Authentication of node in Wireless Integrated Sensor Networks using Certificate Authority

Shruthi N[1], Seema Kousar[2]
[1&2] UG Students Dept. of Computer Science and Engg,
RajaRajeswari College of Engineering,
Bangalore, India.

Anitha K[3]
[3]Asst. Professor Dept. of Computer Science and Engg,
RajaRajeswari College of Engineering,
Bangalore, India.

***Abstract*—Wireless Sensor Networks collects the information from the environment. It consists of large number of Sensor Nodes. To implement a security during the transmission of data from one node to another node, WSNs will use different security techniques. In sensor network Authentication is an essential requirement to maintain a security in the network. Using Wireless Sensor Networks it's difficult to secure due to its dynamic nature. Integrating Wireless Sensor Networks are using to analyse the security issues with mobile networks and can combining both networks to utilize their capabilities and it solves the security issues and 'To' address problem of authentication in WSNs. In propose work, providing an efficient and secure framework which provides authentication to a roaming sensor node. And it allows a sensor node to move across multiple WSNs to solve the issues of Authentication. Encryption and Decryption techniques are provided to secure the data while transmitting data from one node to another. In propose work key management technique are used to provide authentication by using Virtual Certificate Authority.**

***Keywords*— *WSN, Mobile Network, Authentication, VCA*.**

I. INTRODUCTION

Wireless Sensor Networks is a collection of information from the environment. It consists of many sensor nodes, it gathers the sensed the information then put it into processor to perform and then start communication from one node to another. WSN can be used in many fields like residential control, industrial control, patient monitoring, and asset management in a short range. There is a need for security solutions that have not been addressed. The authentication protocol proposed which is Virtual Certificate Authority (VCA) can help to address the problem by providing initial trust between network nodes.

Recently, the convergence of the various communication technologies [2] such as Third Generation mobile communication networks, wireless sensor networks (WSNs), wireless local area network (WLAN) and mobile WiMAX and there are several efforts are continuously progressing for their consolidation. Integration works has been mainly progressing around the mobile networks by simply connecting the sensor networks to the wide area networks (WANs) to provide basic services based on WSN gathered information. As per of security, although deploying the mobile networks for the intermediate connections between WSNs and WANs could reduce the communication overhead of WSNs, since the differences of communication capabilities such as the bandwidth, the range, and the speed between the mobile network and the WSNs are quite significant, there still exists some limitations and inefficiency.

Therefore the motivation is to bring the more benefits from the consolidation of WSNs and mobile network. In propose system provides an efficient and secure authentication protocol between sensor nodes and the mobile network which is VCA. The main approach concentrates on how to minimize the energy consumption and inefficient message transmission in wireless sensor network. Virtual Certificate Authorities can be used for Authentication and well established PKI concepts and designed specifically for constrained devices on distributed ad-hoc networks.

II. BACKGROUND

A. Related Work

Some authentication protocol in WSN has been designed such as μTESLA (Timed Efficient Stream Loss-tolerant Authentication) [10] is an efficient broadcast authentication protocol with low communication and computation overhead. Protocol requires symmetric cryptographic techniques. But it is not applicable in large sensor networks. DOS attacks are there so that the authentication takes time in μTESLA. TESLA requires loose time synchronization between the sender and the receivers. To avoid this problem later muti-Ievel μTESLA [7] was proposed.

Multilevel key chain is applied in a large WSN. Multilevel μTESLA removes the requirement of unicast based initial communication between base station and to increase the lifetime, it uses sensor nodes Multi level chain. Authentication delay is the limitation of this scheme. Key establishment is very difficult task for WSNs. Lot of Key distribution techniques are proposed for solving the problem of authentication in WSN. An authenticated key management protocol for WSN is implemented using Elliptic Curve Cryptography [9] and symmetric key operations. Elliptic Curve Cryptography provides authentication and key generation between two nodes, but it does not consider a network with tiered architecture.

Elliptic Curve cryptography (ECC) has been proposed for Public Key Cryptography (PKC) to solve the problem of authentication in WSN. But ECC based schemes has high energy consumption. The ID based signatures [9], lead to a high computation cost and thus high energy consumption. It is an efficient identity based cryptography technique which

provides online/offline signature schemes. It is quick broadcast authentication and user authentication. Due to size of the signature the communication cost is high. Elliptic Curve Digital Signature Algorithm (ECDSA) [11] requires two point multiplications in order to verify signature.

The pairing is time consuming operations. This scheme has been proposed for secure resource-constrained sensor networks. This is very expensive operation in terms of computational and memory requirements. AVCA [1], a virtual certificate authority, address the issue of initial trust in more detail and solves the issue of initial trust via the structured signing of certificates. It presents AVCA, an authentication solution based on virtual certificate authorities. Third Generation Partnership Project (3 GPP) provides authentication protocol which is authentication and key agreement (EAP–AKA) [5] for secure interworking. It provides mutual authentication between the user equipment (UE) and the authentication, authorization, accounting server The EAP-AKA provides a mutual authentication and guaranty the generation of cipher and integrity keys. Thus, EAP–AKA perform authentication and key agreement procedure between 3GPP and WLAN. Similarly, EAP–SIM [8] is also used to authenticate a user for WLAN access using GSM networks via the SIM card. There are several on-going researches such as [4, 6] enhancing the security of EAP–AKA and EAP–SIM.

B. Performance Evaluation

In wireless sensor network, it is difficult to directly implement the existing security approaches to the area of wireless sensor networks. Sensor network consists of many sensor nodes, has a small battery operated devices, which communicate with more base station, which connects the outside network [12]. The sensor networks have limited processing power, storage and bandwidth and energy and have limited computational and communication resources. The WSNs node consists of 8-bit 4-MHz processors with slow 10-Kbps communication and 8-Kbyte read-only memory and a 512-byte RAM. Therefore it requires more efficient and secure authentication protocols for authentication. This paper evaluates the performance of VCA in terms of memory cost (code size), authentication delay, and power consumption and compare this technique with other authentication protocol [13]. VCA Current consume by wireless module (node to base) [14] at 0 dbm is 21.2 mA and Voltage at node is 3.3 V. Power consume by node = VI =3.3*21.2 =69.96 mwatt =70m watt.

The size of packet is 65 byte, in 1 Second 50000 bits is transmitted. For authentication, no. of bits= 160, for 160 bits time required= 160/50000= 0.32ms (Transmission time) and processing time is=2ms. Total time Require for authentication is=0.32+2=2.32ms. The overall Cost (Time/energy) = 2.32ms /69mwatt. Performance percentage or number of nodes compromised when a single node is captured before it is able to remove any redundant information such as an already used key from its memory. In key distribution technique key is stored on node so node can easily compromised but in VCA private is not on network so it become difficult to temper. So we can said that resilience is 0%. Scalability is evaluating the maximum amount of nodes supported by the network; higher values mean better and VCA is more scalable than other techniques.

III. EXISTING SYSTEM

Different security techniques are used implement security during the transmission of data from one node to another node. Authentication is an essential requirement to maintain security in sensor network. Using Wireless Sensor Networks, security is very difficult due to its dynamic nature.

IV. PROPOSED SYSTEM

In proposed work, providing an efficient and secure framework which provides authentication to a roaming sensor node. And it allows a sensor node to move across multiple WSNs to solve the issues of Authentication. Encryption and Decryption techniques are provided to secure the data while transmitting data from one node to another. In propose work key management technique are used to provide authentication by using Virtual Certificate Authority.

A. System Architecture

In fig: 1 GVCA (Global Virtual Certificate Authority) is the trusted party between the TC and the MCA. GVCA generates a certificate along with signature when it receives certificate request from the TC. MCA (Manufacturer's Certificate Authority) is the trusted third party between TC and ED. MCA receives the certificate verification from the Receiver node. ED (End devices) are divided as sender node and receiver node. Each of the end devices needs to authenticate by using GVCA. ED sender node needs to be request a certificate and ED receiver node needs to verify the signature on a certificates. TC (Trusted Centre) acts as a trusted third party, it's responsible for distribution and implementation of network area control. In Fig. 1 dotted line represents virtual association relationship and straighten line represents a real association relationship. Authentication is very important for sensor nodes that send a data and confidentiality of sensitive data. Virtual Certificate Authority, it provides an initial trust between nodes. The VCA will solve the certificate issues, it is done by creating and verifying certificates. While generating Certificate itself signer is implemented, so it reduces the overhead in WSNs. This scheme is based on PKI architecture and this mechanism is particularly designed for resource constrained devices on distributed ad-hoc networks

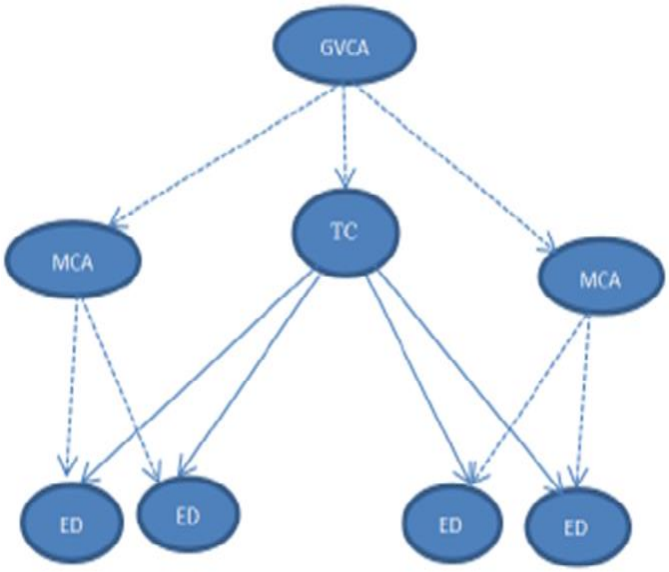

Fig: 1 Virtual Certificate Authority network

VCA architecture does not store the basis for initial trust on any of the sensor devices and hence the devices do not require significant memory. If a device needs to authenticate itself to others on a standard PKI network, then it must provide a certificate that can be verified by the other device. In case if certificate does not signed by a trusted third party then it must contact that trusted third party and request a signature.

The VCA is not a physical device, within the context of VCA at least, it can be considered as fully functional Certificate Authority (CA) with its own address, private-public key pair and its own certificate. It has the responsible for the verification and the signing of other devices certificates. VCA act as the trusted third party while verifying devices and it solves the initial trust between nodes in sensor network. It describes the basic functionality of VCA architecture in which the mobile device has ability to authenticate sensor nodes. VCA defines several different device types.

B. Proposed Methodology

In Fig. 2 shows the association relationship between VCA and End Devices. End Devices can be considered as a Sender node and Receiver node. Association procedure has methodology as follows

1. Request a Certificate
2. Generate a Certificate
3. Distributing a Certificate
4. Signing a certificate
5. Verifying a Certificate

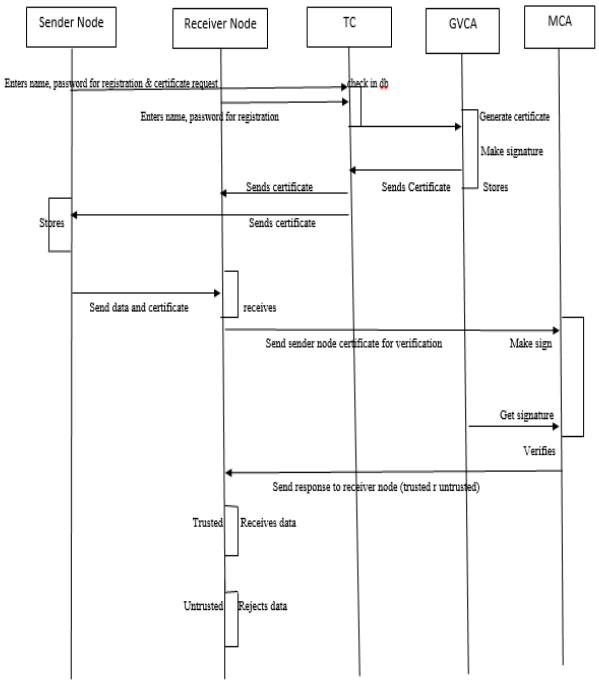

Fig. 2 VCA End Devices Association Procedure

1. Request a Certificate:

Sender node requests a certificate by entering the user name, password and registration. There is no direct connection between ED and GVCA. Sender request a certificate via TC.

2. Generate a Certificate:

When GVCA receives the certificate request from the TC then it generates certificate. Then it sends a generated certificate to the TC.

3. Signing a Certificate:

GVCA provides the signature in the digital format to solve the initial trust between nodes in a sensor network. Then GVCA provides its private key to match the signature with other nodes in verification.

4. Distributing a Certificate:

TC act as trusted third party between End Devices and GVCA. TC main work is to receive certificate request from the ED and distribute the GVCA generated certificate to the ED. After receiving the certificate sender node sends the data and certificate to the receiver node.

5. Verifying a Certificate:

When receiver node receives the message from the sender node it sends the sender node certificate to the MCA to verify the sender node are trusted or untrusted. To verify certificate MCA make signature for the certificate by using GVCA public key. Then verify this signature with the GVCA. After verification it send response to the receiver (trusted or untrusted).

V. ALGORITHM

A. *Encryption algorithm*

Begin
Pick random big Integer P and Q value (i.e that must be probable prime number)
Compute N
Pick random big Integer K value (i.e the value between (1-n-1)
Compute B1=K*P;
Then compute M value (i.e get the plain text in form of bytes means plaintext.getBytes)
Compute B2=M+B1
For end
Encrypt message = B1 , B2
End

B. *Decryption algorithm*

Begin
Pick the encrypted msg
Then split the msg by (,)
Get the split[0] value as B1 value and
Split[1] value as B2 value
Then
Compute M value(i.e M=B2-B1)
Convert m value into byte Array
For end
Get the decrypted msg
End

VI. CONCLUSION

In proposed work introduced the technique Encryption and Decryption, so the data should be secured in Sensor Networks while transmitting data from one node to another node. Authentication is an efficient and secure framework which provides authentication to a roaming sensor node. And it allows a sensor node to move across multiple WSNs to solve the issues of Authentication. Integrating Wireless Sensor Networks are used to analyse the security issues with mobile networks and can combined both networks to utilize their capabilities and it solves the security issues and 'To' address problem of authentication in WSNs. In proposed work introduces the concept of Virtual Certificate Authority, it solves trust between nodes by generating certificate along with signature. And also VCA provides a digital signature along with private key distribution for verification of signature in other node.

REFERENCES

[1] Manjula M. Ramannavar1, Monica M. Jagtap2 "Authentication in Wireless Sensor Networks Using Virtual Certificate Authorities." 1 Gogte Institute of Technology, Belgaum 2 Dr. Daulatrao Aher College of Engineering, Karad 2013 727

[2] K. Han1 K. Kim1 J. Park2 T. Shon3 "Efficient sensor node authentication in third generation-wireless sensor networks integrated networks" In Special Issue on Distributed Intelligence and Data Fusion for Sensor Systems 2011.

[3] 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.

[4] Mun, H., Han, K., Kim, K.: '3G-WLAN interworking: Security analysis and new authentication and key agreement based on EAP-AKA'. Proc. 2009 IEEE Wireless Telecommunications Symp. (WTS 2009), Prague, Czech Republic, 22–25 April 2009

[5] Arkko, J., Haverinen, H.: 'Extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA)'. Technical report draftarkko- eap-aka-kdf-10, November 2008

[6] Tseng, Y.-M.: 'USIM-based EAP-TLS authentication protocol for wireless local area networks' (Computer Standards & Interfaces, November 2007).

[7] 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.

[8] Haverinen, H., Salowey, J.: 'EAP-SIM authentication'. Technical report draft-arkko-pppext-eapsim- 12, IETE, October 2003.

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

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

[11] D.Johnson and A.Menezes,"The elliptic curve digital signature algorithm ecdsa", University of Waterloo, Canad Technical Report CORR99-34, August 1999, updated 2000102/04.

[12] StefaanSeys and Bart Preneel," Security Issues for Distributed Sensor Networks",http://homes.esat.kuleuven.be/~sseys/docs/phd_symposium_2003_abstract.pdf

[13] David Boyle, Thomas Newe, "Securing Wireless Sensor Networks: Security Architectures" JOURNAL OF NETWORKS, VOL. 3, NO. 1, JANUARY 2008.

[14] CC2500 Single Chip Low Cost Low Power RF Transceiver, PRELIMINARY Data Sheet (Rev.1.2).