International Journal of Control and Automation
Vol. 11, No. 2 (2018), pp.45-54
http//dx.doi.org/10.14257/ijca.2018.11.2.05

Encrusted Security for Internet of Things Using MAC-OMURA

Namkyun Baik[1], Santosh Kumar Sharma[2] and Bonomali Khuntia[3]

[1]Korea Advanced Agency of Convergence Technology, IT Venture Tower, 135 Jungdae-ro, Songpa-gu, Seoul, South Korea
[2]Department of Master of Computer Applications, Vignan's Institute of Information Technology (A), Visakhapatnam, AP, India
[3]Department of Computer Science, Berhampur University, Berhampur, Odisha, India
[1]white-knight@naver.com, [2]sharma.santosh83@gmail.com, [3]Bonomalikhuntia@gmail.com

Abstract

The day is not far when the entire universe is moving to adopt smart technology in their regular lifestyle. Every activity and smart objects will be monitored through mobiles and sensor devices from a remote location. Such as smart home appliance, smart home, bright kitchen, smart health, smart farming, and smart harvesting. All this will become possible with internet. But due the sensitivity of the smart object, it can creates the threats to objects, if the control moves to malicious hand, he/she may use in different way, so by observing its sensitivity we have to think about security of the object either for the device itself or providing the security for our data using cryptography technique. Cryptography can be done in two ways with symmetric key cryptography 'or' asymmetric key cryptography, the strength of the security algorithm is the key and one key become vulnerable then it become difficult to secure the system because nothing is advisable other than breaking the key to fire brute force attack, a cryptanalyst needs a small amount of cipher text on the corresponding plain text. Brute force attack is known as Plain text attack. For block cipher the cryptanalyst would need a block of cipher text and corresponding plain text, generally 64- bit. In our proposed system, work is contributed towards private key cryptography associated with digital signature to construct strong security and in send phase this system will become stronger once we apply the MAC, resulting cryptography equation will be represent in the face of $C.T = E_3 [E_2[E_1(P,K)+DS]+MAC]$.

Keywords: *IOT, key Exchange Cryptography, MAC, Digital Signature, Nessi2*

1. Introduction

Now the Internet has become omnipresent and accessible to the entire urban area populations and reachable to the every corner of the world. Since the origin of IOT technology it looks so easy to connect the electrical devices and home appliances to internet and can be control from the remote location as per our requirement. IoT is defined as a mesh structure of integrated objects which is equipped with sensors, actuators, transceiver and processors communicate with each other for serving a specific purpose. Internet of Things is the new technology which made possible for heterogeneous devices on the common platform where all the devices and appliances are connected with each other virtually and sometime physically. IOT collectively achieve specific task that require a high degree of intelligence with the help of smart system and web access. Just

Received (October 26, 2017), Review Result (January 4, 2018), Accepted (January 17, 2018)

ISSN: 2005-4297 IJCA

couple of years back in 2013 the Global Standards projected Internet of Things (IoTs-GSI) defined the IoTs as "the infrastructure of the information society. IOT is a collective approach where devices are built-up with microchips, Circuit and combination of different register and conductors to perform with sensing devices and actuator to perform smartly. IoT become a symbolic smart object of the class cyber-physical systems, which produces the technology in all the major area such as smart grids, smart city, smart garbage management, smart homes, smart medical, smart harvesting *e*. Each and every participated node will be easy to identify through its embedded computing system along with maintain location and resource in existing Internet infrastructure. Experts estimating in coming couple of years IoTs technology will reach to connect and start communication between billion of objects means smart devices –IOT.

2. Related Work

The study of several research papers shows various network related issue for network connectivity and secure data transmission between wireless sensors devices (IOT). Our classification presenting the technologies in the IoT world and we have tried to cover all the subareas and current technological to introduce the new concept of IOT-Security. Kien A. Hua[1] has revealed that the number of connected devices in Internet of Things (IoT) will exceed 28 billion by the year 2020. This poses a new set of challenges and opportunities for collaborative technologies.

Klara Nahrstedt and Jong [2,3] has explored the different application and scope of IOT and the impact of technology on human and how IoT is dominating the daily lives of human being by provide smart devices. Internet of Things at scale is becoming reality with the soul of Internet connectivity among all the things [4, 5, 6]. Saoreen and Mika [7, 8, 9] has discussed the communication between the heterogeneous machine and how difficult to set up the communication between different machine is.

IoT technology has raised several question related to security of the data and how present security standards are fulfilling the requirement for IOT security. Secondary issue associated with IoT is Qi Wang [11] has taken the IOTs devices in WSN and shown the bad usage of the energy consumption which leads to reduces the operation time of sensors and consequently the network lifetime. This is a great implication to make out the network related problem in the rear of IoT development. By observing the wireless sensor network and their analytical relation with Soft-computing is exceedingly appreciable which is proving their compatibility and adaptability to prevail the multifaceted challenges in WSN [14, 17, 18].

Improving Node Security in MANET Clusters and providing comparison of two Fuzzy-based Systems for Enhancing Windows Firewall Security Using Fuzzy Reasoning. Evaluation model of Social security system based on Fuzzy comprehensive evaluation method [20, 21]. Concerning the Security requirements analysis and providing secure mechanism for Big Data in large scale of Internet of Things is a challengeable job.

The Massey-Omura cryptography approach has presented as a private key encryption technique. And it is dedicatedly constructed for the scientific approach to fix the organization. Omura work on the precept of the prime modulus with exponential system. Where the message is generated with secret key and transmits to the receiver side by using prime modulo.

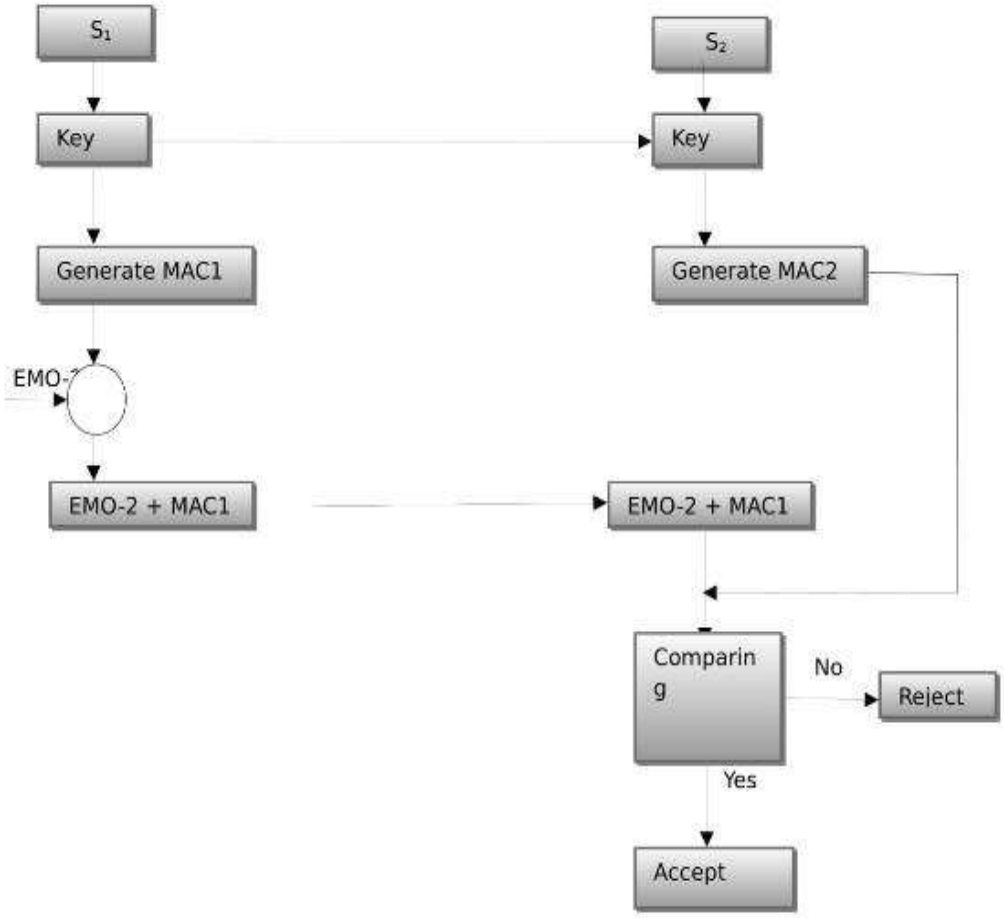

Figure 1. Block Diagram for Generating MAC Code

Algorithm for MAC

1. Let 'X' be a message.
2. 'K' be a Key.
3. $S_1 \leftrightarrow MAC_k(X)=D$
4. Append D $\rightarrow$ X=(X,D)
5. $S_2 \leftrightarrow MAC_k(X)=D^{|}$
6. Compare D and $D^{|}$
7. If($D= D^{|}$)

{
Accept;
}
Else
{
Reject;
}

EMO-1

In this version EMO-1 has introduced with prime modulus concept with composite mechanism to generate the value by performing the product operation for two different prime values. In this way the system is catered with a level of protection similar to that of an RSA public key scheme.

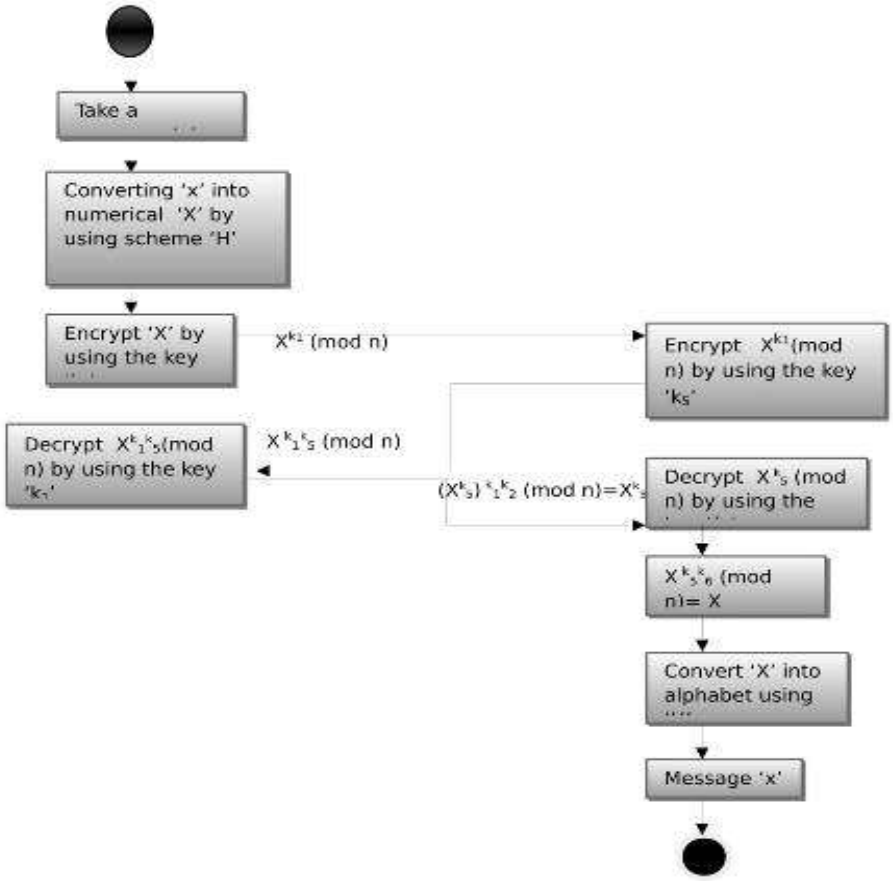

Figure 2. EMO-2 Operation Structure and its Activity

Description of Figure-2

Let 'x' be a message. 'x' is converted into numerical by using the scheme 'H'.S_1 has the keys $w_i=k_1$ $x_i=k_2$ $y_i=k_3$ $z_i=k_4$. S_2 has the keys $w_j=k_5$ $x_j=k_6$ $y_j=k_7$ $z_j=k_8$.

EMO-2 and Digital signature Significances

A complex revised version of new enhanced EMO-2 is created with by adding the digital signature to prime product , Here the use of digital signature permits the receiver of a encrypted message with EMO-2 protocol to provide authentication to the sender identity with more security for the secure communication. The development of the EMO-2 can be further implemented through adding next level of encoding during transmission making tougher task for interceptor to crack the secret code or message, who tries to get access the secret message without authorization. In addition to this integrated feature of MAC and digital signature, makes the receiver side to compare and verify the identity of the sender at two levels, and finally construction of hybrid complex security structure.

Digital signature is used to proof the identity to any document from any type of tampering during accessing and transferring. Digital Signatures are also applied to verify the identity of the sender and receiver objects. The message or document that is transported over a public network is signed or verified using a specific series of numbers which are also known to the transmitter or receiver. Digital Signatures also introduce the concept of non-repudiation which means that verifies neither the sender nor the receiver can delay shipping or picking up a special document or message. Digital Signature can also incorporate automatically date and time stamps, which possess a vital function in business transactions while improving the speed of accuracy of such proceedings.

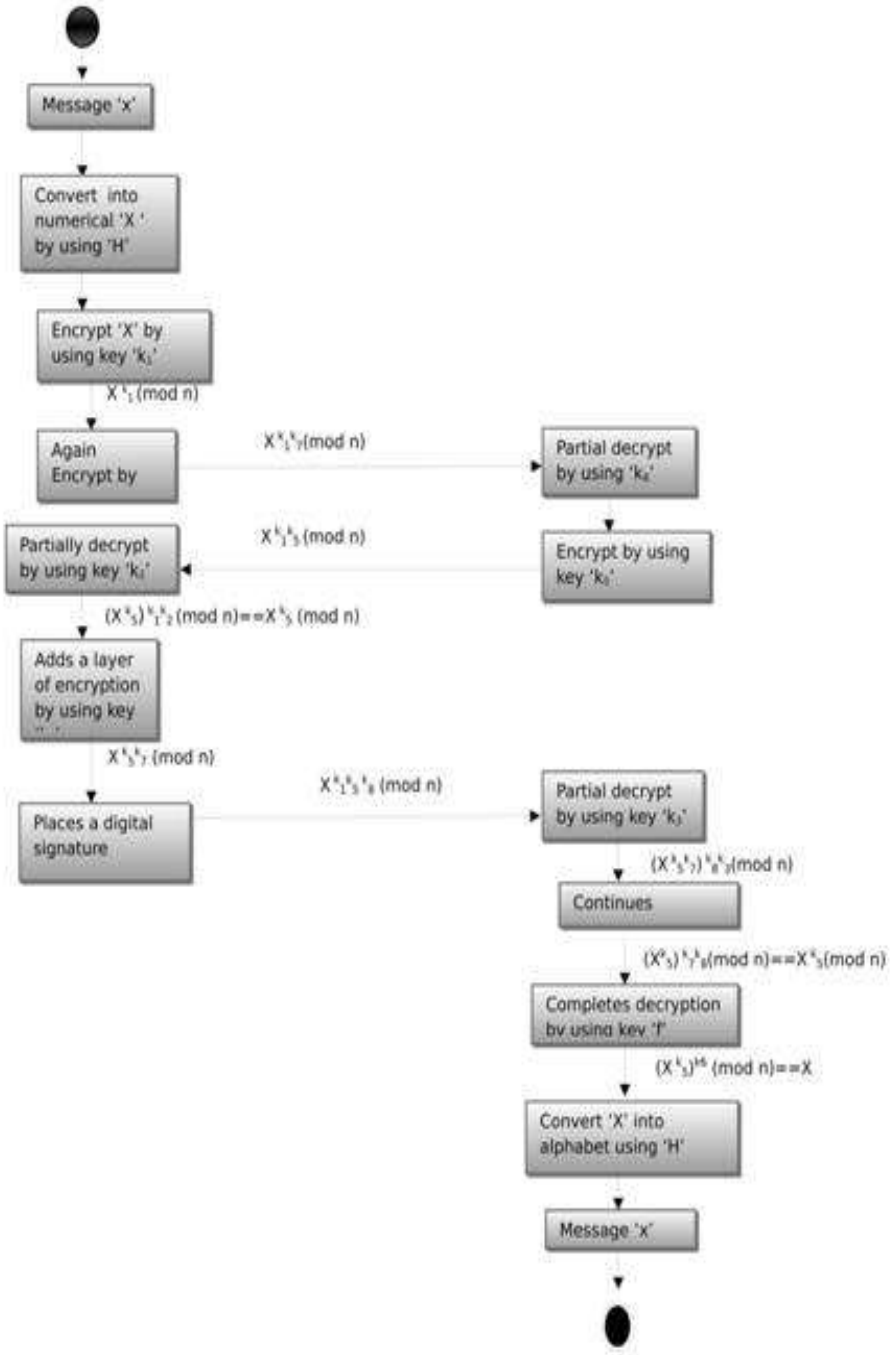

Figure 3. EMO-2 and Digital Signature and Collective Implementation

Description of EMO-2

Let 'x' be a message. 'x' is converted into numerical by using the scheme 'H'.

S_1 has the keys $w_i=k_1$ $x_i=k_2$ $y_i=k_3$ $z_i=k_4$.

S_2 has the keys $w_j=k_5$ $x_j=k_6$ $y_j=k_7$ $z_j=k_8$. In this digital signature is added.

3. Proposed Work

Emo-2 + MAC Significances

From the above EMO-2 technique we have seen that how the digital signature is proving their liability to improve the security but due to minor flaws in digital signature related to economical issue its usage becoming complex to use, but then also by bypassing

all these issues we can make more stronger system by adding the Message authentication code to EMO-2. Message authentication Code is primarily known as tag value which is additional secret alphanumerical or special values associated with the cipher text for additional authentication. It can be elaborate to proof that message come from authentic user and without any alteration, which is verified by the receiver side. MAC is known for maintaining the integrity of the communication parties as well as text message.

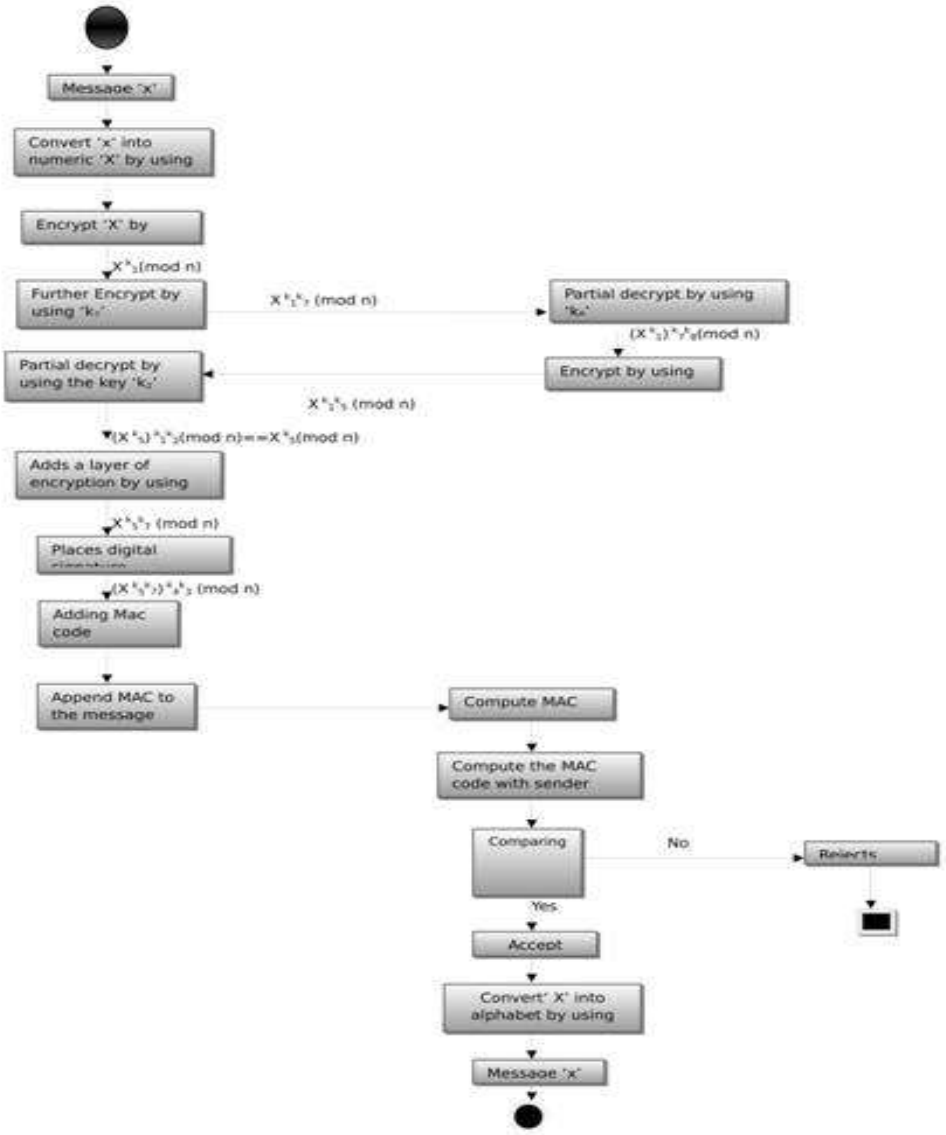

Figure 3. EMO-2+MAC-Collective Flow of with Message Authentication Code

Description of EMO-2 + MAC

Let 'x' be a message. 'x' is converted into numerical by using the scheme 'H'.

S_1 has the keys $w_i=k_1$ $x_i=k_2$ $y_i=k_3$ $z_i=k_4$.

S_2 has the keys $w_j=k_5$ $x_j=k_6$ $y_j=k_7$ $z_j=k_8$. In this a MAC Code is added to the digital signature.

Algorithm: EMO-2+MAC

Step1: Let be a message (msg) 'X'.

Step2: Convert message (msg) 'X' into Num(X) ←H
Step3: $S_1 \leftrightarrow P_0$=Ency + $K_0 \rightarrow C_1$
Step4: $C_1 \leftrightarrow$ P_1=Ency + $K_1 \rightarrow$C2
Step5: $S_1 \rightarrow S_2$ //S_1 sends C_2 , S_2
Step6: $S_2 \rightarrow$ P_1 // Decrypt C_2
Further, $P_1 \leftarrow K_0$ // Encrypt C_3
Step7: $S_2 \leftarrow S_1$ // Sends C_2
Further, Decrypt (C3, K)$\rightarrow P_0$
Step8: S_1 adds layer of Encry key.
Step9: Add P_0 + Digital Signature.
P_0 + Sign → msg →Encoded Text (P_2)
Step10: S_1, Add $P_2 \leftarrow MAC_k(X)$= D
Then, $S_1 \rightarrow S_2$
After, $S_2 \,||\, MAC_x(D) \rightarrow P_3$
If ($P_2 = P_3$)
{
Accept ();
}
Else
{
Reject ();
}
Repeat loop (with new value);

Communication Statement below Algorithm

1. Let 'x' be a message.
2. Convert 'x' into numerical 'X' by using the Scheme 'H'.
3. S_1 Computes encryption by using the key 'K_1'.
4. Further, compute encryption by using the key 'g'.
5. S_1 sends the encrypted message to the S_2.
6. S_2 computes partial decryption by using the key 'z'.
7. Computes encryption by using the key 'y'.
8. S_2 sends the message to the S_1.
9. S_1 computes partial decryption by using the key 'p'.
10. Add a layer of encryption by using 'g'.
11. Add a digital signature to the encrypted message by using 'h'.
12. Add a MAC Code to the digital signature message.
13. S_1 compute $MAC_k(X)$ =D by using the key 'K'.
14. Append D to 'X' and sends to S_2.
15. S_2 computes $MAC_k(X)$ =$D^{|}$ by using the key 'K'.
16. Compare D and $D^{|}$
17. If(D= $D^{|}$)
{
Accept;
}
Else
{
Reject;
}

4. Experimental Setup

For experimental purpose we used to take the environment of Nessi2 tool which is network security tool and simulator for the purpose of security architecture and Simulation.

Network Simulator

NeSSi2 is a security tool which incorporates a variety of features which differentiate it from other simulator such as NS2, Arpanet, Quelnet, Netsim, NeSSi2 is capable to perform based on traffic analysis, automatic attacks triggering support towards detection algorithms for malicious inputs. This simulator is very useful for security research simulation and assessment purpose. NeSSi2 simulator has been tested on different type of attacks analysis such as: Intrusion detection algorithms Network security analysis and construction of complex Security frameworks. NeSSi2 is constructed with the help of Java agent framework (JIAC) consequentially worth full in a distributed and extensible architecture.

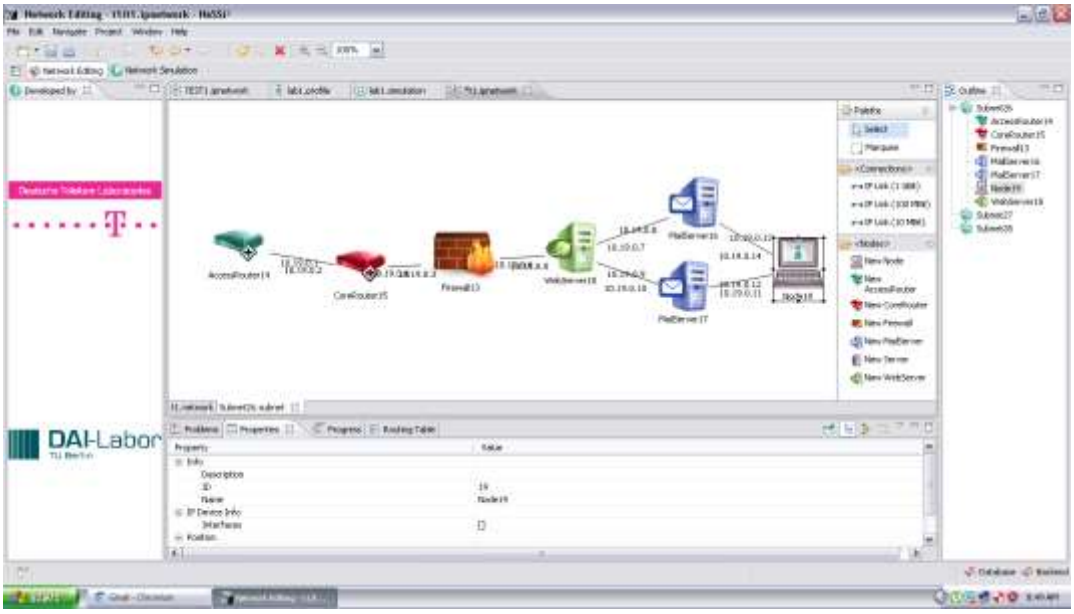

Figure 4. Network Simulator

5. Conclusion and Future Work

Finally here we are able to draw the final resulting cryptography equation will be represent in the face of $C.T = E_3 [E_2 [E_1(P,K)+DS]+MAC]$. From this equation it can be narrated that only one type of security mechanism is not enough to provide the security, so we have to move towards that integrated approach such as public cryptography, Digital signature and Message authentication for peer to peer security. Regarding this we taken the Massey Omura approach with MAC. So by Integral mechanism of MAC and Massy approach proving the strong complexity in front of amateur which makes the system tamperproof. Our future work will move ahead of deep analysis for the smart devices.

References

[1] H. Huang, Member, "Private and Secured Medical Data Transmission and Analysis for Wireless Sensing HealthCare System", Citation information: Transactions on Industrial Informatics, **(2017).**

[2] S. Challa, M. Wazid, A. K. Das and N. Kumar (Member, IEEE), "Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications", IEEE Access, **(2017)**.

[3] M. Sain, Y. J. Kang and H. J. Lee, "Survey on Security in Internet of things: state of the art and challenges", **(2017)**.
[4] S. Huh*, S. Cho* and S. Kim*, "Managing IoT Devices using Block chain Platform", **(2017)**.
[5] B. F. Zahra and B. Fatima Zahra, "Risk Analysis in Internet of Things using EBIOS", **(2017)**.
[6] 'A. Majeed , "Internet of Things (IoT): A Verification Framework", **(2017)**.
[7] T. Abels, R. Khanna and K. Midkiff, "Future Proof IoT: Composable Semantics, Security, QoS and Reliability", **(2017)**.
[8] T. El-Maliki, J.-M. Seigneur, "Efficient Security Adaptation Framework for Internet of Things", **(2016)**.
[9] M. Mohsin_y, Z. Anwar_y, G. Husariy, E. Al-Shaery, M. Ashiqur Rahman, "IoTSAT: A Formal Framework for Security Analysis of the Internet of Things (IoT)", **(2016)**.
[10] O. Ben Abderrahim, M. Houcine Elhdhili and L. Saidane, "TMCoI-SIOT: A Trust management system based on communities of internet for the Social Internet of Things", **(2017)**.
[11] N. Sklavos and I. D. Zaharakis, "Cryptography and Security in Internet of Things (IoTs) : Models , Schemes, and Implementations", **(2016)**.
[12] M. Nawir, A. Amir, N. Yaakob and O. Bi Lynn, "Internet of Things (IoT): Taxonomy of Security Attacks", **(2016)**.
[13] G. Baldini, Member, IEEE, A. SKarmeta, E. Fourneret, R. Neisse, B. Legeard, and F. L. Gall, "Security certification and Labelling in Internet of Things", **(2017)**.
[14] W. Zada Khan, H. Mohammed Zangoti, M. Y. Aalsalern, M. Zahid and Q. Arshad, "Mobile RFID in Internet of Things: Security Attacks, Privacy Risks, and Countermeasures", **(2016)**.
[15] L. Metongnon, E.C. Eziny and R. Sadre, "Efficient probing of Heterogeneous IoT Networks", **(2017)**.
[16] I. Nakagawa and S. Shimojo, "IoT Agent Platform mechanism with Transparent Cloud Computing Framework for improving IoT Security", **(2017)**.
[17] O. Ben Abderrahim, M. H. Elhedhili and L. Saidane, "CTMS-SIOT: A Context-based Trust Management System for the Social Internet of Things", **(2017)**.
[18] J. Zouari, M. Hamdi and T.-H. Kim, "A Privacy-Preserving Homomorphic Encryption Scheme for the Internet of Things", **(2017)**.
[19] D. Midi, A. Rullo, A. Mudgerikar and E. Bertino, "Kalis- A System for Knowledge-driven Adaptable Intrusion Detection for the Internet of Things", **(2017)**.
[20] B. Dorsemaine, J.-P. Gaulier and P. Urien, "A New Threat Assessment Method for Integration an IoT Infrastructure in an Information System", **(2017)**.
[21] S. K. Sharma, "A Survey on Layered Approach for Internet of Things Security", SERSC, ASTL, SMART DSC-2017, vol. 147, pp. 26-33.

