International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Volume 1 Issue 6 (July 2014) http://ijirae.com

# A Case Study on Authentication of Wireless Sensor Network based on Virtual Certificate Authority

M.Bharat*

*M.Tech in Information Technology,*
*Jawaharlal Nehru Technological University*
*Kukatpally, Hyderabad, India*

Dr.K.Santhi Sree

*Professor of Computer Science Department,*
*Jawaharlal Nehru Technological University*
*Kukatpally, Hyderabad, India*

***Abstract— Wireless Sensor Networks (WSN) is a group of sensor nodes, each equipped with its own sensors, processor and radio transceiver. Sensor nodes are characterized by low bandwidth, small memory sizes, limited power supplies and limited energy. Without physical protection and in unattended environments all the Sensor nodes are deployed in open, so security is important, as they prone to different types of malicious attacks. Wireless Sensor Network (WSN) is useful for collecting the information from the Environment. The nodes will sense the information from the environment and sends the data to other nodes or Base Stations. During the process of transmission of data, many security techniques and methods are used. But the Wireless Sensor Networks are very difficult to secure the data, due to its mobility. Key Management is important for implementing security in a wireless Sensor Network. In this paper, moving sensors will provide security for the data collected and transmitted. The security is provided by using the Virtual Certificate (VC), issued by the Virtual Certificate Authority (VCA). This mechanism overcomes the difficulties in the Wireless Sensor Network. This mechanism verifies the validity of the proposed schemes and analyzes the consumption of energy, communication overhead and packet loss.***

***Keywords- Sensor, Base Station, Virtual Certificate Authority, Virtual Certificate.***

## I. INTRODUCTION

Wireless Sensor Network (WSN) is a collection of sensor nodes, each equipped with its own sensors, processor and radio transceiver [5]. Sensor nodes are characterized by limited power supplies, low bandwidth, memory sizes are small and very limited energy. Without physical protection and in unattended environments all the Sensor nodes are deployed in open, so security is important, as they prone to different types of malicious attacks. In WSN the security problem is one of the most fundamental aspects. To secure the data which is transfer from one node to another node it is necessary to use cryptographic mechanisms with secret keys. The sensor nodes in the WSN will either be static or move within a single WSN. The WSN applications become richer, there are number of applications that require sensors to move across WSNs such as monitoring application. A sensor is attached to the human body; it periodically collects heartbeat, temperature and transmits to the Base Station. The Base Station sends the information to the Monitoring System. The information which is send to the Base Station should be protected, this information transmitted securely. Fig. 1. Show the wireless sensor network.

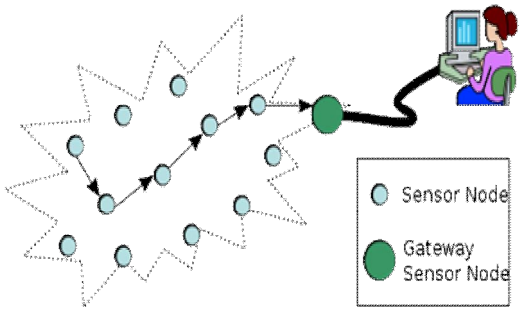


Fig. 1: Typical multi-hop wireless sensor network architecture.

The wireless sensor networks concept is based on a simple formula:

*Processor + Sensing + Radio = many potential applications.*

 

As soon as people understand the capabilities of a wireless sensor network, many of the applications strike to mind. It looks like a correct combination of modern technology. However, clubbing sensors, radios, and processor to form an effective wireless sensor network requires a detailed understanding of the both capabilities and limitations of each of the underlying hardware components, as well as a detailed understanding of modern networking technologies and distributed systems theory. Each individual node are designed to provide the set of primitives needed to synthesize the interconnected web that will emerge as they are made, while meeting requirements like size, cost and power consumption. The challenge is to map the full system requirements down to individual device capabilities, actions and requirements. Inorder to make the wireless sensor network vision a reality, architecture should be developed that synthesizes the envisioned applications out of the underlying hardware capabilities.

## II. EXISTING WORK

In WSN, the Key establishment is very difficult task. The shared keys by all the sensor nodes are secure. Many Key distribution techniques are proposed for solving the problem of authentication in WSN. The properties of sensor networks make previous authentication protocols impractical. Elliptic Curve cryptography (ECC) [3] has been proposed for Public Key Cryptography(PKC) for solving the problem of authentication in WSN. ECC based schemes and Identity (ID) [3] based schemes have high energy consumption. The ID based signatures require tate pairing or weil pairing. Computation which leads to a high computation cost and energy consumption is high. The communication cost is high due to size of the signature. The signature based schemes have been proposed for resource constrained networks. Elliptic Curve Digital Signature Algorithm (ECDSA) [2] requires two point multiplications in order to verify signature. The pairing is time-consuming operations. The pairing operation is used to secure resource-constrained sensor networks. This operations is expensive in terms of computational and memory requirements. The below Algorithm ECDSA[7] is used for signature generation.

***ECDSA Signature Generation***

*Input*: domain parameters (E,P), private key d, message m.
*Output:* signature (r,s).

*Step 1.* Pick $0 < k < q$ randomly
*Step 2.* $(xR,yR) \leftarrow kP$
*Step 3.* $r \leftarrow xR \bmod q$
*Step 4.* if $r = 0$ then goto 1
*Step 5.* $k \leftarrow k^{-1} \bmod q$
*Step 6.* $e \leftarrow H(m)$
*Step 7.* $s \leftarrow k(e + rd) \bmod q$
*Step 8.* if $s = 0$ then goto 1
*Step 9.* Return (r,s)

The source authentication protocols for WSN used for cryptographic techniques, which don't require computational and high communication overhead. Some of the authentication protocol in WSN is **μ**TESLA [1]. This protocol requires symmetric cryptographic techniques. One way hash chain is used for generating authentication keys. In **μ**TESLA, it sends the key chain commitments using unicast, it consists of starting time and duration of the time interval, but it is not applicable in large sensor networks. In order to avoid problem, muti-level **μ**TESLA was used. Multi level key chain is applied to very large WSN. The higher level is used for authenticate the lower level. The lower level is used to authenticate the message. Multi level chain is used for increasing the lifetime. The limitation of this scheme is to suffer from authentication delay. AVCA which follows as a PKI architecture. It is based on PKI architecture and designed for resource constrained devices on distributed networks. Many of the existing surveys on key Distribution mechanisms for WSNs cover a wide range of solutions; the main difference in my work is that it focuses on the energy efficient key management. Compared with other scheme, the proposed scheme has better performance on security and storage overhead.

### *A. Link Score Value Calculation*

Fig.2 shows the link score calculation [5] between the nodes when they transfer the data. Two links of different routes with the same hub distance competing to be admitted to the routing table then the link score value is calculated. The link

 

replacement is initiated, if a new link is received and the routing table is full. If there is more than one entry with the same link score, then the longest length is selected for replacement. The link score can be calculated by using a formula.

***Link score= (E * W + T * A)***

Where, E-Energy level of the next hop node
W-Weight for E
T –Transmission Success rate
A-Assigned weight T.

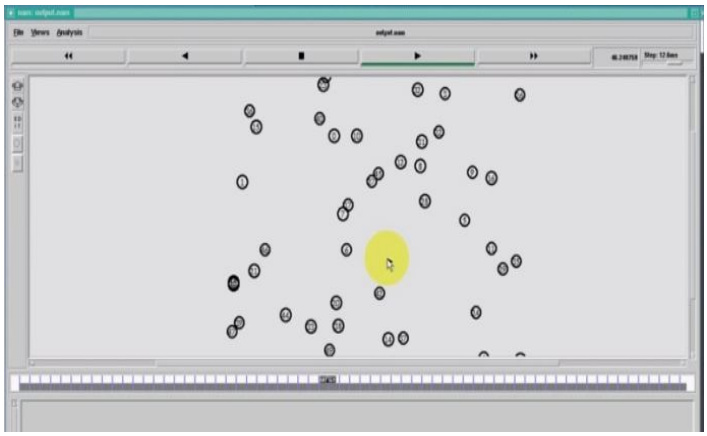

Fig.2 Link score value Calculation

The best path is based upon maximum of link score value and minimum of path length. The path is selecting according to the multiple class scheduler.

## III. PROPOSED SCHEME

When a sensor node wants to relocate, the Trust Centre or Central Base Station will control the node which is roaming. In Fig.l shows how the sensor node roams from one location to another location. All the node information is stored in the CBS (Central Base Station). The secret key, Communication key will be generated by the CBS. In the proposed system how the node is secure by using Virtual Certificate, when the node relocate their position.

### *A. Authentication of Virtual Certificate*

Authentication using Virtual Certificate authority will provide an initial trust between nodes. This is done by creating and verifying certificates. The certificates built before the deployment. The VC authority is responsible for the WSN nodes are placed in the network by calculating the Link score value. The VC authority will issue the certificate to each node. Before that malicious nodes are detected based on some threshold value. The major devices used in this architecture are TC(Trust centre), which is the device responsible for starting the network, defining the communication channel, key management, key distribution and implementation of a network access control policy. The end sensor node in the architecture is the MED (Manufacturer's End Device) and MCA (Manufacturer's Certificate Authorities) acts as a trusted third party between the MED and the TC. The GVCA stands for Global Virtual Certificate Authority and it is the trusted third party between the TC and the MCA. It is also responsible for signing the certificates of the TC and the MCA prior to deployment at the time of manufacture.The second virtual device i.e., Manufacturer's Virtual Certificate Authority (MVCA), is the trusted third party between the MCA and the MED. Both the MED and the MCA have their certificates signed by the MVCA and implanted prior to the deployment. The below figure Shows the AVCA Architecture [4].

### *B. Node Relocation*

When a node wants to join a new Base Station, it sends a leaving request to the previous Base Station. The Base Station removes all the related certificates and Keys of it. After relocation of the node, it will send a joining request to the new Base Station. If it accepts the node request then it sends a validation request to TC. After validating by CBS, the virtual certificate is issued to the new node.By using Identification number the TC knows about the MCA.

 

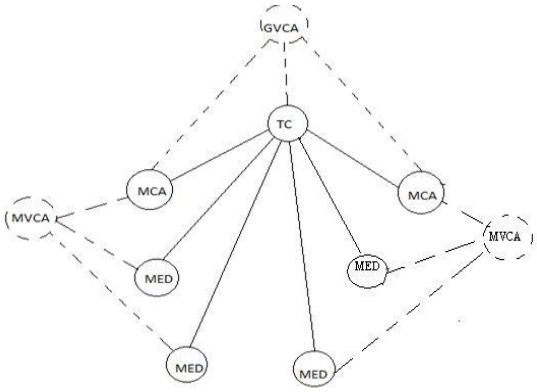


Fig 3. AVCA network with Virtual Certificate Authorities

The TC does not have the certificate. It requests the certificate to MCA. Before distributing the certificates MCA authenticates the TC. And TC authenticates MCA.MED issues a pre- authentication request to the TC for a certificate of an MCA device. The certificates are implanted on MCA. MCA sends the certificate to TC.Then TC sends it to MED. MED verifies MCA.After authentication MED request to TC for certificate. Then the certificate is signed by MVCA and Sended to the node. Fig 4. Shows the node relocation.

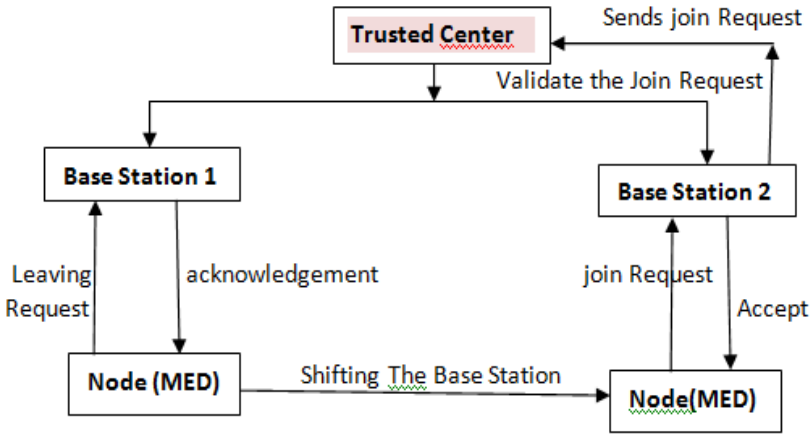


Fig 4: Node Relocation

## IV. PERFORMANCE EVALUATION

### A. *Analysis of Security*

1. The private key of the VCA is not stored Anywhere on any the device.
2. Replay Attack
3. Man-in-the-middle Attack
4. Overhead is reduced because Certificate of the device are implanted at the time of deployment.
5. Manufactures will manage the Control Access Policies of the device.

### B. *Simulation results*

The simulations were done in NS2. The nodes got collide with time has been analyzed and observed that the proposed Virtual Certificate Scheme performs better when compared with the previously discussed Algorithms. The NS2 simulation output of the Collision is displayed below in Fig 5.

 

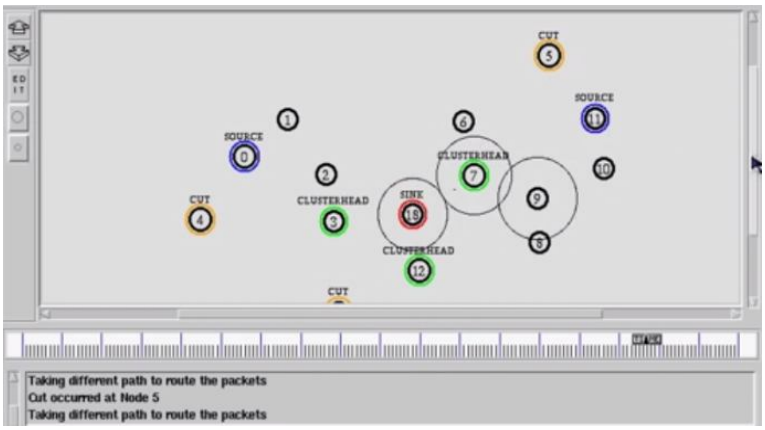


Fig 5: The collision overcomes with Virtual Certificate

## V. CONCLUSIONS

The wireless sensor network application is expected to grow in all fields. The data which is obtained from these networks should be secure. In this paper, it explains about a key management scheme that allows sensors to seamless roam across multiple WSNs. VCA method supports node authentication and a private key distribution mechanism. It also enhances design goals including simplicity, scalability, interoperability and control for individual manufacturers. This scheme retains the full advantage of Public key cryptography, highly-secure nodes in the network.

## REFERENCES

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

[2] D.Johnson and A.Menezes,"The *elliptic curve digital signature algorithm ecdsa*",University of Waterloo, Canada, Technical Report CORR99-34,August 1999, updated 200/01/02/04.

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

[4] 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), pp(92-99), Cambridge, 2010.

[5] L.Sujihelen, C.JayaKumar, " *Authentication in wireless sensor network based on Virtual Certificate Authority* " ,International Conference on circuits, power and computing technologies , 2013.

[6] Manjula M. Ramannavar, Monica M. Jagtap, "Authentication in Wireless Sensor Networks Using Virtual Certificate Authorities" International Journal of Emerging Technology and Advanced Engineering, , Volume 2(11), November 2012.

[7] Michael Braub, Anton Kargl, "A *Note on Signature Standards*", in Proc. Otto-Hahn-Ring 6, Siemens Ag Corporate Technology, Munich,September 10,2007.

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

[9] S. Choi, V. Sarangan, J. Thomas, S. Radhakrishnan, "*Secure Access Control Protocol for WSNs with inter network roaming*",proc. of the 35th Annual IEEE Conference on Local Computer Networks, pp.(256 – 259), Colorado,2010.

 