Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 11 (2016) pp. 058-066
© MIR Labs, www.mirlabs.net/jias/index.html

A Novel Security Layer for Internet of Things

Hamoud M. Aldosari, Vaclav Snasel, Ajith Abraham*
VŠB-Technical University of Ostrava
17. listopadu 15/2172, 708 33 Ostrava - Poruba, Czech Republic
*Machine Intelligence Research Labs (MIR Labs), Scientific Network for Innovation and Research Excellence, Auburn, Washington 98071, USA
mub0002@vsb.cz, vaclav.snasel@vsb.cz, ajith.abraham@ieee.org

Abstract: **Mobile Ad Hoc Networks (MANETs) and Wireless Sensor Network (WSN) technologies have been using for many aspects of our day living. The rapid increase in the number of these devices in communicating–actuating networks creates the Internet of Things (IoT) concept that appears in a number of unconventional applications. To achieve this connectivity, the IoT needs a communication model such as the TCP/IP communication model. In addition to the complexity of the IoT, where multiple heterogeneous devices, located in various contexts, could exchange information with each other, the design of interoperable, efficient, and scalable security mechanisms is much difficult. This paper, proposes a solution, which could be considered as a step forward for a centralized management of all security mechanisms into a single layer. The Security Layer aims to confirm the identity of the sender/receiver to help to block connections to potentially vulnerable services. Furthermore, this centralization would leave other IoT's communication reference model layers to perform their specified functions without paying attention to any security problems. The experimental results conducted using Network Simulator (NS2) simulator and the results were evaluated using different measures, packet dropped, packet delivery ratio (PDR), normalized routing load (NRL), throughput and end-to-end delay. These results showed that the proposed solution performed better than the normal communication model.**

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

I. Introduction

Ubiquitous sensing enabled by MANET and WSN technologies have been rapidly grows in daily live. These sensing capabilities offer the ability to measure and understand environmental indicators such as natural resources and urban environments. This rapidly increase of these networks creates the Internet of Things (IoT) concept. In such concept, the sensors and actuators can seamlessly integrate with the environment around us, as well as the information can be shared across platforms to develop a common operating structure [1]. In general, the IoT aims to interconnect huge numbers of heterogeneous devices in order to provide unconventional applications to improve our quality of life.

The IoT-A project [2] was aiming to propose a design of an Architectural Reference Model (ARM) using a number of particular tools and guidelines. The main goal of this ARM model was to optimize the interoperability between isolated IoT applications such that to build a global ecosystem of services with a common understanding. However, this proposed (IoT-A) has overlooked the security and privacy services, which are very important in the IoT environment. Generally, the IoT needs global accessibility and connectivity such that anyone can access the IoT at anytime and anywhere. This leads to a number of attacks and hence, the security mechanisms are needed. Because of IoT complexity where different devices exchange their information together, the design of a powerful security mechanism is difficult challenge. Furthermore, integrating the IoT with the clouding and ubiquitous computing makes the privacy problem much urgent. [3] proposed the idea of modified the TCP/IP model by adding a new cross layer to TCP/IP model called a new security layer that concerned only in security.

II. Background and Related Work

The term "Internet-of-Things" is defined as an umbrella of various aspects concerning with the extension of the Web and the Internet into the physical realm. This can be realized though the widespread deployment of distributed devices including embedded identification, sensing capabilities [37]. The nature of the IoT can make it possible to support numerous applications. Currently, only a few numbers of applications are being deployed. In the near future, it is estimated that there will be IoT-based applications in different fields, such as smarter transportation systems, smarter homes and offices, smarter hospitals, smarter factories and enterprises, Aerospace and Aviation Industry, Environment Monitoring, etc [38]. For example, in the environment monitoring, the IoT technologies (e.g., using wireless identifiable devices) can be deployed in green applications and environmental conservation, which are considered as one of the most promising projects in the future. Also, the IoT could be very promising technologies for the automotive industry.

Advanced trains, buses, cars, and bicycles could be equipped with sensors, actuators for increased processing powers. Examples of applications in the automotive industry could include the use of smart sensors to monitor and report various parameters from pressure in tyres to proximity of other vehicle [39], [40].

The Internet of Things is an evolving global Internet-based architecture, which can facilitate the exchange of services and goods in global supply chain networks. This architecture emerges security and privacy concerns for the involved stakeholders. Measures and actions, which ensure the architecture's elasticity to attacks, access control, data authentication, and client privacy, are a must. The main architecture of the IoT is given in Figure 1.

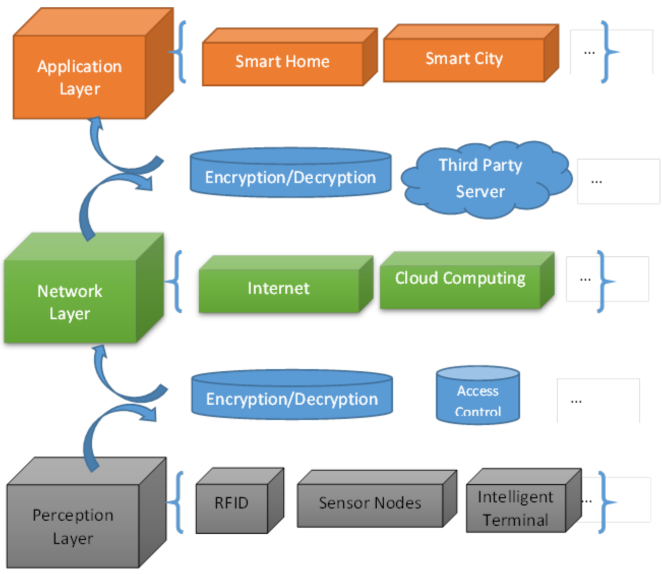

Figure 1: The IoT architecture [32]

To utilize the benefits of the IoT, it is very crucial to address its security issues. Securing the communication between networks components is still open research area. The IoT will lead to the increase of the dependency on computer technology for business, critical infrastructures, communications, and various IoT objects. This makes IoT applications are subject to major attacks, which could cripple the economic infrastructure [4]. Therefore, there is a strong need for establishing a scalable and sustainable cyber ecosystem within the IoT that actively detects and mitigates threats while being reliable, robust, and affordable. To achieve this ecosystem, there are a number of efforts have been done.

Jincy, and Sudharsan [5] described a mechanism that will help IoT designers to determine the suitability of the best security mechanism for each entity involved in the IoT system. The main advantage of this mechanism is that it is an opening a door for building a complete E2E security framework with several degrees of security protection interfaces.

De Rubertiset al. [6] have presented a performance evaluation of two well-known security protocols designed basically for wireless sensor networks (WSNs), the IPsec [7] and the Datagram Transport Layer Security (DTLS) [8] protocols, to investigate their applicability for a number of IoT devices. The result of the evaluations brought a conclusion that the use of both protocols in their typical structure may result in bad effects on the E2E security mechanism required for the IoT devices.

The BlinkToSCoAP security framework [33] is an integration of three security protocols (DTLS, Constrained Application Protocol (CoAP), and the IPv6 over Low power Wireless Personal Area Networks Protocol (6LoWPAN protocol)) over TinyOS. A number of modifications have been applied for these combined protocols in order to enhance the overall performance such as: the maximum queue dimension of the IPv6 packets and the number of IPv6 addresses which have been reduced. The performance evaluations of the framework show the feasibility of the framework in terms of memory usage, energy consumption, transmission latency, and packet overhead.

In order to not waste the resource of the wireless sensor networks, Vucinic et al. [34] have introduced the concept of offloading the burden of authentication from constrained servers placing it on more powerful third parties devices (physically secured nodes in the network and/or hosts in the Cloud). The role of such devices is to authenticate individual consumers and share with them appropriate access secrets and access tokens. In other words, they proposed a system called object-based security architecture (OSCAR) which provides efficient E2E without affecting the radio duty-cycling operation of the constrained objects. Additionally, it provides access control, decouples confidentiality and authenticity trust domains, and intrinsically supports multicast, asynchronous traffic and caching.

Yang et al. [32] have suggested a multi-layer security model consisting of three layers for the IoT: Perception layer, Network layer and Application layer, as illustrated in figure 4. Their detailed description follows in the text below:

- Perception Layer: It is located at the bottom and it is most important layer of the IoT architecture. The main functionalities of the layer are recognizing and collecting information from the physical world to implement management procedures. The temperature sensors, the sound sensors, the vibration sensors, and the pressure sensors are examples of the wireless mediums which operate through that layer. Due to the flow of information through the wireless medium, an attacker can easily gain access to that medium. Therefore, this layer may suffer from a number of potential security risks such as: the eavesdropping of the communication link [35] and data flow analysis [36].
- Network Layer: It is also called the Transport Layer or Transmission Layer since it provides a channel for information transmission between different platforms via a network. The network layer needs a certain ability to process and manage information to deal with huge amounts of information collected by the perception layer from real world applications. Due to its open characteristic, the IoT faces many identity authentication problems. Moreover, the increased amount of redundant data causes a network congestion problem. This may result in the denial of service (DOS) attacks to be mounted against this layer, so there is a need for ensuring the availability of the network. This could be achieved by some kind of filtration device to be inserted between the transmission and application layers.

• Application Layer: The main function of this layer is to process the received data in a smart way to make sure that such processed information can be used by the end user. There are many types of user applications dealing with IoT to make our lives more convenient and reduces our workload. Nonetheless, due to large amount of data including some private information is collected using these applications, the protection of such important data, known as privacy issues, is very crucial and still needs further researches to be resolved.

The main problem of the above solution, the proposed (IoT-A) is that, it has overlooked the security and privacy services, which are very important in the IoT environment.

Zhang et al. presented "Comparison and Analysis of GPGPU and Parallel Computing on Multi-Core CPU". They presented that RSA algorithm is very compute intensive and CPU is not suitable to perform the modular exponentiation part of it. However, GPU due to its high parallel processing power is more suitable to perform such operations. They implemented RSA algorithm on GPGPU and perform the comparative analysis between the results obtained from GPGPU and CPU. They used the method of threads and threads block for the parallel implementation of RSA on GPU. The computation part of the program is divided into threads that in turn composed the thread blocks. Their experiments results showed that the GPGPU version of RSA algorithm gives 45x speedup as compared to its CPU counterpart. [9]

Masumeh Damrudi and Norafida Ithnin, in [10] presented "Parallel RSA encryption based on tree architecture". They applied parallel processing on RSA using tree structure. They proposed that by parallelizing RSA the speedup and the performance of RSA could be improved.

Sonam Mahajan and Maninder Singh in [11] described that the GPU as a coprocessor of CPU can be used to implement massive parallelism. They designed parallel RSA algorithm for GPU using CUDA framework and tested for both small and large prime numbers. The proposed algorithm reduce the security threats due to the use of small prime numbers and to increase the speed of the algorithm.

Xin and Yang studied the mechanisms of some existing routing protocols such as AODV, DSR and OLSR, which is widely used in Ad Hoc networks. Then they exploited its performance in IoT circumstances to find an appropriate routing mechanism for the future IoT. The routing overhead, average end-to-end delay and throughput were also compared to find a suitable routing protocol for the IoT. Simulation result showed that, the DSR protocol performs better in terms of routing overhead than other considered routing protocols and the AODV protocol can have better performance in terms of throughput [12].

Agrawal et al. proposed Secure Ad Hoc On-Demand Distance Vector (SAODV) Routing protocol, which is a modification of AODV protocol [13]. It is based on the proposition that each node possesses certified public keys of all network nodes. SAODV providing security features like integrity, non-repudiation and authentication. It is a challenge in ad hoc network for each node to know the others public keys [14].

The proposed approach in this paper focuses on embedding the RSA encryption in a new single layer between the internet and the network access layers. The idea is to text the performance of the AODV protocol as it is our testbed for further enhancements as step forward towards collecting security mechanism in a single layer.

III. Preliminaries

This section gives overviews of the techniques and protocols used in the designed and implantation of the proposed solutions.

A. MANETs

(MANETs) consist of self-configuration mobile devices that communicate wirelessly [15]. The network doesn't have a fixed structure (topology) that each device has the ability to move freely and frequently communicate with other devices [16]. As for the data routing, each of MANET devices is considered either a host or a router if it received unrelated data. Although, the MANET used the UTP and TCP transport protocols, a number of protocols were proposed based on the modification of this legacy TCP transport protocols and to standardizing these networks 'configurations [17]; Such as Ad Hoc On-Demand Distance Vector (AODV) [18], Optimized Link State Routing (OLSR) [19], and Dynamic Source Routing (DSR) [20]. A number of networks had inherited the MANET procedures, such as: the Vehicular Ad-hoc Networks (VANETs); which is a communication infrastructure for the intelligent transportation systems [21]. The Internet Based Mobile Ad-hoc Networks (iMANET) that at least one of the network's devices is connected to the internet [22]. Although this advances in MANET a number of interesting and challenging issues are still open research areas in the MANET field [23] such as the dynamicity behavior of the devices, the device discovery and update facilities, the constrained resources especially the power sources, and the security threats.

B. AODV Routing Protocol

Ad hoc On-Demand Distance Vector (AODV) Routing Protocol is an Ad-hoc On-Demand Routing Protocol and categorized as the reactive routing protocol for MANET networks. The routing table is maintained by each node which provides next hop so that a packet can reach the destination. All the mobile nodes can communicate with their neighboring nodes to forward the packets to the nodes which are not directly connected to them. AODV consist of the following basic messages-: HELLO message, Route Request (RREQ), Route Reply (RREP) and Route Error (RERR) The message HELLO is sent to the other node to check whether the neighboring node is in communicating range or not. The Route Request (RREQ) is broadcast from source node to the neighboring node. The response to RREQ message is given by sending Route Reply (RREP) message to the source node if the path to the destination node is available otherwise the current node will rebroadcast it to the further node. When the RREP message is send to the source node the path is established. This information is updated in the routing table as this information will help in constructing the reverse path for the RREP message. When there is link failure or breaks occur then RRER message is propagated. As shown in Figure 1, source node S broadcasts RREQ to its neighbour A and C which further broadcasts it to B and D. When RREQ reaches destination D, RREP is unicasted back to source node [24], [25].

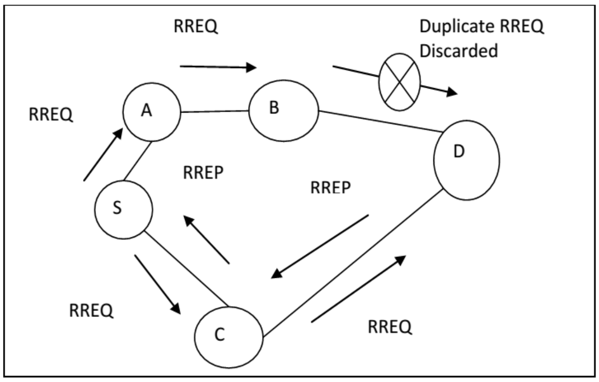

Figure 1. Illustrate of the AODV route discovery process

The following flow chart in Figure 2 summarizes the action of an AODV messages except hello message [26]

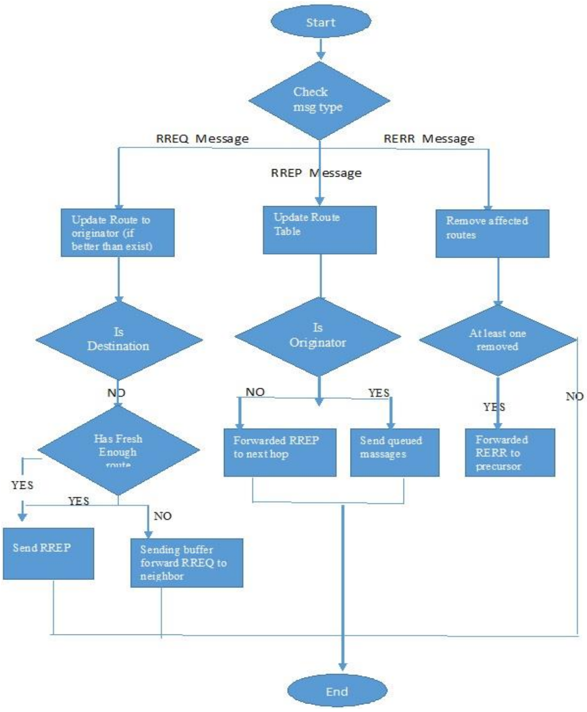

Figure 2. Illustrate the AODV Messages

C. RSA Algorithm

There are many public key based cryptographic algorithms are available. Some of the popular algorithms are RSA, Digital Signature and Diffie-Hellman Key Exchange Algorithms. The RSA algorithm [27] was invented by Ronald Rivest, Adi Shamir and Leonard Adleman in 1978 and it is named after their names. It is one of the most popular Public Key Cryptography based algorithm mainly used for digital signatures, encryption/decryption. It is based on the mathematical scheme of factorization of very large integers which is a compute-intensive process and takes very long time and more power consumption to perform [28]. The RSA consist of three algorithms which are Key Generation Algorithm, Encryption Algorithm, and Decryption Algorithm.

1.2 Key Generation Algorithm

It is a step-wise process, which is as follows:

1. Choose two very large random prime integers p and q, with bit size at least 512 or more

2. Calculate modulus m as, m = p*q

4. Calculate φ(n) as φ (n) = (p-1) (q-1)

5. Choose an integer e, 1 < e < φ (n) such that: GCD (e, φ (n)) = 1, Where GCD is greatest common denominator

6. Calculate d, 1 < d < φ (n) such that: ed ≡ 1 (mod φ (n))

Here “e” is used as Encryption exponent and “d” is used as Decryption exponent therefore “e” and “n” are published as public key and “d” and “n” are secured as the private key.

1.3 RSA Encryption	**1.4 RSA Encryption**
The RSA encryption can b applied on variable size of message block. Therefore data can be divided into th blocks of data using any padding scheme such as PCKS#1 and following procedure is applied to it C = M^e % m, where M is the message block and C is sent as the cipher text to the other 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. Illustrate of the of encryption and decryption pseudo code

IV. The Proposed Security Layer

As it was previously explained, the proposed idea is to create an independent single layer that will meet most of the required security mechanisms, which have been distributed over other layers in a network protocol. As for the current statute we focus on the embedding the RSA that previously expressed into that proposed layer. That proposed layer intended to be placed between the Internet layer and Network Access layer as a filtration layer before the processes of sending and receiving data. The proposed layer is to receive the data after the Network Access layer ensure that incoming data has been received successfully. Figure 3 illustrates a scenario of end-to-end communications through a scenario with AODV algorithm including the proposed security layer. The layers were established programmatically through the use of Object Oriented Programming within the NS2 through the following steps and as illustrated in the flow chart in Figure 4.

1- The new security layer send/receives the data packet between the Internet layer and Network access layer.

2- Apply the RSA encryption and decryption over the send/receive data.

3- The encrypted data is to be transferred to the Network Access layer.

4- The decryption data is to be transferred to the internet layer.

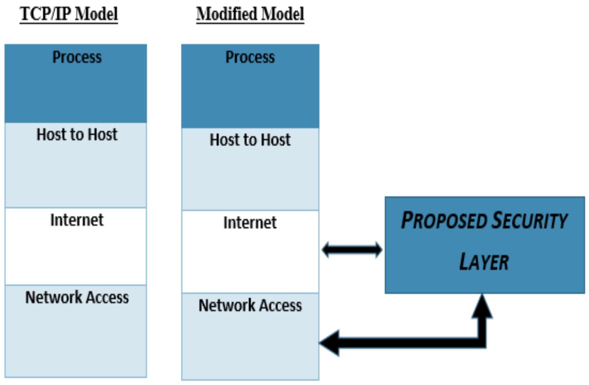

Figure 3. Illustrate of the Proposed Layer (Modified Model)

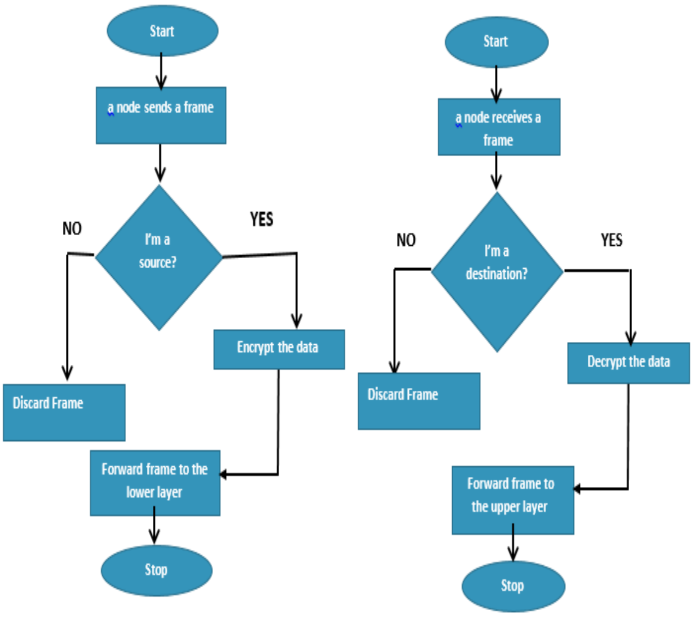

Figure 4. Illustrate of the Security Function in new security layer Flow chart

V. Simulation Results and Analysis

In this section, the performance of the proposed solution will be evaluated using the ns-2 simulator. The ns-2 is an event driven simulation tool that has proved to be useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using the ns-2. In general, the ns-2 provides users with a way of specifying such network protocols and simulating their corresponding behaviours. On the other hand, as reported in [29], the ns-2 doesn't implement any security features, therefore in this paper, the required security function was first implemented and added to the ns-2 libraries and then used to test the features of the proposed security layer.

V.1 Exponents Setup

All the simulation experiments were conducted under the network simulator (ns-2) (version allinone-2.35) which installed in Ubuntu (14.04 LTS) in core i7 and 8GB RAM machine. IEEE 802.11 was used as the MAC layer protocol. NS-allinone-2.35 simulator was used. To obtain the results, the tcl language has been used to write tcl script (Scenario) and generating corresponding nam and trace files.

Different scenarios were considered to evaluate the security layer. The first scenarios were to test the layer under various network size. In this case, networks with 5 nodes, 10 nodes, 15, 20, and 25 nodes were tested. Each node in each experiment starts its move at random speed from its initial position to a random target position within the simulation area which was 1000 m x 1000 m. When a node reaches the target position, it waits for a pause time period, and then selects another random location and moves toward it. The simulation time was 25 seconds. Table 1 illustrates the simulation parameters of the conducted experiments.

PARAMETER	VALUE
Channel type	Wireless channel
Number of nodes	5, 10, 15, 20, 25
Traffic type	CBR/UDP
Mobility	RWP
Area of simulation	1000 m X 1000 m
Routing Protocol	AODV
Time of simulation	25 sec

Table 2. Parameter Used In Simulation Scenario

V.2 Performance Metrics and Simulation Results

To evaluate the performance of the proposed layer with the AODV routing protocol, the following measures have been considered: packet dropped, packet delivery ratio (PDR), normalized routing load (NRL), throughput and end-to-end delay by varying number of nodes. **The results of these measures will be discussed below.**

- **Dropped Packets:** Mobility-related packet dropped may occur at both the Internet layer and the Network access layer. In this work, packet dropped concentrates for the Internet layer. **The dropped packets is defined as follows:**

Dropped Packets = Data Packet Sent – Data Packet Received

Figure 5 illustrates the results of the dropped packets measure in case of different network size (5, 10, 15, 20, and 25). From this figure, it can be seen that there is no different in the value of packet dropped when applying security in both the new proposed layer and without this layer. Therefore, it can be said that that the packet drop in TCP/IP model are equal to packet drops in new security layer model this mean that the new security layer dos not affect the number of drop of packets. It can be also said, that the proposed layer can support different size of network without affecting the delivery of the packets.

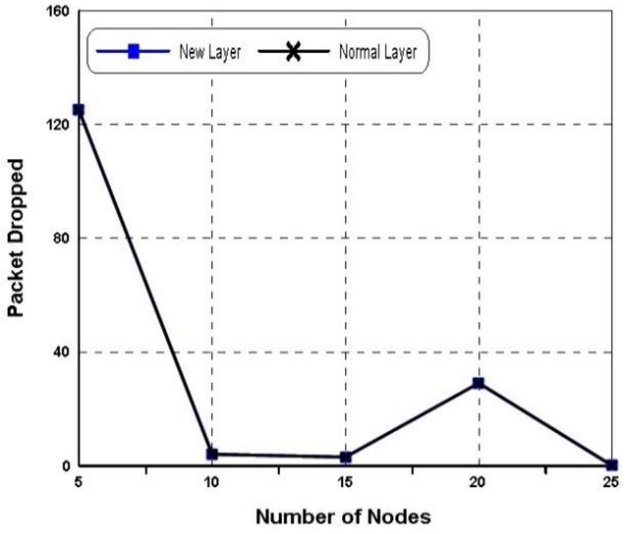

Figure 5. Illustrate of the packet drop vs node number

- **Packet delivery ratio (PDR %):** it is the ratio between a number of packets received by destination and the number of packet already originated and is defined as:

Packet delivery ratio PDR = (Data Packet Received / Data Packet Sent) * 100

The simulation results of PDR in case of applying the new layer and without applying are summarized in Figure 6. From these results, it can be noticed that, (1) the PDR in case of the new security layer is better than when using the security in the normal scenario, (2) a network with the new layer could have higher throughput than a network without the new layer, and (3) in terms of scaling the network size, the PDR is the same in case of applying the new layer or without it.

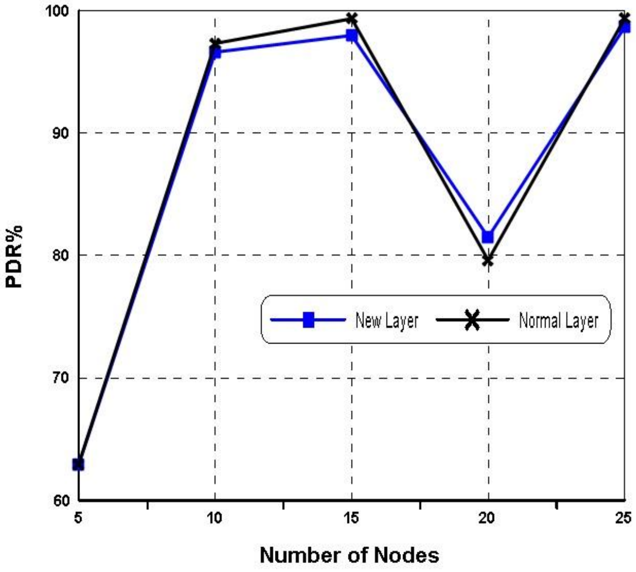

Figure 6. Illustrate of the PDR% vs node number

- **Normalized Routing Load (NRL): It is defined as** the number of routing packets transmitted per data packet delivered at the destination. The NRL can be defined as the ration of all routing control packets sent by all nodes by the number of received packets at the destination nodes. In other words, Normalized **Routing Load (NRL) =** (Total Routing Packet Sent / Total Routing Packet Received)

The results of the NRL are given in Figure 7. These results demonstrate that the NRL in the network when using the security in a new security layer almost closed to the when using the normal scenario. This means that a network with the new layer would have the same routing functions like a network with the traditional layering scheme. Also, when scaling the network size, the routing functions are is still the same in case of applying the new layer or without it

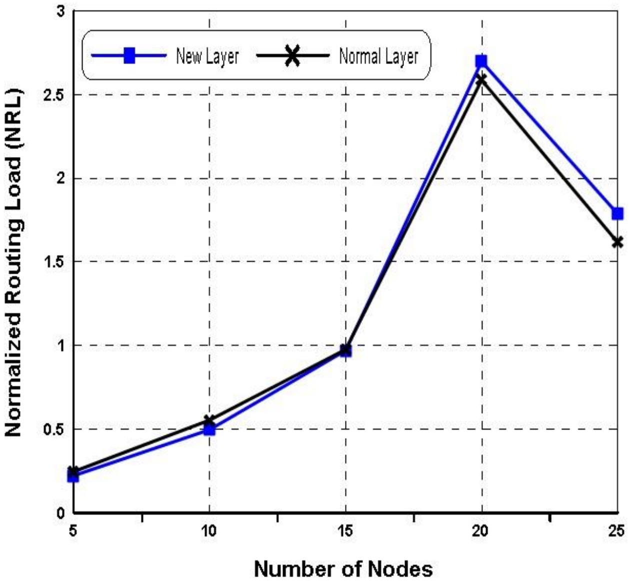

Figure 7. Illustrate of the normalized Routing Load in New security layer

- **Throughput:** It is the amount of data per time unit that is delivered from one node to another via a communication link [30] and it can be formally defined as:

Throughput = (Number of data packets Received * Packet size*8) / Simulation Time.

Figure 8 shows the results of the throughput measure evaluated in case of applying the new layer and without applying it. It can be noticed that the average throughput in both case is almost the same. This means that the new security layer could functions properly under different size of networks without affecting their throughput. This also indicates that the routing protocol could reach the convergence state as speed as using the traditional layering scheme.

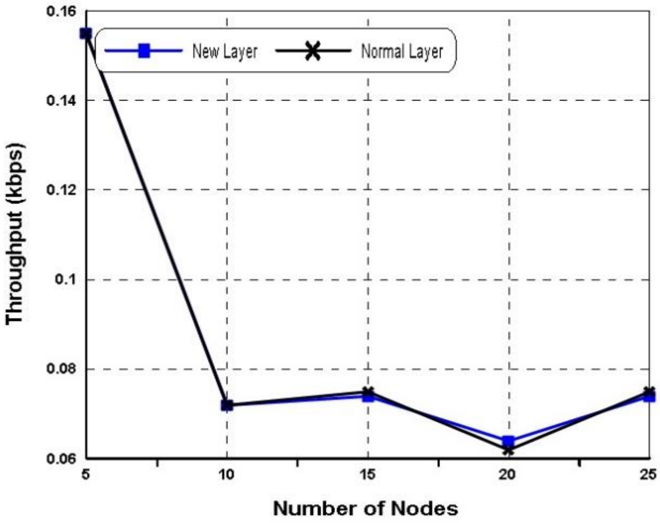

Figure 8. Illustrate of the Average Throughput in New security layer

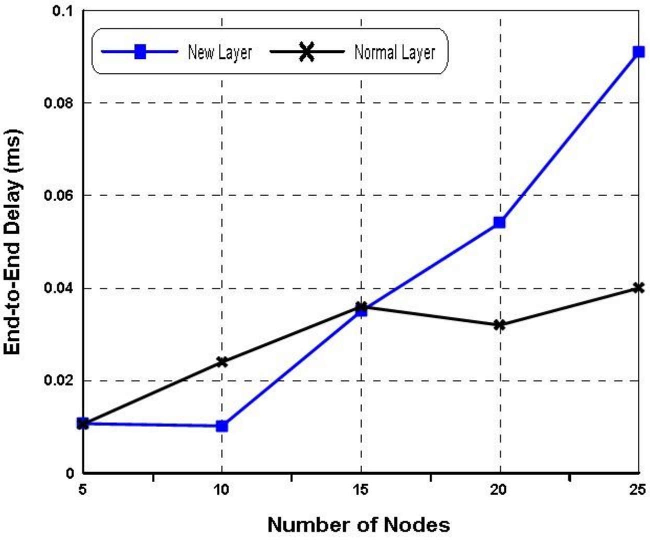

Figure 9. Illustrate of the End-to-End Delay in New security layer

- **Average End-to-End Delay:** An average end to end delay includes all possible delays caused by the buffering process during the route discovery latency, queuing at the interface queue, retransmission delays at the network access, and propagation and transfer times of data packets.

The simulation results in case of applying the new layer and without applying it is given in Figure 9. From this figure, it can be seen that the average end-to-end delay of the network when applying the security in a new layer is lower than that of the normal layer for small size network. So, it can be said that in the small size network, the new layer could show better performance (the lower value of end to end delay means the better performance of the protocol). On the other hand, with the high density network (high number of nodes), the average end-to-end delay, when using the new layer, is increased than when using the normal layer. This is because the routing protocol firstly applies to the security functions at the new security layer and then the new security layer sent the secured data to the network interface layer this increase the time delay [31]. Thus, in the large size network, the delay in case of the new layer could be justified as to support the security threats that could be mounted from any node (in case 25 node, there would be 25 threat arise). Thus, the security functions, applied at each node before sending the data to the network layer, could cause more delay when applying the new layer.

From the above discussion, it can be said that the network under different size (5, 10, 15, 20, and 25 node size) using the proposed security layer is almost functioning (in terms of the performance measurements above) like the case of the traditional layer. However, in case of collecting all security functions of the network layers in one layer, the other network layers could be only performing their specified functions without looking after to any security problems, thus supporting centralized troubleshooting processes which is much required in the ear of networks (MANET, WSN, IoT, … etc.)

Conclusion

In this paper, we have proposed a modification in the TCP/IP model by adding a new security layer to it between the internet layer and network access layer. This layer, instead of that included in both internet and transport layers, is concerned with handling the security mechanisms needed by IoT environments. The proposed layer was implemented by the NS-2 simulator and evaluated using different measures, packet dropped, packet delivery ratio (PDR), normalized routing load (NRL), throughput and end-to-end delay. The simulation results of these measures indicated that, the new security layer performed similar and in some cases better than the simple TCP/IP model. These results could be considered a promising direction toward a centralized security layer which included all security functions in the TCP/IP model. This would contribute to make the troubleshooting much easier. In Future work, we can extend this work to study the impact of node movement speed, other protocols and more than one malicious node in MANETs.

References

[1] Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future Generation Computer Systems 29.7 (2013): 1645-1660.

[2] Bassi, Alessandro, Martin Bauer, Martin Fiedler, Thorsten Kramp, Rob Van Kranenburg, Sebastian Lange,

and Stefan Meissner. Enabling things to talk. Springer, 2013.

[3] Alhamedi, Adel H., et al. "Internet of things communication reference model." Computational Aspects of Social Networks (CASoN), 2014 6th International Conference on. IEEE, 2014.

[4] Fonash, Peter, and Phyllis Schneck. "Cybersecurity: From Months to Milliseconds." Computer 1 (2015): 42-50

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

[6] [De Rubertis, Antonio, Luca Mainetti, Vincenzo Mighali, Luigi Patrono, IlariaSergi, M. L. Stefanizzi, and Stefano Pascali. "Performance evaluation of end-to-end security protocols in an Internet of Things." In Software, Telecommunications and Computer Networks (SoftCOM), 2013 21st International Conference on, pp. 1-6. IEEE, 2013]

[7] S. Kent and K. Seo: “Security Architecture for the Internet Protocol”. RFC 4301, December 2005.

[8] Rescorla, Eric, and NagendraModadugu. "Datagram transport layer security version 1.2." (2012).

[9] Hang, Hong, Da-fang Zhang, and Xia-an Bi. "Comparison and Analysis of GPGPU and Parallel Computing on Multi-Core CPU. (2012)"

[10] Damrudi, Masumeh, and Norafida Ithnin. "Parallel RSA encryption based on tree architecture." Journal of the Chinese Institute of Engineers 36, no. 5 (2013): 658-666.

[11] Sonam Mahajan, and Maninder Singh. "Analysis of RSA algorithm using GPU programming." arXiv Preprint arXiv: 1407.1465 (2014).

[12] Routing Protocols Analysis for Internet of Things, http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=7120644&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D7120644

[13] Agrawal, Sudhir, Sanjeev Jain, and Sanjeev Sharma. "A survey of routing attacks and security measures in mobile ad-hoc networks." arXiv preprint arXiv:1105.5623 (2011).

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

[15] Shenbagapriya, R., and Kumar 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).

[16] Veni, R. Marutha, and R. Latha. "Mobile Ad hoc Network." International Journal of Science and Research (IJSR) 2.4 (2013).

[17] Conti, Marco, and Stefano Giordano. "Mobile ad hoc networking: milestones, challenges, and new research directions." Communications Magazine, IEEE52, no. 1 (2014): 85-96.

[18] Perkins, Charles, Elizabeth Belding-Royer, and Samir Das. Ad hoc on-demand distance vector (AODV) routing. No. RFC 3561. 2003.

[19] Clausen, Thomas, and Philippe Jacquet. Optimized link state routing protocol (OLSR). No. RFC 3626. 2003.

[20] Johnson, David, Y. Hu, and D. Maltz. The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4. No. RFC 4728. 2007.

[21] Kuhlmorgen, Sebastian, Ignacio Llatser, Andreas Festag, and Gerhard Fettweis. "Performance Evaluation of ETSI GeoNetworking for Vehicular Ad hoc Networks." In Vehicular Technology Conference (VTC Spring), 2015 IEEE 81st, pp. 1-6. IEEE, 2015.

[22] Sharma, Samrudhi, Manali Trivedi, and Lakshmi Kurup. "Using Ontologies to Model Attacks in an Internet based Mobile Ad-hoc Network (iMANET)."International Journal of Computer Applications 110, no. 2 (2015).

[23] Bang, Ankur O., and Prabhakar L. Ramteke. "MANET: History, Challenges and Applications." International Journal of Application or Innovation in Engineering & Management (IJAIEM) 2, no. 9 (2013): 249-251.

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

[25] Arora, Tanvi, Amanpreet Kaur, and Mandeep Singh. "Review of Various Routing Protocols and Routing Models for MANETs." (2015).

[26] http://jist.ece.cornell.edu/docs/040421-swans-aodv.pdf

[27] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and publish key Cryptosystems. Communications of the ACM, 21(2):120{126, 1978.

[28] Saxena, Sapna, and Bhanu Kapoor. "State of the art parallel approaches for RSA public key based cryptosystem." arXiv preprint arXiv: 1503.03593(2015).

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

[30] A. Valarmathi and R. Chandrasekaran, “Congestion aware and adaptive dynamic source routing algorithm with load-balancing in MANETS," International Journal of Computer Applications, vol. 8, no. 5, pp. 1{4, 2010}

[31] A. K. Gupta, H. Sadawarti, and A. K. Verma, “Performance analysis of aodv, dsr & tora routing protocols," IACSIT international journal of Engineering and Technology, vol. 2, no. 2, pp. 226-231, 2010.

[32] YANG, Xue, et al. A Multi-layer Security Model for Internet of Things. In: Internet of Things. Springer Berlin Heidelberg, 2012. p. 388-393

[33] Peretti, Giulio, VishwasLakkundi, and Michele Zorzi. "BlinkToSCoAP: An End-to-End Security Framework for the Internet of Things." (2015(.

[34] Vučinić, Mališa, Bernard Tourancheau, Franck Rousseau, Andrzej Duda, Laurent Damon, and Roberto Guizzetti. "OSCAR: Object security architecture for the Internet of Things." Ad Hoc Networks (2014)

[35] YOON, Seokung; PARK, Haeryong; YOO, Hyeong Seon. Security Issues on Smarthome in IoT Environment. In: Computer Science and its Applications. Springer Berlin Heidelberg, 2015. p. 691-696

[36] Gosain, Anjana; Sharma, Ganga. Static Analysis: A Survey of Techniques and Tools. In: Intelligent Computing and Applications. Springer India, 2015. p. 581-591.

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

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

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

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