monitoring, aerospace, enterprises, hospitals, factories, offices, homes and transportation systems [5].

The field of environment monitoring as an example representing the use of the IoT technology in environmental preservation and green applications, which are efficient applications that can offer various benefits for future projects. In the field of automotive industry, it can be used to equip bicycles, cars, buses and trains with actuators and sensors in order to enhance the processing powers. As an example in the field is the use of smart sensors to control pressure parameters of vehicle wheels [6, 7].

Another benefit of the IoT technology is its help in exchanging both goods and services in large-scale supply chain networks with ensuring security for all stakeholders. Furthermore, it includes various actions and measures to monitor and control the vulnerability to attacks, data verification, client security and access control [8]. Figure 1 shows the general IoT architecture.

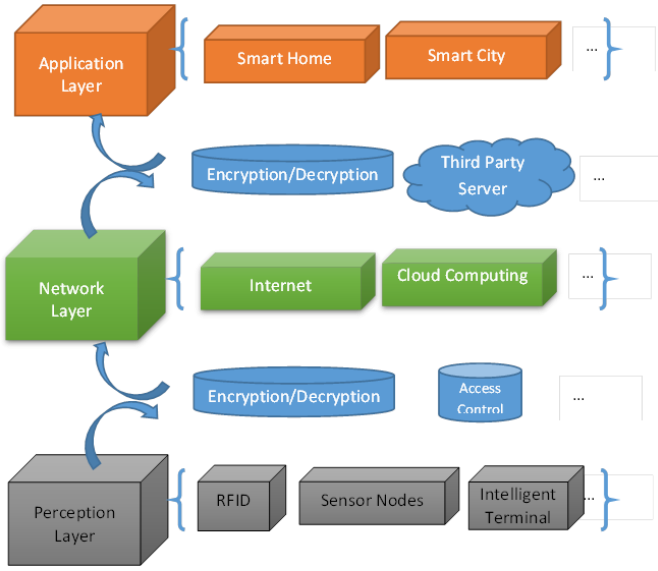

Figure 1. General architecture of the IoT [8]

The efficient deployment of the IoT depends mainly on addressing and assessing its security and privacy issues. Practically, there is still a need for more enhancements concerning the security of communication among components within networks. The deployment of the IoT increases the dependence on serious infrastructures, computer technologies, communications and several IoT objects. This in turn increases the vulnerability of IoT application to various types of attacks [9]. Thus, sustainable and scalable cyber ecosystem must be developed in the IoT technology to discover and recognize attacks. To address this problem, various efforts were conducted in the recent years.

Jincy and Sundararajan [10] developed an efficient mechanism to assist IoT system designers in signifying the optimal security method for each one of its entities. This mechanism in turn facilitates establishing a totally encrypted End-to-End (E2E) security structure with various levels of security defense interfaces.

De Rubertis et al [11] evaluated the performance of two security protocols developed and applied for WSNs, namely; the Internet Protocol security (IPsec) proposed by Kent and Seo and Datagram Transport Layer Security (DTLS) proposed by Rescorla and Modadugu [13]. This was performed in order to assess their applicability for several IoT devices. The obtained results proved that the application of these protocols using their traditional structures had bad impacts on the required E2E security structure for IoT devices.

Giulio et al [14] developed a hybrid security framework that combined three security protocols, namely; Constrained Application Protocol (CoAP), DTLS and IP version 6 (IPv6) Low power Wireless Personal Area Networks Protocol (6LoWPAN) over TinyOS component dependent operating system. This hybrid security framework is called the BlinkToSCoAP. Authors conducted several amendments on these three protocols to improve the performance. One of these amendments is reducing both the number of addresses and the highest queue dimension of packets of IPv6. The obtained results demonstrated proved the efficiency of the presented framework and its efficient enhancements to the energy consumption, memory usage, transmission delay and packet loss.

Mališa et al [15] presented the offloading of the verification load from restricted servers to place it on more network efficient devices, such as secured nodes and/or hosts within the cloud. This was performed to save resources of WSNs. The main purposes of these devices are verifying individual clients and sharing suiTable access tokens and secrets with them. Thus, authors developed an efficient Object-based Security Architecture (OSCAR) system to offer effective E2E security with no impacts on the restricted objects' duty-cycling operation. Furthermore, this system is able to offer access control, validity trust domains and decouples privacy as well as it essentially sustains caching, asynchronous traffic and multicast.

Yang et al [8] presented a security model with three IoT layers; perception, network and application layers as shown in Figure 1. The layer in the bottom is the perception one, which is the most essential layer for the architecture of the IoT. This layer recognizes and gathers data from the surrounding environment through sensors to be used in designing efficient management procedures. The most common types of sensors used in this layer are the temperature, vibration, pressure and sound. However, the flow of data through these wireless sensors makes them vulnerable to attacks, where this results in various security risks within this layer, such as analysis of data flow [16] and communication link eavesdropping [17].

The middle layer is the network one or as called also the transmission later. It offers a channel to transmit packets among various platforms within a network. Due to the huge amount of data gathered by the previous layer, the network layer requires adequate ability in order to process and control all these data effectively. This in turn results in several identity verification problems in the IoT. Another problem that may occur is the network congestion, which results from the huge amount of redundant data. These problems make the network layer vulnerable to the denial of service (DOS) attacks. Thus, the network availability must be guaranteed based on adding several filtration devices among the network and application layers [8].

The top layer is the application one, which process the delivered data in an efficient manner in order to guarantee that these data will be deployed by legal end users only. Several user applications cope with the IoT in order to make the life more suiTable and to decrease the workload. However, protecting huge amount of data gathered using these applications is vital and requires conducting more efforts to enhance it [8].

Therefore, it can be noticed that the proposed IoT-A solution has a problem in overlooking the privacy and security services that are very essential in the environment of the IoT.

Hong et al [18] compared and analyzed the General Purpose Graphics Processing Unit (GPGPU) and parallel computing

on a Central Processing Unit with multiple cores. Authors illustrated that the Rivest-Shamir-Adleman (RSA) algorithm, which is a cryptosystem method used to encrypt and decrypt messages is compute intensive algorithm. Therefore, they developed the GPGPU using the RSA algorithm and carried out a comparison among their algorithm and the CPU. The parallel development of the RSA algorithm on the GPU was based on deploying the method of threads and threads block. This depended on segmenting the program computation part into various threads, which in turn divided into small thread blocks. The obtained results presented that the proposed method offered forty five times speedup in comparison with the CPU counterpart.

Masumeh and Ithnin [19] presented the application of a parallel processing on the RSA encryption algorithm with deploying on a tree structure. It was presented that both the performance and speed of the RSA algorithm were enhanced based on parallelizing it.

Mahajan and Singh [20] presented that massive parallelism can be developed using the GPU as a coprocessor for the CPU. Therefore, they proposed the development of a parallel RSA algorithm for the GPU with the use of the Compute Unified Device Architecture (CUDA) framework. It was then evaluated for both large and small prime numbers. The obtained results demonstrated that this algorithm had enhanced speed and decreased the security threats with the use of small prime numbers.

Xin and Yang [21] evaluated the mechanisms of several available routing protocols deployed in Ad Hoc networks. These routing protocols are the Ad hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR) and Optimized Link State Routing (OLSR). Then, they determined the optimal routing protocol for IoT based on examining and comparing the performance of these protocols in terms of throughput, E2E delay and routing overhead. The obtained results demonstrated that the DSR routing protocol outperformed other protocols in the routing overhead, while the AODV offered the best throughput in comparison with the other protocols.

Sudhir et al [22] modified the AODV protocol to be Secure AODV (SAODV). This was performed depending on the suggestion that each one of the network node possesses practiced general keys of the whole other nodes. The presented modified protocol offers several features, such as verification, non-repudiation and integrity. However, Christy and Palanisamy [23] presented that the main problem of this protocol is the difficulty in determining the general keys of all nodes.

In this paper, the developed algorithm depends on embedding the RSA encryption algorithm in a layer added among the internet and network access layers. This is performed to enhance the performance of the AODV protocol and to use this research in the future as a base to embed several security algorithms in that new layer.

III. Preliminaries

The main deployed protocols and techniques in the development of the presented security algorithm are presented in this section.

A. MANETs

Generally, these networks include specific self-configuration mobile devices with wireless communication among them [24]. These devices are able to move freely and communicate with any other device, thus, these networks have irregular structures [25]. When they receive unrelated data, each network acts as a router or a host. The main deployed protocols in MANETs are the User Datagram Protocol (UTP), Transmission Control Protocol (TCP) and Cluster Based Routing (CBR) protocol. However, various other protocols were presented depending on modifying these two protocols to standardize the 'configurations of MANETs [26]. Some of these protocols are: DSR [27], OLSR [28] and AODV [28].

On the other hand, the procedures of MANETs were inherited by various other networks, such as the Vehicular Ad-hoc Networks (VANETs) which are communication infrastructures used in intelligent transmission systems [30]. One type of MANETs is the internet MANET (iMANET), in which minimally one device of the network is connected with the internet [31]. In practice, MANETs have some problems that have to be solved, such as security threats, restricted resources, mainly the power ones, update and discovery facilities of devices and devices' dynamicity behavior [32].

B. AODV Routing Protocol

It is a reactive routing protocol used for MANETs. With the use of this protocol, packets arrive to their target destination nodes based on offered next hops according to the routing Table of each source node. This protocol allows all mobile nodes to communicate with their neighbors in order to allow sending packets to nodes that there are no direct connection links with them.

There are various included messages in the AODV routing protocol; the first message is HELLO, which transmitted by a node to another one in order to check if they are neighbors or not. The second message is the Route Request (RREQ), which is a broadcast from the source node to its neighbors. The third message is the Route Reply (RREP), which is a response to the RREQ message to determine if the path among both nodes is available or not. If it is not available, the source node rebroadcasts it to another neighbor. The last message is the Error Reply (RRER), which is sent when there is a link failure or break. Information in the routing Table of each node is updated continuously to assist in constructing the reverse path for the RREP message. Figure 2 shows the route discovery process of the AODV protocol, in which the source node (S) sends a RREQ message to its neighbors A and C, where they in turn send this message to nodes B and D. When the message reaches the destination node (D), it is uni-casted to the source node (S) again [33, 34].

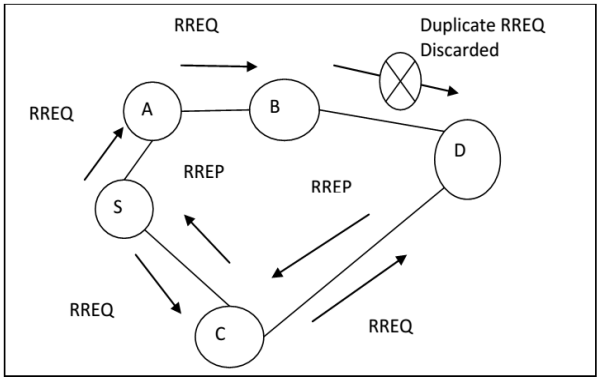

Figure 2. Route discovery process of the AODV routing protocol

Figure 3 illustrates the process of sending AODV messages [35].

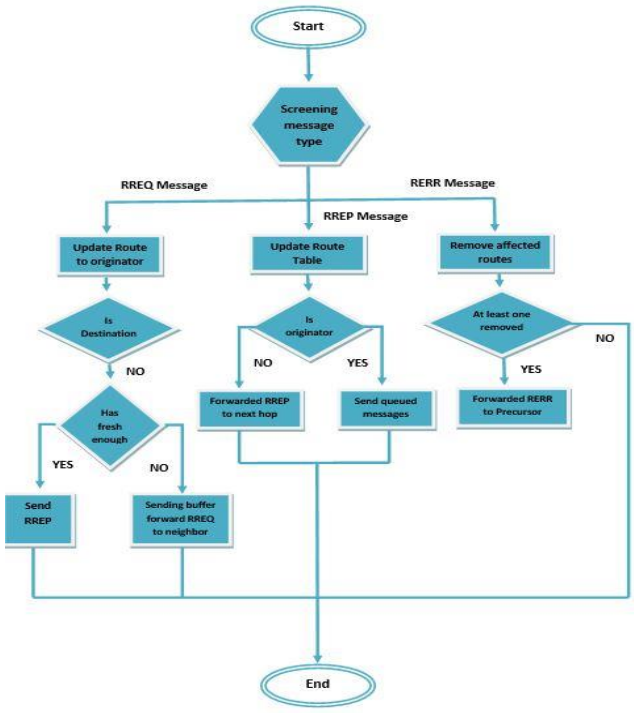

Figure 3. Process of sending AODV messages

C. RSA Algorithm

The most common cryptographic algorithms are the RSA, Diffie-Hellman Key Exchange and Digital Signature. The RSA algorithm is an efficient public key cryptography dependent algorithm deployed for encryption/decryption and digital signatures. It was introduced and developed by Ronald Rivest, Adi Shamir and Leonard Adleman in 1978 [36]. This algorithm depends on the factorization mathematical model of large integers. This results in an intensive process of computation that needs long time and high power consumption to carry it out [37]. It includes three algorithms; encryption, decryption and generation algorithms.

D. Key Generation Algorithm

The main stages of this algorithm are:

1. Selecting two very large prime integers randomly p and q, with bit size equals to 512 as a minimum
2. Computing the modulus m, which equals to p*q
4. Computing $\varphi(n)$ as $\varphi(n) = (p-1)(q-1)$
5. Selecting a specific integer e, $1 < e < \varphi(n)$, in which GCD $(e, \varphi(n)) = 1$, Where GCD represents the maximum common denominator
6. Computing d, $1 < d < \varphi(n)$, in which: $ed \equiv 1 \pmod{\varphi(n)}$

With using e as encryption exponent and as decryption exponent, both e and n are available as the public key, while d and n are encrypted as the private key. The Table below illustrates the encryption and decryption pseudo code.

1.3 RSA Encryption	1.4 RSA Encryption
The RSA encryption can applied on variable size of mes block. Thus, data can be div into the blocks of data using padding scheme such as PCk and following procedur applied to it, C = M^e % m, w M is the message block and sent as the cipher text to the party	In order to decrypt the cipher text following procedure is applied to it M = C^e % m, where M is the original plain text and C is the Cipher text

Table 1 Illustration of encryption and decryption pseudo code

IV. The Proposed Security Layer

The main purpose of this work is to generate an independent single security layer between the internet and network access layers to be used as a filtration layer before transmitting packets. The aim of this layer is to meet and manage almost all of distributed security mechanisms in other layers with a focus on embedding the RSA algorithm. The network security layer checks that all packets are received successfully to be then sent to the proposed security layer. Figure 4 shows the modified end-to-end communication model with AODV algorithm after creating the proposed security layer. The Object Oriented Programming in the NS2 simulator was used to make the proposed layer. All sensors of the network are assumed to be variables. Thus, the code was run for many times were achieved values were then averaged. The generation of the proposed layer is conducted based on repeating the following stages that demonstrated also in Figure 5:

1- Packets are transmitted/received by the proposed security layer located between the internet and network access layers
2- The RSA encryption/ decryption algorithm is applied over the transmitted/received packets

3- The resultant encrypted packets are transmitted to the network access layer
4- The resultant decrypted packets are transmitted to the internet layer

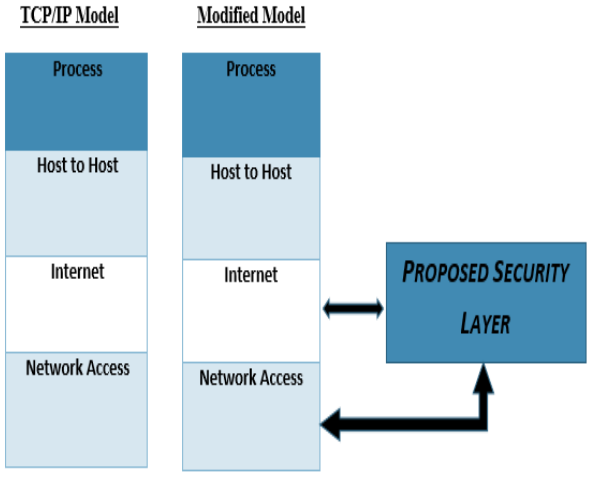

Figure 4. The modified model after creating the proposed security layer

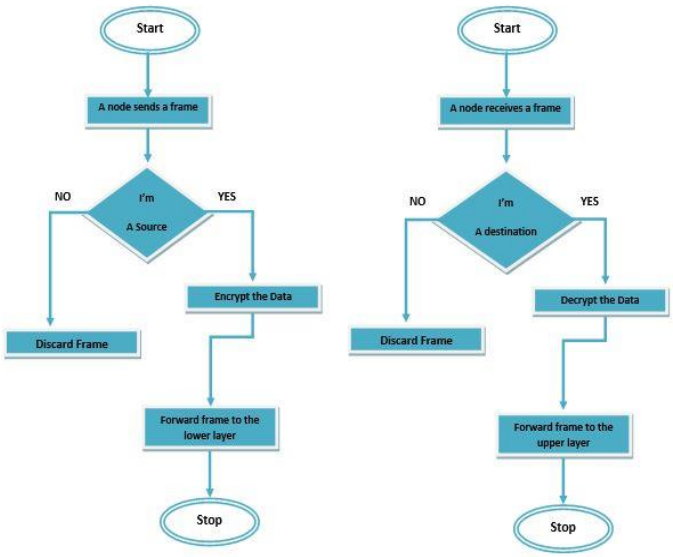

Figure 5. Flowchart of the security function in the proposed security layer

V. Simulation Results and Analysis

The created security layer is evaluated using the NS2 simulation tool, which offers efficient analysis in the investigation of communication networks' dynamic nature. The NS2 can be used to simulate both wired and wireless network functions and protocols, such as UDP, TCP and routing protocols as the CBR one. In addition, it allows users to determine network protocols and simulated their related performance. However, the NS2 cannot be used to implement any security features [38]. Thus, security function were implemented initially in this work and then added to the NS2 libraries to be utilized in evaluating the proposed security layer features.

V.1 Experiments Setup

In this paper, the NS2 version allinone-2.35 installed in Ubuntu (14.04 LTS) in Desktop i5 and 16 RAM machine was used to perform all simulation experiments. Furthermore, the IEEE 802.11 protocol was deployed as the Media Access Control (MAC) layer one protocol. In addition, the Tool Command Language (TCL) was used to write the TCL scenario and produce related trace and nam files

The proposed security layer was evaluated using various scenarios under Wireless channel and CBR/UDP traffic. In the first scenario, the layer was evaluated under different network sizes (10, 20, 30, 40, and 50 nodes) and variable sensors. The nodes move from their initial locations to random target locations at random speeds within the simulated 500 m x 500 network area. When a node reaches its target location, it waits for a specific time period and then chooses another random position to move toward it. In this work, the simulation time was 60 seconds. The assumed simulation parameters in the performed experiments are demonstrated in Table 2.

PARAMETER	VALUE
Channel type	Wireless channel
Number of nodes	10, 20, 30, 40, 50
Traffic type	CBR/UDP
Area of simulation	500 m X 500 m
Routing Protocol	AODV
Time of simulation	60 sec

Table 2 Simulation parameters assumed in conducted experiments

V.2 Performance Metrics and Simulation Results

The performance of the proposed security layer with the AODV routing protocol was evaluated in terms of: *packet dropped, PDR, NRL, throughput and E2E delay using 10, 20, 30, 40, and 50 nodes.* These measurements are discussed below.

- **Dropped Packets:** Mobility associated packets can be dropped at both the internet and network access layers. In this work, the focus is on packets dropped at the internet layer. The dropped packets can be expressed as follows:

Dropped Packets = transmitted packets– received packets

The obtained results of dropped packets in the internet layer with and without adding the security layer for different network size (10, 20, 30, 40, and 50 nodes) are shown in Table 3 and Figure 6 below.

Number of nodes	*Without new layer*	*With new Layer*
10	0	0
20	2	2
30	5	7
40	15	26
50	39	56

Table 3 Dropped packets of both models for various network sizes

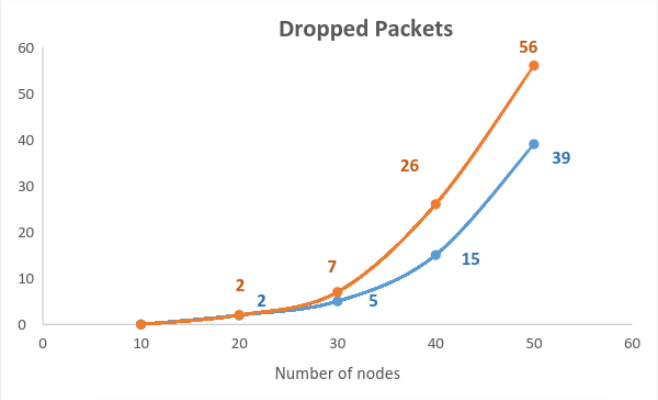

Figure 6. Dropped packets of both models for various network sizes

It can be noticed that when the number of nodes is 10 and 20, the number of dropped packets is the same for both models. When the nodes are more than 30, the dropped packets rate of the new model is less than that of the model without the new layer. Therefore, the addition of the proposed security layer decreased the number of dropped packets for various network sizes

- **PDR percentage:** It represents the ratio of the number of received packets by the destination node to the number of originated ones. It can be expressed using the following formula:

PDR Percentage= (Number of received packets / number of transmitted packets) * 100%

The results of testing PDR with and without adding the security layer at different network size (10, 20, 30, 40, and 50 nodes) are illustrated in Table 4 and Figure 7.

Number of nodes	*Without new layer*	*With new Layer*
10	100	100
20	99.9	99.88
30	99.17	99.58
40	99.37	98.85
50	98.62	98.03

Table 4 PDR percentages of both models for various network sizes

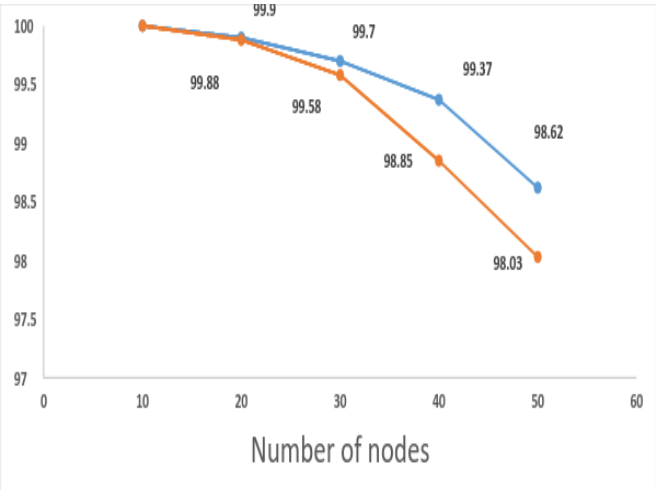

Figure 7. PDR percentages of both models for various network sizes

Based on these results, the new model after adding the security layer outperformed those of the traditional model (i.e. without the security layer). Thus, the throughput of the network with the proposed security layer is higher than that of the normal network without this layer. On the other hand, the PDR percentage of both models decreases with the increase in the number of nodes.

- **NRL:** It represents the number of sent routing packets per delivered packets at the destination node. In addition, it represents the ratio of transmitted routing packets via the whole network nodes to the number of packets received at the destination nodes. The NRL can be represented as follows:

NRL = (Total transmitted routing packets / Total received routing packet

The results of evaluating NRL measurement in case of using the added security layer and without using it for different network size (10, 20, 30, 40, and 50 nodes) are shown in Table 5 and Figure 8.

Number of nodes	*Without new layer*	*With new Layer*
10	0.1725	0.1725
20	0.3454	0.3454
30	0.5188	0.5256
40	0.6997	0.7136
50	0.9443	0.9616

Table 5 NRL results of both models for various network sizes

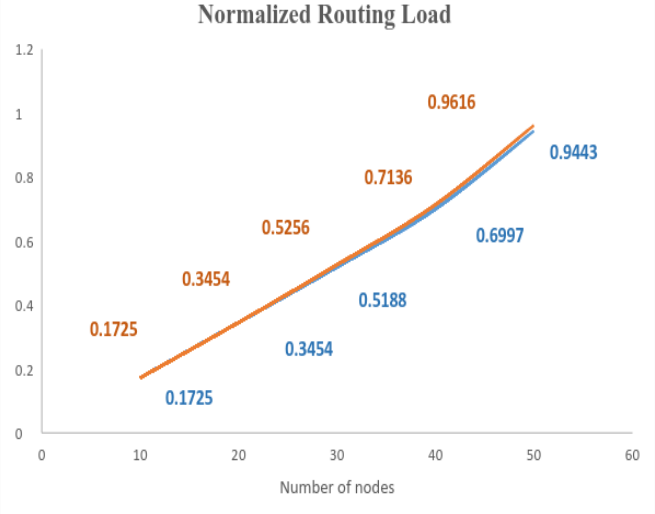

Figure 8. NRL results of both models for various network sizes

From Figure 8, it can be noticed that there is no difference between the NRL results before and after adding the security layer. Thus, the network after adding the security layer has routing functions similar to those before adding it. In addition, the NRL value increases with the increase in the number of nodes for both models.

- **Throughput:** It represents the amount of transmitted from one node into another by a communication link per unit time [39]. It can be expressed as follows:

Throughput = (Number of received packets * packet size*8) / Simulation Time.

The results of testing the throughput with and without adding the security layer at different network size (10, 20, 30, 40, and 50 nodes) are demonstrated in Table 6 and Figure 9.

Number of nodes	*Without new layer*	*With new Layer*
10	22.272	22.272
20	25.6	25.6
30	26.83	26.8
40	27.39	27.26
50	27.60	27.43

Table 6 Throughput results of both models for various network sizes

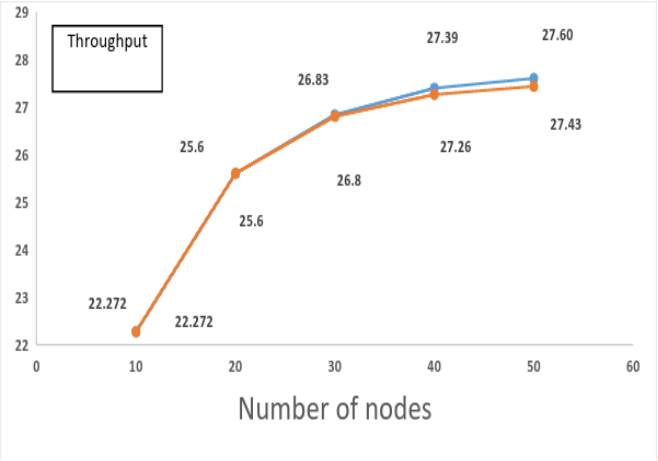

Figure 9. Throughput results of both models for various network sizes

From these results, it can be remarked that both models has a close the average throughput. Thus, the added security layer can work under various network sizes with no impact on its throughput. In addition, the throughput value increases with the increase in the network size. Furthermore, the routing protocol can achieve the convergence state in the same speed in both models.

- **Average End-to-End Delay:** It represents all probable delays resulted from the buffering process throughout the route detection delay, propagation and sending times of packets, resending delays at the network access layer and queuing at the interface line.

The simulated results of testing the E2E delay with and without adding the security layer at different network size (10, 20, 30, 40, and 50 nodes) are highlighted in Table 7 and Figure 10.

Number of nodes	*Without new layer*	*With new Layer*
10	2.46	2.46
20	2.67	2.67
30	2.86	2.94
40	3.16	3.22
50	3.75	3.86

Table 7 E2E delay results of both models for various network sizes

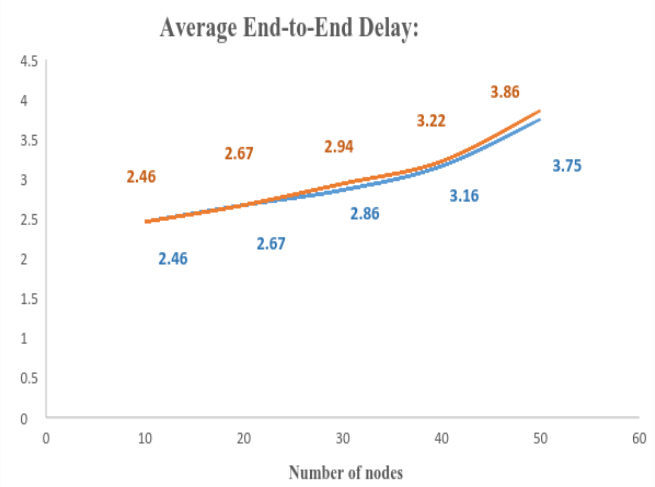

Figure 10. E2E delay results of both models for various network sizes

From these results, it can be said that the model after adding the security layer has a slightly lower average E2E delay than the normal model. Thus, the security layer could improve the network performance. On the other hand, the E2E delay is directly related to the increase in the network size, which leads to low performance. Since the routing protocol is initially applied to the security functions at the security layer, when the secured data are transmitted to the network interface layer, latency time increase [40]. In addition, the applied security functions at each node before transmitting packets to the network layer may increase the delay after applying the new layer

From the above results and their discussion, the following remarks can be drawn. Firstly, the addition of the proposed security layer to the network under different size (10, 20, 30, 40, and 50 nodes) did not affect the performance of the traditional network model. On the other hand, the simulation results showed that , in the case of gathering network layers' security functions in one layer, these layers can only carry out their specific functions regardless of any security problems. Therefore, adding new security layer could help in supporting new centralized troubleshooting processes that are mostly needed in the presented networks; WSNs, MANETS and IoT. This, in turn, could help to improve the security of the IoT, thus improving its deployment in a wide range of domains and fields.

VI. Conclusion

This paper presented a solution for improving the security of the traditional communication model by introducing a new security layer to be added between the internet and network access layers. This layer aims to support the majority of security mechanisms required in the IoT environments. The NS2 simulator was used to design the suggested layer and evaluate it in terms of dropped packets, PDR, NRL, throughput and E2E delay. The simulation results illustrated that the proposed security layer offers better (in some scenario) or the same performance as that of the traditional model. Those results can be considered as bases for more investigations concerning centralized security layers including the whole security functions in the TCP/IP model. This in turn can result in easier troubleshooting. In the future, we aim to investigate the effect of the new security layer to the other protocols, e.g., UPD.

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*, 29 (7), pp.1645-1660, 2013

[2] A. Bassi, M. Bauer, M. Fiedler, T. Kramp, R. Van Kranenburg, S. Lange and S. Meissner, "Enabling things to talk", *Springer*, 2013.

[3] A. H. Alhamedi, V. Snasel, H. M. Aldosari and A. Abraham, "Internet of things communication reference model", *6th International Conference on Computational Aspects of Social Networks (CASoN)*, 2014.

[4] D. Miorandi, S. Sicari, F. De Pellegrini and I. Chlamtac, "Internet of things: Vision, applications and research challenges", *Ad Hoc Networks*,10 (7), pp. 1497-1516, 2012

[5] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization", *Wireless Personal Communications*, 58 (1), pp.49-69, 2011

[6] S. Peters, J. H. Chun and G. Lanza, "Digitalization of automotive industry–scenarios for future manufacturing. Manufacturing Review", 3(1), 2016

[7] R. Kirk, "Cars of the future: the Internet of Things in the automotive industry", *Network Security*, (9),pp. 16-18, 2015

[8] X. Yang, Z. Li, Z. Geng and H. Zhang, "A Multi-layer Security Model for Internet of Things. In: Internet of Things", *Springer Berlin Heidelberg*, pp.388-393, 2012

[9] P. Fonash and P. Schneck, "Cybersecurity: From Months to Milliseconds", *Computer*, 1, pp.42-50, 2015

[10] V. J. Jincy and S. Sundararajan, "Classification Mechanism for IoT Devices towards Creating a Security Framework", *In Intelligent Distributed Computing, Springer International Publishing*, pp. 265-277, 2015

[11] A. De Rubertis, L. Mainetti, V. Mighali, L. Patrono, I. Sergi, M. L. Stefanizzi and S. Pascali, "Performance evaluation of end-to-end security protocols in an Internet of Things." *21st International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pp.1-6, 2013

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

[13] E. Rescorla and N. Modadugu, "Datagram transport layer security version", 1 (2), 2012

[14] G. Peretti, V. Lakkundi and M. Zorzi, "BlinkToSCoAP: An End-to-End Security Framework for the Internet of Things", 2015

[15] M. Vučinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon and R. Guizzetti, "OSCAR: Object security architecture for the Internet of Things", *Ad Hoc Networks*, 2014

[16] A. Gosain and G. Sharma, "Static Analysis: A Survey of Techniques and Tools", *In: Intelligent Computing and Applications. Springer India*, pp.581-591, 2015

[17] S. Yoon, H. Park, H. S. Yoo, H. S., "Security Issues on Smarthome in IoT Environment", *In: Computer Science and its Applications, Springer Berlin Heidelberg*, pp. 691-696, 2015.

[18] H. Hang, D. Zhang and X. Bi, "Comparison and Analysis of GPGPU and Parallel Computing on Multi-Core CPU", 2012

[19] M. Damrudi and N. Ithnin, N.,"Parallel RSA encryption based on tree architecture", *Journal of the Chinese Institute of Engineers*,36 (5), pp. 658-666, 2013

[20] S. Mahajan and M. Singh, "Analysis of RSA algorithm using GPU programming." *arXiv Preprint arXiv* 1407 (1465), 2014

[21] H. Xin and K. Yang, "Routing Protocols Analysis for Internet of Things", *2015 2nd International Conference on Information Science and Control Engineering (ICISCE), pp.* 447 – 450, 2015

[22] S. Agrawal, S. Jain, S. and S. Sharma, "A survey of routing attacks and security measures in mobile ad-hoc networks". *arXiv preprint arXiv*,1105 (5623), 2011

[23] S. S. Christy and V. Palanisamy, "Secure Based Routing Protocol With Cryptography Data Encryption Technique For MANET", 2015

[24] R. Shenbagapriya and K. Narayanan, "An Efficient Proactive Source Routing Protocol for Controlling the Overhead in Mobile Ad-Hoc Networks", *Indian Journal of Science and Technology*,8 (30), 2015

[25] V. R. Marutha and R. Latha, "Mobile Ad hoc Network." *International Journal of Science and Research (IJSR)*, 2 (4), 2013

[26] M. Conti and S. Giordano, "Mobile ad hoc networking: milestones, challenges, and new research directions", *Communications Magazine*, 52 (1), pp.85-96, 2014

[27] D. Johnson, Y. Hu and D. Maltz, "The dynamic source routing protocol (DSR) for mobile ad hoc networks for IP", 4 (RFC 4728), 2007.

[28] T. Clausen and P. Jacquet, "Optimized link state routing protocol (OLSR)", 2003.

[29] C. Perkins, E. Belding-Royer and S. Das, " Ad hoc on-demand distance vector (AODV) routing", 2003.

[30] S. Kuhlmorgen, I. Llatser, A. Festag and G. Fettweis, "Performance Evaluation of ETSI GeoNetworking for Vehicular Ad hoc Networks." *IEEE 81st conference on Vehicular Technology Conference (VTC Spring), pp.* 1-6, 2015.

[31] S. Sharma, M. Trivedi L. and Kurup, "Using Ontologies to Model Attacks in an Internet based Mobile Ad-hoc Network (iMANET)", *International Journal of Computer Applications*, 110 (2), 2015

[32] A. O. Bang and P. L. Ramteke, "MANET: History, Challenges and Applications", *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, 2 (9), pp. 249-251, 2013

[33] S. M. Sheikh, R. Wolhuter, and G. J. van Rooyen. "A comparative analysis of MANET routing protocols for low cost rural telemetry Wireless Mesh Networks", *2015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, IEEE, 2015.

[34] T. Arora, A. Kaur and M. Singh, "Review of Various Routing Protocols and Routing Models for MANETs", 2015

[35] C. Lin, "AODV Routing Implementation for Scalable Wireless Ad-Hoc Network Simulation (SWANS)", 2004

[36] R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and publish key Cryptosystems", *Communications of the ACM*, 21 (2), pp.120-126, 1978.

[37] S. Saxena and B. Kapoor, "State of the art parallel approaches for RSA public key based cryptosystem", *arXiv preprint arXiv*, 1503 (03593), 2015

[38] C. He, "Effects of Security Features on the Performance of Voice over WLAN", *EE384C Final Project Changhua He, Electrical Engineering, Stanford University,*. 2004.

[39] A. Valarmathi and R. Chandrasekaran, "Congestion aware and adaptive dynamic source routing algorithm with load-balancing in MANETS", *International Journal of Computer Applications*,8 (5), pp. 1-4, 2010

[40] A. K. Gupta, H. Sadawarti, and A. K. Verma, "Performance analysis of aodv, dsr & tora routing protocols", *IACSIT international journal of Engineering and Technology*, 2 (2), pp. 226-231, 2010.