Design and Implementation of a Dynamic Key Management Scheme for Node Authentication Security in Wireless Sensor Networks

Sagar D. Dhawale **Dr. B. G. Hogade** **Dr. S. B .Patil**

Abstract*-Security and authentication are critical in wireless sensor networks[WSNs].** ***These networks are deployed in nasty environment under very less or no human supervision and mostly in unattended areas. Autonomous nature with tiny, resource constrained sensor nodes coupled with wireless nature make them unique and at the same time challengeable. The features are most unique, thus making these networks useful in diverse areas. The tasks assigned to these networks are generally of sensing the values or parameters which humans can't gather or sense. This includes environment monitoring, emergencies, health monitoring, battlefield surveillance and target tracking systems. This is because the environment and conditions where these networks are deployed. This makes networks prone to malicious users' and physical attacks due to some factors like radio nature of network, un-trusted transmission, unattended nature and open access. **Due to lack of resources a sensor node hinders the use of dynamic key management solutions designed for wired and adhoc networks** ***This paper proposes an authentication security for a sensor node in wireless sensor networks using zero knowledge protocol. The technique hides the keys from attacker while authentication and attacker will not have any knowledge about key. The proposed work uses rekeying mechanism with a system to use dynamic keys for node authentication. Moreover, a proposed technique is able to mitigate various attacks occurring on WSNs. The results show that the technique used is efficient.***

Index Terms: Wireless Sensor Networks, Attacks, Security, Keys, Algorithm.

Sagar Dhawale*, Department of Electronics Engineering, University of Mumbai Terna Engineering College, Nerul, Mumbai(India)*
Dr. Balaji Hogade *Department of Electronics Engineering, University of Mumbai Terna Engineering College, Nerul, Mumbai(India)*
Dr. S.B. Patil *Principal, MBT campus, Islampur.*

1. INTRODUCTION

Wireless sensor network (WSN) is a network of collection of tiny sensor nodes called as motes which are densely deployed over target area. The sensor are able to sense the data through events occurring in their coverage area and are able to either forward the data or process the data in some cases as shown in Fig 1. A sensor network node typically consists of Radio transceiver, a microcontroller and battery or typical form of an embedded type of energy source. There are three main research areas related to wireless sensor networks namely, deployment, operation and security. The deployment includes the establishment of network and the structure of overall network. It includes static or dynamic nature and planer or non planer networks. The operation involves actual data transmission protocol used and overall working of the network [1]. The security part is most crucial as it encompasses many dimensions of security. There might be requirement of data security, integrity, node authentication security and security against various attacks on WSNs.

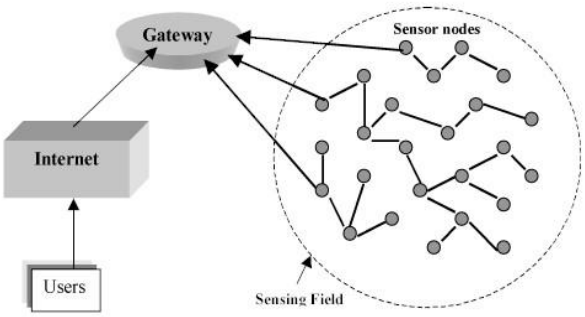

Fig 1: A sample WSN.

One can't directly apply the security techniques to WSN which are already available for wired networks. The main reason behind this is risk due to limited physical protection of the devices and openness of the wireless communication channel. Other reasons include limited energy source, processing capability and less memory size. A large number of sensor nodes are deployed to monitor the physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants detection and for the surveillance in the military applications and many other security systems. We address the security area for wireless sensor networks. As nodes can be compromised to

ISSN: 2278 – 7798

break security protocol and keys, the demand of these networks for security has increased. The security threats in WSN have been analyzed. We propose the authentication security for wireless sensor nodes with optimum use of keys. We further apply some countermeasure to overcome attacks in WSN.

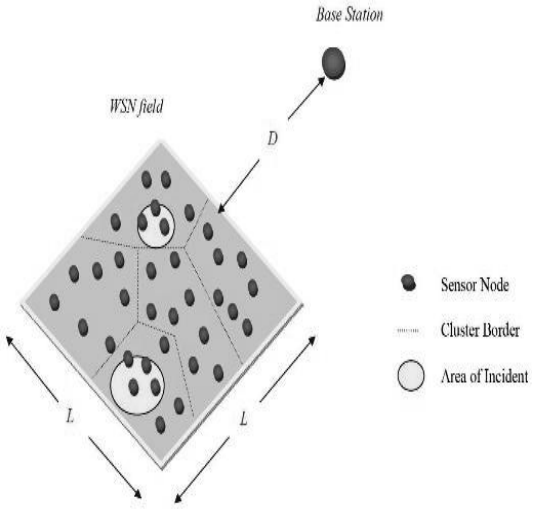

Fig 2: Deployment of Wireless Sensor Nodes in same plane.

There are some constraints on wireless sensor networks like Energy, Memory, Computational speed and power, Communications and Band width. These constraints are due to unique nature and cost possessed by sensor nodes. Also, along with this these networks are having some issues like scalability, dynamic nature and issues related to coplanar and non coplanar networks.

As WSNs are usually deployed in remote or even hostile environments and sensor nodes are prone to node compromise attacks, there is requirement of some rekeying mechanism to have dynamic keys. The dynamic keys allow the node to have different keys at the particular time. However, the resource-constrained nature of sensor nodes hinders the use of dynamic key management solutions designed for wired and ad hoc networks. Hence, many dynamic key management schemes[2][3] have been proposed for WSNs recently. The issues related with dynamic keys are key size, compatible with scalability and computational time. We propose a technique of secure authentication of nodes in WSN with the help of rekeying mechanism using zero knowledge protocol. The technique used does not directly pass the secret key, thus attacker is not able to read key. Also dynamic keys add some more security. The results show that the proposed technique is efficient with respect to key size and time required for computation.

II. Related Work

In random key distribution schemes, nodes are loaded with some keys before they are deployed to monitoring area. Then these nodes will establish shared key to form security link by performing the key discovery progress. The shared keys exist between two nodes in probably. Eschenauer and Gligor[4] proposed the basic random key pre-distribution scheme, which is based on pair-wise key. In this scheme, all the sensor nodes randomly choose several keys from a big pool to form a key chain. The security channel could be established between two nodes, which have the same key in their key chain. This scheme is very grist to attack. To improve the robustness of this scheme, H. Chan and A. Perrig[5] mended the random key pre-distribution scheme and proposed *q*-composite key pre-distribution scheme and random pair wise key scheme. This scheme requires the number of shared keys between two nodes must be more than *q*, which is different with the basic random key distribution scheme. Du et al. [6] proposed a new random key pre-distribution scheme based on the knowledge of deployment. The nodes are grouped with their anticipated deployed sub-area, and different group has different key pool. The neighboring sub-key pools which group is neighborly share keys through parameter *a*. The keys stored in nodes of this scheme are less than that of basic random key distribution scheme. And the ability to resist node capture attack is improved.

Eltoweissy[7] proposed a dynamic key management protocol: EBS(exclusion basis system). In this scheme, the *k* keys is selected from *K* keys in the pool, and loaded in a node. Anytime the node is captured, the key will be updated for all the net. The shortcoming of this scheme is the easily discovered key space. Lock is a kind of EBS [8]. In this scheme, each node is loaded with some spare keys, which are only shared with base station. This scheme needs the direct communication between base station and all the cluster nodes. It is not suitable for the large scale network.

Du et al. [9] utilized the multi-to-one communication method, and proposed an effective key management protocol, which is driven by routing. In this scheme, the shared key is established only between the neighbor nodes, which need to communication. This scheme decreases the communication and memory cost. A pair-wise key pre-distribution of multi-key space was proposed by W. Du [10], which is based on Blom key predistribution model. Huang et al. [11] proposed a forward authentication key management scheme for heterogeneous sensor networks, it is also a dynamic key management scheme. In these proposed methods, the pre-distribution key scheme requires

ISSN: 2278 – 7798

more memory to story pre-distributed key, and the connection between nodes is poor. For the geo-oriented key pre-distributed scheme based on the geography information of nodes, the key configuration is complex and the disorder deployment of nodes will make the network out of work.

III. Attacks And Their Impact on WSNs

In this section some attacks are discussed which are usually strike the WSNs. An attacker may physically capture only one or few of legitimate nodes, then clones or replicates them fabricating those replicas having the same identity like IDs or keys with the captured node, and then tries to add these nodes in network to get access to complete network[5]. Also an attacker may listen to communication and try to get information like nature of protocol and keys or some information related to keys. After getting these information, an attacker at some other time try to retransmit the data and try to get access to network. There are some harmful physical attacks which are described in following sections,

A. Node replication attack or Clone node attack

As wireless sensor network has open nature and nodes can be easily physically touched or carried out to another place, an attacker may capture some nodes and study them [12]. Attacker may find the ID [13] and other parameters of node. Now, he may try to replicate the node and place the compromised node in network.

B. Man-in-the-middle attack

In this type of attack, an attacker listens to communication in network either while data transfer or while some authentication being carried in network. Here, attacker may get information and try to study it.

C. Replay attack

If somehow attacker gets some information from network i.e. from man-in-the-middle attack, then attacker may try to resend old information through the network. In this case the network should be smart enough to identify such unauthorized information coming from unknown node.
Causes of node replication attack are as follows:

- It creates various attacks by extracting all the secret credentials of the captured node.
- It corrupts the monitoring operations by injecting false data.
- It can cause jamming in the network, disrupts the operations in the network and also initiates the Denial of Service (DoS) attacks too.
- It is difficult to detect replicated node and hence authentication is difficult.
- It creates an extensive harm to the network as the replicated node also has the same identity as the legitimate member.

IV. PROPOSED SYSTEM

The proposed work uses dynamic keys for authentication of nodes. A key pre-distribution scheme is used and rekeying mechanism helps the nodes to change the keys for every authentication process. Moreover, it uses zero knowledge protocol for authentication so that the secret keys are not passed directly and attackers will not have any knowledge of finding or guessing the secrets. The process of authentication involves challenge-response method that would be sufficient to identify the true node. The dynamic keys are helpful to regenerate the keys so that no previously used keys will be used again in near future authentication process. The proposed system is implemented in MATLAB as simulation tool. The nodes are organized in clusters and having a single base station.

A. Rekeying Mechanism

Due to the on-going cryptanalytic attacks, the keys used in WSNs have to be refreshed periodically[12]. Rekeying is also performed on demand or upon the high vulnerability of revealing any key polynomials. Rekeying is the most important phase in the dynamic key management and enhances the resilience against a node capture and a collusion attack. This paper presents a solution over such attacks using rekeying mechanism.

B. Proposed Algorithm

The future proposed work can be based upon following algorithm,
1. Using Super imposed code find the fingerprint codeword for each node.
2. Base station will maintain N as public key which will be product of two large primes.
3. The base station generates a secret code. Base station will not directly transfer secret, it will instead generates $v=s^2 \bmod N$ and gives to verifier.
4. This secret code will be changing for every authentication process. The change of bits will be done diagonally so that complete key need not to change.
5. Prover will select any random number r and send ($p= r^2 \bmod N$) to verifier.

ISSN: 2278 – 7798

6.Verifier will pass now a challenge e=0 or e=1 and will ask prover the value of ($y = r\ s^e \bmod N$).
7. If e=1 verifier got y=r s mod N. Verifier don‟t know s. So calculates y^2 mod N= ((r s mod N) (y^2mod N)= (r2mod N) * (s^2mod N)
$y^2 = p * v$.

Verifier got both p and v from steps above steps. So it compare s with y^2 and confirms authenticity of prover node.

V. IMPLEMENTATION RESULTS

The network deployment is done prior to key distribution. The network model is shown in Fig 3 and Fig 4. Network can have many variable nodes and topologies based on these nodes. Once the number of nodes are given the model is fixed and further processing is done on this model. The network is having cluster based approach where nodes and divided into clusters and clusters are connected to single base station. The base station is so powerful that it cannot be compromised. There is no direct communication among sensor nodes, but nodes communicate through cluster heads.

Dynamic keys for node 4 in following Fig 3:

101101101
110110001
100011010
010010010

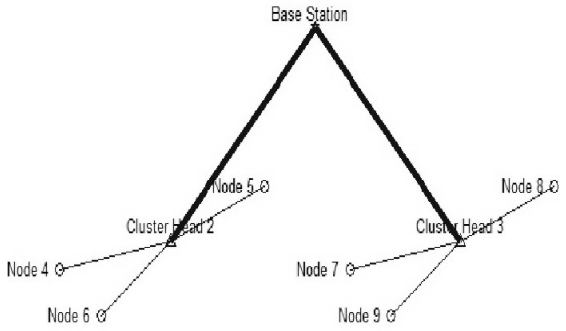

Fig 3: Network Model with 2 Clusters

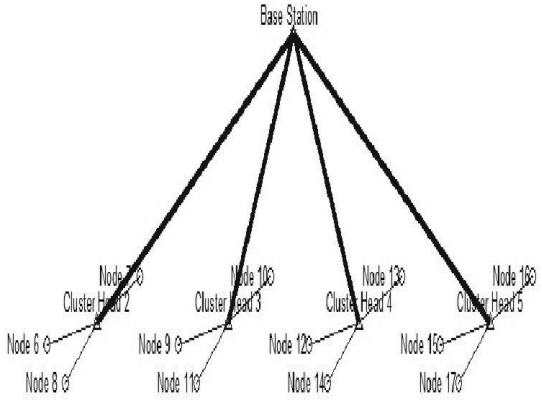

Fig 4: Network Model with 4 Clusters

Fig 5 shows sample network for implementation of 25 nodes.

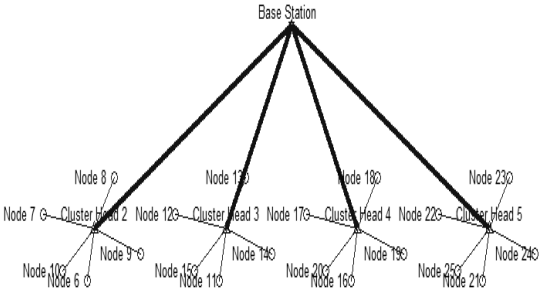

Fig 5: Network Model of 25 Nodes

Followings are the keys for above network column wise. Each column belongs to each node as secret key. First column is for base station, next is for cluster heads and then for nodes respectively.

ISSN: 2278 – 7798

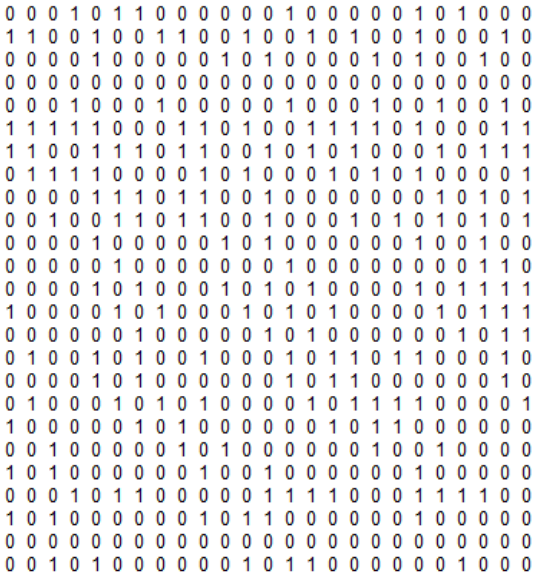

Fig. 6: Secret keys for 25 Nodes.

Following shows the running of authentication protocol for some sample node.

```
Base Station selects any prime number N   :  53

N is public key
Verifying various nodes of Experimental Model

Prover Node= 23  of Cluster 5
Verifier Cluster Head : =5
        :  Verification Process Started :
        : Verifier Informs Base station
        :  Base Station sends (v=s^2 mod N)  to verifier : v=40
        :  Prover Selects a random no : r =11
        :  Prover sends (p=r^2 mod N) to verifier : p= 15
        :  Verifier sends challenge (e) to Prover :  e= 0
        :  Prover sends (y=rs^e mod N) to verifier: y= 11
        Verifier dont know (s) so find y^2 and if e=0
         mod(y^2,N) is:  15and  mod(p,N) is: 15
         verifier verifies for iteration : 1


        Verification successful, Node can be allowed
```

Fig 7: Simulation of algorithm for Sample Node

Elapsed time is 0.001602 seconds.

The profile for above network is as follows,

Table I: Profile Summary

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
comm Node	1	0.014 s	0.003 s	
num2str	24	0.009 s	0.004 s	
strvcat	18	0.004 s	0.004 s	
int2str	13	0.004 s	0.004 s	
num2str>handleNumericPrecision	11	0.001 s	0.000 s	
num2str>convertUsingRecycledSprintf	11	0.001 s	0.001 s	
log10	13	0 s	0.000 s	
bin2dec	2	0 s	0.000 s	
iscellstr	2	0 s	0.000 s	

Following Fig 7 shows the occurrence and overcoming of clone attack on above network.

```
Public Key Selected by Base Station is :  53

CLONING ATTACK
Type-1 A: For Nodes : Placed in other Cluster

PART I:  Attack Scenario: Cloning of Node 8
Clonned of Node8 is placed in Different Cluster:5
Prover Node=8 of Cluster:2
Verifier is Cluster Head:5

PART II ALERT!
Message From Base Station: Attack in Cluster:5
The node 8 is not member of Cluster: 5

at 0.01 :  Verification Process Started :
 The FingerPrint of original node is :  01001000000001000010000000
 The FingerPrint of attcker node is :  00010100010001010101000011
 The FingerPrint mismatch!

PART III Now overcoming Attack
Verifying for iteration1
at 0.02 :  Base Station sends v to verifier : v=49
at 0.02 :  Prover sends p to verifier : 46
at 0.04 :  Verifier sends challenge e to Prover : e=1
at 0.05 :  Prover sends y to verifier : y=36
at 0.05 :  Verifier not verifies for iteration :1
```

Fig 8: Attack overcoming

ISSN: 2278 – 7798

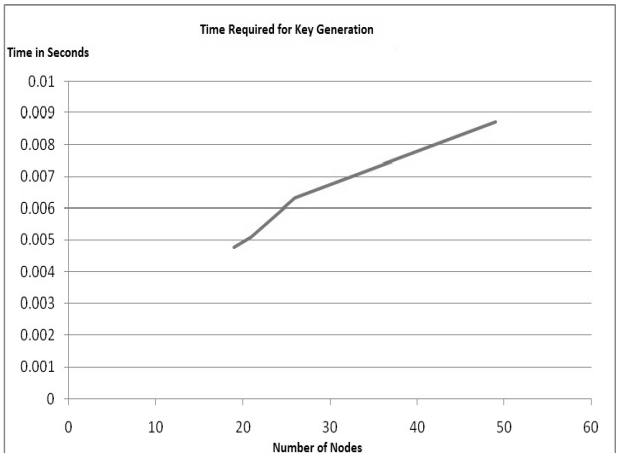

Fig 9 : Key Generation time for various nodes .

The Fig 9 shows time in seconds required for generation of keys for nodes of various networks. X-axis denoted the number of nodes and Y axis denotes time required for verification in seconds. Thus, it shows that the proposed technique is applicable to scalability and has efficient computation.

VI. CONCLUSION

Wireless sensor networks come with huge application domain but on the other hand require the same level of security. The paper discusses various authentication techniques available in wireless sensor network and analyzes them. Some techniques are very helpful but come with some disadvantages. The effort is also done to point out these difficulties. Authentication is one of the best security solutions which protects whole sensor network. The proposed security using authentication without revealing the secret information is highly secured and will not be broken. If the zero knowledge protocol is used for repeated challenges then it will be very secured and sure scheme for the security of entire network. The computational cost of this technique also appears to be very less as there are no high calculations required. So this will reduce the energy, storage requirements of the sensor node. Thus much effort should be given to develop such highly secured authentication schemes.

VII. ACKNOWLEDGEMENT

I owe a great many thanks to a great many people who helped and supported me during the writing of this paper. My deepest thanks to Dr. B. G. Hogade, the Guide of the project for guiding and encouraging me in this research. I express my thanks to Head of the Department ,Principal and all the Faculty members of my college and Library Staff for their helpful nature. I also extend my heartfelt thanks to my family and well-wishers. At last I thank and request God to give me strength and power for my Progress.

VIII. REFERENCES

[1] Feng Zhan Leonides J.Guibus, “Wireless sensor Network An information processing Approach”, Elsevier, 2007.

[2] Vijay Anand H.M, G.Varaprasad, “Dynamic Key Management Method for Wireless Sensor Networks”, Ninth International Conference on wireless and Optical Communications Networks (WOCN), IEEE ,2012 .

[3] Chen Chen, Zheng Huang,” A Novel Dynamic Key Management Scheme for Wireless Sensor Networks”, Proceedings of IEEE IC-BNMT 2011.

[4] L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks,” Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington, 2002.pp.41-47.

[5] H. Chan, A. Perrig and D. Song, “Random key predistribution schemes for sensor networks,” Proceedings of IEEE Symposium on Security and Privacy, Berkeley, California, 2003. pp.197- 213.

[6] W. Du, J. Deng, Y.S. Han, S. Chen, P.K. Varshney,”A key management scheme for wireless sensor networks using deployment knowledge,”Proceedings of the IEEE Infocom, Piscataway,2004, pp.586-597.

[7] M. Eltoweissy, H. Heydari, L. Morales,H. Sudborough, “Combinatorial optimization of key management in group communications,” Journal of Network and Systems Management, 2004,Vol.12(1),pp.33-50.

[8] M. Eltoweissy, M. Moharram, R. Mukkamala, “Dynamic key management in sensor networks,” IEEE Communications Magazine, 2006,Vol.44(4),pp.122-130.

[9] X. Du, M. Guizani, Y. Xiao, S. Ci, H. Chen, “A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks,” IEEE Transactions on Wireless Communications, 2009, Vol.8(3),pp.1223-1229.

[10] W. Du, et al. “A pairwise key predistribution scheme for wireless sensor networks,” The ACM Transactions on Information and System Security, 2005.pp.1-10.

[11] Jen-Yan Huang, I-En Liao, and Hao-Wen Tang, “A Forward Authentication Key Management Scheme for Heterogeneous Sensor Networks,” EURASIP Journal on Wireless Communications and Networking, 2011, Article ID 296704, 10 pages.

[12] A. D. Dhawale and Prof. Chandak, “ Design & Implementation of Secured Authentication Scheme for Wireless Sensor Networks”, IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 2, No.4, August 2012.

ISSN: 2278 – 7798

[13] Mohamed-Lamine Messai "Classification of Attacks in Wireless Sensor Networks" International Congress on Telecommunication and Application'14 University of A.MIRA Bejaia, Algeria, 23-24 APRIL 2014.

[14] Raju M et al, "An Approach in Detection of Replication Node in Wireless Sensor Networks: A Survey ",International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014, 192-196.

Sagar D. Dhawale received his bachelor's degree in Electronics and Telecommunication Engineering from Amravati University and he is currently pursuing master's degree in Electronics Engineering from the University of Mumbai. His research interests include Wireless Communication, Advance Digital Communication and Operating systems. This research work is published as a part of the research work done for the fulfillment of the degree of Master.

Dr. Balaji G. Hogade r eceived Ph.D. in EXTC (Smart antenna for wideband wireless communication) From NMIMS Mumbai in 2014, M.E. in Power Electronics from Gulbarga University,Karnataka, in 1999. He is Professor in Electronics Engineering Department in Terna Engineering College, He has guided number of projects and thesis in graduate and post-graduate level program. He has produced several national and international publications. He was a Member of BOS in Electronics Engineering in University of Mumba.His research interests include Wireless Network, Smart Antenna and Power Electronic and Drives.

Dr. S. B. Patil received Ph.D. in Eletronics . He is currently working as Principal in MBT campus is lslampur. He has guided number of projects and thesis in graduate and post-graduate level program. He has produced several national and international publications. He is a Member of ISTE, IJERIE.

ISSN: 2278 – 7798