Secure Authentication Technique in Wireless Integrated Sensor Network: Virtual Certificate Authority

Rashmi P. Fulare[1], **Apeksha V. Sakhare**[2]

[1&2]Department of Computer Science and Engineering, G. H. Raisoni
College of Engineering, Nagpur, India

Abstract

Wireless sensor network wireless sensor networks are continuously growing, so does the need for effective security mechanisms. WSN consists of large number of Sensor Nodes (SN). During the transmission of data from one node to another node, different security techniques are used. But the Wireless Sensor Networks are very difficult to secure due to its mobility. So that to analyze the security issues that arise try to solve by integrating Wireless Sensor Networks (WSN) with the mobile network. This is enabling us to experience variety of applications based on multi-sensor attached mobile network. The enhanced security procedures are operated through the mobile network in order to maximize the lifetime of the sensor networks and to apply the combined capabilities of both networks. This paper presents such mechanism to provide security for the data while allowing a sensor node to move across multiple WSNs. The proposed key management technique to provide secure authentication is by using Virtual Certificate Authority (VCA). It provides a solution to overcome the difficulties in securing the networks.

Keywords: WSN, Mobile Network, Authentication, VCA.

1. INTRODUCTION

Wireless sensor network (WSN) consist of Wireless sensor network(WSN) which consist of many sensor node which are limited in computation, storage and energy , can gather data in the distributed area, then process and transport data to users. WSN has a wide range of applications including residential control, industrial control, patient monitoring, and asset management.

Recently, the convergence of 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. However, such 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. From the aspect of security, although deploying the mobile networks for the intermediate connections between WSNs and WANs could reduce the communication overhead of WSNs. The integration of wireless sensor networks (WSNs) and mobile networks are enabling us to experience variety of ubiquitous applications and we can utilized capability of both network.

Therefore our motivation is to bring the more benefits from the consolidation of WSNs and mobile network. We propose an efficient and secure authentication protocol between sensor nodes and the mobile network which is VCA. Our approach concentrates on how to minimize the energy consumption and inefficient message transmission in wireless sensor network.

This paper presents “Virtual Certificate Authorities(VCA) for Authentication”, which is based on commonly based on PKI concepts and designed specifically for resource constrained devices on distributed ad-hoc networks. The rest of this paper is organized as follows: previous related work is discussed in Section 2. Our proposed Scheme are explained in Section 3. Performance evaluation is discussed in section 4 and advantages in 5. We conclude our paper in Section 6.

2. RELATED WORK

Some authentication protocol in WSN has been designed such as TESLA (Timed Efficient Stream Loss-tolerant Authentication) [10], an Efficient broadcast authentication protocol with low communication and computation overhead. But it is not applicable in large sensor networks. More DOS attacks are there so that the authentication is delayed in TESLA. TESLA requires loose time synchronization between the sender and the receivers. To avoid this problem later multilevel TESLA [7] was proposed. Multi-level key chain is applied in a large WSN.

Multi-level TESLA removes the requirement of unicast based initial communication between base station and sensor nodes ,Multi level chain is used for increasing the lifetime. The limitation of this scheme is that it suffers from authentication delay.

An authenticated key management protocol for WSN is implemented using Elliptic Curve Cryptography and symmetric key operations. This scheme provides authentication and key generation between two nodes, but it does not consider a network with tiered architecture. Elliptic Curve cryptography (ECC) [9] 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 [9,11], 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.

Lot of Key pre-distribution techniques are proposed for solving the problem of authentication in WSN. Key pre-distribution schemes [4, 6] as they require a significant memory cost and a certain threshold of devices in the distributed network.

LEAP is a key management protocol for sensor networks that is designed to support in–network processing. . LEAP supports four types of key for each sensor node. LEAP also includes a protocol for broadcast authentication. LEAP is designed to support security service such as confidentiality and authentication .It has some drawback such as it assumes that sink node is never compromised. it cannot completely prevent the DoS attacks .LEAP is that it only works in static environment. SPINS is authentication scheme based on random key pre-distribution was never fully completed and implemented. Key pre distribution schemes as they require a significant memory cost.

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.

TinyECC[5] is a building block of broadcast authentication protocol based on digital signature. It provides a digital signature scheme (ECDSA), a key exchange protocol (ECDH), and a public key encryption scheme (ECIES). Application of TinyECC in large sensor networks will be limited to a few nodes with more memory support . It has the scalable problem. TinyECC is not suitable for very frequent broadcast authentication.

TinySec is a lightweight and an efficient link-layer security protocol that is adapted to the sensor networks, [8]. It provides three basic security features: Access Control, Message Integrity and Message Confidentiality for. The drawback of Tinysec is Tinysec packets are longer than normal WSN packets. So extra computation and energy are needed for cryptography. Tinysec does not attempt to protect against replay attacks.

3. PROPOSED WORK

3.1 Wireless Integrated Sensor Network

There are several efforts of integrating mobile network and WSN. In this scenario, the mobile network is deployed at the intermediate part in the network. While the communication is through WSNs at the end points, the intermediate communication is through the mobile network. There are the significant performance gaps between WSN and mobile network which show limitation of the overall network performance because of the weaker capability of the sensor network.

Thus, our main motivation is to overcome such difficulty and maximize the synergy of interworking between mobile network and WSN networks by concentrating on the most procedures for the authentication of the sensor nodes into the mobile network communication. Figure 1 shows our proposed model that the sensor attached smart phone communicates to the authentication server via mobile network, and directly communicates to the sensor. In the architecture, the sensor network can be a kind of third party application in the mobile network applying authentication using the VCA.

Authentication using VCA is integrated with mobile network in order to increase the range of coverage of the nodes. We defined here the two cases of the network as follows:

Case1: The WSN environment that communications like raw data sensing, control and data transmission under sensor network are operated by sensor nodes. In this case, due to the longer hop distance it invokes more energy consumption. When the hop distances are increased, the energy cost is also increased for the authentication as in Table 1.

Case 2: Proposed integrated WSN networks that the sensor network is integrated as one of applications of mobile networks. Such integration provides the more efficiency in the authentication process. Since the information for the mutual authentication between mobile device and sensor network is transmitted under the mobile network and the communication in the sensor network is only necessary for the direct communication between mobile and sensor network.

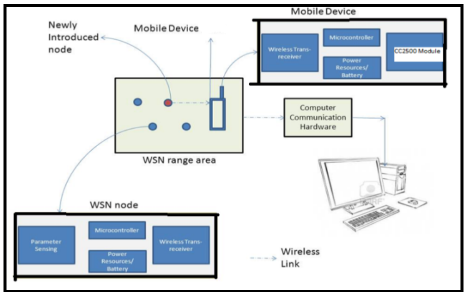


Figure 1 Integrate sensor network as one of application into mobile network

Table 1: Comparison

Parameter	Case 1	Case 2
Network model	WSN	Integrated WSN
WSN Integrated as	Network	Application
Required number of nodes for authentication	>1	1
Total message required	More	Less
Total energy consumption	More	Less
Range	Low (30-50 m)	High (3-5 km)

3.2 Authentication Using Virtual Certificate Authority

Authentication of sensor nodes that supply data and confidentiality of sensitive data are very important. Virtual Certificate authority will provide an initial trust between nodes. The VC authority will issue the certificate to each node. This is done by creating and verifying certificates. Certificate of the device and certificate of the signer are implanted at the time of deployment. So it reduces the overhead. It is based on PKI architecture and this mechanism is particularly designed for resource constrained devices on distributed ad-hoc networks. VCA [3] 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 another on a standard PKI network, the first step is to provide a certificate that can be verified by the other device. If it doesn't have a certificate signed by a trusted third party 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 is considered to be a fully functional Certificate Authority (CA) with its own address, private-public key pair and its own certificate. It is responsible for the verification and the signing of other devices' certificates. The VCA can act as the trusted third party to verify devices and act as a basis for initial trust.

We have two devices shown in figure 2 and their association to other devices which indicates that these two devices are virtual authority. The GVCA stands for Global Virtual Certificate Authority and it is the trusted third party between the TC and the MCA. The second virtual device i.e., Manufacturer's Certificate Authority (MCA), is the trusted third party between the TC and the MED. This section describes the basic functionality of VCA architecture in which the mobile device has ability to authenticate sensor nodes. The BS (Base Station) is one device that is responsible for starting the network. This device is responsible for Key Management, Key Distribution and implementation of a network access control policy. This device is called as Trust Center (TC). A MED are End Devices needs to be able to request a certificate, verify the Signature on a certificate. Each of them needs to be authenticated by the Global VCA. Each device has some basic functionality such as ED needs to be able to request a certificate, verify the signature on a certificate as well as partake in a challenge and response procedure. In addition, an MCA is required to be able to sign certificates.

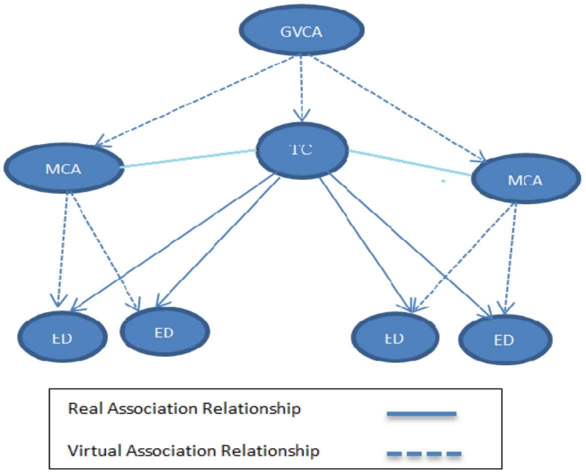

GVCA
MCA
TC
MCA
ED
ED
ED
ED
Real Association Relationship
Virtual Association Relationship

Figure 2 Networks of Virtual Certificate Authorities

3.2.1 Requesting a Certificate

Due to the nature of the infrastructure, every device must have its own certificate. ED that has just been powered on, or comes into range of a network, can request the certificate of a MCA from the same manufacturer, signed by a known CA, without having any specific data. For this the requesting device need to specify manufacturer's id in the one request This is very significant because it means that a typical end device needs only to know its own certificate and that of a trusted GVCA.

3.2.2Verifying a Certificate

The certificate verification plays a vital role in the overall authentication procedure. The verification of a certificate implies that the data on the certificate presented is correct and can be trusted. The verification process involves using the VCA's public key or MCA's public key to verify the certificate.

3.2.3Challenge and Response

Once the certificate is verified, it is proven that the trusted third party trusts the information on the certificate. It does not necessarily mean that the device presenting the certificate actually owns it. To eradicate this possibility and authenticate the device, a challenge and response procedure has to be undertaken. There are many different proven challenge response mechanisms which utilize public key encryption and cryptographic nonce. By verifying the certificate and performing a successful challenge and response procedure one device can determine that the certificate is valid and that the device presenting it has the private key. At this stage the device can be considered authenticated.

Ex.- Challenge would be
Y=2X+1
Then,
Response is expected from requesting node is
X=0; Y=1,
X=1; Y=3,
X=2: Y=5.

3.2.4 Signing a Certificate

On receipt of a signature request, the MCA must authenticate the initiating device before it signs the certificate. Upon successful authentication of this device, the MCA can then sign the certificate presented. The newly signed certificate is then sent to the requesting device.

3.2.5 Certificate Revocation

Certificate revocation is intended to convey a complete withdrawal of trust certificate and thereby protect the people using a site against fraud, eavesdropping, and theft. There are varying levels of verification a third-party Certificate Authority (CA) may carry out. Sometime a certificate need to be revoked when it has had its private key compromised or the owner of the certificate no longer controls the certificate was mistakenly signed. An attacker with access to an un-revoked certificate who also has access to the certificate's private key can perform a man-in-the-middle (MITM) attack by presenting the certificate to unsuspecting users. Its revocation will prevent all type unauthorized access. This revocation can be performed by refreshing certificate on demand.

3.3 VCA End Device Authentication

In this authentication mechanism that allows two devices that have no prior knowledge of each other to perform secure authentication. The MCA can establish the address of the TC from the beacon. It will request the TC's certificate signed by a trusted third party (the GVCA). The MCA will then verify the TC's certificate by using the GVCA's public key. On successful verification of the TC's certificate it can initiate a challenge and response procedure using the TC's public key. This is illustrated in Figure 3

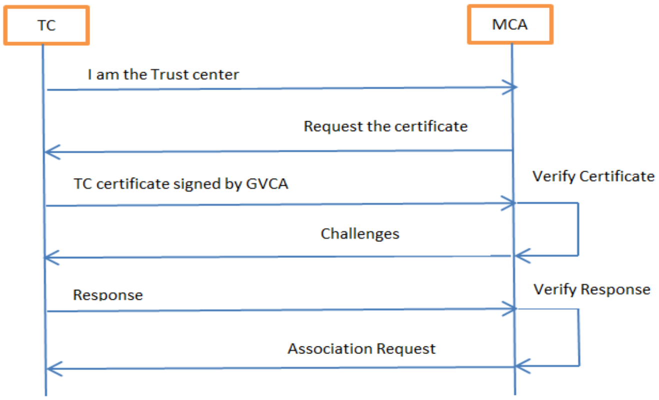


Figure 3 VCA end device authentication procedure

3.4 VCA End Device Association

In this authentication procedure, MCA authenticates the TC as described above and requests to associate to the network. The TC then authenticates the MCA and authorizes it to associate. Before the MED joins the network, an MCA from that device's manufacturer must first join the network. The MED issues a per-authentication request to the TC for a certificate of an MCA device. The MCA passes two parameters in the certificate request:

I. The manufacturer's id and

II. The address of the trusted GVCA

The TC does not have this certificate. It has previously authenticated an MCA from the same manufacturer. It requests this certificate from the MCA. This certificate has been implanted on the MCA which forwards it to the TC which in turn forwards it to the unauthenticated MED which finally authenticates the MCA and the process continues as shown in the Figure 4

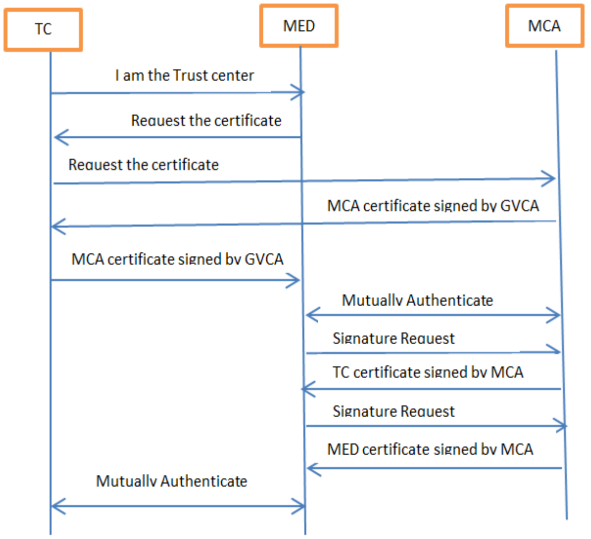


Figure 4 VCA end device association procedure

4. PERFORMANCE EVALUATION

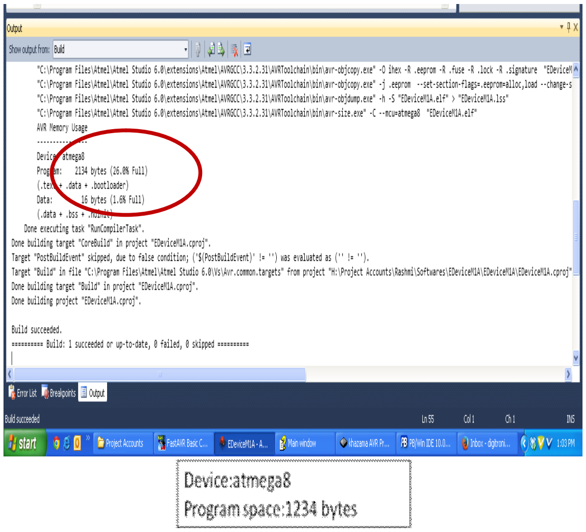
In wireless sensor network, it is difficult to directly employ the existing security approaches to the area of wireless sensor networks due to resource constraints. Therefore, to develop useful security mechanisms for WSN. One typical sensor network consists of nodes, small battery powered devices, which communicate with more powerful base station, which in turn connected to the outside network [12]. The sensor networks have limited processing power, storage and bandwidth and energy and have limited computational and communication resources. Sensor node typically consists of 8-bit 4-MHz processors with slow 10-Kbps communication and 8-Kbyte read-only memory and a 512-byte RAM. So there is a need for new more efficient and secure authentication protocols.

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[15] in table 2. In VCA Current consume by wireless module(node to base)[16] at 0 dbm is 21.2 mA and Voltage at node is 3.3 V. So Power consume by node = VI =3.3*21.2 =69.96 mwatt =70m watt. If size of packet is 65 byte, in 1 Second 50000 bits is transmitted . For authentication no. of bits= 160 is required. For 160 bits time required= 160/50000= 0.32ms(Transmission time) and processing time=2ms. Total time Require for authentication is =0.32+2=2.32ms. The overall Cost(Time/energy)= 2.32ms/69mwatt.

Resilience is 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 other 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 .

4.1 Memory

Figure 6 shows the memory consumption of protocols such as SPINS, Tinysec, Minisec, LEAP and VCA. The VCA uses RC5 block cipher for CBC-MAC and encryption. Figure 5 shows the program space required was about 2.134 KB, and it consumed around 1 KB of EPROM to store certificate. Protocols SPINS occupy 2KB memory and protocol LEAP occupy 17.5KB memory.



```
        "C:\Program Files\Atmel\Atmel Studio 6.0\extensions\Atmel\AVRGCC\3.3.2.31\AVRToolchain\bin\avr-objcopy.exe" -O ihex -R .eeprom -R .fuse -R .lock -R .signature  "EDeviceM
        "C:\Program Files\Atmel\Atmel Studio 6.0\extensions\Atmel\AVRGCC\3.3.2.31\AVRToolchain\bin\avr-objcopy.exe" -j .eeprom  --set-section-flags=.eeprom=alloc,load --change-s
        "C:\Program Files\Atmel\Atmel Studio 6.0\extensions\Atmel\AVRGCC\3.3.2.31\AVRToolchain\bin\avr-objdump.exe" -h -S "EDeviceM1A.elf" > "EDeviceM1A.lss"
        "C:\Program Files\Atmel\Atmel Studio 6.0\extensions\Atmel\AVRGCC\3.3.2.31\AVRToolchain\bin\avr-size.exe" -C --mcu=atmega8  "EDeviceM1A.elf"
        AVR Memory Usage
        ----------------
        Device: atmega8
        Program:    2134 bytes (26.0% Full)
        (.text + .data + .bootloader)
        Data:         16 bytes (1.6% Full)
        (.data + .bss + .noinit)
      Done executing task "RunCompilerTask".
    Done building target "CoreBuild" in project "EDeviceM1A.cproj".
    Target "PostBuildEvent" skipped, due to false condition; ('$(PostBuildEvent)' != '') was evaluated as ('' != '').
    Target "Build" in file "C:\Program Files\Atmel\Atmel Studio 6.0\Vs\Avr.common.targets" from project "H:\Project Accounts\Rashmi\Softwares\EDeviceM1A\EDeviceM1A\EDeviceM1A.cproj"
    Done building target "Build" in project "EDeviceM1A.cproj".
    Done building project "EDeviceM1A.cproj".

    Build succeeded.
    ========== Build: 1 succeeded or up-to-date, 0 failed, 0 skipped ==========
```

Device:atmega8
Program space:1234 bytes

Figure 5 Memory consumption of VCA

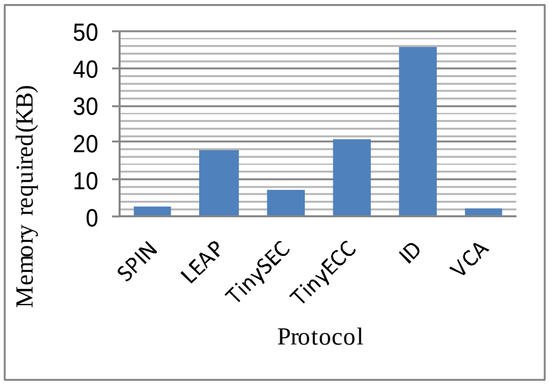


Figure 6 .Memory requirements of different security protocols

4.2 Bandwidth

Figure 7 shows bandwidth requirement of security protocols. Protocol SPINS transfer data at the rate of 30bytes per second. TINYSEC transfer data at the rate of 80 bytes per second. The MAC used for authentication in VCA is CBC-MAC. Texas Instruments provide CC2500 transceiver [16], which compatible with ATmega8 microcontroller having Programmable data rate up to 500 kbps. As the formula shows, $R_{DATA} = \frac{(256 + DRATE\_M) \cdot 2^{DRATE\_E}}{2^{28}} \cdot f_{XOSC}$ =(500+59).2^{13}=444.33=445Kbps =55.6KB/s. For VCA , approx. 56 byte per second.

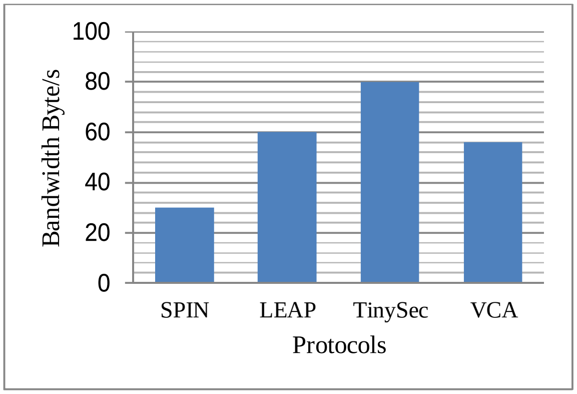
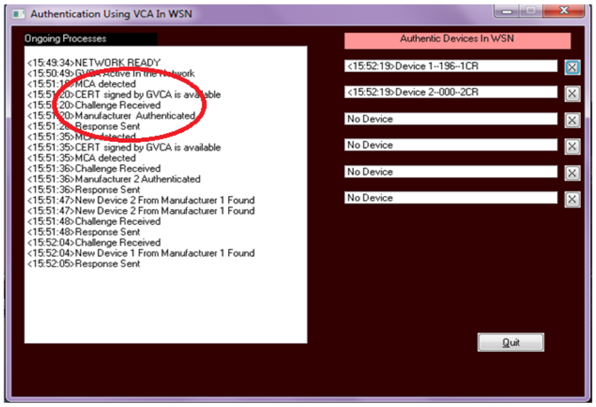


Figure 7 Bandwidth occupied by different security protocols

4.3 Analytical Result

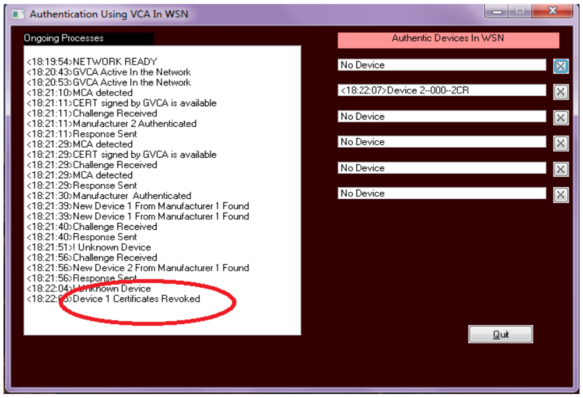
As seen from the two outputs, we can see the key exchange and the challenge response phases of the VCA architecture. Also we can see in the output that whenever a private key compromised or the certificate was mistakenly signed then certificate revocation is performed by CA. Its revocation will prevent all type unauthorized access.



```
<15:49:34>NETWORK READY
<15:50:49>GVCA Active In the Network
<15:51:19>MCA detected
<15:51:20>CERT signed by GVCA is available
<15:51:20>Challenge Received
<15:51:20>Manufacturer  Authenticated
<15:51:20>Response Sent
<15:51:35>MCA detected
<15:51:35>CERT signed by GVCA is available
<15:51:35>MCA detected
<15:51:36>Challenge Received
<15:51:36>Manufacturer 2 Authenticated
<15:51:36>Response Sent
<15:51:47>New Device 2 From Manufacturer 1 Found
<15:51:47>New Device 2 From Manufacturer 1 Found
<15:51:48>Challenge Received
<15:51:48>Response Sent
<15:52:04>Challenge Received
<15:52:04>New Device 1 From Manufacturer 1 Found
<15:52:05>Response Sent
```

```
<15:52:19>Device 1--196--1CR
<15:52:19>Device 2--000--2CR
No Device
No Device
No Device
No Device
```

Figure 8 Result Analysis



```
<18:19:54>NETWORK READY
<18:20:43>GVCA Active In the Network
<18:20:53>GVCA Active In the Network
<18:21:10>MCA detected
<18:21:11>CERT signed by GVCA is available
<18:21:11>Challenge Received
<18:21:11>Manufacturer 2 Authenticated
<18:21:11>Response Sent
<18:21:29>MCA detected
<18:21:29>CERT signed by GVCA is available
<18:21:29>Challenge Received
<18:21:29>MCA detected
<18:21:29>Response Sent
<18:21:30>Manufacturer  Authenticated
<18:21:39>New Device 1 From Manufacturer 1 Found
<18:21:39>New Device 1 From Manufacturer 1 Found
<18:21:40>Challenge Received
<18:21:40>Response Sent
<18:21:51>! Unknown Device
<18:21:56>Challenge Received
<18:21:56>New Device 2 From Manufacturer 1 Found
<18:21:56>Response Sent
<18:22:04>! Unknown Device
<18:22:05>Device 1 Certificates Revoked
```

```
No Device
<18:22:07>Device 2--000--2CR
No Device
No Device
No Device
No Device
```

Figure 8 Result Analysis

Table II: Security Architecture Comparison Table

Protocols	Node Authentication	Number of prestored keys	Authentication	Memory Requirement	Freshness	scalability	Resilience	Cost(time/energy)
SPIN	yes	One	CBC-MAC	2674 Byte Max	Yes	worst	100%	7.2ms/20%
LEAP	Yes	Four	CBC-MAC	ROM-17.8 KB RAM- No. of neighbors	No	worst	100%	Variable (no. of neighbors)
TinyEcc	Yes	One	ECDSA	20818 Byte	No	worst	-	20266.47ms/486.4mJ
ID	Yes	ONE	IBOOS	RAM-1634 Byte ROM-45,612 byte	No	worst	100%	2.43s/79.90 mW
TinySec	Yes	One	CBC-MAC	RAM- 728 Byte Program Space-7146 Byte	No	worst	-	0.38ms/9.1%
ProposedVCA	yes	None	CBC-MAC	2134 bytes	Yes	Excellent	0%	2.32ms/69 mW

5. ADVANTAGES

1) Due to integration of sensor network with mobile network will increase the transmission range of node
2) By using virtual certificate, the private key of the VCA is not stored in any sensor device.
3) Certificate of the device and certificate of the signer are implanted at the time of deployment. So it reduces the overhead.
4) Devices manufactured after deployment can still authenticate themselves to the devices already deployed.
5) Access control policies are managed by the individual manufacturers.

6. CONCLUSION

Security is critical issue for many sensor networks. Providing security and privacy to a sensor network is a challenging task due to the limited capabilities of sensor nodes. In this paper we try to enhance the overall performance by integrating the sensor network and the mobile network. Based on the literatures we introduced the concept of VCA, a virtual certificate authority. It also enhances many WSN design goals including simplicity, scalability, interoperability and control for individual manufacturers. VCA solves issue of initial trust via the structured signing of certificates and supports node authentication and a private key distribution mechanism.

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. DaulatraoAher College of Engineering, Karad 2013.

[2] 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] A. Perrig et al. SPINS: Security protocols for sensor networks. Proceeding for Mobile Networking and Computing, 2001

[5] A. Liu and P. Ning, “TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks,” Department of Computer Science, North Carolina State University, Tech. Rep. TR-2007-36, Nov. 02 2007, mon,05 Nov 2007

[6] S. Zhu, S. Setia, and S. Jajodia. Leap: Efficient security mechanism for large-scale distributed sensor networks. In Proc. of the 10th ACM. Conference on Computer and Communications Security (CCS ’03).

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

[8] Chris Karlof, Naveen Sastry and David Wagner, “TinySec: A Link Layer Security Architecture for Wireless Sensor Networks”, SenSys’04, November 3–5, 2004, Baltimore, Maryland, USA

[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] Rehana YASMIN, Eike RITTER, and Guilin WANG “An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures: Implementation and Evaluation”, The Institute of Electronics, Information and Communication Engineers.2010

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

[13] GauravSharmaa* SumanBalaa, Anil K. , “Security Frameworks for Wireless Sensor Networks-Review” 2nd International Conference on Communication, Computing & Security [ICCCS-2012]

[14] M.Rameshkumar, Dr.C.SureshGnanaDhass,” Design an Enhanced Certificate Based Authentication Protocol for Wireless Sensor Networks”International Journal of Advanced Research in Computer Science and ,Software EngineeringVolume 2, Issue 10, October 2012

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

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

[17] Rasmita Rautray, Itun Sarangi,” a survey on authentication protocols for wireless sensor network”, International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 5 May 2011

[18] S.V.Annlin Jeba, B. Paramasivan, D.Usha,”Security Threats and its Countermeasures in Wireless Sensor Networks: An Overview”, International Journal of Computer Applications, Volume 29– No.6, September 2011