EFFICIENT SENSOR NODE AUTHENTICATION IN WIRELESS INTEGRATED SENSOR NETWORKS USING VIRTUAL CERTIFICATE AUTHORITY

Project report submitted in partial fulfillment of the requirement for the degree of Bachelor of Technology

In

Computer Science and Engineering

By

Brijesh Nand Diwakar (141287)

Under the supervision of

Dr. Ravindara Bhatt

To

Department of Computer Science & Engineering and Information Technology

Jaypee University of Information Technology Waknaghat, Solan-173234, Himachal Pradesh

CERTIFICATE

I hereby declare that the work presented in this report entitled **"Efficient sensor node authentication in wireless integrated sensor networks using virtual certificate authority"** in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering** submitted in the department of Computer Science & Engineering and Information Technology**,** Jaypee University of Information Technology, Waknaghat. This is an authentic record of my own work carried out over a period from August 2017 to May 2018 2017 under the supervision of **Dr. Ravindara Bhatt** (Assistant Professor (Senior Grade)).

The matter embodied in the report has not been submitted for the award of any other degree or diploma.

(Student Signature)

Brijesh Nand Diwakar (141287)

This is to certify that the above statement made by the candidate is true to the best of my knowledge.

(Supervisor Signature)

Dr. Ravindara Bhatt

(Assistant Professor (Senior Grade))

Computer Science & Engineering and Information Technology

Dated:

DECLARATION

This is to declare that this report has been written by us. No part of the report is plagiarized from other sources. All information included from other sources has been duly acknowledged. We aver that if any part of the report is found to be plagiarized, we are shall take full responsibility for it

Date:

Student Name Roll No. Signature

CONTENTS

List of Figures

ABSTRACT

Wireless Sensor Network (WSN) is a collection of sensor nodes, which are responsible for the data accumulation, from the wireless connected network. In WSN the information is gathered from the implemented network application. As data transmission happens in wireless environment this leads to the problem of data insecurity. Thus security issue becomes one one of the important problem. Data that is transmitted from one node to another node while moving in same WSN or multiple WSN is protected by applying different cryptographic techniques. VCA is one the techniques that is employed to resolve the issue of security in wireless medium.

Chapter 1
INTRODUCTION

1.1 **INTRODUCTION**

Wireless network consist of sensor nodes that ae responsible data storage of various observation collected from the equipped environment. It can be applied in so many numbers of daily life application that requires data to be gathered and analyzed like monitoring of test and experiments of certain application. Sensor nodes have unique properties like its sensors and radio transceiver that are responsible for data collection from surrounding and pass it to the base station for the further analysis. Sensor node collects the data by continuous movement across the wireless sensor network. Transmission of data across the nodes is somehow insecure and can easily be altered, so the different security measures are implemented like Key management.

Virtual Certificate Authority (VCA) is one of the technique that can eradicate the issue of security of wireless sensor network. It is issued by virtual certificate which verifies the authenticity of sensor nodes. However, there are many limitations that hinder the implementation like restricted power supplies, short bandwidth, small memory sizes and energy consumption. So each node is designed to synthesize the inter connected web.

1.1 PROBLEM STATEMENT

Security is one of the important issue for the data that are transmitted from nodes to nodes. Because of ad-hoc nature of sensor nodes, it becomes a challenge in itself to provide security against eaves drop, data theft, data manipulation and alteration into test results from adversary. As sensor nodes interact with different network from time to time, it put data at risk of information tampering.

That is why wireless sensor network needs a unique security implementation to protect the information from the attacker. A security method that provide initial trust between nodes, which interact with different nodes at different time and location (i.e. Environment where they are implemented) in wireless medium.

1.2 OBJECTIVES

PKI architecture implements security measure that provide different devices from several manufacturers to involve in secure data transmission in wireless medium. AVCA ("Authentication using Virtual Certificate Authorities") is a PKI architecture that are designed to provide a technique to resolve the issue of security in non-tamper proof devices. As the devices are resource constrained like of initial trust, scalability, interoperability and do not have enough of memory sizes, AVCA resolves these issues and enhances the protocol.

1.3 METHODOLOGY

The provision of providing initial trust between nodes is done by Virtual certificate Authority (VCA). There are certificates that are responsible for managing validity of nodes that are issued by VCA. These certificates are created and employed onto the devices before the implementation into wireless networks. Signer's certificates and devices certificates are deployed into their respective nodes that reduces the overhead charge.

1.4 ORGANIZATION

CHAPTER-1

INTRODUCTION: Introduction regarding the wireless sensor network (WSN) and various security threats to data transmission. WSN nodes are not safe and works over an unsecure wireless medium so VCA ("Virtual certificate Authority") is applied.

CHAPTER-2

LITERATURE SURVEY: Various project related papers we used to complete the project. In this project, reference from some of the different research papers are included

- "Authentication using Virtual Certificate Authorities (2010)"
- "LoENA : Low-overhead encryption based node authentication in WSN (2015)"
- "Authentication Solutions for Wireless Sensor Network Based On Virtual Certificate Authority (2013"
- "Efficient Sensor Node Authentication in Wireless Integrated Sensor Networks Using Virtual Certificate Authority (2014)"

CHAPTER-3

SYSTEM DEVELOPMENT: "Authentication using Virtual Certificate Authorities" (AVCA), Different types of AVCA, working of Certificate validation and authorization, many aspects related to security like Key management, Node Reallocation, Public Key Infrastructure, X.509 Authentication Service, then implementation in medical department gives the idea of wireless medical sensor network.

CHAPTER-4

RANDOM WAYPOINT MOBILITY MODEL: Study of movement of nodes under different circumstances in wireless sensor network.
ALGORITHMS: A program code to study the random mobility waypoint of sensor nodes.

CHAPTER-5

RESULT AND PERFORMANCE ANALYSIS: Analysis of traveling design of a mobility node using the Random Waypoint Mobility Model and obtain the result at various position and direction at different stance of time.

CHAPTER-6:

CONCLUSION: Lastly conclusion regarding the implementation of VCA to resolve the issue of security and for efficient authentication we integrate mobile network to wireless sensor network.

Chapter 2
LITERATURE SURVEY

1) **"Authentication using Virtual Certificate Authorities, 2010 Ninth IEEE International 2010"**

This paper depicts the concept of AVCA, a virtual certificate authority resolves the problem of initial trust between the nodes validating and signing of certificates. Private key distribution mechanism of AVCA improvise the interoperability of sensor node in the wireless sensor network. It also simplify design aim of WSN. Along with, ZigBee protocol stack, AVCA can be easily integrated with other WSN protocols. Potentially it can provide solution to many other security concern of WSN.

2) **"Authentication Solutions for Wireless Sensor Network Based On Virtual Certificate Authority 2013"**

This paper deals with sensor node and their confidentiality of data when they move from networks to networks. The end node gathers all data securely and refers it to the base station (BS). Virtual certificate provide a management technique that reduces the power consumption and cost of communication. It likewise upgrades plan objectives including effortlessness, versatility, interoperability and control for singular manufactures. This plan holds the full favorable position of Public key cryptography, exceedingly secure nodes in the network.

3) "**LoENA : Low-overhead encryption based node authentication in WSN, 2015"**

This paper discussed about LoENA, low overhead energy efficient node authentication scheme which uses encryption technique. The algorithm implement lightweight operations (Ex-OR, bitwise shuffle) to make it low overhead. The strength of the scheme is calculated on the basis of solving the probability and its dealing with time. The strength encourages us in settling the tradeoff between correspondence overhead and power along these lines setting the plan rule by deciding the size of the key insight to be implanted into the transmitted message. In this method message authentication and node authentication can be integrated in future to resolve the security issues of WSNs. Lastly whole scheme can be reevaluated in real time stimulator to compare the analysis given by performance system.

4) **"Efficient Sensor Node Authentication in Wireless Integrated Sensor Networks Using Virtual Certificate Authority, 2014"**

This paper deals with integration of wireless sensor network with mobile network. By implementing this scheme, the performance of the wireless network is enhanced in the terms of scalability, interoperability and control. The certificate verification and validation through VCA confirms the authentication process of the network. there were several limitations because of the significant gap between two networks. Authentication process involves the signing of certificates which resolves the issue of initial trust between nodes.

Chapter 3
SYSTEM DEVELOPMENT

"Authentication using Virtual Certificate Authorities" (AVCA) is responsible for verifying the certificates by signing and validating to authenticate the sensor nodes. This method overcomes the issue of security by setting up an initial trust between the node and further data is transmitted. These certificates are implanted before the deployment at the manufacturing time. Trust center or Centre base Station is responsible for monitoring the sensor node movement across the network. These trust centers collects all the information regarding the key management and authentication of nodes. In the projected system, nodes are secured by virtual certificate authority, when node change their position from location to another (i.e. node relocation).

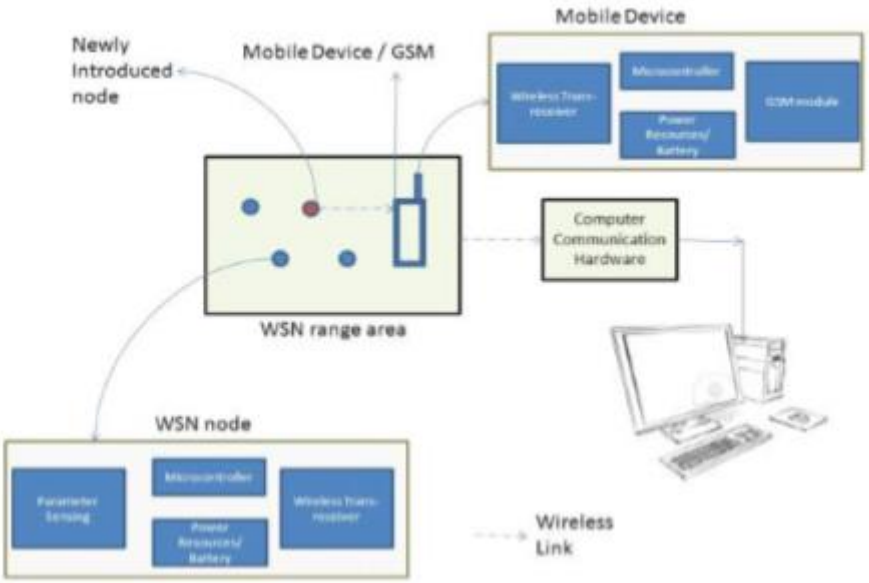


Figure 1: Wireless sensor network

Node Relocation

Node detaches from the previously connected base station by deleting all the involved certificates and keys from it and sends new joining request to the new base station after the relocation. A request for validation is sent to TC after the request is granted. The CBS issues a certificate after validating the node. Further the authentication process of AVCA proceeds using various AVCA devices.

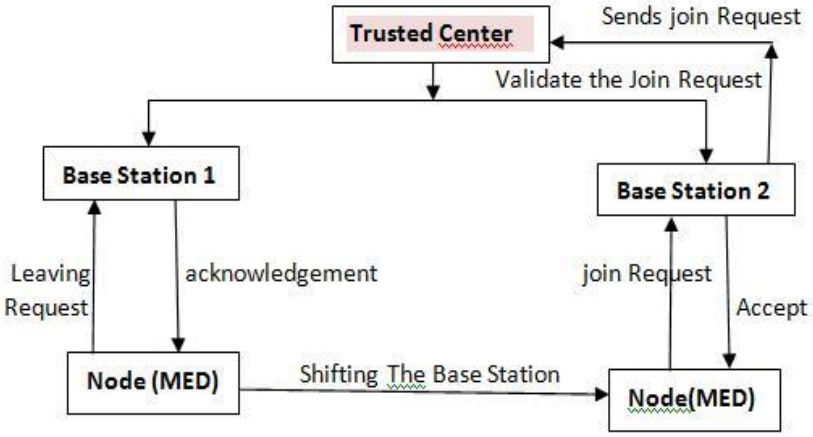


Figure.2 node reallocation

AVCA Architecture Devices

The architecture of AVCA consist of major devices as follows:

TC (“Trust Centre”): These devices are responsible for initiating the network, describing the communication medium, key management and distribution and implementation of a network access control strategy.

MED (“Manufacturer’s End Device”) are the end sensor nodes.

MCA (“Manufacturer’s Certificate Authorities”) acts as a trusted third party between the MED and the TC.

GVCA (“Global Virtual Certificate Authority”): It is the reliable third party between the TC and the MCA.

MVCA (“Manufacturer’s Virtual Certificate Authority”): It is the reliable third party between the MCA and the MED.

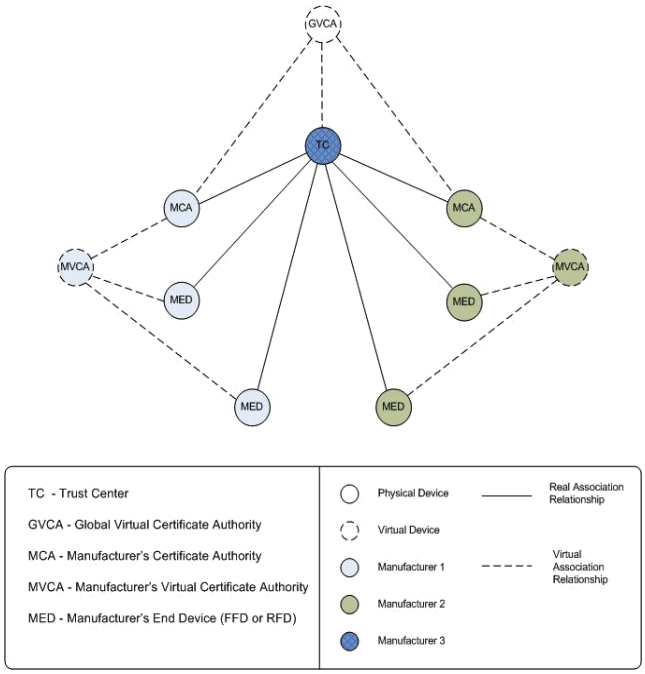


Figure 3: AVCA Star Network with Virtual Certificate Authority

Public-key infrastructure

Public-key infrastructure (PKI) as the arrangement of hardware, programming, individuals, approaches, and strategies expected to make, oversee, store, circulate, and revoke digital certificates based on asymmetric cryptography. The main aim for developing a PKI is to permit secure, convenient, and efficient acquisition of public keys. The "Internet Engineering Task Force" (IETF), "Public Key Infrastructure" and X.509 (PKIX) collaborate to set up a proper model based on X.509 that is appropriate for setting up a certificate-based architecture on the Internet. This section describes the PKIX model.

- End entity: A general term to represent end nodes (e.g. servers), or any other entity that can be identified in the subject field of a public key certificate.
- Certification authority (CA): The guarantor of certificates and (generally) certificate revocation lists (CRLs).
- Registration authority (RA): A discretionary segment that can accept various authoritative functions from the CA.
- CRL issuer: A discretionary segment that a CA can delegate to distribute CRLs.
- Repository: A nonspecific term used to mean any strategy for putting away certificates and CRLs with the goal that they can be recovered by End Entities.

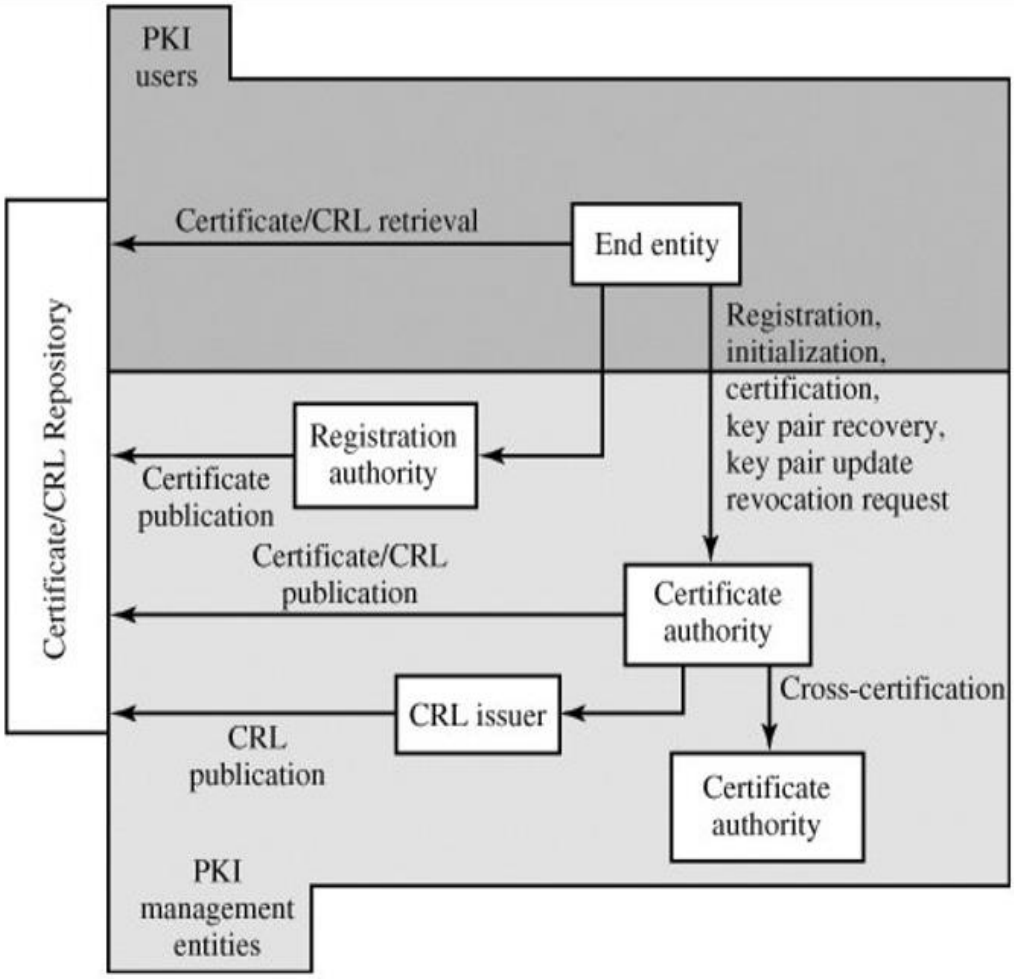


Figure 4: PKIX Architectural Model

X.509 Authentication Service[4]

X.500 directory provides authentication service to its users by defining an outline of X.509. The directory may fill in as an archive of public-key certificates. In every authentication process private key of trusted authority sign's the public key of users. Moreover, X.509 describes substitute authentication rules based on the use of public-key certificates, cryptography and digital signatures. The digital signature scheme is expected to require to implement of a hash function which is not dictated.Figure 3 shows the generation of a public-key certificate.

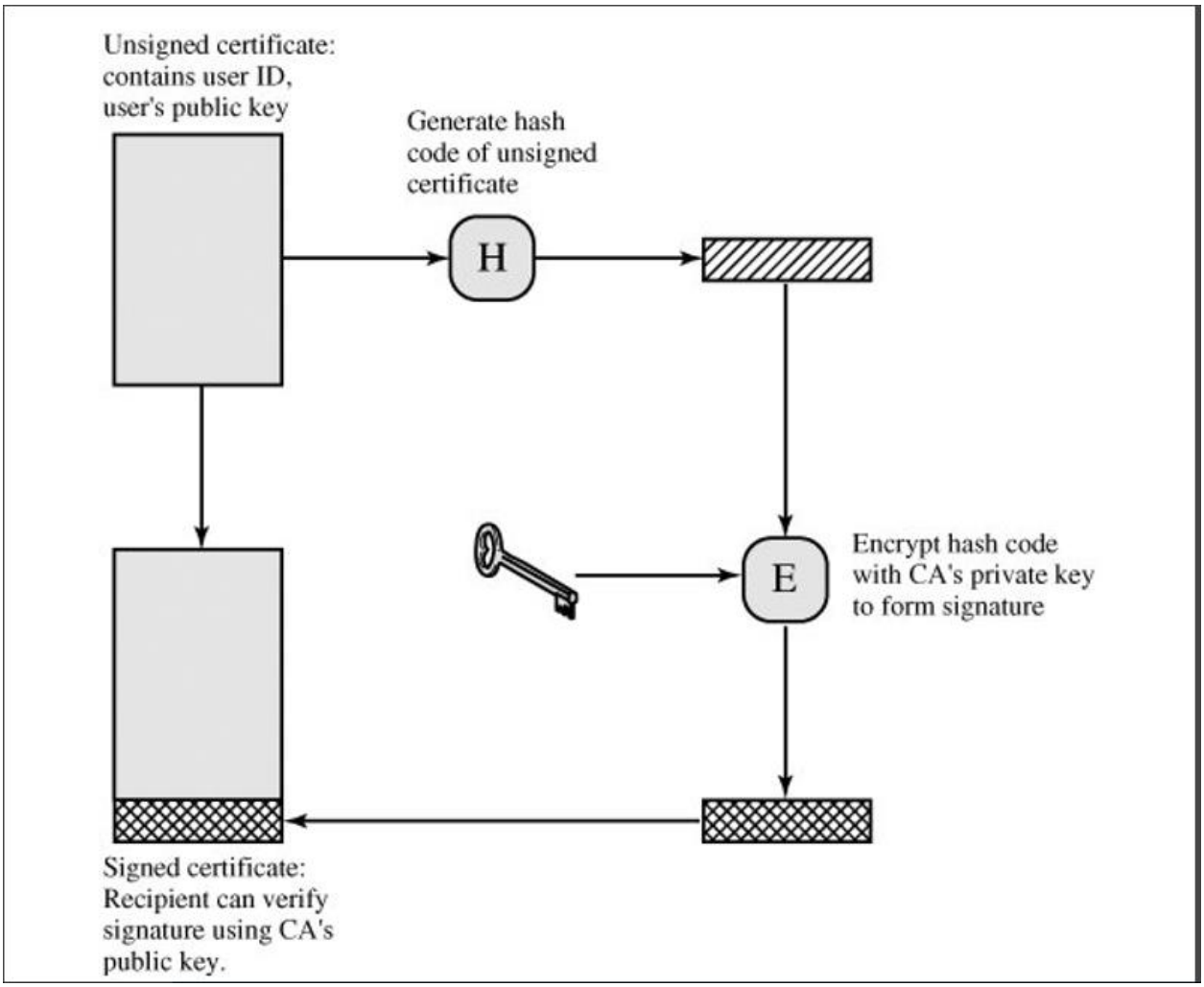


Figure 5: Authentication Service

B. Virtual Certificate Authorities

For the authentication of device itself it has to provide a certificate that can verified by another device into same PKI network. In the absence of certificate, it has to contact a trusted third party for a signed certificate. However, because of mobile nature of network it cannot be easily implemented.

Therefore, virtual certificate authority (VCA) is employed. As VCA act as trusted third party. A signed certificate is deployed onto the device at the time of manufacture so there is no necessity for requesting of signature is required. The VCA's certificate is employed as root certificate of devices.

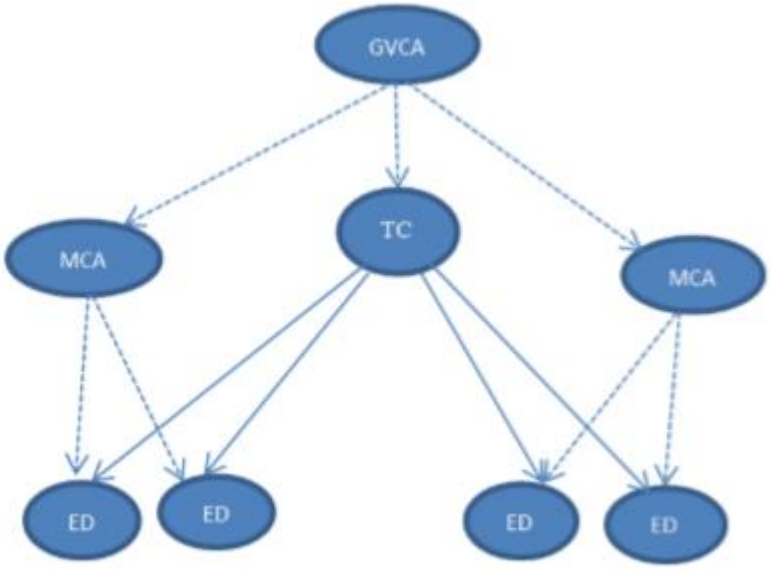


Figure 6: Virtual Certificate Authorities network

The basic function of VCA is to verify and sign other devices certificate. Public key of VCA verifies the certificate of another device, which has signed certificate of trusted third party, employed as root. Signature of the VCA that becomes the base for primary trust.

AVCA defines two types of VCAs; a GVCA ("Global Virtual Certificate Authority") and a MVCA ("Manufacturer's Virtual Certificate Authority")

C. AVCA Basic Functions

The basic functions of VCA are that it can verify the requesting and verification of certificate by MED and can involve in challenge and response process.

1) Requesting a Certificate

MED is unaware of the MCA address on a network, so it request MCA certificate by many different ways. AVCA states four terms through which a certificate can be requested:

- Capability Information
- Manufacturer's Id
- Device Address
- Signer's Address

  Any number of above parameters can be specified in single request by MED. By this MED is activated and request for the certificate of a MCA from the same manufacturer, signed by a recognized MVCA

2) Verifying a Certificate

. The verification process only verifies the data that of the given certificate but the device authenticity cannot be trusted. This process involves using the VCA's public key or already authenticated MCA's public key to verify the certificate.

3) Challenge and Response

There are a wide range of demonstrated challenge components which use public key encryption and cryptographic nonce. AVCA does not indicate which ought to be utilized. The challenge response competency for a device is defined in the “Security Schemes and Parameters” field on a devices certificate. On successful verification of certificate and effectively applying the challenge and response mechanism, certificate is validated for the further process.

4) Signing a Certificate

MCA authenticates the device, before signing the certificate, on receiving the request for signature. After the confirmation of authenticity of device, MCA signs the given certificate. IT adds the new address and signature after the removal of authenticated device certificate and signature. The freshly signed certificate is then sent to the requesting device.

D. AVCA End Device Authentication

The AVCA device authentication process involves to perform authentication without having any previous interaction before securely. The MCA can set up the address of the TC from the signal. It will request the TC’s certificate signed by a trusted third party (the GVCA). The MCA will then check the TC's certificate by utilizing the GVCA's public key. On clear verification of the TC's certificate it can start a challenge and response method utilizing the TC's public key. A right reaction will affirm that the TC is genuine. This is illustrated in Figure 6 below.

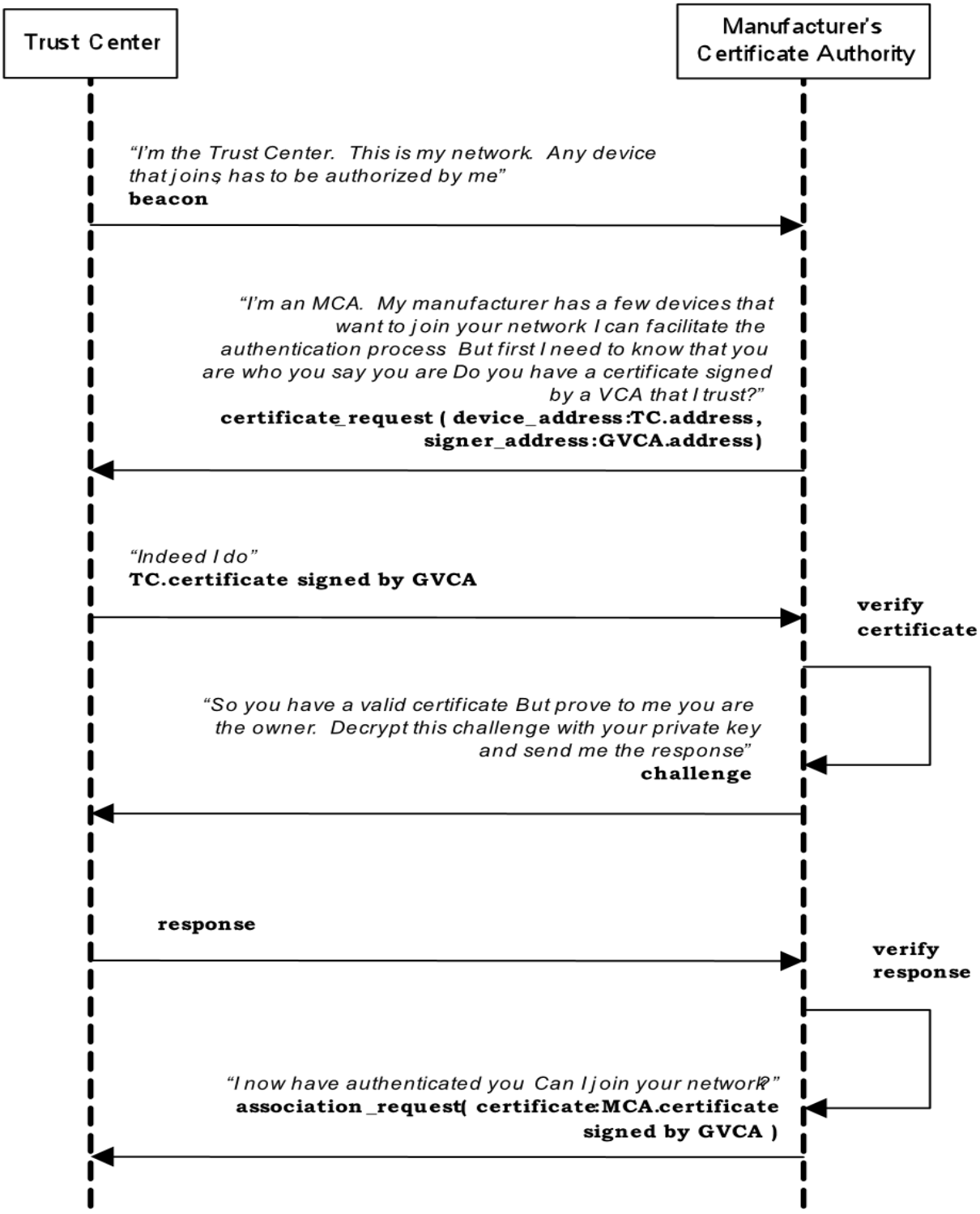


Figure 7. Sample AVCA End Device Authentication Procedure

AVCA End Device Association Procedure

The following procedure dictates the steps involved in association of MED to a given network.

1) TC is authenticated by MCA and a request from MCA is sent to associate with network.
2) In the same way TC authenticate and authorizes to associate with MCA.
3) The MED issues a request prior to authentication to the TC for a certificate of an MCA device. The MED passes the manufacturer's id and the address of the trusted MVCA as a parameters in the certificate request:
4) As there is absence of certificate to TC. It requests this certificate from the MCA because it was already authenticated from same manufacturer.
5) MCA forwards it to the TC.
6) The TC in turn forwards this to MED.
7) The MED validates the MCA and afterward asks for the TC's certificate marked by the MCA.
8) The MED would now be able to validate the TC before asking for to associate. MVCA signed certificates is presented as association request by MED.
9) The TC can ask for the MCA to confirm the certificate, before validating the MED.
10) On the completion on authentication process TC allows MED to associate.

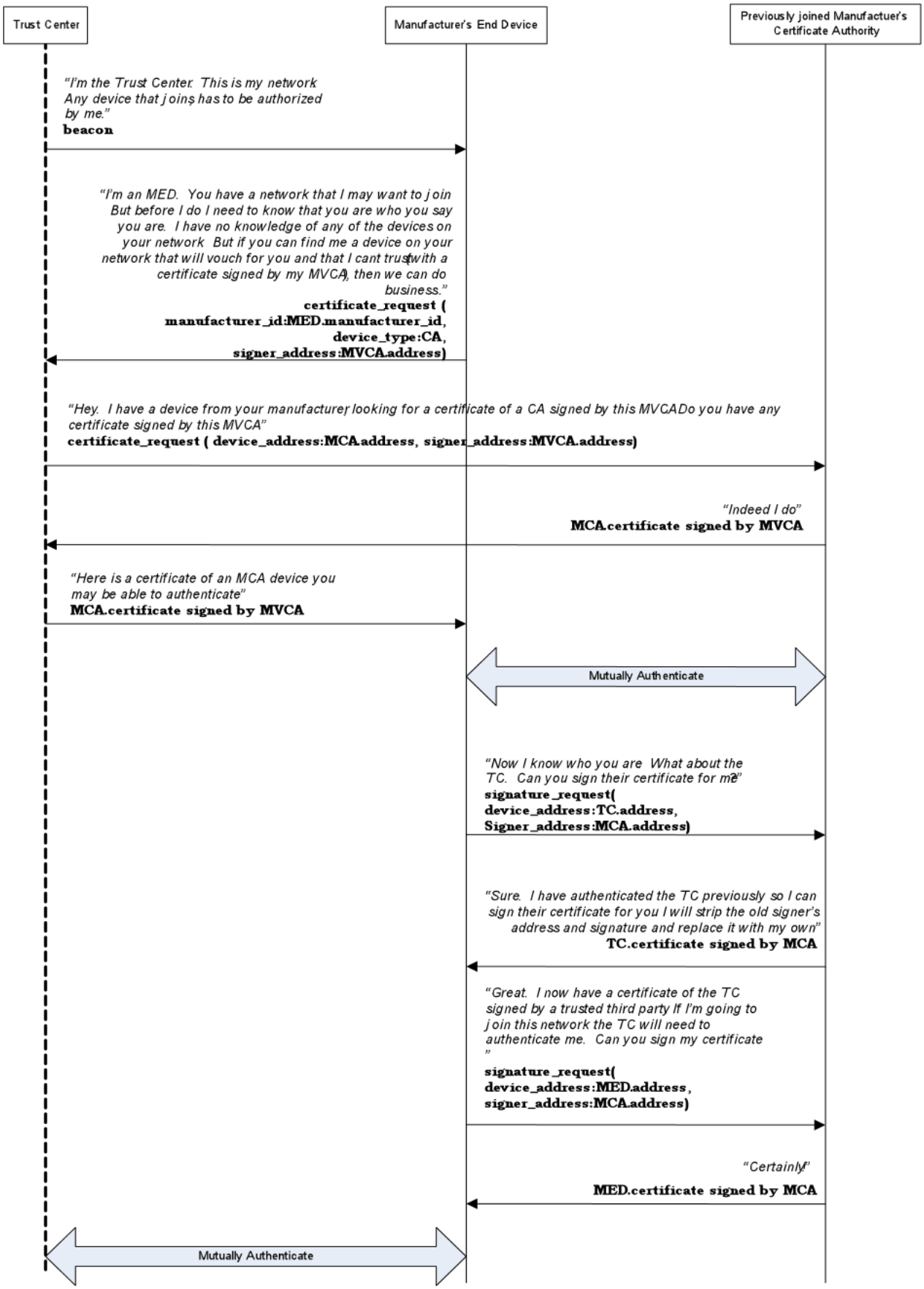


Figure 8. Sample AVCA End Device Association Procedure

A Mutual Authentication Framework for Wireless Medical Sensor Networks

Authentication provision can be employed into hospitals and many other medical departments. There are various type of data and readings that to be analyzed. That's why Wireless medical sensor networks is introduced. WMSN consist of of scattered sensors, which are responsible for collecting physiological signs of human and monitor their health condition. As these data is very critical, it become challenge itself to secue the information of the patient. The data passing is done by means of the public divert in WMSN. In this way, the patient, delicate data can be gotten by spying or by unapproved utilization of handheld gadgets which the wellbeing experts use in checking the patient. So the implementation of VCA becomes a priority to secure data in medical field also.

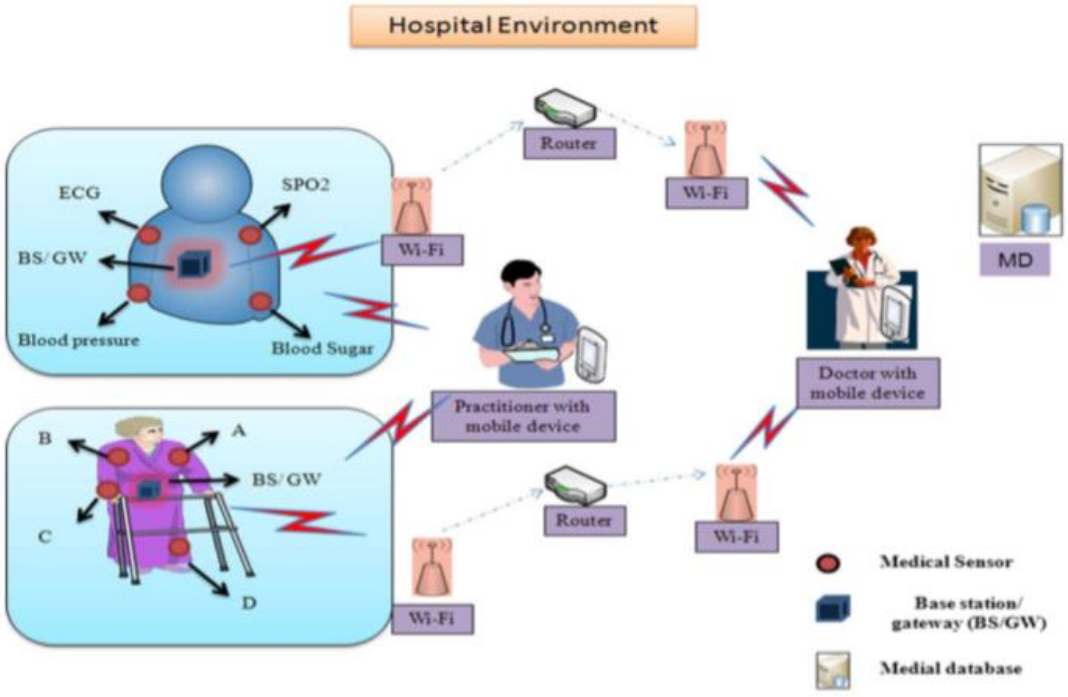


Fig. 9: Authentication in WMSN

Key Management and Distribution

Key Distribution[6]

Key distribution is technique in which two parties exchange and share the same key for symmetric encryption that key must be protected from access by others. Besides, visit key changes are generally alluring to restrain the measure of information traded off if an aggressor takes in the key. In this way, the quality of any cryptographic framework rests with the key appropriation strategy, a term that alludes to the methods for conveying a key to two gatherings who wish to trade information, without enabling others to see the key.

For two gatherings An and B, key conveyance can be accomplished in various courses, as takes after:

1. A can choose a key and physically convey it to B.

2. An outsider can choose the key and physically convey it to An and B.

3. On the off chance that An and B have beforehand and as of late utilized a key, one party can transmit the new key to the next, scrambled utilizing the old key.

4. On the off chance that An and B every ha a scrambled association with an outsider C, C can convey a key on the encoded connects to An and B.

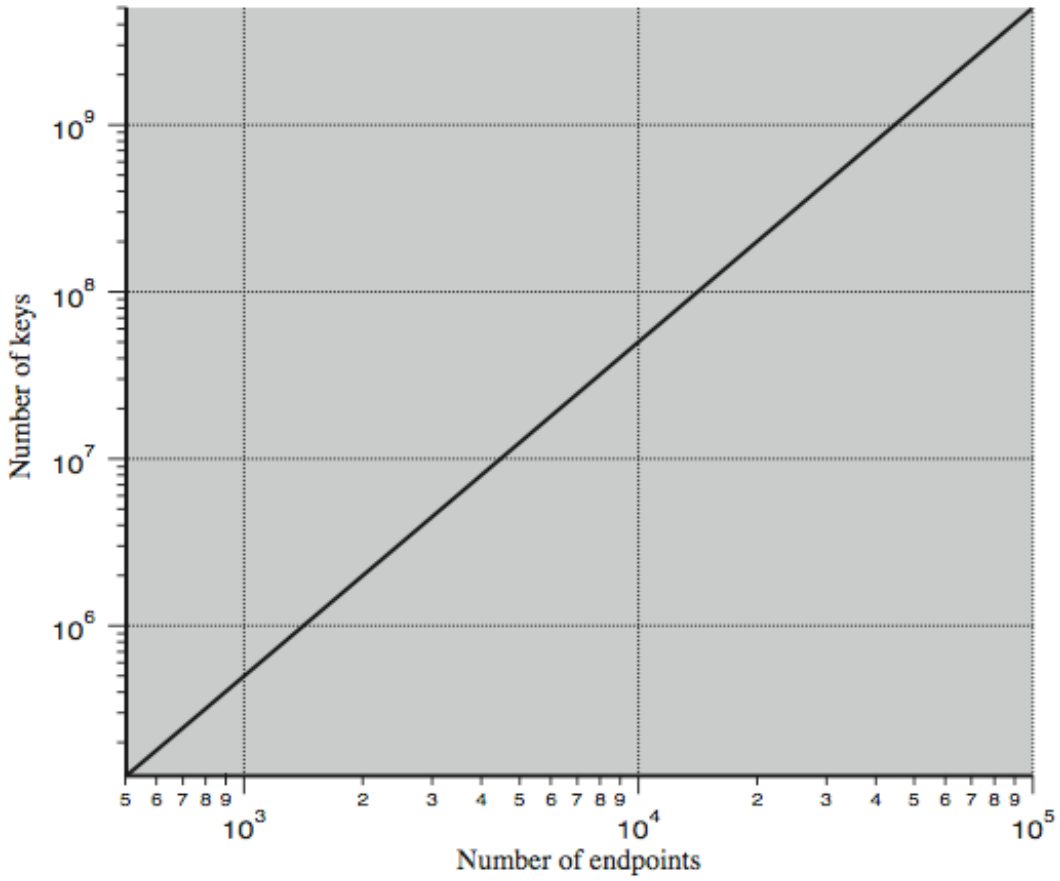


Fig.10

Choices 1 and 2 call for manual conveyance of a key. For connect encryption, this is a sensible necessity, in light of the fact that each connection encryption gadget will be trading information just with its accomplice on the opposite end of the connection. Be that as it may, for end-to-end encryption, manual conveyance is cumbersome. In a disseminated framework, any given host or terminal may need to take part in trades with numerous different hosts and terminals after some time. Consequently, every gadget needs various keys provided powerfully. The issue is particularly troublesome in a wide zone appropriated framework.

The utilization of a key circulation focus depends on the utilization of a chain of command of keys. At the very least, two levels of keys are utilized. Correspondence between end frameworks is encoded utilizing an impermanent key, frequently alluded to as a session key. Normally, the session key is utilized for the span of a consistent association, for example, an edge hand-off association or transport association, and afterward disposed of. Every session key is acquired from the key appropriation focus over the same systems administration offices utilized for end-client correspondence. As needs be, session keys are transmitted in scrambled frame, utilizing an ace key that is shared by the key appropriation focus and an end framework or client

Chapter-4

Algorithms

As the worthiness of wireless networks are increasing, more and more monitoring applications are implemented in order to accumulate data from network using nodes. mobility assumes a key part in such manner and has driven the improvement of numerous new developments. Clearly, developers must assess the effect of their conventions on network characteristics and break down the practices of the system under the proposed conditions. Reenactments of remote systems utilize a few parts basic to the precision of the recreations, a standout amongst the most vital being the decision of versatility demonstrate, which makes the development examples of portable hubs that structures the differing topology of the system. An average versatility display first places the portable hubs in their underlying areas and characterizes the way that the hubs move inside the system.

RANDOM WAYPOINT MOBILITY MODEL

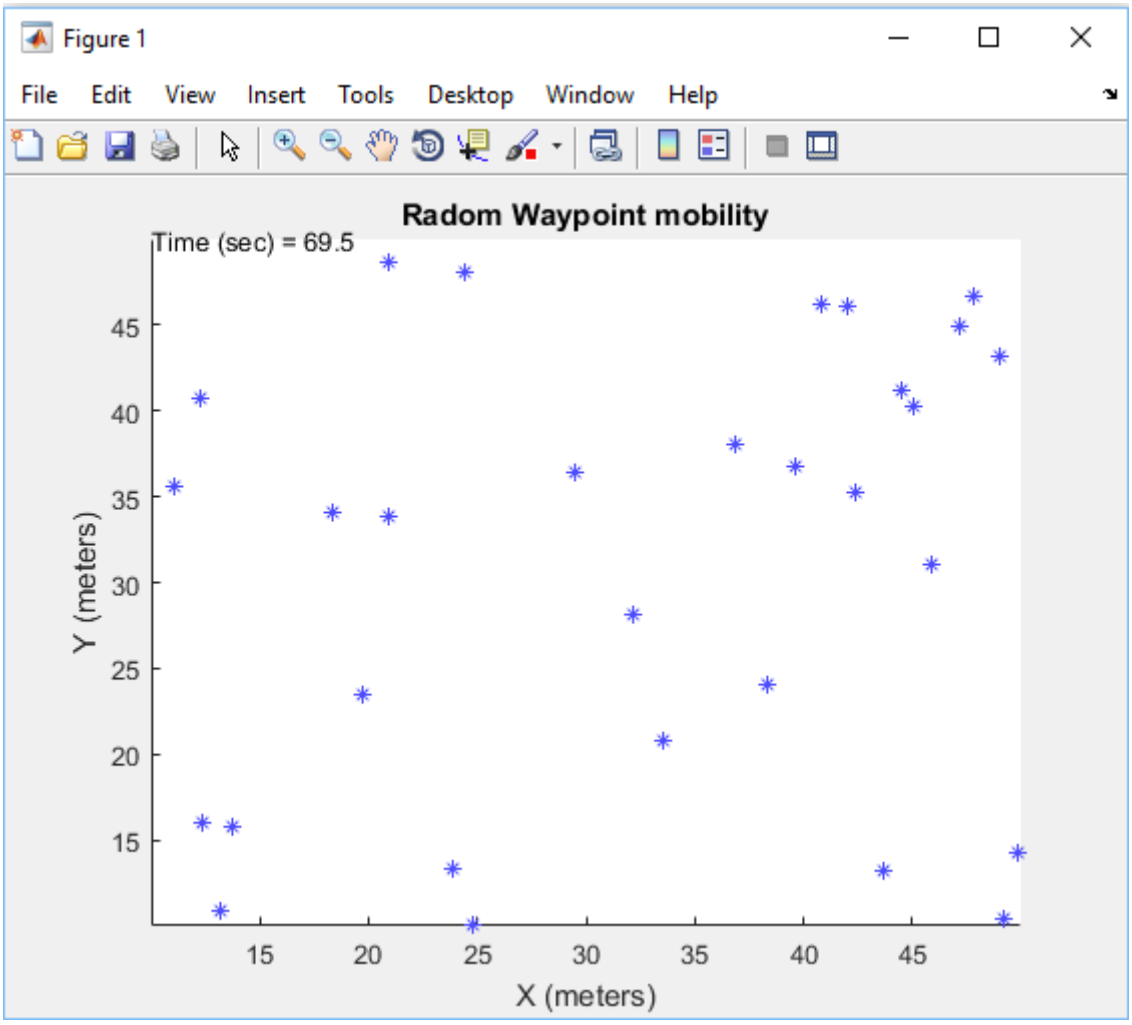
The random waypoint mobility model presents precise pause times between movements i.e. changes in direction and speed. An MN moves from one location to another after a certain period of time. As the time expires mobility node moves to the random position with different speed range [0, MAXSPEED]. It at that point goes towards the recently picked goal at the chose speed. Upon entry, the MN enjoys another reprieve before beginning the procedure once more.

To explain these movements we implement this model on a stimulator (MATLAB) and obtain different results.

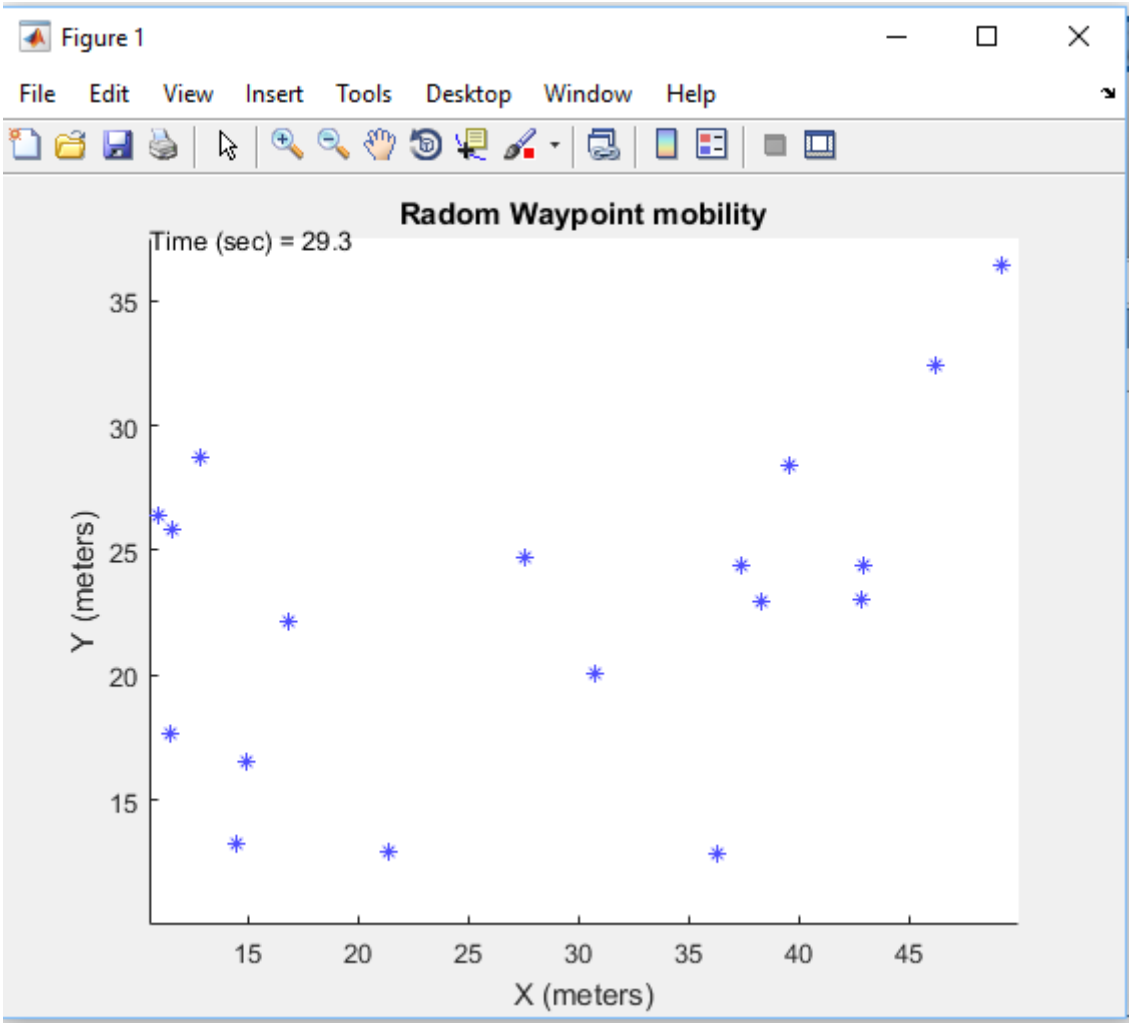
Chapter-5

Results and Performance Analysis

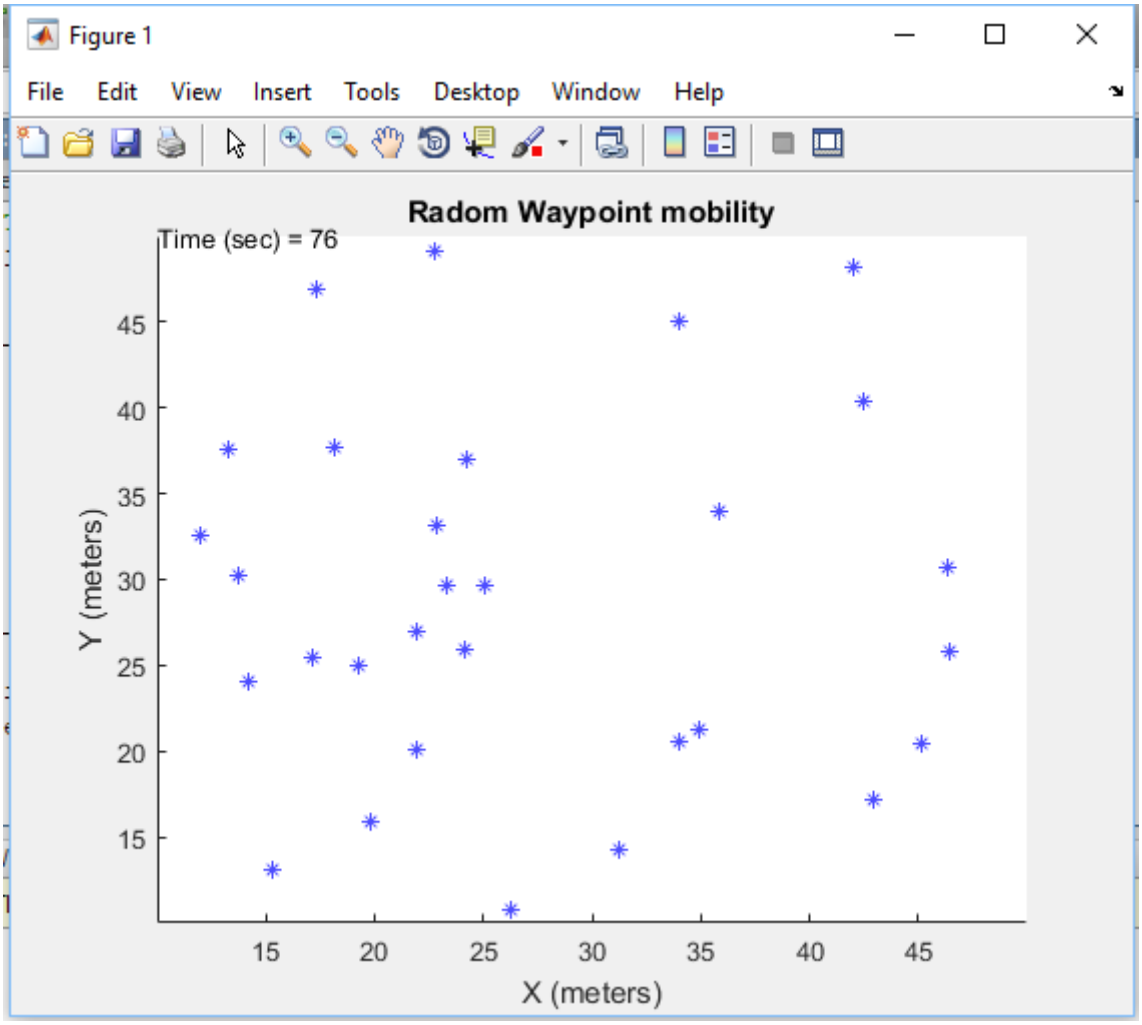
On the implementation of random waypoint mobility we have observed the different type of movement of nodes. They can be analyzed on the basis of their movement in term of speed interval, direction, pause time, position interval.



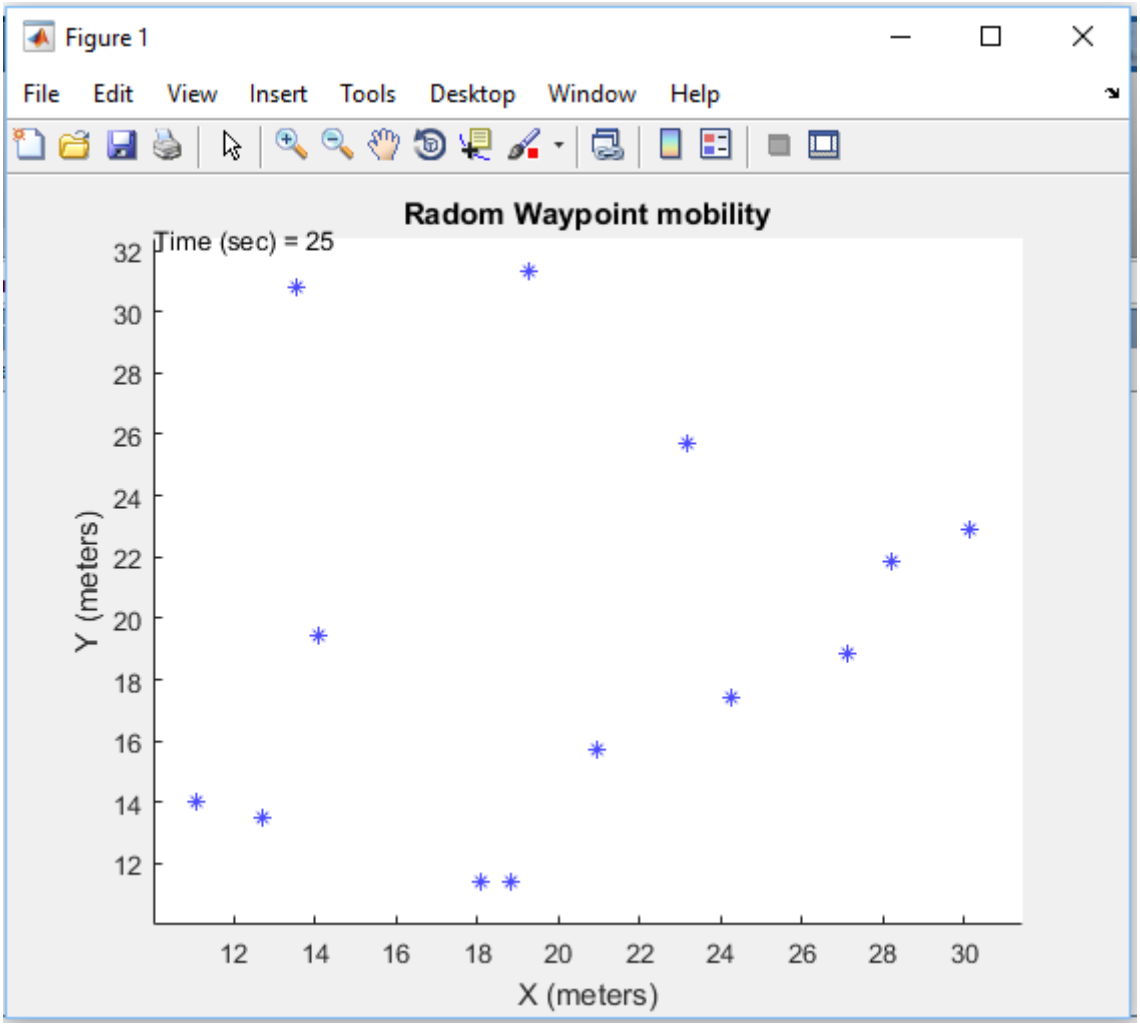
Observation of nodes in random waypoint mobility model at `POSITION_X_INTERVAL',[10 50 POSITION_Y_INTERVAL',[10 50]`



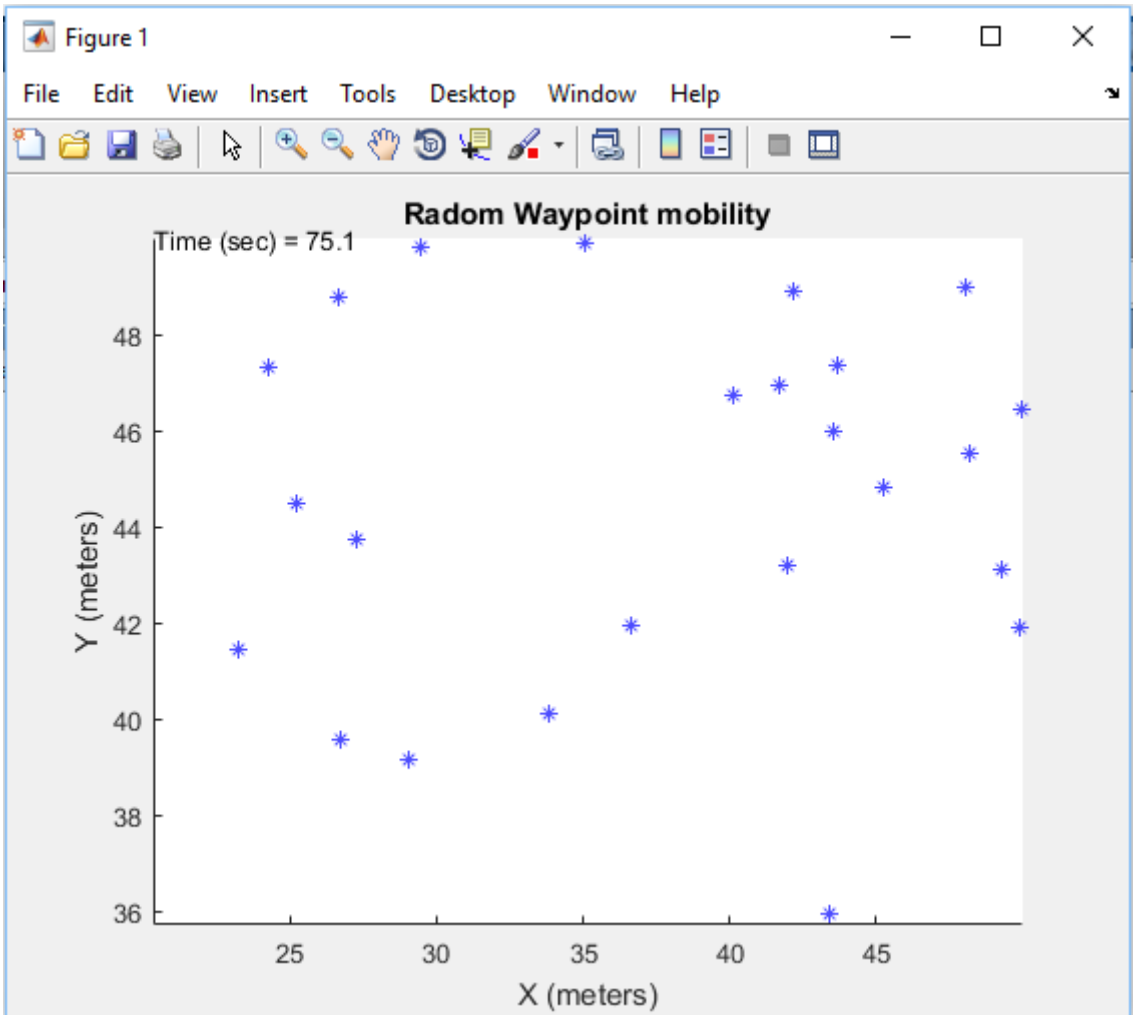
Observation of nodes in random waypoint mobility model at `SPEED_INTERVAL',[1.0 1.0]`



Observation of nodes in random waypoint mobility model at `SPEED_INTERVAL',[2.0 2.0]`



Observation of nodes in random waypoint mobility model at `WALK_INTERVAL',[3.00 7.00]`



Observation of nodes in random waypoint mobility model at `DIRECTION_INTERVAL',[-90 180]`

Chapter-6
Conclusions

Wireless interconnectivity of devices makes it easier to associate different type of network together. As the implementation of wireless network application is keep on increasing, in modern technological life, more and more employment of sensor nodes are involved. Hence the threat to data transmission increases. For the security of these information the concept of VCA is introduced into this paper. The VCA, which is issued by certificate authority, provides a complete node authentication so that the threat to the data breach can be rescued. In this project VCA resolved the issue of initial trust between the nodes by signing of certificates. Furthermore, VCA supports node authentication and a private key distribution mechanism. It also enhances many WSN design goals including simplicity, scalability, interoperability and control for individual manufacturers

REFERENCES

[1] Holohan, E.Schukat, M., "Authentication Using Virtual Certificate Authorities: A New Security Paradigm for Wireless Sensor Networks", proceedings of 9th IEEE International Symposium on Network Computing and Applications (NCA), Cambridge, pp:92 - 99,2010.

[2] S. Choi, V. Sarangan, J. Thomas, S. Radhakrishnan, "Secure Access Control Protocol for WSNs with internetwork roaming", proceedings of the 35th Annual IEEE Conference on Local Computer Networks, Colorado, pp: 256 - 259, 2010.

[3] S. Camtepe and B. Yener, "Key Distribution Mechanisms for Wireless Sensor Networks: a Survey", Rensselaer Polytechnic Institute, Troy, March 2005.

[4] Donggang Liu, Peng Ning,"Multilevel TESLA: Broadcast authentication for distributed sensor networks", ACM Transactions on Embedded Computing Systems, Volume 3, Issue 4, pp: 800 - 836, 2004.

[5] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol", RSA CryptoBytes, vot. 5, 2002.

[6] F.Hess, "Efficient identity based signature schemes based on pairings", in Proc. SAC., St.John's, Newfoundland, Canada, August2002.

[7] D.Johnson and A.Menezes,"The elliptic curve digital signature algorithm ecdsa", University of Waterloo, Canada Technical Report CORR99-34, August 1999, updated 2000102/04.1007

[8] IEEE Computer Society. IEEE 802.15.4 Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specification for LowRate Wireless Personal Area Networks (LR-WPANs), May 2003.

[9] ZigBee Alliance. ZigBee Specification, Dec 2004.

[10] Heile, B. The ZigBee Alliance. Now and Tomorrow.The Wireless Japan Expo, Tokyo,. July 2009.

[11] M. Knight. Wireless security - How safe is Z -wave? Computing & Control Engineering Journal, Volume 17, Issue 6, Dec.-Jan. 2006, pages 18 - 23.

[12] T. Lennvall, S. Svensson and F. Hekland. A comparison of Wireless HART and ZigBee for industrial applications. In International Workshop on Factory Communication Systems 2008 (WFCS 2008).

[13] Koopman, P. Embedded Internet & Security Overview. 18-649 Distributed Embedded Systems. Carnegie Mellon, April 25, 2009.

[14] Certicom. Securing sensor networks, getting it right from the start, with public key. March 2006.

[15] R. Rada et al. HIPAA Best Practices and Best Tools. HIMSS 2002 Conference Proceedings, Atlanta, GA Jan. 27-30, 2002.

[16] J. D. Hart. Internet Law: A Field Guide. Bna Books 2007. ISBN: 1570186839. [10] K. Papadopoulos. Sensor networks security issues in augmented home environment. IEEE International Symposium on Consumer Electronics, 2008 (ISCE 2008).