ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

# Identification of a Clone Nodes in Static Wireless Sensor Network using Secure Key Distribution Mechanism

N.S.Usha[1], K.Srilekha Nivetha[2]

Associate Professor, S.A Engineering College, Chennai, Tamil Nadu, India[1]

Dept. of Computer Science Engineering, S.A Engineering College, Chennai, Tamil Nadu, India[2]

**ABSTRACT**: Usuallyin Wireless Sensor network,the sensor nodes are deployed in unreachable environment where they can be easily attacked by many serious attacks. One of such attacks is Node Replication Attack where the attacker creates multiple duplicate nodes as legitimate nodes and deploy them in the network .Adversary mainly deploys such nodes to disrupt the services of the network .Many researches have been done to identify the clone node in the network, but all these schemes ends with some demerits. The secure transmission in wireless sensor networks can be ensured effectively by means of secured key distribution mechanisms. Normally Key managementscheme includes severalimportant phases like key updating, key distribution and key generation to detect the clone node in the network. Thispaper mainly focuses on the various key distribution mechanisms implemented to identify clone nodes in the network. Also,it highlightsthe merits and demerits of various mechanisms

**KEYWORDS:** Wireless Sensor Network, Node Replication attack, Key Distribution Scheme, Clone Node

## I. INTRODUCTION

Wireless sensor network are collection of distributed sensor nodes, which are small, tiny and low cost. They have been to monitor the environment and collect the data. These collected information obtained by monitoring can be stored and sent to the desired locations. These sensors have the ability to monitor the environmental conditions like sound, temperature, pressure etc. The applications of wireless sensor network include military applications, healthcare and industrial monitoring applications[1].

In WSN, Many attacks are done to the sensor nodes, one of the major attack for sensor network is Node Replication Attack. In node replication attack, the attacker captures any node in the network and places to collect all information from that node. If the base station is attacked it is very difficult to recover such replication attacks. Node replication attacks creates replicas and places them in various position in the network to disrupt its operations. In centralized system, the nodes communicates with others via base stations. Theneighbor nodes submit ID to the base station. If the base station receives two information with same ID, It declares that node as a clone node.

In [2] , The sensor nodes are efficient in sensing the environment and delivering the data to the base station, thus those nodes should be secured using many schemes like zone routing scheme, key distribution scheme etc.

A Wireless Sensor Network is an Independent configuring network of small sensor nodes which communicate with each other using radio signals or Network based system and deployed in various places to sense the environment for various applications. WSN helps to communicate between the real world and virtual world. WSN helps in sensing places where human or any living being can sense. WSN has huge scale of application in different fields such as military, environmental and commercial applications. Remote sensor systems (WSNs) comprise of lightweight gadgets

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

with minimal effort, low power, and remote correspondence. The sensors can speak with each other to frame a system. In WSNs, communicate transmission is generally utilized alongside the greatest use of remote systems and their applications. Thus, it has turned out to be urgent to validate communicate messages. Key administration is likewise a dynamic research theme in WSNs. A few key administration plans have been presented, and their advantages are not perceived in a specifics application. Security administrations are imperative for guaranteeing the respectability, validness, and privacy of the basic data. In this manner, the validation systems are required to help these security benefits and to be strong to particular attacks. Different verification conventions, for example, key administration conventions, lightweight confirmation conventions, and communicate validation conventions are thought about and broke down for all protected transmission applications.

The two types of WSN are Static wireless sensor network (SWSN) and Mobile wireless sensor network (MWSN). In SWSN, the position of the sensor nodes are fixed at the time of deployment and does not change and they use fixed routing. In MWSN the sensor nodes move freely after deployment in the network and use dynamic routing mechanism to route.

## II. THE OSI MODEL

The role of the OSI model deals with the communication between the users and the developers. It also describes the step by step analysis of the message transmission between different layers of the network. Each layer of the model uses the other layer as the base and passes information to higher level layers in the network.

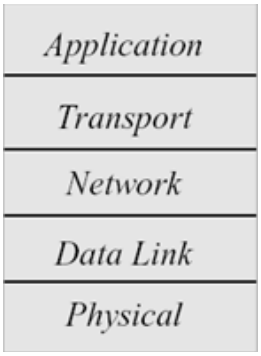


Fig.1- OSI layers

## III. ATTACKS ON WSN

The attacks on WSN is differentiated into various types:

1. **Layer Dependent Attacks** are mainly depended on different applications of the OSI model. The layer dependent attacks are Routing attack, Data Integration attack, Localization attack and Time synchronization attack.
2. **Layer Independent attacks** are independent for applications.The layer independent attacks are Node Replication attack and Sybil attack.

### Passive attack versus Active attack

In passive attack, the attacker catches the information/data but doesn't modify the content. It just delays the data transmission, tries to modify the content and then transmit it in the network. Routing attack belongs to active attack family some of the routing attacks are as follows:

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

1. **Black hole attack** consists of various malicious nodes that advertise their route as the optimized shortest path to specific destination and gather all network traffic and also drop all packets. As a result, there is a loss in critical information in the network.
2. **Sybil Attack (Network Layer)** is a node assumes itself as another node and thus causes several replicas in the network. This attack degrades the security, data integrity, and also the resource utilization. This results in data loss which is a great threat to the network.
3. **Jamming (Data Link Layer)** isthe jammer interfere with the transmission and reception of wireless communications. Jamming is a kind of Denial of Service attack. The nodes prevent other nodes from communicating to the channel by occupying itself.
4. **Worm Hole Attack (Network Layer)** can be easily launched without the prior knowledge about the network. `The attacking node fakes the route that is shorter than the original and thus confusing the routing mechanisms in the network. The attacking node captures the packet and transmits to other nodes which distributes them locally.
5. **Hello Flood Attack** is the attacker nodes broadcasts the hello message to the nodes in the network and acts like the destination.
6. **Node replication Attack** is the attacker captures a legitimate node and creates multiple clone nodes with the same ID and information and deploys them at various locations. These replicas acts like original node and tries to get all the information and causes threat to security of the data.

**Node Replication Attacks in WSN**

In Node replication attack, the attacker captures a legitimate node and then copies all the information from the captured node. It creates many replicas with the same ID to act as legitimate nodes which are deployed at different locations in the network in order to disrupt the network functionality

**Steps Involved in Occurrence of Node Replication Attack**

1. The sensor nodes are deployed in the network (fixed).
2. After their deployment, the adversary tries to capture one legitimate node in the network.
3. The attacker node extracts all the confidential and cryptographic information from the captured node.
4. The attacker creates multiple replicas of the captured node.
5. These clone nodes have with same ID as captured node are deployed in the network at various locations in order to disrupt the network services.

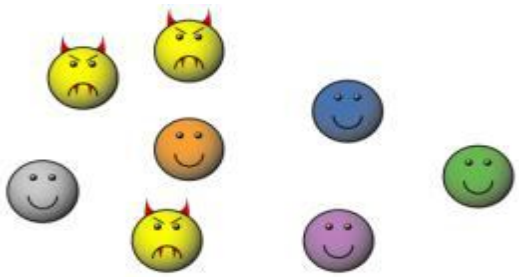

Fig.2- Node Replication attack

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

## IV. RELATED WORKS

Many researches have been carried out to identify clones in network. Some of the works are as follows:

In [5], Probabilistic Key Predistribution in Mobile Networks Resilient to Node-Capture Attacks Analysis on connectivity and resilience are widely studied by q-composite key predistribution scheme. Forconnectivity, ensuring two sensors to find a path through conditions such asNode capture attack, Sensormobility, Physical transmission constraints, and the boundary effects of network field, Link reliability .In Existing model,it allows the adversary capture of random set of sensors but in Proposedmodel, it allows the adversary capture of arbitrary set of sensors.

In [10], Random key predistribution scheme is used for securing heterogeneous wireless sensor networks. Each of the n-sensors in the network is classified into r-classes Class -1 sensor is assigned to K1 cryptographic keys .Once deployed, a pair of sensors can communicate securely if and only if they have a common key. Communication topology of this network by newly defined in homogenous random key graph by establishing scaling conditions on parameters p and {k1……kr}. It does not contain any isolated nodes. Also the nodes are connected with highly secured probability. The results are given in the form of zero-one laws and the number of sensors n growing unboundedly large.

In [7], current conditions to guarantee unassailability and unsplittability in secure sensor organizes under the q-composite plan. Unassailability guarantees that an enemy catching any set comprising of an immaterial portion of sensors can trade off just an unimportant part of correspondence joins in spite of the fact that the enemy may bargain correspondences between non-caught nodes, which happen to utilize keys that are shared by caught nodes. Unsplittability implies that when an irrelevant division of sensors are caught, nearly the greater part of the rest of the nodes are still safely associated. Based on the effects of network, unassailability, and unsplittability, secure sensor systems are deployed.

In [8], Researchon k-availability in secure remote sensor arranges under the irregular pairwise key predistribution conspire with unreliable links. When remote correspondence joins are displayed as autonomous on-off channels, this adds up to dissecting an irregular chart demonstrate shaped by converging an arbitrary K-out chart and an Erd˝os-Rényi diagram. Current conditions on the best way proportional the parameters of this convergence demonstrate so that the subsequent chart is k-associated with drawing closer to one (resp. zero) as the quantity of nodes gets extensive. The coming about zero-one law is appeared to enhance and overcome the past outcome on the 1-availability of a similar model. It moreover results in numerical outcomes.

## V. PROPOSED MODEL

In proposed model, the nodes are created and deployed in the network with assignment of key values to each node. The assigned keys are used as the primary key to the nodes by using Diffie-Hellman algorithm. After generation of keys from the nodes, the proposed algorithm called as ECC (ELIPTIC CURVE CRYPTOGRAPHY) algorithm is used to identify the next secured node in the network to transmit data from sender to receiver.

### *Key Distribution Mechanism*

Key distribution scheme is the major security mechanism for detecting the node replication attacked nodes in the network. Using key distribution scheme the secret key is distributed to all the nodes in the network. when the message is to be transmitted from the source node to the base station it gets the key from the source node and encrypt the message and look for the same message in next node , if both are same it transmits the data to the neighbouring node or the base station .

### *Categories of Key Distribution Schemes*

1. Location-Independent key distribution scheme
2. Location-dependent key distribution scheme

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

***Key Management Life Cycle***

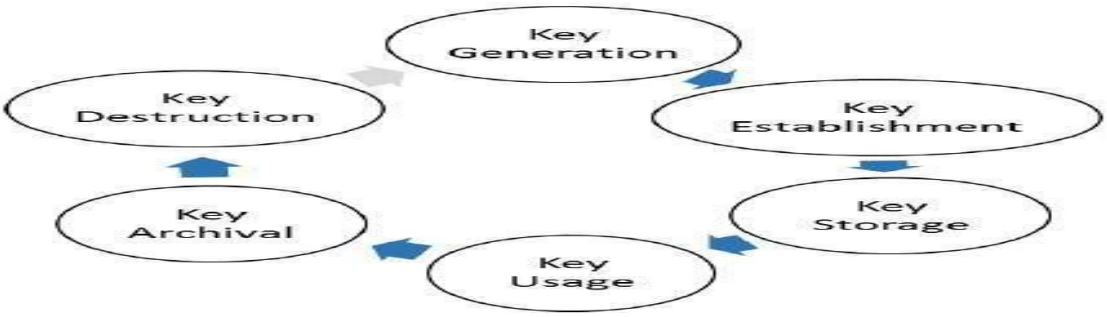


**Fig.3- Key Management life cycle**

***Key Agreement in Wireless Sensor Network***

Two neighboring nodes establish a shared secret key only to themselves.

The shared key is prerequisite for

1. Message encryption / decryption

2. Message Authentication.

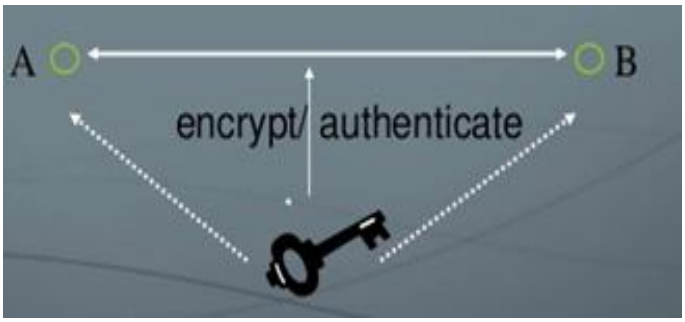


Fig.4- Key authentication phase

**VI. MAJOR METRICS FOR USED FOR EVALUATING KEY DISTRIBUTION SCHEME**

**Detection Rate-**Detection of clone node is the major metric where using key distribution scheme the node replication attack is detected and it is recovered from the sensor network.

**Bandwidth-Bandwidth** is the capacity and number of nodes that can be connected to the network .bandwidth should be large to provide large better performance.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

**Power Consumption** -Power consumption is the metric where the every node has some power for transmitting data from one node to another, thus the power consumption should be minimised to improve the life of the sensor so that it will enrich the duration of the node existing in the network.

**Limited Memory Resources** - The flash memory of a single sensor node is at most tens of megabytes.

## VII. COMPARISON OF VARIOUS KEY DISTRIBUTION SCHEME

The table summarizes the effects of various key distribution scheme based on the metrics of evaluation.

| Methods | Storage | Computational Complexity | Transmission Complexity |
|---|---|---|---|
| 1. Single key scheme | 1 | 0 | 0 |
| 2. Fully pairwise key scheme | n-1 | 0 | 0 |
| 3. Bloom's method | $O(\lambda)$ | $O(\lambda)$ | 0 |
| 4.Random perturbation-based key establishment scheme | $O(t)$ | $O(t)$ | 1 |
| 5. Eschenauer and Gligor's method | $O(r)$ | $O(r)$ | $O(r)$ |
| 6.*q*-Composite scheme | $O(r)$ | $O(r)$ | $O(r)$ |
| 7. Multiple space key pre-distribution scheme | $O(\lambda * \tau)$ | $O(\lambda * \tau)$ | $O(\lambda * \tau)$ |
| 8. Polynomial pool-based key pre-distribution scheme | $O(t^*\|Fi\|)$ | $O(t^*\|Fi\|)$ | $O(t^*\|Fi\|)$ |
| 9. Combinatorial design-based key pre-distribution scheme (BIBD-based method) | $O(r)$ | $O(r)$ | 0 |
| 10. Combinatorial design-based key pre-distribution scheme (hybrid design-based method) | $O(r)$ | $O(r)$ | $O(r)$ |
| 11. Expander graph-based key pre-distribution scheme | The expansion factor of the underling expander graph | The expansion factor of the underling expander graph | The expansion factor of the underling expander graph |
| 12. PIKE key pre-distribution scheme | $O(n^{0.5})$ | $O(1)$ | $O(n^{0.5})$ |
| 13. Random assignment set selection key pre-distribution scheme | $O(n^{0.5})$ | $O(1)$ | $O(n^{0.5})$ |
| 14. Pseudo-random function-based key pre-distribution scheme | $O$(r) | $O(1)$ | $O(1)$ |
| 15. Method by Tsai *et al.* | $O(1)$ | $O(1)$ | $O(1)$ |
| 16. BABEL key pre-distribution scheme | $O$(r) | $O$(r) | $O$(r) |
| 17. Method by Law *et al.* | $O$(r) | $O$(r) | $O$(r) |
| 18. Noninteractive key establishment scheme | $O(\lambda)$ | $O(\lambda)$ | 0 |

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

## VIII. CONCLUSION

The results of various key distribution scheme for detecting node replication attack for transmission of data in wireless sensor network is improvised to provide maximum Security, bandwidth and reduces the power consumption of the sensor nodes. Key distribution scheme uses various algorithms and distribution mechanisms to provide efficient security for the network .Because of the nature of limited resources on wireless sensor nodes, many researchers have conducted different techniques to propose different types of key distribution mechanisms. In this paper, we first summarize the characteristics, limitations, and evaluation metrics for key distribution in wireless sensor networks. Then, the state-of-the-art techniques of existing solutions are categorized and described. The key distribution schemes are presented in a chronological order and divided into location-independent key distribution schemes and location-dependent key distribution schemes. Key distribution in wireless sensor networks is still an active research area. More researches are needed to address the challenges before wireless sensor networks can be deployed efficiently and effectively.

## REFERENCES

[1] Osman Yagan,"Zero-One Laws for Connectivity in Inhomogeneous Random Key Graphs",Accession Number: INSPEC 16138964, DOI: 10.1109/TIT.2016.2574742,IEEE Transactions on Information Theory( Volume: 62, Issue: 8, Aug 2016 ).
[2]Guoqiang Mao; Brian D. O. Anderson,"Towards a Better Understanding of Large-Scale Network Models", INSPEC Accession Number: 12673835, DOI: 10.1109/TNET.2011.2160650, Published by: IEEE/ACM Transactions on Networking( Volume: 20, Issue: 2, April 2012 ).
[3]Tao Yang; Guoqiang Mao; Wei Zhang, "Connectivity of Large-Scale CSMA Networks",INSPEC Accession Number: 12786908 ,DOI: 10.1109/TWC.2012.041912.111475, Published by: IEEE Transactions on Wireless Communications( Volume: 11, Issue: 6, June 2012).
[4]Osman Yagan, "Performance of the Eschenauer–Gligor Key Distribution Scheme Under an ON/OFF Channel",INSPEC Accession Number: 12728184 ,DOI: 10.1109/TIT.2012.2189353,Published by: IEEE Transactions on Information Theory( Volume: 58, Issue: 6, June 2012 ).
[5]Jun Zhao,"Topological Properties of Secure Wireless Sensor Networks Under the $q$ -Composite Key Predistribution Scheme With Unreliable Links", INSPEC Accession Number: 16962259 ,DOI: 10.1109/TNET.2017.2653109, Published by: IEEE/ACM Transactions on Networking( Volume: 25, Issue: 3, June 2017 ).
[6]Guoqiang Mao; Brian D. O. Anderson,"Connectivity of Large Wireless Networks Under A General Connection Model", INSPEC Accession Number: 13307136 ,DOI: 10.1109/TIT.2012.2228894, Published by: IEEE Transactions on Information Theory( Volume: 59, Issue: 3, March 2013 )
[7]Faruk Yavuz; Jun Zhao; Osman Yağan; Virgil Gligor,"k -Connectivity in Random $K$ -Out Graphs Intersecting Erdős-Rényi Graphs",INSPEC Accession Number: 16669110, DOI: 10.1109/TIT.2016.2634422, Published by: IEEE Transactions on Information Theory( Volume: 63, Issue: 3, March 2017 ) .
[8]Jun Zhao," On Resilience and Connectivity of Secure Wireless Sensor Networks Under Node Capture Attacks",INSPEC Accession Number: 16596037,DOI: 10.1109/TIFS.2016.2613841, Published by: IEEE Transactions on Information Forensics and Security( Volume: 12, Issue: 3, March 2017 ).
[9]Dae Hyun Yum; Pil Joong Lee,"ExactFormulae for Resilience in RandomKeyPredistributionSchemes" INSPEC Accession Number: 12728726 ,DOI: 10.1109/TWC.2012.031212.110887, Published by:IEEE Transactions on Wireless Communications( Volume: 11, Issue: 5, May 2012)
[10]Jun Zhao,"Probabilistic Key Predistribution in Mobile Networks Resilient to Node-Capture Attacks", INSPEC Accession Number: 17171178 ,DOI: 10.1109/TIT.2017.2721424, Published by: IEEE Transactions on Information Theory( Volume: 63, Issue: 10, Oct. 2017 ).