
AN EFFICIENT PROTOCOL FOR GROUP KEY ESTABLISHMENT IN INTERNET OF THINGS

AMREESH KUMAR

Department of C.S.E
R.C.E, Roorkee, Uttrakhan

ANURAG CHANDNA

Department of C.S.E
R.C.E, Roorkee, Uttrakhand

ABSTRACT:

Internet of Things (IoT) extends our capability to explore, monitor and control the physical world. It has so many applications in health monitoring, smart city, smart transport system etc. For efficient message deliveries among resource-constrained sensor nodes it is important to have group communication instead of device to device communication in the IoT-enabled WSNs. Secure and efficient key management techniques are used to protect the authenticity, integrity, and confidentiality of multicast messages. The main challenge in IoT is to design a group key establishment protocol which is time and energy efficient and use less bandwidth. In this paper, we propose a novel scheme for establishing group key for every group that is encrypted using combination of haar and dna. Using the above technique for group key establishment, we get a secure group key establishment protocol that uses less energy, less time and less bandwidth in IOT networks. In this in this paper we have defined some analysis metrics and implemented a simulator which fully satisfies the requirement to test our candidate algorithms. The behavioral analysis of chosen algorithms in the case of different scenario is completely reported in this in this paper. The analysis and experiments show that our protocol is efficient and practical, and achieves better performance than the previous approaches.

Keywords:IOT, Key distribution, Encryption

1. INTRODUCTION

Internet of things is a technology that dispenses chance for devices to connect and communicate with each other. The deployment of devices connected through internet means Internet of Things is growing swiftly. In the coming days it is advised that the chance of increasing the use of will be very rapidly.

According to Gartner Ink report in 2020 around 26 billion devices will be connected wirelessly through Internet of Things. The IOT term was invented by Kevin Ashton of the Radio Frequency Identification (RFID) development community in 1999, and it has now become more meaningful to the practical world largely because of the increase of mobile devices, embedded and ubiquitous communication, cloud computing and data analytics.

In Internet of Things, multiple collaborative nodes in wireless sensor networks can be used to track an event, jointly prepare a report and then send it to one or more Internet nodes for further processing [15].

The meaning of Internet of things is a group of internet network and electronic appliances (mobile, ac, fridge etc.) in which the people are connected with things through cloud computing, data capture and network communication. This first product launches in 1982 when the coke machine was built and it was connected through internet. Internet of Things is fundamentally a network of uniquely identifiable and interconnected objects or things. These things are devices, mainly sensors or actuators, these devices are continuously collecting information of different kind to supply it as data sources.

2. OBJECTIVE

The purpose of this project is to present a theoretical model for network deployment and develop a key management protocol which is more energy, time efficient and use low bandwidth. These networks are battery operated. A responder node gathers data and passes it on to the initiator for further use. The nodes are also capable of monitoring the spectrum for empty channel. This monitoring, passing and receiving of data make use of most of the energy of the network. So energy consumption is the major factor

of concern for advanced operation and it increases the lifetime of the network. In this project a network model is proposed which gives an efficient algorithm for encryption. Performance is evaluated and output is compared with a comparable protocol on the basis of time, network bandwidth and energy consumption

3. LITERATURE SURVEY

This chapter gives a detailed description of key establishment protocols in IoT. This chapter also discusses some existing key establishment protocols and detailed theoretical comparison of key management protocols also given in this chapter.

In 1984 Shamir et al. [1] introduced the first Identity Based Key Transfer Protocol. In this paper Shamir represented a concept of public and private key in which the public key was represented as an identity and the private keys were produced by this identity using a PKG (public key generator). This scheme eliminates the need of certificates.

In 2009 P. Szczechowiak et al. [2] proposed TinyIBE – it is a very simple authenticated key distribution scheme based on IBE for heterogeneous sensor networks. This technique does not require any pairing calculation. In this scheme it is able to get a session key for two nodes after only exchange of two messages.

D. Boneh et al.[3], L. Yang et al. [4], C. Gentry et al. [5] introduced identity based concept using Elliptic Curve Cryptography RSA or Elgamal. The disadvantage of this concept was that it was too costly because the calculations in these schemes needed exponentiation operations with a large exponent.

In 2012 T. Kohmayr [6] implemented DTLS using the help of hardware on the sensor nodes. This scheme shows that each sensor is connected to with a TPM (Trusted Platform Module). A TPM is an embedded chip that is used to produce cryptographic keys and sealed storage and hardware support for cryptographic algorithms.

In 2012 S. Ray [7] presented a mechanism to provide security associations using IKE protocol with IPsec. They also proposed another alternative for IKE based on ECC-based public key certificate for authentication and ECDH for key agreement instead of RSA and DH protocol

In 2013 R. Moskowitz et al. [8] presented HIP-DEX (Host Identity Protocol Diet Exchange) that uses Diffie-Hellman protocol to generate a session key between two entities after only a 4-messages exchange. This protocol is an extension of HIP Base Exchange [9] which was presented by R. Moskowitz et al in 2012. This protocol was designed to lower the complexity computations in cryptography. It needs the smallest possible set of cryptographic primitives and removes digital signatures and process static ECDH to encrypt the session key, etc.

3. SYSTEM DESIGN AND PROPOSED METHODOLOGY

MATERIALS

This chapter deals with the software tools required for the completion of the proposed work. The coming section deals with a brief introduction to the material required with detailed description of the proposed work.

SOFTWARE USED

MATLAB is the main software that is used in formalizing the proposed work. Windows 7 is used as a platform and basic utilities of this platform are also used.

REASONS FOR USING MATLAB

MATLAB (Matrix Laboratory) is mainly used by scientists and engineers who are involved in numerical and technical computing. Most of these people use MATLAB because they are able to obtain the results very quickly than other programming languages like Open CV. MATLAB has several advantages over other languages:

- I. It has a very large library of built-in pre-written functions for many common numerical computing tasks
- II. MATLAB has a long history of clarification

III. MATLAB has very good user documentation and a helpful community

IV. It is quite an informal language, allowing new comers to get going and get results quickly.

INTRODUCTION TO MATLAB

MATLAB environment which includes complete functionality for image processing tasks is used for programming. No external software, other than MATLAB, is required for programming purpose. The important steps used for using MATLAB components are described as follows:

I. Opening MATLAB in the micro-computer lab

II. Access the Start Menu, Proceed to Programs, and Select MATLAB 7.14 from the MATLAB folder or Open through C:\Program Files\MATLAB\R2013a

The M-file is a MATLAB document the user creates to store the code they write for their specific application. An M-file is useful because it saves the code the user has written for their application. It can be operated and tested until it meets the user's specifications.

I. Creating an M-file: To create an M-file, select File\New ►M-file.

II. Saving: In the M-file window, select File\Save as... Choose a location.

III. Opening an M-file: To open a M-file, open MATLAB and then, open the M-file by going to File\Open..., and selecting your file.

IV. Writing Code: After creating and saving your M-file, the next step is to begin writing code. Comments are declared by using a % symbol before them.

V. Saving: Save your code by going to File\Save.

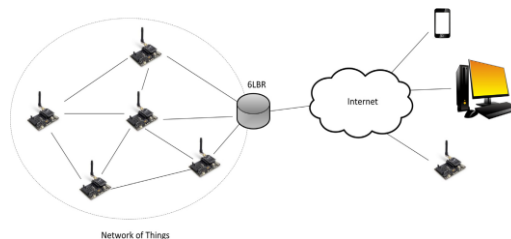
VI. Running Code: To run code, go to the main MATLAB window and type the name of your M-file after the >> prompt.

VII. Loading an Image: Image can be read or loaded using imread command.

VIII. Writing an Image: This is done in MATLAB by the imwrite function. This function allows you to save an image as any type of file supported by MATLAB.

NETWORK MODEL

The term multicast group describes a particular group of nodes, these nodes are interested in or authorized to receiving the common set of information or instructions. The total number of nodes taken in the multicast network is n , which includes the initiator node and $(n - 1)$ multicast group members. In the following multicast group members, also known as the responder nodes are named as U_j for $j = 1, 2, \dots, (n - 1)$. A common group key, which is known by the initiator and the responders of one group, is used for secure communication within the multicast group. An image is distributed to all responders and all responders store it and encrypted image (key) is stored in the initiator at factory setting. For this type of scenario, the size of the multicast network should be equal or greater than four: $n \leq 4$.



Network Architecture of our Scenario

SYSTEM MODEL

In this in this paper, we take a smart lighting control system as a group in a building as a main use-case scenario. In this system, lighting devices in the building set up mesh networks and communicate with each other reacting on events those are possible happen, e.g.in the absence and presence of people. However, all

these devices are configured and controlled by a back-end server from that is existed at some place on the Internet. The back-end server can periodically send many command information to the devices in the network and also centralized commands to turn on/off the light. There might be other devices in the network then lightning devices which can also be controlled by the back-end server.

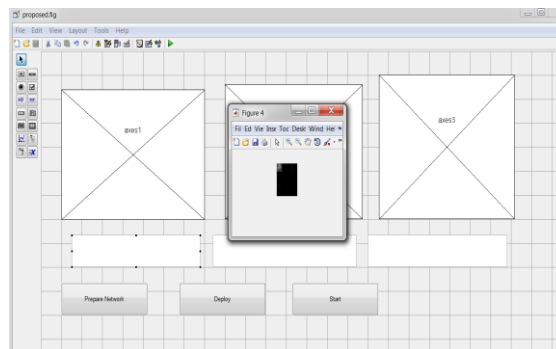
The network established with the lighting devices is a constrained network with resource constrained devices. Each device has an IEEE 802.15.4 interface. Firstly, IEEE 802.15.4 2006 edition is considered to be used, however, it might be considered to move towards a more powerful version of the standard which is IEEE 802.15.4g [3]. Devices set up a mesh network over the IEEE 802.15.4 interface. IPv6 is used as a network protocol and RPL protocol is used as a routing protocol for this network and UDP - as a transport protocol. The transmission of the IPv6 and UDP over constrained environment is used as denied. All the lighting devices form separate multicast groups are to be configured by the back-end server. Hence, the communication scenario with one sender and many listeners (1-to-M) is considered. All of the lighting devices have the same hardware resources, while one device per multicast group acts as a border router receiving the multicast message from a server and distributing it to the rest of the group members. A device acting as a border router has an Ethernet interface as well. The border router receives a multicast message through the Ethernet interface from the server and distributes the message through the IEEE 802.15.4 interface to the remaining nodes of the group. In this project, we assume that the infrastructure, which is used to send an insecure multicast from back-end server to the constrained network, is already in place. In our use-case, the back-end server is a powerful device with no restrictions on memory or computation resources.

4. RESULTS AND DISCUSSION

This chapter describes the observation and findings of various simulations conducted in MATLAB. In the subsequent sections the experimental observations have been recorded, analyzed and discussed systematically for different combination of variables.

PERFORMANCE ANALYSIS OF PROPOSED ALGORITHM

Pawani Porambage et al. [2] is taken as a base paper and performance is improved. Base paper provides the modeling of two acceptable group key establishment protocols for securing multicast in IoT enabled WSN application paradigms. These two protocols are based on ECC operations. The simulation results show that proposed algorithm performs better in comparison to base paper. Shows the preparation of network. It shows three axes. All three axes represent the existence of nodes in the network. There are three buttons- prepare network, deploy and start. On clicking the 'Prepare Network' button the images are get stored in the initiator as the group key for the connection establishment.



Network Preparation

Table 4.1 shows the original images and their respected encrypted images. The encrypted images are taken as group keys. The images are encrypted using the proposed encryption algorithm.

ORIGINAL AND ENCRYPTED IMAGES














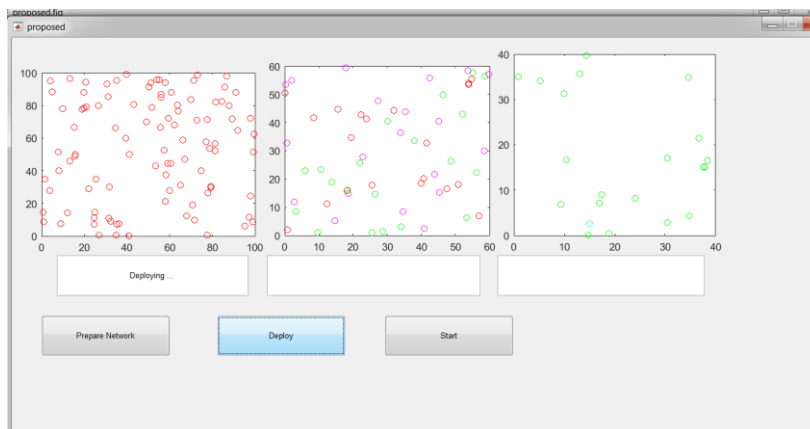
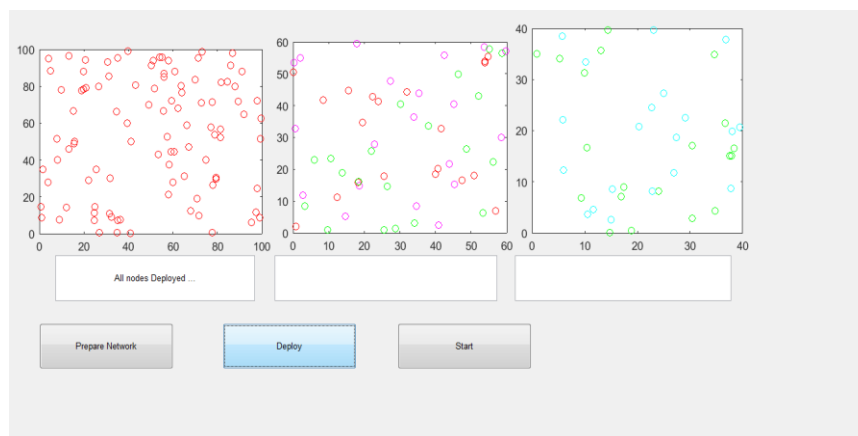
Original Images	Encrypted Images
	
	
	
	
	
	
	

Figure 4.2 shows the initial deployment of nodes. On clicking the ‘Deploy’ button the three axes gets deployed with nodes.



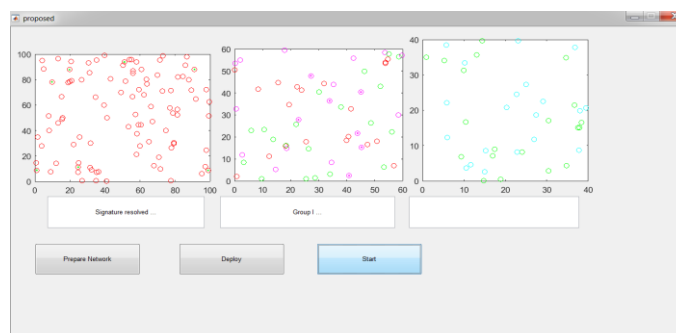
Deployment of nodes

Shows the completion of deployment process. After deployment all nodes get their locations.

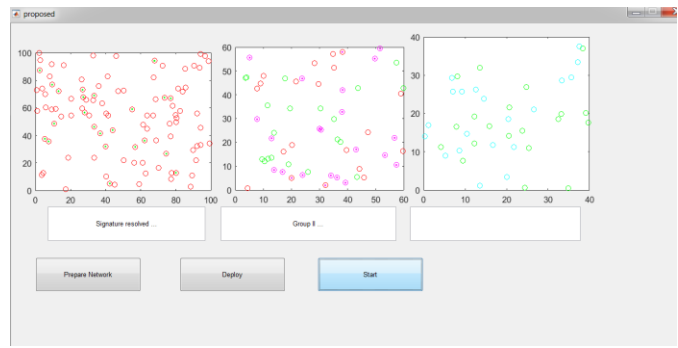


Completion of Deployment of nodes

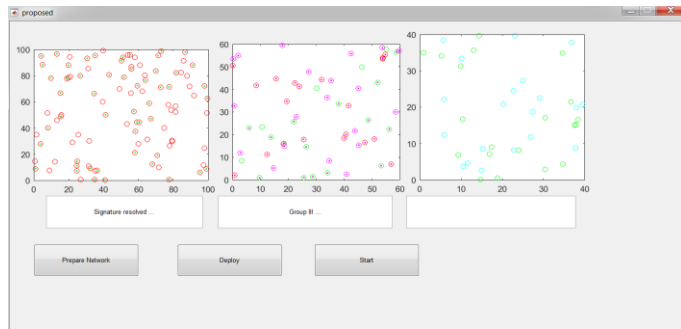
Figure 4.4, 4.5, 4.6, 4.7, 4.8 shows the signature resolving phase in which the member of Group I, Group II, Group III, Group IV and Group V resolving their signatures respectively.



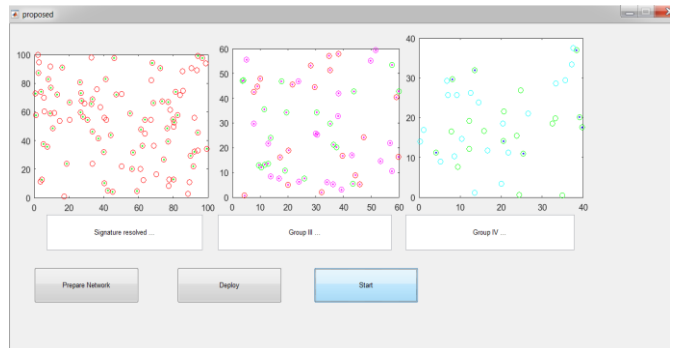
Signature resolving process for Group I



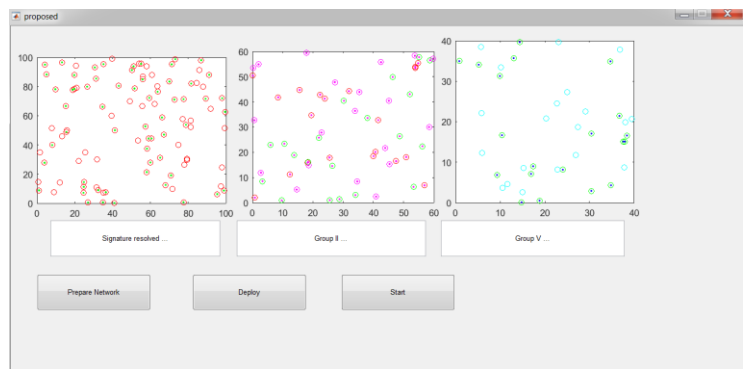
Signature resolving process for Group II



Signature resolving process for Group III



Signature resolving process for Group IV



Signature resolving process for Group V

From Plot in Figure 4.9 it is quite clear that initially almost same time is consumed but then proposed system starts saving more time than the conventional system giving overall better performance. We can safely say that the proposed model consumes lesser time as compared to the existing technique.

The Plot in Figure 4.10 clearly shows that the time consumed by the proposed model is much less than existing technique though the energy climbs as the network progresses but even then it remains much lower than the existing technique.

Shows that the proposed system starts at about 1.05 Mbps and as the network warms up and more network flows in it reaches round 2.15 Mbps whereas the existing technique in startup itself requires high bandwidth (about 2.05 Mbps) and maintains to require higher bandwidth during the entire cycle of the experiment.

5. CONCLUSION AND FUTURE SCOPE

This chapter discusses the conclusion of the work presented in this in this paper. The chapter ends with a discussion of the future direction which this work will take. The conclusion of the carried work shows better performance and result as compared to base paper.

CONCLUSION

In this paper we have proposed a group key based multicast protocol in which we take encrypted image as a group key. This in this paper is designed and analyzed secure group key establishment mechanisms for multicasting in IoT applications. The key derivations also implicitly authenticate group members, whereas the key can be further used for securing multicast messages. According to the performance evaluations results, computation and communication energy consumptions of this protocol are authorized by the resource-constrained nodes. The security analysis assures the less use of energy, bandwidth and time of protocols proposed compared to two protocols given in base paper.

This protocol is designed to provide real time support and energy efficiency to Internet of Thing (IoT) networks. In this in this paper the encrypted image is taken as a group key and signature provides individual authentication to every node. The IoT network may be divided into different groups and each group(n) has one initiator(i) and other are responders ($j=1,2,\dots,n-1$). The encryption algorithm uses combination of Haar and DNA to encrypt the image. The protocol is divided into two phases. First is factory setting phase in which group key (image) is selected for every node and encrypted with proposed algorithm and manually stored into the initiator and signatures are also stored into initiator. In the second phase which is connection establishment phase the initiator request responders with the encrypted image and it is decrypted by responders to verify the image, after verification signature is sent to initiator for verification of node, if it verified the connection gets established.

Proposed protocol is compared with existing protocols in base paper and results show that proposed work gives better lifetime, better bandwidth and better energy utilization. Proposed protocol can be used in real time large scale networks like smart home, healthcare etc.

FUTURE SCOPE OF THE WORK

In this paper new group key establishment protocol is proposed by using image as a group key and is encrypted with the combination of Haar and DNA algorithms. Results are better in comparison to both protocols in the base paper. We have improved the bandwidth, network lifetime and energy utilization.

Future work is explained as follows.

- In future if we can design a new protocol with wider range coverage area.
- Clouds can be used in future for IoT services.

6. REFERENCES

1. A. Shamir, Identity-based cryptosystems and signature schemes, Santa Barbara, California, USA, 1984
2. D. Boneh et al., Identity-based encryption from the Weil pairing, *SIAM J. Comput.* 32 (2003) 586–615.
3. L. Yang, C. Ding, M. Wu, Establishing Authenticated Pairwise Key using Pairing-based Cryptography for Sensor Network, 2013.
4. C. Gentry, Practical identity-based encryption without random oracles, Springer-Verlag, 2006, pp.445–464.
5. P. Szczechowiak, M. Collier, TinyIBE: identity-based encryption for heterogeneous sensor networks, 2009.
6. R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *ACM* 21(2), 120C126 (1978).
7. Pandey A., Bansal K.K.(2014): “Performance Evaluation of TORA Protocol Using Random Waypoint Mobility Model” *International Journal of Education and Science Research Review* Vol.1(2)
8. Tiwari S.P., Kumar S., Bansal K.K.(2014): “A Survey of Metaheuristic Algorithms for Travelling Salesman Problem ” *International Journal Of Engineering Research & Management Technology* Vol.1(5)
9. Federal Information Processing Standard for Digital Signature Standard (DSS)” Federal Register, (1991).
10. S. Turner et al. Transport Layer Security, 2011.
11. T. Kothmayr et al., A DTLS based end-to-end security architecture for the Internet of thing with two-way authentication, 2012.
12. Tim Polk et al., Security Challenges For the Internet Of Things, tim.polk@nist.gov & Sean Turner turners@ieca.com IETF Security Area Directors February 14, 2011
13. T. Kothmayr, C. Schimit, et al., A DTLS based end-to-end security architecture for the Internet of thing with two-way authentication, 7th IEEE International Workshop on Practical Issues in Building Sensor Network Applications, 2012.
14. L. Yang et al., Establishing Authenticated Pairwise Key using Pairing-based Cryptography for Sensor Network, 2013
15. A. Perrig, R. Canetti, D. Song, and J. D. Tygar. Efficient and secure source authentication for multicast. In *Proceedings of the Symposium on Network and Distributed Systems Security (NDSS 2001)*, pages 35–46. Internet Society, February 2001.J.