

Implementation of Rekeying Mechanism for Node Authentication in Wireless Sensor Networks

Anand D. Dhawale¹ and M.B.Chandak²

¹Department of Computer Science & Engineering,
Shri Ramdeobaba College of Engineering and Management, Nagpur-INDIA
dhawaleanand@yahoo.com

²Associate Professor & Head, Deptt of CSE RCOEM-Nagpur-INDIA
chandakmb@gmail.com

ABSTRACT

Wireless sensor networks (WSNs) are composed of sensor nodes usually called as motes organized in a cooperative network. These networks are especially cooperative because motes collect data from environment and the data is passed through network. Further data is collected at base station for processing. The networks are installed in rough environments and where traditional networks are not possible to function well. Such installation is called as deployment. Generally there are three issues of research in wireless sensor networks like deployment, operation and security. WSNs got high popularity due to broad range of applications. These networks have attracted tremendous researchers due to their unique characteristics that differ them from traditional wired networks. WSNs are special networks having great future ahead but at the same time suffer from many hazards due to their unique characteristics. They are having large number of low cost sensor nodes with constraints like low power (usually operated by battery), low processing ability, and communication and storage limitations. Due to deployment nature and radio links the nodes are easily targeted by attacker like physical attack of node capture. If we think of applying security to WSNs we have to face the resource limitations constraints. The resource limitations don't allow for applying traditional mechanisms having large overhead and computational powers. Out of many security solutions authentication seems to be one of the best solutions to secure the whole network. The network can be made secure if we allow only true information to be inserted from true node. Authentication can be efficiently used to check valid, fake and modified communication. Such authentication techniques in wireless sensor networks are analyzed in this paper. Further this paper describes the implementation of a secured node verification scheme that authenticates the true nodes to access network and detects attacker nodes. The scheme never opens the secret keys during this process. The rekeying mechanism used also adds much security. The mitigation of some attacks is also explained with desired results.

KEYWORDS

Wireless Sensor network, attacks, fingerprint, authentication, security.

1. INTRODUCTION

Wireless Sensor Networks are generally deployed in a spatially distributed environment. The environment is targeted area which creates some events. The sensors catch the events. The events include sensory information like physical or geological changes. The collected data and information is transmitted from one node to other node through wireless medium. The applications include monitoring ,controlling and tracking areas like object or human tracking, battlefield monitoring, habitat monitoring. Many of the applications collect and maintain the secured data. The large numbers of sensor nodes are mounted and once deployed there is no

manual maintenance and monitoring till long time. Due to this scenario it creates a security problem. Nodes are more likely to be affected by various physical attacks which further cause node compromise, node cloning, man-in-middle attack and replay attack. Lot of researchers are attracted towards the security of wireless sensor network because until no concrete mechanism is established in this case. The reason to this is resource constraint and distributed unattended environment of sensor networks. The resource constraints include limited battery, limited memory and limited processing power. The research shows that lot of work has been done on the development of wireless sensor networks for application purpose but very little attention is paid for the great security mechanism. The different schemes are applied for data transfer. In some cases all nodes transfer data to base station where nodes collect data on their own responsibility. As the application domain of wireless sensor networks is increasing and with the emergence of high data rate sensor network applications there is a need for high security and high performance networks. [1] The access to the network might be on some security criteria or on the basis of some subscription amount. The user authentication in wireless sensor networks is critical task. The resource constraints don't allow traditional security solutions to work on WSNs. There are certain user authentication schemes for other applications but we can't directly use them for sensor networks. Some shortcomings are there in applying security schemes.[2]

1.1 Motivation

Physical tampering causes major damage to sensors and further to complete network. If sensors are distributed in an unprotected area, an attacker may collect the sensor nodes, analyze the electronics, may study the node to find identity and steal cryptographic keys. To protect the sensor nodes from such attacks, sensors must be tamper-proof or they must erase all permanent and temporary storage when compromised. Secure key rotation mechanisms can also mitigate the threat of stolen cryptographic keys. Also due to the strong constraints that the sensor nodes have (memory storage, computing capacity, limited battery), the existing security protocols are too heavy to be used this. Some of the protocols that address security on the node to node communication use several keys for every sensor node, which introduces more storage and computation capacity needs.

2. SECURITY IN WIRELESS SENSOR NETWORKS

In this section general security scenario of wireless sensor network is explained. Wireless sensor networks provide great range of application. Any system which provides applications needs to be secured [3]. During the study of any domain more concentration is given to the security rather than applicability. If we study signal systems, more you need to concentrate on noise factor which affects the signals. Many of the WSNs are used for confidential data processing. So, they need to be secured.

2.1 Attacks

The various attacks that are interested in literature are listed here.

2.1.1 Privacy attack

Privacy attack is mainly to get secret information. Attacker monitors the network traffic, listen and study data. The attacker may get the content of communication and may guess the role of nodes. Attacker then may insert a node or compromise a node.

2.1.2 Clone Attack

Attacker may insert with the keys and identity of compromised node and make clone of true node. The attacker node attempts to behave like true node and try to access network [3].

2.1.3 Traffic analysis attack

The attacker gets the knowledge of traffic in the network. It guesses that more traffic is towards base station. This makes the network completely useless.

2.1.4 Sybil attack

A single node is copied and attacker presents several identities to the network. This affects the routing protocol of network. Using Sybil attack one node may be present in multiple locations. This attack is somewhat less efficient and easy to guess [4].

2.1.5 Replay Attack

The attacker node transmits previous messages and tries to have access to the network. It is difficult for the receiver to distinguish between a normal message and replayed message.

2.1.6 Selective forwarding attack

The attacker node forwards some packets and selectively drops others. It passes some packets to aware neighbours that this node is not dead. By doing this it is hard to detect such attacker node.

2.2 Limitations to Security in Wireless Sensor Networks

Certain obstacles are present to apply security mechanisms in wireless sensor networks. They make it difficult to apply traditional security mechanisms directly.

2.2.1 Limited resources

The memory size of sensor node is very limited. Thus, complex security mechanisms requiring much memory do not allow applications to run well. The key size and number of keys needs to be considered. The energy is also a constraint. Extra energy is needed for the security scheme implementation. Obviously security adds extra processing power and communication overhead.

2.2.2 Unreliable communication

Any type of security system mainly depends upon the communication strategy of the network. The wireless network makes it easier to attacker to have easy access to data from the wireless links. This also causes damage to network security.

2.2.3 Unattended operation

Once the sensor network is deployed there is no manual supervision and is left unattended for long time. This makes network exposed to physical attacks. Also the networks are managed remotely so, it is very difficult to guess if a node has been physically attacked.

3. RELATED WORK

The most important security services required are confidentiality and authentication. There is relatively little work in the area of securing sensor networks. Like their mobile ad-hoc counterparts sensor networks lack a fixed infrastructure and the topology is dynamically deployed. [5] In the context of WSNs, security means to protect sensor data against unauthorized access and modification and to ensure the availability of network communication and services in spite of malicious activities. If collected data is private and sensitive such as user location information, then privacy issues are also of concern.

The classical means to ensure integrity and confidentiality of data is to use cryptographic algorithms. In all modern crypto primitives, the security more or less depends on the security of the cryptographic keys hence the distribution and management of keys has a vital importance. In Eschmauer and Gligor's[6] scheme the keys are drawn randomly from key pool. A code based key management system was proposed by Al-Shurman and Yoo [7]. where a matrix along with a vector is used for generating codeword. Camtepe and Yener [8] proposed a deterministic key pre-distribution scheme using combinatorial designs. [9] shows a survey of different pre key-distribution schemes for Distributed Sensor Networks.

Ruj and Roy[10] proposed a scheme where Reed Solomon code is used for key pre-distribution and each node is given a unique polynomial. Key Pre-distribution Schemes in Distributed Wireless Sensor Network using Combinatorial De-signs were revisited by Pattanayak and Majhi[11]. Sarkar , Saha and Chowdhury[12] proposed a scheme where communication and connectivity model is introduced. Where if two nodes want to communicate with each other then it has to match both of the connectivity key and communication key. As discussed in paper[13] the connectivity matrix of the network is considered.

The most of the existing security systems are based on different requirements of specific networks. While studying security solutions one may not find a standard methodology that will suit to most of the wireless sensor networks. On the basis of various categories of networks here is the short background of available security schemes defined for wireless sensor networks.[14]

3.1 Public key-based user authentication scheme [15]

It is assumed that public key operation is feasible for even a tiny sensor node. All of the public key-based schemes utilize a certificate which is generated by base station and used for user authentication. But, public key operation is slower and consume much energy than symmetric key(private key) operation. Thus, if an attacker launches DOS attack, the attacker can easily exhaust the limited energy of sensor node.

3.2 Symmetric key-based user authentication scheme [16]

A key distribution scheme for dynamic conferences is a method by which initially an (off-line) trusted server distributes private individual pieces of information to a set of users. Later, each member of any group of users of a given size (a dynamic conference) can compute a common secure group key. In this setting, any group of the users can compute a common key by each user computing using only his private initial piece of information. Keys are secure against coalitions of up to k users, that is, even if k users pool together their pieces they cannot compute anything about a key of conference comprised of other users.

3.3 A lightweight user authentication scheme [17]

It provides mutual authentication and session-key agreement. The scheme is executed on both sides; the WSN's coordinator side playing the role of the server, and the user's device side acting as a client. It is assumed that there is an administrator, which is responsible for loading necessary secret keys in the WSN and for registration of users. First, the administrator chooses a secret key x and then loads the system server and the coordinator with this secret key x . The system server uses this secret key for registration of users. The coordinator uses this secret key in order to verify the authenticity of users.

3.4 An Efficient Scheme for User Authentication [18]

In this paper, a distributed user authentication scheme suitable for sensor networks based on self-certified keys cryptosystem (SCK) is proposed. First of all, SCK is modified to use the Elliptic Curve Cryptography (ECC) to establish pair-wise keys in sensor networks, because ECC is said to be feasible for WSN even without special hardware support. But this method is vulnerable to node capture attacks and it also requires synchronization between nodes.

3.5 Fast Authenticated Key Establishment protocols

The paper "Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks" was written by Qiang Huang et. al at Princeton University and Mitsubishi Electric Research Laboratories to create an "efficient authenticated key establishment protocols between a sensor and a security manager in a self organizing network"[20]. In this research the researchers used elliptic curve cryptography (ECC) to provide encryption for the sensor nodes. ECC was chosen because only small key lengths are needed in order to get a reasonable amount of security. To authenticate keys, certificates are used to find out if the public key is in fact a trusted sensor.

4. PROPOSED METHODOLOGY

The proposed work addresses verification of nodes of the wireless sensor network ensuring that the nodes of network are all true nodes. The verification includes challenge response communication where care is taken that the secret of the node is not opened. Thus attacker will not get secret information. The research work includes the model of wireless sensor network. The clustering approach of network is used here. The network is divided into base station, cluster heads and member nodes. Base station is powerful and has information of total network. The network is divided into clusters. Each cluster has limited nodes. Each cluster has one cluster head. The verification (authentication) of any sensor node of particular cluster is done by respective cluster head. Verification of cluster head will be done by Base station. Each node knows its immediate neighbours. If certain attack occurs on the network, base station will alert to network especially to particular cluster head. Cluster head then carries verification for that node and doesn't allow it to enter the network. Thus network will be secured.

The nodes of wireless sensor network are subjected to various physical attacks. The physical attacks like node capture, cloning attack, replay attack, compromising nodes and man-in-middle attacks are very harmful in this case. It is easy for attacker to capture the node and copy the cryptographic information like keys. Attacker can also produce an identical node of existing node (cloning) and inject that node into network. Such nodes are inserted in network. The proposed work addresses such types of attacks. The proposed scheme is allowing the identification and verification without revealing any secret information during the conversation between the nodes. In verification the main task of proving node is to convince verifier of some secret through series of communication. The communication may have questions and challenges

[13]. The only true node can correctly prove the identity. Here ID of node can also be considered. This scheme is very much secured as the attacker node will not get any of the secret information out of intercepted messages. The clustering technique like following can be used.

4.1 Objective

The objective of this research work is to design a secured authentication scheme for node authentication in Wireless Sensor Network. Every node whether member node or foreign node will have to pass security challenges imposed by algorithm to have participation in network. In verification process, we are using zero knowledge protocol so the secret key of node is not revealed making network more secure. In this way all the nodes which are in network will be true nodes and communication through them will be surely secured.

4.2 Assumptions

- Cluster based network approach is used. Nodes are divided as Base station, Cluster head and member nodes.
- Every cluster head knows its members.
- Base station has all information about network.
- There is no direct communication between member nodes.
- The level of authentication responsibility is like member nodes are verified by respective cluster heads and cluster head is verified by base station.

The proposed research work involves

- Network Model for explanation.
- Finding Fingerprint (Secret) for nodes based on Code word and Connectivity matrix.
- Implementation of Algorithm for existing nodes.
- Checking and avoiding the system for attacks.

4.3 Algorithm

The algorithm includes verification process for a sensor node. The secret fingerprint 's' for each node in the network is obtained based on code word matrix and connectivity matrix. Base station maintains N as public key which is prime number.

- a) A node (Prover) tries to verify at particular cluster. So verifier node will ask for secret of prover node to Base Station.
- b) Base station will not directly transfer secret, it will instead generates $v=s^2 \text{ mod } N$ and gives to verifier.
- c) Prover will select any random number 'r' and send $(p=r^2 \text{ mod } N)$ to verifier.
- d) Verifier will pass now a challenge $e=0$ or $e=1$ and will ask prover the value of

$$(y = r s^e \text{ mod } N).$$

- e) If $e=1$ verifier got $y=r s \text{ mod } N$. Verifier don't know s. So calculates

$$\begin{aligned} y^2 \text{ mod } N &= ((r s \text{ mod } N)^2 \text{ mod } N) \\ y^2 &= (r^2 \text{ mod } N) * (s^2 \text{ mod } N) \\ y^2 &= p * v. \end{aligned}$$

Verifier got both p and v from steps b and c . So it compares with y^2 and confirms authenticity of prover node. The algorithm never directly passes the secret key. Instead the key is enclosed in

some operations. These operations make the attacker to find the key difficult. Even if by trying much attacker gets the secret key of certain node attacker will not be able to verify because in next verification process that key will have been changed and will not be valid due to rekeying mechanism.

5. IMPLEMENTATION OF PROPOSED METHODOLOGY

The implementation of the proposed methodology is divided into following parts

- Network topology is obtained as network for explanation.
- Finding unique fingerprint for each node.
- Verifying existing nodes of the model
- Detecting the various attacks and securing the network from attacker nodes.

The implementation of this research work is done in Matlab software.

5.1 Network topology

Based upon number of nodes and number of clusters heads a network model is formed and further verification will be carried out on this network itself. For Ex we consider network model as,

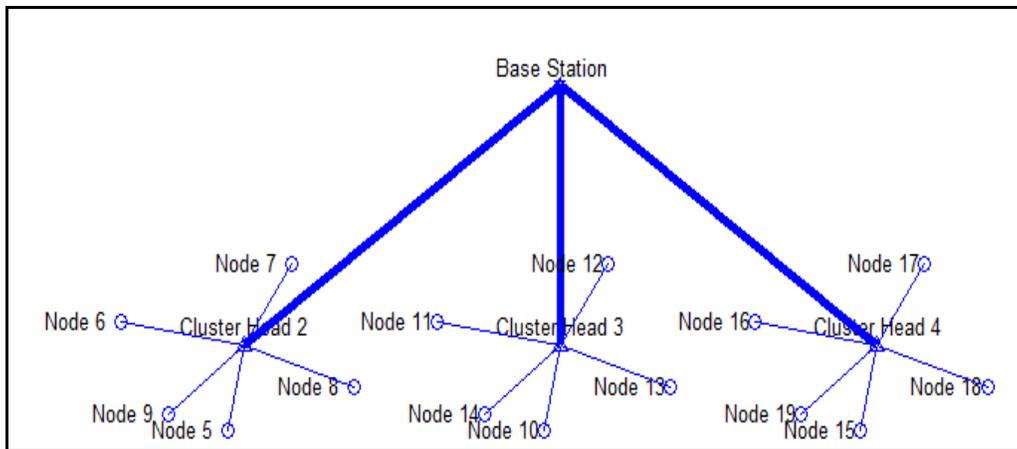


Figure 1. Existing model for explanation.

5.2 Unique fingerprint for each node

Depending upon number of nodes in the wireless sensor network, a Node code word is designed for each node in the network. Also, based upon the network architecture, a connectivity matrix is obtained. With the help of code word and connectivity matrix secret for each node can be obtained. The fingerprint is the binary unique combination. This is called as fingerprint which is surely unique for each node and it always changes immediately in each verification process. So, much of security is assured.

5.2.1 Connectivity Matrix

A connectivity matrix is obtained for the existing model. The connectivity matrix describes the connectivity of particular node with other member nodes and preserves the social characteristics of the network.

5.2.2 Superimposed Node codeword

The node codeword used to generate fingerprint using the connectivity matrix. For each sensor node, a node code word is formed of particular strength. The strength of the codeword is the maximum connectivity available in the network. The size is equal to number of total nodes of the network.

Let \mathbf{X} be a $m \times n$ binary matrix, the scheme considers a matrix \mathbf{X} with a constant column weight P and a constant row weight W . Then,

$$\sum_{i=1}^m X_{i,j} = P$$

$$\sum_{j=1}^n X_{i,j} = W$$

Where $1 \leq i \leq m, 1 \leq j \leq n$. The binary matrix \mathbf{X} can be used to define a binary codeword.

The node codeword is represented column wise; sequence is base station, cluster heads and member nodes. Here BS is base station, CH is cluster head and N is representative for member node.

	BS	CH2	CH3	CH4	CH5	N6	N7	N8	N9	N10	N11	N12	N13	N14	N15	N16	N17	N18	N19
0	1	0	0	1	0	0	0	1	0	0	0	0	1	1	0	0	1	0	0
1	0	0	1	0	0	0	1	0	0	0	0	1	1	0	0	1	0	0	0
0	0	1	0	0	0	1	0	0	0	0	1	1	0	0	1	0	0	1	0
0	1	0	0	0	1	0	0	0	0	1	1	0	0	1	0	0	1	0	0
1	0	0	0	1	0	0	0	0	1	1	0	0	1	0	0	1	0	0	0
0	0	0	1	0	0	0	0	1	1	0	0	1	0	0	1	0	0	1	0
0	0	1	0	0	0	0	1	1	0	0	1	0	0	1	0	0	1	0	0
0	1	0	0	0	0	1	1	0	0	1	0	0	1	0	0	1	0	0	0
1	0	0	0	0	1	1	0	0	1	0	0	1	0	0	1	0	0	0	0
0	0	0	0	1	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0
0	0	0	1	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1
0	0	1	1	0	0	1	0	0	1	0	0	1	0	0	0	1	0	0	0
0	1	1	0	0	1	0	0	1	0	0	1	0	0	0	1	0	0	0	0
1	1	0	0	1	0	0	1	0	0	1	0	0	0	1	0	0	0	0	0
1	0	0	1	0	0	1	0	0	1	0	0	0	1	0	0	0	0	0	1
0	0	1	0	0	1	0	0	1	0	0	0	1	0	0	0	0	0	1	1
0	1	0	0	1	0	0	1	0	0	0	1	0	0	0	0	0	1	1	0
1	0	0	1	0	0	1	0	0	0	1	0	0	0	0	1	1	0	0	0
0	0	1	0	0	1	0	0	0	1	0	0	0	0	1	1	0	0	1	0

Figure 2. Superimposed Node codeword for each node.

5.2.3 Unique fingerprint

Based upon node codeword and connectivity matrix the unique fingerprint for each node is obtained. The fingerprint is binary unique combination of 0s and 1s. The technique of fingerprint formation is not revealed for the security. The mechanism is like finding the neighbourhood information based on connectivity matrix and having binary operations with node codeword. The fingerprint having the spatiality that it changes for every verification process.

5.2.4 Re-keying mechanism of fingerprint

The unique fingerprint of the node is changing for each verification process. This is for the security that even by any way attacker gets the fingerprint; attacker will not be able to verify itself because that fingerprint secret is older. This is because the node now having some another secret fingerprint. This is called as re-keying mechanism. By introducing a re-keying mechanism, a base station can conveniently update a sensor nodes secret fingerprint without the intervention of back-end system for the purpose of reducing the communication interactions and management burden. For example the unique fingerprint for above network is,

BS	CH2	CH3	CH4	CH5	N6	N7	N8	N9	N10	N11	N12	N13	N14	N15	N16	N17	N18	N19
1	0	0	0	0	1	1	1	1	0	0	0	1	1	0	1	1	1	1
0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1
1	0	1	1	0	0	1	1	0	1	0	1	0	0	1	1	1	0	0
0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	1	1	1	0
0	1	0	0	1	0	1	0	0	1	0	1	0	0	1	1	1	1	0
1	0	0	0	0	1	0	1	0	1	1	0	0	0	0	1	1	1	0
1	0	1	0	1	0	0	1	0	1	1	0	1	1	1	1	0	0	0
1	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	1
0	0	0	1	0	0	1	0	0	1	0	0	0	1	0	1	0	1	1
1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	0	1	0	1
1	0	0	1	0	1	1	0	1	1	1	1	0	1	0	1	1	1	1
1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0
0	1	0	0	0	0	1	0	0	1	0	0	1	0	0	0	0	0	1
0	1	0	0	1	1	1	0	0	0	1	0	1	0	1	0	0	1	0
1	0	1	1	1	1	0	0	0	1	0	1	1	1	0	0	1	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1
1	0	0	0	0	1	1	0	0	0	0	0	0	0	1	0	0	0	1

Figure 3. Unique fingerprint secret for each node

One may observe the fingerprint is unique for all nodes. The sequence of fingerprint is column wise base station, cluster heads and member nodes. The fingerprint is converted to decimal at the time of verification process.

5.3 Simulation for Authentication Process

In this case nodes of network undergo verification process and they are checked whether they are true nodes or not. The node which is trying to verify is called as prover and the node which verifies called as verifier. Each node will undergo a series of iteration process with a new challenge and respective response from prover node is expected every time

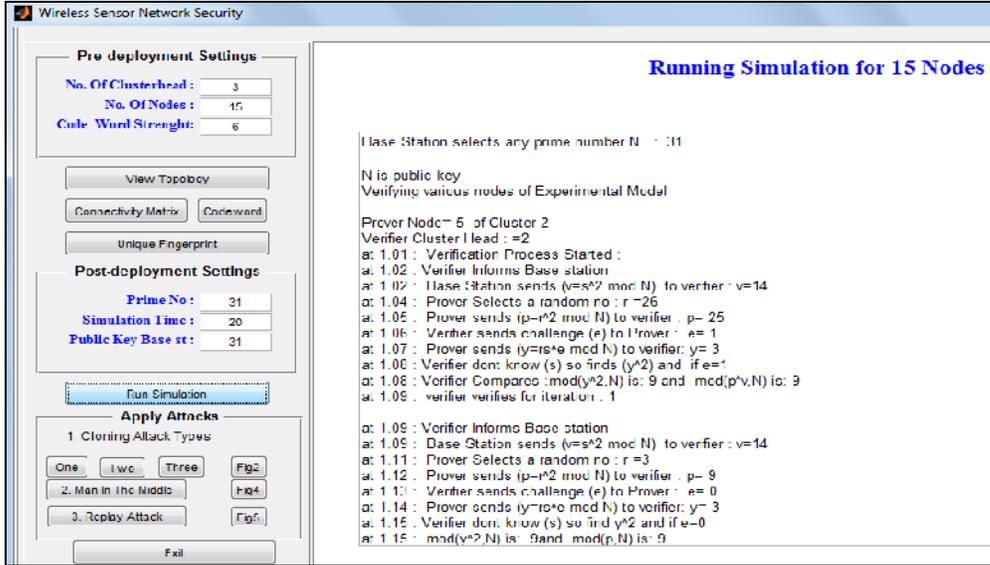


Figure 4. Verification of various nodes of network.

Iterations are at least for 5 times to have different values of challenge e ($e=0$ or $e=1$) to make attacker difficult to get verified. If in any single iteration attacker fails to provide true values, attacker node will not be allowed access and will not be authenticated. So this will secure system much more.

Thus the node is verified and confirmed as true node.

5.4 Detecting attacks and securing system

The proposed work verifies the system for various attacks like

5.4.1 Cloning attack

The attacker node may try to capture some nodes of network and make clone nodes having some secret key and identity number of original node. Then attacker will try to authenticate that cloned node. We have considered in this case three two types of cloning attack.

Type 1. Cloning of sensor nodes

Cloning of member sensor nodes is done and they try to verify .We considered two subtypes based upon to which cluster head attacker node requests for verification.

- **Type 1 A. Cloning of node of one cluster is done and placed in another cluster.**

In this case as the cloned node shows identity of another cluster it will not be allowed. Base station will alert the respective cluster and verified by cluster head for confirming that it is attacker node. As the attacker node is selecting any random key it will not be able to pass all the challenges given by verifier node.

- **Type 1 B. Cloning of node of some cluster is done and cloned node is placed in same cluster.**

In this case the node will have to pass the challenges of protocol passed by cluster head. Also attacker node is not having secret key of the node whose identity is shown by attacker node.

Type 2 Cloning of Cluster head

Cloning of Cluster head is done and attempts to authenticate. In this case cluster head is cloned and then cloned cluster head is placed. Base station is the verifier. Now the attacker cluster head will select any random key and attempts to authenticate. But the fake secret key will not allow the attacker node to have verified.

5.4.2 Man-in-the-Middle attack

The attacker node tries to make independent connection and attempts to verify with possible information it has got through intercepting the network. But the attacker node will not have any guess of the fingerprint secret, so it will not be verified.

5.4.3 Replay attack

In this case, attacker node makes independent connection with network and tries to pass the previous communication responses. Random selection of keys makes it impossible for attacker node to get authenticated.

In all the above attacks even if attacker tries to authenticate using different keys (secret fingerprints), it has to try surplus number of keys. Also rekeying mechanism changes the keys of the network for every verification process. Because key size is not much more it will not add large overhead on the network. This makes attacker node nearly impossible to guess the secret fingerprints of the nodes.

5.5 Simulation of Cloning Attack Scenario

At last stage various attacks with their prevention are simulated. The research addresses three main types of attacks cloning, man-in-the middle and replay attack on wireless sensor network. The methodology for attack implementation includes

1. Base station finds if fingerprint of node matches with true data. Obviously fingerprint secret of attacker node will not match.
2. Base station also checks whether node belongs to the respective cluster if particular number of node is mentioned.
3. It then verifies node for minimum five times and makes it not verified and thus will not have entry in network.

Various attacks are shown to be impossible on the network. This is due to unique fingerprint of the nodes that attacker can't get.

Example of attack implementation:

- Clones of nodes are made and placed in network.
- Type : Node of one cluster is cloned and placed in another cluster

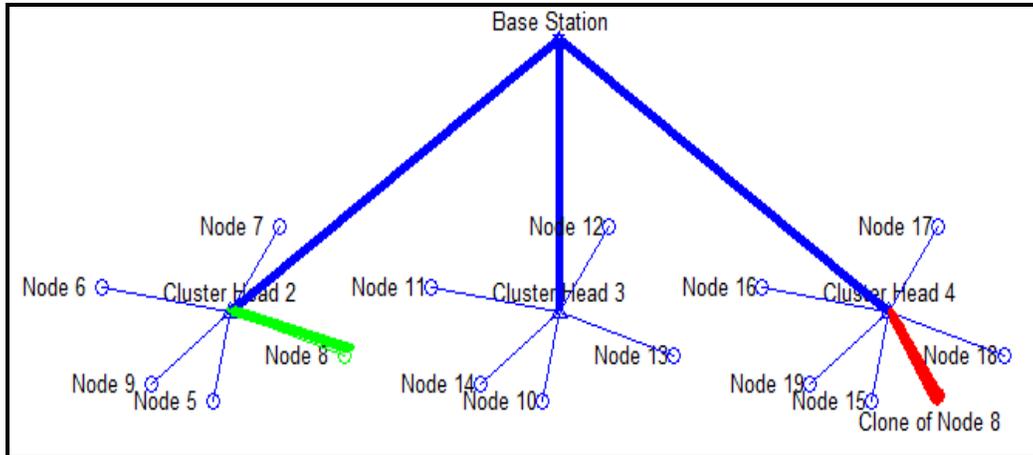


Figure 5. Cloning attack scenario

```

Public Key Selected by Base Station is : 31

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

PART I: Attack Scenario: Cloning of Node 8
Cloned of Node8 is placed in Different Cluster:4
Prover Node=8 of Cluster:2
Verifier is Cluster Head:4

PART II ALERT!
Message From Base Station: Attack in Cluster:4
The node 8 is not member of Cluster: 4

at 0.01 : Verification Process Started :
The FingerPrint of original node is : 1001001110100000000
The FingerPrint of attcker node is : 0001000100100001000
The FingerPrint mismatch!

PART III Now overcoming Attack
Verifying for iteration1
at 0.02 : Base Station sends v to verifier : v=18
at 0.02 : Prover sends p to verifier : 20
at 0.04 : Verifier sends challenge e to Prover : e=1
at 0.05 : Prover sends y to verifier : y=20
at 0.05 : Verifier not verifies for iteration :1
    
```

Figure 6. Verification for above cloning attack

Thus, Verification failed. Attacker Node not allowed. Network is SECURED.

6. RESULT ANALYSIS AND DISCUSSION

This section discusses the result analysis of the proposed system. The proposed system is found to be reliable and more secure for the wireless sensor networks which are having resource constraints.

The attacker node will not have any confirm chances of finding fingerprint. If any attacker tries to find out fingerprint it will be having one of the chances from 2^N . So the probability reduced to $(1/2^N)$. If even though attacker finds the fingerprint, that fingerprint might have been changed due to the technique re-keying mechanism. So there are very less number of chances to have secret fingerprint of node and have attack through them.

- Re-Keying is secure technique.
- Fingerprint guessing is nearly impossible.

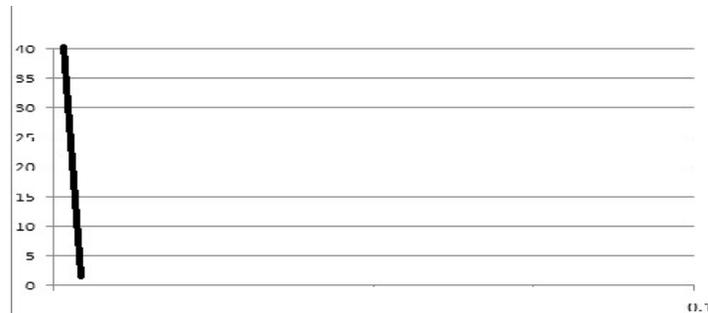
The Table 1 and Figure show the details of probability to find secret key . Attacker is having one of the chances from 2^N . So the probability reduced to $(1/2^N)$.

Table 1. Probability for finding secret

SR. NO.	No. of Nodes	Probability to find secret
1.	13	0.000122
2.	19	0.000001907
3.	28	0.000000003725
4.	31	0.000000000465
5.	38	0.0000000000036

The scheme supports scalability in the respect of number of nodes. This model is scalable because many numbers of nodes can be entered and scheme can be implemented on them

Y axis- Number of nodes



X axis - Probability to find secret.

Figure 7. Graph of probability for finding secret

7. FUTURE SCOPE

The various attacks avoidance makes system more secure. As we have considered the neighbourhood of node the future scope of this system will be to make system more powerful with neighbourhood information. Also it will be more fantastic if the whole system is implemented on real hardware. The node codeword preserves the neighbourhood information and further the social characteristics of particular node may be analysed and used for more security by neighbour nodes. In any type of system the more emphasis should be given to the security of system than the applicability. Thus this security of wireless sensor networks may achieve greater heights if many of the passive and active attacks scenarios are implemented.

8. CONCLUSIONS

Authentication is one of the best security solutions which protects whole sensor network. The security algorithm used will no longer transmit the knowledge (secret) and thus secures whole network. The main aim of this work is to design a system where each node will be authenticated before accessing or participating in network. The network is available to nodes only if they are able to satisfy all the condition of network algorithm. This technique requires less number of computations and is not having any complex operations so the scheme is very useful in resource constraints networks wireless sensor networks. The proposed security using authentication without opening the secret information is highly secured and will not be broken. Thus much of the security is obtained using this proposed scheme.

REFERENCES

- [1] O. Chipara, C.Lu, and J.A. Stankovic, "Dynamic Conflict free Query Scheduling for Wireless Sensor Networks", IEEE International Conference on Network Protocols (ICNP'06), November 2006.
- [2] Canming Jiang, Bao Li and Haixia Xu "An Efficient Scheme for User Authentication in Wireless Sensor Networks", 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07) 2007 IEEE.
- [3] Wood, A. D. and Stankovic, J. A., "Denial of service in sensor networks," IEEE Computer, vol. 35, pp. 54-62, 2002.
- [4] Chris Karlof and David Wagner, "Secure Routing in Wireless Sensor Networks :Attacks and Countermeasures," Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, USA., (2003).
- [5] Jeffery Undercoffer, Sasikanth Avancha, Anupam Joshi and John Pinkston, "Security for Sensor Networks", Academic Report, University of Maryland Baltimore County Baltimore.
- [6] L. Eschenauer, V. D. Gligor, A key-management scheme for distributed sensor networks In: Atluri, V. (ed.) ACM Conference on Computer and Communications Security, pp. 41-47. ACM, New York, 2002.
- [7] M. Al-Shurman and S. M. Yoo, Key pre-distribution using mds codes in mobile ad hoc networks, In: ITNG, pp. 566-567. IEEE Computer Society Press, Los Alamitos, 2006.
- [8] Seyit Ahmet Camtepe and Bulent Yener. Combinatorial design of key distribution mechanisms for wireless sensor networks. In Pierangela Samarati, Peter Y. A. Ryan, Dieter Gollmann, and Refik Molva, editors, ESORICS, volume 3193 of Lecture Notes in Computer Science, Springer, 2004.
- [9] S. A. Camtepe, B. Yener, Key distribution mechanisms for wireless sensor networks:A survey 2005. Technical Report, TR-05-07 Rensselaer Polytechnic Institute, Computer Science Department, March 2005.
- [10] S. Ruj, B. Roy, Key Predistribution Schemes Using Codes in Wireless Sensor Networks Inscript 2008, LNCS 5487, pp. 275- 288, 2009. Springer-Verlag Berlin Heidelberg, 2009.
- [11] Anupam Pattanayak, B. Majhi Key Predistribution Schemes in Distributed Wireless Sensor Network using Combinatorial Designs Revisited National conference on modern trends of Operating Systems MTOS -2009 Bhubanaswaer,2009.

- [12] Pinaki Sarkar, Amrita Saha and Morshed Udan Chowdhury, Secure Connectivity model in Wireless Sensor Networks (WSN) using 1st order Reed- Muller codes, International Association for Cryptologic Research , 2010.
- [13] Siba Ugata, Alefiah Mubeen and Samrat Sabat “ Wireless Sensor Network security using zero knowledge Protocol. IEEE communications ICC 2011 Proceedings.
- [14] Shakera Shaikh & Veena Gulhane,, “User Authentication Techniques for Wireless Sensor Networks : A Survey”, International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) ISSN No. 2248 9738 Volume 1, Issue 4, 2012.
- [15] Ismail Butun and Ravi Sankar,2011.” Advanced Two Tier User Authentication Scheme for Heterogeneous Wireless Sensor Networks”. 2ndIEEE CCNC Research Student Workshop.
- [16] X.H. Le, S. Lee, and Y.K. Lee. ”Two-Tier User Authentication Scheme for Heterogeneous Sensor Networks.” the 5th IEEE International Conference on Distributed Computing in Sensor Systems, (DCOSS '09), Marina Del Rey, California, USA, June 8-10, 2009.
- [17] Omar Cheikhrouhou^{1,2}, Anis Koubaa^{3,4}, Manel Boujelben¹, Mohamed Abid¹,2010.” A Lightweight User Authentication Scheme for Wireless Sensor Networks” International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing.
- [18] C. Jiang, B. Li, and H. Xu, “An efficient scheme for user authentication in wireless sensor networks” in 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), 2007.
- [19] L. Lazos and R. Poovendran. “Secure Broadcast in Energy-aware Wireless Sensor Networks”. IEEE International Symposium on Advances in Wireless Communications (ISWC'02), 2002.
- [20] Huang, Q., Cukier, J., Kobayashi, H., Liu, B., Zhang, J. Fast authenticated key establishment protocols for self-organizing sensor networks. In: ACM WSNA 03, 2003.