DYNAMIC CIPHER FOR ENHANCED CRYPTOGRAPHY AND COMMUNICATION FOR INTERNET OF THINGS

[1]GURPRATAP SINGH WARAICH, [2]BALJINDER SINGH

[1,2]Asra College of Engineering & Technology Bhawanigarh, Patiala, India
E-mail: -[1]gurpratapwaraich@gmail.com, [2]baljinderdachar@gmail.com

Abstract - Security represents a vital element for sanctioning the widespread adoption of Internet of Things technologies and applications. While not guarantees in terms of system-level confidentiality, credibility and privacy the relevant stakeholders are unlikely to adopt Internet of Things solutions on an oversized scale. In early-stage Internet of Things deployments (e.g., supported RFIDs only), security solutions have principally been devised in an advert hoc approach. This comes from the very fact that such deployments were sometimes vertically integrated, with all elements beneath the management of one body entity during this work we have a tendency to propose a brand new dynamic cipher to access quite one device at the same time during a network employing a single controller by creating use of Dynamic variable cipher security certificate protocol. This protocol uses key matrices thought during this protocol we have a tendency to create use of key matrices and store same key matrix the least bit the human action nodes. So once plain text is encrypted to cipher text at the causing facet, the sender transmits the cipher text while not the key that's to be won't to decode the message. To access more than one device simultaneously in a network using a single controller by making use of Dynamic variable cipher security certificate protocol.

Keywords - Internet of things, Security, Encryption, Dynamic Cipher.

I. SECURITY IN IOT

As with the advancement of IoT, the application of IoT/M2M is affecting our daily lives. So it is very important to ensure the security of the IoT/M2M system. As IP addresses are being used in order to develop IoT/M2M systems, the system has become the target of various intruders and attacks. With time these attacks will grow complex and more sophisticated and it is necessary to stop such attacks by incorporating various security measures in the IoT/M2M system. Also there are large number of endpoints in the IoT system, so the intruder can enter through any of the end-point in the system, thus making it more complex to establish security in the system. The potential attack can span from just minor stalking to damage to infrastructure or loss of life.

As seen, the threats to the IoT system may be similar to that of the conventional system but the damage that can be done is significantly different. That is why there are many efforts to analyze the threats and risks.
One of the fundamental elements in securing an IoT infrastructure is around device identity and mechanisms to authenticate it. Many IOT devices may not have the required compute power, memory or storage to support the current authentication protocols. Today's strong encryption and authentication schemes are based on cryptographic suites such as Advanced Encryption Suite (AES) for confidential data transport, Rivest-Shamir-Adleman (RSA) for digital signatures and key transport and Diffie-Hellman (DH) for key negotiations and management. While the protocols are robust, they require high compute platform and a resource that may not exist in all IoT-attached devices. Authentication and authorization need to be done in an appropriate way in order to make our new IoT world threat free.
The authentication and authorization protocols need human intervention which is not possible in some cases due to limited access to IoT devices. Therefore these devices need initial configuration to be done to protect from tampering, thefts and any other form of attack throughout its life. In order to overcome these issues new authentication and authorization need to be built using the experience of today's strong encryption algorithms.

II. RELATED WORK

Most of the security for IoT depends on encryption. As new work process come up for sensors and elements connected to internet, devices might outlive the effectiveness of encryption method. The communication and data transport channels should also be secured to allow devices to send and receive data with no effect from outside. Various Algorithms and methods have been developed by researchers to provide security in IoT domain including.
(Antonio f Skarmeta-2014) proposed a paper that provides various challenges that are present in this field and also provides description of some challenges that need to be overcome in coming years for full acceptance of IoT by the society. The paper also proposes a capability-based access control mechanism which is built on public key cryptography in order to eradicate or overcome these challenges. Its solution is based on token used to access the constrained application protocol (CoAP). It also uses an optimized implementation of Elliptical curve Digital Signature Algorithm (ECDSA) inside the smart entities.

(Xu Xingmei -- 2013) proposed a paper that introduces various aspects like basic characteristics, network architecture, key technologies and Security problems of internet of things. The basic characteristics include overall perception, reliable transmission and intelligent processing. The network architecture is divided into layers via- sensing layer, transport layer and application layer. The Key technologies comprise of radio frequency identification (RFID), Sensor technology and network and embedded system technology. The paper also describes some method to provide security in internet of things.

(Jungyub Lee et al- 2015) have published a paper on securing internet of things network. As we know that using the present internet, data owners can provide integrity and authentication when data is getting generated. But confidentiality is not implemented by the owners as it is implemented by the symmetric keys between ends. But in internet of things confidentiality cannot be implemented suitably using this method as there are many consumers. Also consumers differ in their ability to use only a specific a part of the cipher text as the nodes don't know about the context. In this paper they have shown work as how confidentiality can be done in IoT. They have proposed a way in which producer encrypts the data along with context. They have improved key policy attribute based encryption and cipher text policy attribute based encryption to allow consumers to decrypt data according to context.

(jong jin Lee e al) proposed an authentication scheme based on elliptical curve cryptosystem and opened in the internet of things. In internet of things secure communication should be designed between one node and the other. In this paper they have focussed on an efficient secure key establishment based on ECC. This proposed method can prevent attacks like eavesdropping, man in the middle, replay attacks.

(Pierre de Leusse et al) proposed a paper on internet of things. In this paper it has stated as in internet of things large number of items can be addressed through internet and thus various attacks can be done. Therefore, it has led to the conclusion that current internet cannot be used as the platform to IoT. In this paper the authors has also stated various requirements for resources that will make them to be used in IoT environment. Also the authors have proposed an architectural model of self managed security cell.

(Giulio Peretti et al) proposed a paper entitles "An end to end security framework for internet of things". The paper describes a framework called as BlinkToSCoAP. The name due to the integration of three lightweight technologies of DTLS, CoAP and 6LoWPAN over tinyOS.

(Christina Hochleitner et al) proposes a paper in which they have given a method of making the end points trustworthy. One of the important end point of internet of thing environment are mobile phones. These end points help users to interact with their appliances known as "things" in IoT. This paper presents an approach that provides users with the underlying security information on mobile systems and helps them to establish trust in internet of things.

(Sasa Radomirovic et al) proposed a paper in which they provide a security model which allows to ponder about security and privacy of communication protocols in the internet of things. The model they provided is designed on few assumptions and on various observations on various threats that we may face in internet of things.

(Hui Suo et al) proposed a paper in security of internet of things. In the past decade internet of things is finding its use in full throttle. The key features of IoT application are security and privacy. With such advancement in technology Internet of things is still facing various enormous challenges in its application. The paper proposed by the author puts emphasis on these key features i.e. security. The paper has discussed the status of the key technologies being used in implementation of internet of things. These technologies include encryption mechanism, communication security, protection of sensor data and various cryptographic algorithms.

(Quangang Wen -- 2012) proposed a paper that describes the security structure of sensor level, network layer and application layer in internet of things. The paper analyses the security feature of the sensor layer and then applies a protocol called as Dynamic variable Cyber security certificate, a new method for authentication mechanism among various nodes in sensor level. This certificate is based on the principle "one time one cipher" between communicating nodes. This technology or method uses time stamp technology band timeliness is guaranteed between two parties. Dynamic variable cipher certificate can be applied for communication among various nodes in IoT. The dynamic variable security certificate is an authentication protocol; based on request-reply mechanism.

Internet of thing is one of the latest technologies that are widely being accepted. We can make use of this technology in our day to day life and thus reducing human workload. With the help of this technology we can access any object to which an IP address can be assigned. One of the toughest challenges of this technology is its security. There have been many proposals in order to achieve secure transmission between the nodes. One of the proposed method is making use of "Dynamic variable Cipher Security Certificate" Protocol. We can make the use of same protocol and combine multiple cipher texts and transmits the cipher text to multiple devices in the network. The devices will make use of the specific part of the cipher text for its operation. Thus we can access multiple devices using a single controller that will generate a combined cipher text for all the devices.

III. DYNAMIC VARIABLE CIPHER SECURITY CERTIFICATE

Dynamic variable cipher security certificate is a protocol that works on reply-request mechanism. In this protocol a key matrix is generated and same key matrix is stored at all communicating parties. The advance thing in using this protocol is that the sender does not need to send decryption key instead it sends the co-ordinate of the key matrix where this key is stored. As same key matrix is stored at all the nodes, the recipient will use the co-ordinate sent by the sender and will get the key from its key matrix using this co-ordinate. The authentication process of this protocol is shown between two parties A and B as client and server respectively.

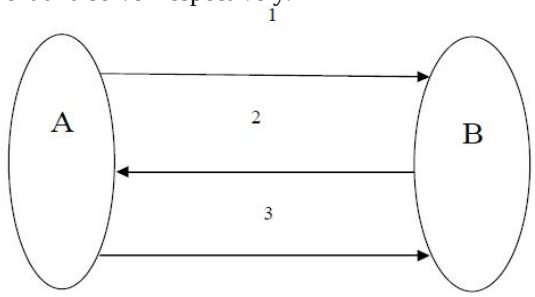


Fig 1: Reply Request Mechanism of Dynamic Cipher certificate Protocol

The process is as follows:

1. A B: Pos_x1_y1, E(Kab1: ID_A, cmd, Ta1)
2. B A: Pos_X2_Y2, E(Kab2: ID_B, Com_x_y, Ta1, Tb1)
3. A B: E(Kab3: Text, ID_A, Ta2, Tb1)

Where ID_A, ID_B means ID number of node A and node , Cmd means connection request, Pos_X_Y means coordinates of the key matrix, TA and TB means timestamp of node A and node B, E(Kab:m) means using password Kab to code message m, Text means message constant.

As seen from the above description, three steps exists, In the first step client node A send the encrypted information ID_a, a connection request Cmd, and a timestamp Ta1, and at the same time client A starts a timer and id it does not receive acknowledgment in allotted time then cancels the session.

If some information is received by server B, it will verify the ID_a from node A. if A validates it then B sends an encrypted information to A. the encrypted information consists of encrypted information ID_b, co-ordinates of key matrix Com_x_y, Timestamp Ta1, Timestamp Tb1 and at the same tie B starts a timer. If it does not receive any feedback from client A, it will cancel the session.

When some information is received at A, it will verify the encrypted information Ta1. If B is validity the A gets a communication password Kab according to co-ordinates of the key matrix. Then A generates a new time stamp ta2, combines with ta1 and sending message constant. Whole of this will be sent to B and up to this point a communicational channel is set between two parties.

IV. SIMULATION PARAMETERS

Following table describes the simulation parameters for IoT mobility in MATLAB, each node properties is defined in MATLAB Structure.

Parameter	Value
Node POSITION_X_INTERVAL	10-30
Node POSITION_Y_INTERVAL	10-30
Node SPEED_INTERVAL	0.2-2.2
Node PAUSE_INTERVAL	0-1
Node WALK_INTERVAL	2.00-6.00
Node DIRECTION_INTERVAL	-180-180
SIMULATION_TIME	500
Number of Nodes	20
Public Key Encryption	RSA
Private Key Encryption	AES
Packet Size	512 Bytes

Node POSITION_X_INTERVAL: X position of the Node at any given moment, updates due to Random Way Point Model

Node POSITION_Y_INTERVAL: Y position of the Node at any given moment, updates due to Random Way Point Model

Node SPEED_INTERVAL: Speed Range of Each Node factor of 0.2 to 2.2x speed with respect to stationary nodes.

Node PAUSE_INTERVAL: For how long a node will stay stationary

Node WALK_INTERVAL: For how long a node will stay moving

Node DIRECTION_INTERVAL: In which direction the node will be moving.

SIMULATION_TIME: 3. Overall Simulation Time of the Node.

Number of Nodes: Total number of nodes present in the Simulation (default: 20)

Public Key Encryption: Encryption Scheme used to Encrypt Messages using Public Key of the node and Decryption using the Private keys.

Private Key Encryption: Encryption Scheme used to encrypt Private Key of the Node using the Location of each node before sending any data.

Step 1: Receiver R Requests data from the node S, only receiver knows the exact location of itself.

Step 2: On receiving request from the R node the sender initiate public key Exchange using RSA algorithm and stores keys P_k as Private Key of the node R and P_u as the public key to encrypt the data.

Step 3: Node S then Request the Location L_{Rxy} of the node R.

Step 4: After receiving request from the node S the R sends its location L_{Rxy} to the node S.
Step 5: S then Encrypts the private key of the by using L_{Rxy} as Private Key using AES algorithm
Step 6: for multiple recipients the same process in repeated and a matrix is formed in following manner and forwarded to recipients.

Encrypted Data (RSA)	L_{Rxy} private key of the receiver 1 (AES)
	L_{Rxy} private key of the receiver 2 (AES)
	….
	L_{Rxy} private key of the receiver N (AES)

Fig 2: Packet Data format for Dynamic Cipher Protocol

Step 7: After receiving the packet the recipient decrypts the private key using its location and then decrypts the data sent by the sender.
The nodes need to send data between each other. But if the nodes will send the data in plain text, any attacker or intruder can get that data and misuse it or even alter it. So in order to restrict an intruder to carry out any sort of attack on the data, the data is sent in a form that is not easily understandable by any third party person. We used AES algorithm to encrypt the private key of the authenticated user by estimating its exact location.

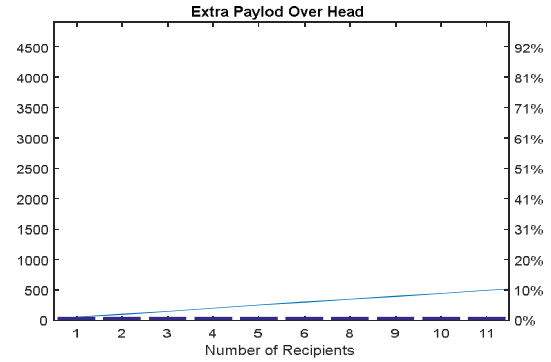


Fig 3: Number of Recipients and network overhead (payload)
As for each location a new private key is generated and attached to the packet, we require that there must not be a significant overhead as the Number of recipient grow.

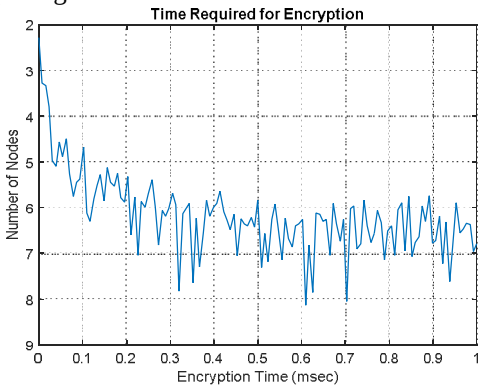


Fig 4: Time Required for Encryption 512 bytes data packet used

The two main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks and its speed and efficiency in doing so. This speed surmounts the symmetric encryption problem of managing secret keys. As on the other hand, this unique feature of public key encryption makes it mathematically less prone to attacks. However, asymmetric encryption techniques are slower than symmetric techniques, because they require more computational processing power. As it can be seen from above fig the encryption time does not increases too much when number of nodes increase as seen in above figure. So does the decryption process as seen below.

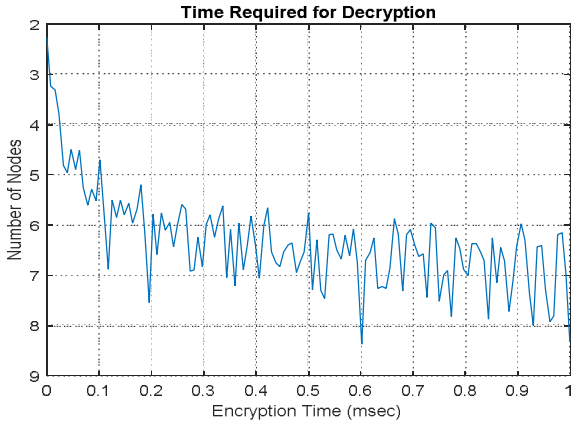


Fig 5: Time required for decryption 512 bytes data packet used

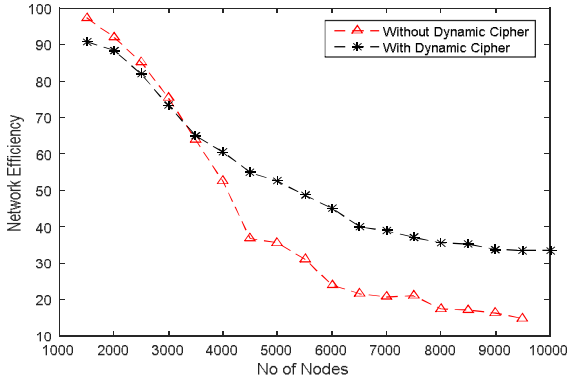


Fig 6: Network Efficiency of Dynamic Cipher certificate Protocol

The Results demonstrate that the Dynamic Cipher certificate Protocol is more secure and efficient than existing works. We further demonstrate that as the Number of node increases, the efficiency of all proposed scheme increases, but the efficiency gained by the more flexible and dynamic Cipher certificate Protocol schemes over the fixed scheme increases also. We also observe that the as the number of nodes increase the overall quality of service in encryption and decryption time is preserved.

CONCLUSION AND FUTURE SCOPE

The presented simulation results showed that proposed method has a better performance than other common encryption algorithms used. Since it

becomes very difficult to estimate the exact location of the node and has not any known security weak points so far, which makes it an excellent candidate to be considered as a standard encryption algorithm for communication between IoT nodes? Using hybrid encryption has although added extra processing time, but overall it was relatively negligible especially for certain application that requires more secure encryption to a relatively large data blocks. The Results demonstrate that the Dynamic Cipher certificate Protocol is more secure and efficient than existing works. We further demonstrate that as the Number of node increases, the efficiency of all proposed scheme increases, but the efficiency gained by the more flexible and dynamic Cipher certificate Protocol schemes over the fixed scheme increases also. We also observe that the as the number of nodes increase the overall quality of service in encryption and decryption time is preserved. In future we can work on dynamic block based encryption for IoT specific hardware to solve such issues. Also for future work, we aim at a deeper feasibility analysis of the discussed protocols in different settings and for different trust models

REFERENCES

[1] Kopetz, Hermann. "Internet of things." In Real-time systems, pp. 307-323. Springer US, 2011.

[2] Feldhofer, Martin, Sandra Dominikus, and Johannes Wolkerstorfer. "Strong authentication for RFID systems using the AES algorithm." In Cryptographic Hardware and Embedded Systems-CHES 2004, pp. 357-370. Springer Berlin Heidelberg, 2004.

[3] Smith, Donald R., and James T. Palmer. "Universal fixed messages and the Rivest-Shamir-Adleman cryptosystem." Mathematika 26, no. 01 (1979): 44-52.

[4] Jara, Antonio J., Pablo Lopez, David Fernandez, Jose F. Castillo, Miguel A. Zamora, and Antonio F. Skarmeta. "Mobile digcovery: discovering and interacting with the world through the internet of things." Personal and ubiquitous computing 18, no. 2 (2014): 323-338.

[5] Xingmei, Xu, Zhou Jing, and Wang He. "Research on the basic characteristics, the key technologies, the network architecture and security problems of the Internet of things." In Computer Science and Network Technology (ICCSNT), 2013 3rd International Conference on, pp. 825-828. IEEE, 2013.

[6] Lee, Jungyub, Sungmin Oh, and Ju Wook Jang. "A Work in Progress: Context based encryption scheme for Internet of Things." Procedia Computer Science 56 (2015): 271-275.

[7] Lee, Jong Jin, Youn-Sik Hong, and Ki Young Lee. "An Authentication Scheme Based on Elliptic Curve Cryptosystem and OpenID in the Internet of Things." In Proceedings of the International Conference on Security and Management (SAM), p. 192. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2015.

[8] Peretti, Giulio, Vishwas Lakkundi, and Michele Zorzi. "BlinkToSCoAP: An end-to-end security framework for the Internet of Things." In Communication Systems and Networks (COMSNETS), 2015 7th International Conference on, pp. 1-6. IEEE, 2015.

[9] Hochleitner, Christina, Cornelia Graf, Dominik Unger, and Manfred Tscheligi. "Making devices trustworthy: security and trust feedback in the internet of things." In Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU), Newcastle, UK. 2012.

[10] Van Deursen, Ton, and Sasa Radomirovic. "Attacks on RFID Protocols." IACR Cryptology ePrint Archive 2008 (2008): 310.

[11] Suo, Hui, Jiafu Wan, Caifeng Zou, and Jianqi Liu. "Security in the internet of things: a review." In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 3, pp. 648-651. IEEE, 2012.

[12] Wen, Quangang, Xinzheng Dong, and Ronggao Zhang. "Application of dynamic variable cipher security certificate in internet of things." In Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on, vol. 3, pp. 1062-1066. IEEE, 2012.

[13] Wang, Y., Wong, K.W., Liao, X. and Xiang, T., 2009. A block cipher with dynamic S-boxes based on tent map. Communications in Nonlinear Science and Numerical Simulation, 14(7), pp.3089-3099.

[14] He, Debiao, Yitao Chen, and Jianhua Chen. "Cryptanalysis and improvement of an extended chaotic maps-based key agreement protocol." Nonlinear Dynamics 69, no. 3 (2012): 1149-1157.

[15] Botta, Alessio, Walter de Donato, Valerio Persico, and Antonio Pescapé. "Integration of cloud computing and internet of things: a survey." Future Generation Computer Systems 56 (2016): 684-700.

[16] L Marin Marin, Leandro, Marcin Piotr Pawlowski, and Antonio Jara. "Optimized ECC implementation for secure communication between heterogeneous IoT devices." Sensors 15, no. 9 (2015): 21478-21499.

[17] D HEMALATHA HEMALATHA, D., and BANU E. AFREEN. "Development in RFID (Radio Frequency Identification) Technology in Internet of Things (IOT)." Development 4, no. 11 (2015).

[18] S Sicari Sicari, Sabrina, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. "Security, privacy and trust in Internet of Things: The road ahead." Computer Networks 76 (2015): 146-164.

[19] A Agarwal Whitmore, Andrew, Anurag Agarwal, and Li Da Xu. "The Internet of Things—A survey of topics and trends." Information Systems Frontiers 17, no. 2 (2015): 261-274.

[20] H Shafagh Shafagh, Hossein. "Toward computing over encrypted data in IoT systems." XRDS: Crossroads, The ACM Magazine for Students 22, no. 2 (2015): 48-52.

[21] JM Bohli Bohli, Jens-Matthias, Roman Kurpatov, and Mischa Schmidt. "Selective decryption of outsourced IoT data." In Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on, pp. 739-744. IEEE, 2015.

[22] J Granjal Granjal, Jorge, Edmundo Monteiro, and Jorge Sa Silva. "Security for the internet of things: a survey of existing protocols and open research issues." Communications Surveys & Tutorials, IEEE 17, no. 3 (2015): 1294-1312.

[23] A Patil Patil, Abhijit, Gaurav Bansod, and Narayan Pisharoty. "Hybrid Lightweight and Robust Encryption Design for Security in IoT." (2015).

[24] HJ Kim Kim, HakJu, and Kwangjo Kim. "Toward an Inverse-free Lightweight Encryption Scheme for IoT." In 2014 Conference on Information Security & Cryptography. 2014.

[25] J Pescatore Pescatore, John, and G. Shpantzer. "Securing the Internet of Things Survey." SANS Institute, January (2014).

★★★