Node Replication attack detection using Dydog in Clustered sensor network

Dissertation submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering

in

Information Security

Submitted By

Harpreet Kaur

(Roll No. 801533009)

Under the supervision of:

Dr. Sharad Saxena

Assistant Professor, CSED

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

July 2017

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "Node Replication attack detection using Dydog in Clustered sensor network ", in partial fulfillment of the requirements for the award of degree of Master of Engineering in Information Security submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of Dr. Sharad Saxena and refers other researcher's work which are duly listed in the reference section. The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Harpreet Kaur

Harpreet Kaur

801533009

ME (IS)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Sharad Saxena)

Assistant Professor, CSED

Thapar University, Patiala

ACKNOWLEDGEMENT

I would like to express my gratitude to my supervisor Dr. Sharad Saxena for his valuable advice, constant guidance, inspiration and cooperation throughout my research work at Thapar university, Patiala. Without his guidance, this research work would never have been a successful one. He helped me to find the problem statement, proposed solution and generate desired results. I also want to thank Dr. Maninder Singh, Head of Department, Computer Science & Engineering, Thapar University, for his cooperative support during the work. Last, but not the least I would like to thank my parents, my closest and dearest friends who have been the constant source of motivation throughout the work.

Harpreet Kaur

(801533009)

ABSTRACT

Wireless sensor network is an emerging area in which multiple sensor nodes are deployed to perform monitoring tasks. Sensor nodes are deployed in an open environment or infrastructure which can be easily affected by number of mischievous attacks such as wormhole attack, Sybil attack and node replication or duplication attack etc. security is the important consideration in wireless sensor environment. Node replication attack is one of the dangerous types of attack in which attacker may generate the replica or clone of existing node in the same network by extracting all the credentials. There may be case when the attacker replicates the whole cluster and attack the multiple nodes in one go. So, we use the Dydog detection method for defending against node replication attack. It is the intrusion detection process which is based on the monitoring nodes. The clustered network is taken into consideration in which clustering is done by underwater density based clustering sensor network (UWDBCSN) algorithm. The detection approach is integrated with sleep/wake scheduling algorithm to enhance the network performance. The parameters evaluated by simulating the clustered sensor environment in NS2 are packet delivery ratio, delay, network overhead, energy consumption and throughput.

Keywords: WSN, UWDBCSN, Dydog, Sleep/wake scheduling

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVATIONS

WSNs	Wireless Sensor Networks
MANETs	Mobile ad-hoc networks
CH	Cluster Head
BS	Base Station
LEACH	Local Energy Adaptive Clustering Hierarchy
LNCA	Local Negotiated Clustering Algorithm
UWDBCSN	Under-water density based clustering sensor network
AMC	Adaptive multi-hop cluster based scheme
HEED	Hybrid, Energy Efficient, Distributed Clustering
MIMA	Man in the Middle attack
DOS	Denial of service attack
DDOS	Distributed Denial of service attack
NAM	Network Animator
TCL	Tool Command Language
PDR	Packet delivery ratio

CHAPTER 1

INTRODUCTION

1.1 Introduction

Wireless sensor networks (WSNs) consist of large number of tiny sensor nodes which are emerging in an area that is easily affected by malicious users. Sensors are basically small devices which has the ability to sense, record and process the information. Sensors network are found to be present everywhere [1] [2]. They are meant for measuring some physical parameters like pressure, sound, temperature, chemical composition etc. Each sensor contains some components like transceiver, microcontroller, external memory, power source etc. Due to ease of deployment and inexpensive nature of sensor nodes, WSN is used in various important applications such as military and security application, seismic monitoring, health monitoring, industrialized automation, robust monitoring etc. wireless sensor network is considered as a broad area of research because many critical applications directly or indirectly depend upon sensor networks [3]. Sensor nodes communicate through various routing protocols. Sensor nodes may be mobile and static. Mobile sensor nodes can be able to communicate through mobile ad-hoc networks (MANETs). In an ad-hoc network, nodes are distributed in an area communicating through multiple hops with each other by forwarding data packets [4].

Due to increase in the dependability on sensor network, there is decrease in the security of data. They are easily affected by attackers as they possess less security mechanisms. Security is a major concern as any malicious user can be able to misuse the critical information by launching dangerous types of attacks such as wormhole attack, denial of service attack, node replication attack, routing attack, spoofing attack etc. So, there is a need to equip the sensor network with some security mechanism in order to ensure confidentiality, integrity and authenticity of data [5].

1.2 Structure of WSN

WSN is an emerging area that consists of multiple sensor nodes (either mobile or static), a sink station, wireless medium and a base station (task manager). The components of WSN are described below and shown in figure 1.1:

- **Sensor field:** Sensor field is like a coverage area for example a forest, an ocean, home etc. in which sensors are deployed in distributed manner.
- **Sensor node:** Sensor node is a small device which contains four components that are transceiver, power source, microcontroller, sensing unit and processor. Working of sensor node is to collect, process and record all the data traffic that is communicating through whole network.
- **Sink:** Sink is the point where every sensor node forwards the collected data which is later aggregated in order to start communication with the sink station.
- **Base station:** Base station is the interface point between the end users and the network. It provides all the services to the user according to their requirements. It manages all the communicating tasks that are going in between the sensor nodes. So, it is also called task manager.

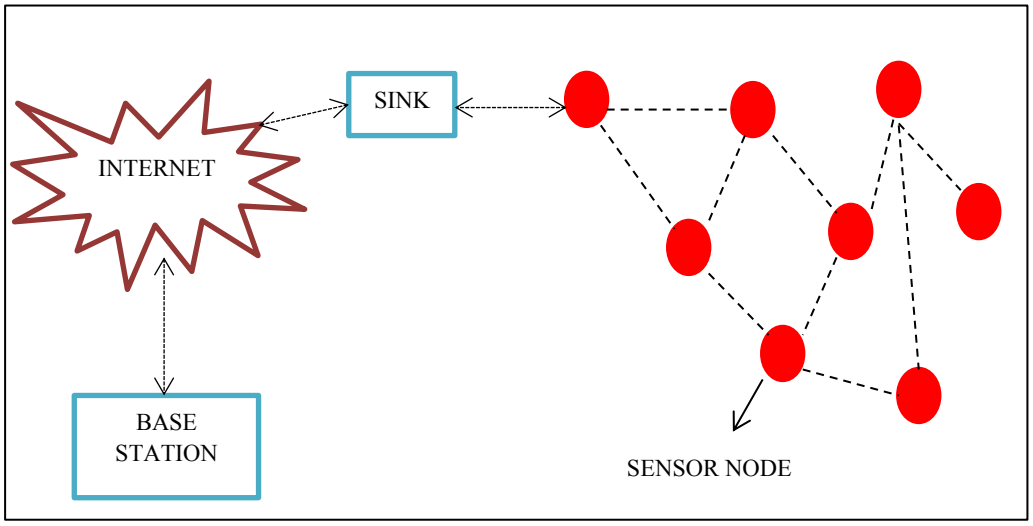

Figure 1.1: WSN structure

1.3 Characteristics of WSN

The important characteristics of WSNs are described below:

1. **Scalability:** Sensor networks possess dynamic topology in which we can either increase or decrease the number of sensor nodes. So WSNs are scalable enough to handle the large number of sensor deployment.
2. **Resilience:** WSNs are highly resilient that's provide an immediate service if any fault or node failure occurs within the network. It has the capability to cope with all the structural changes which will never effect the normal operation of sensor nodes.
3. **Self-organized:** The randomly deployed sensor nodes can adjust easily and work in a cooperative manner. Sensor nodes may be mobile or static depends upon whether we are using ad-hoc network or not. They tend to communicate with each other by forwarding the data packets in the organized way from one hop to another.
4. **Multi-hop communication:** Sensor nodes transmit the data packets through multiple hops present in between the sender and the receiver. In this way, every sensor nodes check the authenticity of the data packet and then forward to the next hop until the data packet reaches to its destination node securely.
5. **Application- oriented:** The vary nature of WSNs depend upon the type of application used. The deployment of the sensor nodes done accordingly and its behavior vary from application to application.

1.4 Application of WSN

WSN is used everywhere including security and military application, environment monitoring, health monitoring, industrialized automation, seismic monitoring etc. Some of the important applications are discussed below [3] [6]:

- **Environment monitoring:** Sensor nodes are working in an area to measure the parameters like temperature, pressure, humidity etc. which tells the user about environmental conditions that may happen like natural disasters, forest fire detection, air pollution and landslide. In this way preventive measure can be taken earlier.
- **Seismic monitoring:** Seismic monitoring is basically related to the detection of earthquake and measure the relative motion of earth's surface. There are

special types of sensors used for measuring relative motion called seismometers which are placed inside the surface of earth.

- **Security and military application:** For security and military applications, there are some tracking sensor devices that are placed inside the area which track the movement of any enemy vehicle and alert the army to take preventive measure. WSNs were first used in defense application. So it has great significance in various security based applications.
- **Health monitoring:** There is also some body area sensor network which has the ability to sense the different parts of the body and accordingly they give the required information about the health of an individual. These types of sensors are used in hospitals.

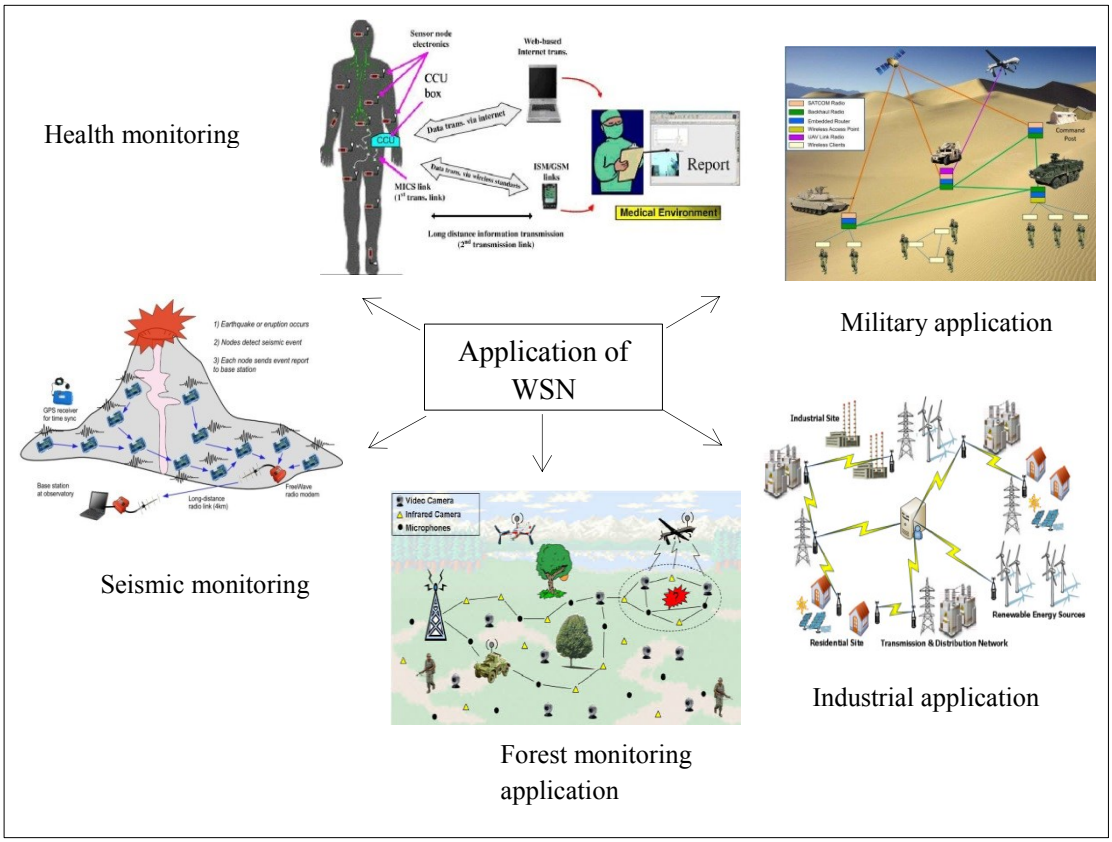

Figure 1.2: Application of WSN

1.5 Challenges in WSN

1. **Real time operation:** Mostly the critical application of WSNs deal with real time environment. Successful transmission of data packets in real time is somewhat difficult. Message loss by intermediate nodes, congestion, disturbing noise and other transmission problems delay the operation of sensor

nodes. So the delivery of packets cannot be done in time which is the main challenge in WSN.

2. **Security:** To maintain the security in WSN is the biggest challenge. Sensor networks are deployed in an environment where they can easily be affected by the malicious activities. There should be security methods associated with every sensor node.
3. **Unreliable communication:** All the data packets are broadcasted through multiple hops with connectionless routing protocols. In this way communication between nodes is not reliable. So there is need to use connection oriented protocols.
4. **Data consistency:** According to security perspective, to maintain the consistency of data is a major challenge. In the network, even the genuine node may perform some malicious activity to disrupt the whole network.
5. **Energy:** To maintain the overall energy of sensor network is a big challenge. Every sensor nodes have their own energy which is consumed when the node transmit the packets. If there are large numbers of sensors, then energy used is more. There may be the case when regular power becomes low or negligible. So there should be some technology which works in the area of energy consumption of sensor network.
6. **Computation:** There are some raw data that is left during transmission like energy source, power monitoring system, sensor devices, packets which carry encrypted information etc. must be used in an efficient way. So it may be the challenge against sensor nodes that how to process this raw data.
7. **Communication:** If you want to communicate over large distance, then you need to add more number of sensors and communication link which increases the overhead on the sensor nodes. As it takes extra cost to add the sensors on large area and communication between nodes become unreliable.

1.6 Clustering in WSNs

Clustering is the logical way of organizing the sensor nodes into clusters. Cluster head is elected who is responsible for all the conversation between clustered nodes and there is one sink node [7]. Figure 1.3 shows the clustering in sensor network consists of two cluster head and a base station (BS).

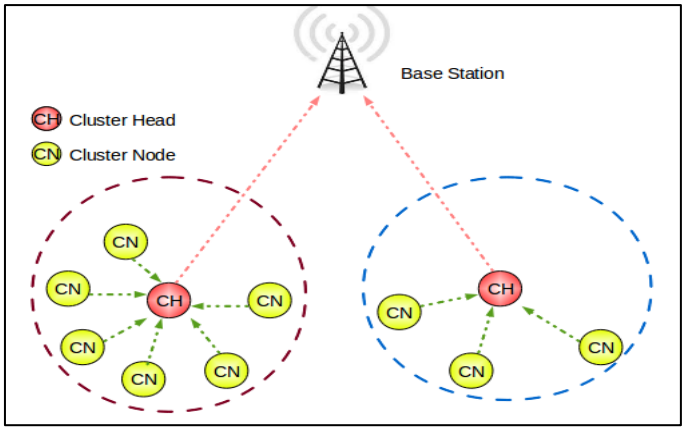

Figure 1. 3: Clustering in WSNs

There is no need to process the packets through individual nodes. If a node wants to transmit the data packets to the sink node then it first sends the packets to their elected cluster head which further forwards the data to the sink node or BS [8] [9]. So, overall energy used is less and also clustering reduces the excessive amount of energy used by each sensor. Hence increase the lifetime of network [10]. Figure 1.4 shows the different clustering protocols categorized into four categories which are explained below:

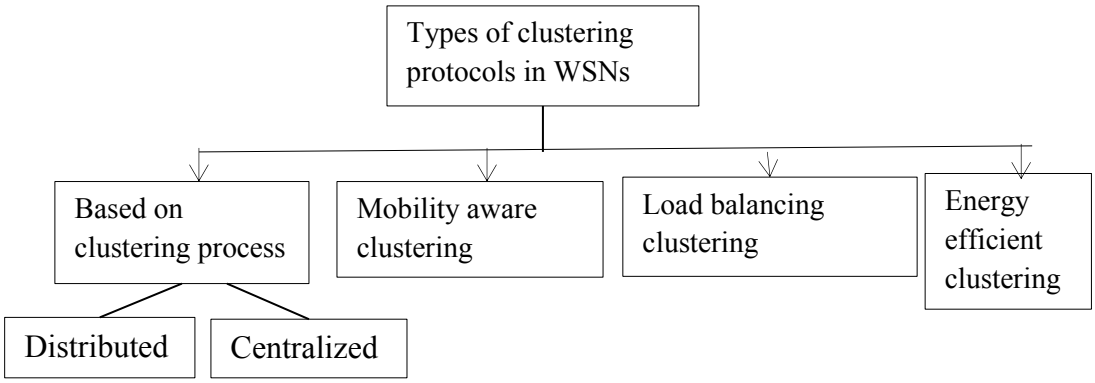

Figure 1.4: Clustering algorithms in WSNs

1. Based on clustering process: Clustering process can be divided into two types of clustering which are centralized clustering and distributed clustering.

Centralized clustering: In centralized clustering, selection of cluster head is done by base station. Centralized low energy adaptive clustering hierarchy (LEACH-C) [11] [12] protocol is an example of centralized clustering which includes the selection of

optimal number of cluster head as compared to LEACH. The two phases of LEACH-C protocol are defined below:

Set-up phase: In this phase, cluster head election is done by base station which utilizes the positioning information and current energy value of all the sensor nodes. Then average energy is calculated by base station which is a threshold value. The node which have energy greater than this threshold value is elected as cluster head by BS and other nodes become their members.

Steady-phase: This phase consists of actual transmission of packets from one cluster head to other and further forwarded the packets to BS. Figure 1.5 shows the cluster head selection phase.

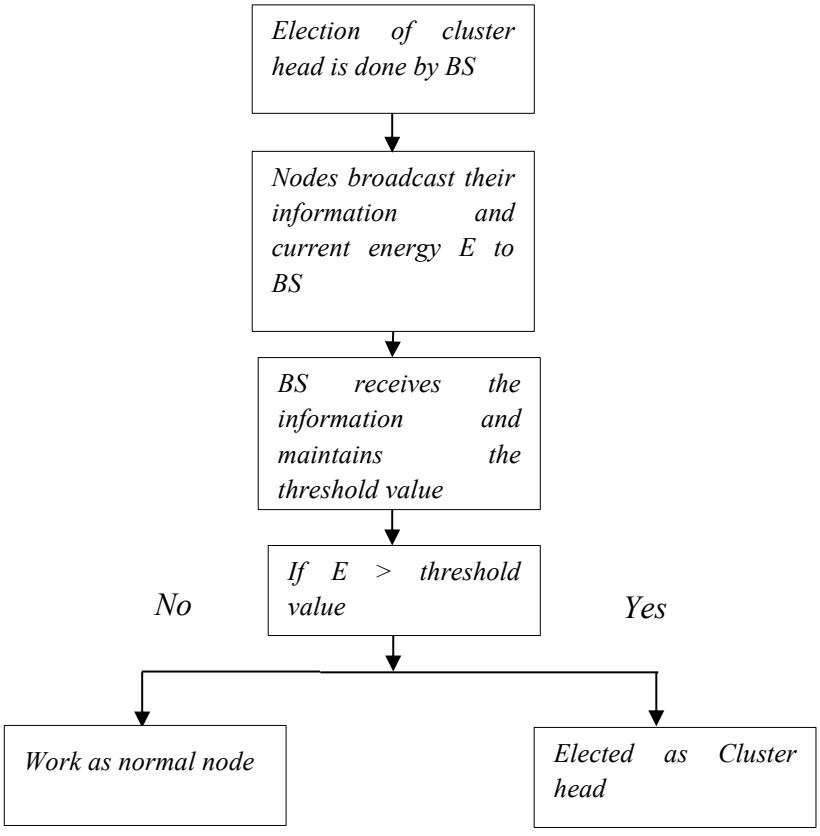

Figure 1.5: Flow diagram of set-up phase of LEACH-C protocol

Distributed clustering: In this clustering, selection of cluster head is done by nodes themselves. Low energy adaptive clustering hierarchy (LEACH) [13], Local

negotiated clustering approach (LNCA), and underwater density based clustering sensor network (UWDBCSN) are examples of distributed clustering.

LEACH [12] [13]: LEACH protocol consists of two phases which are described below:

Set-up phase: in this phase, cluster head is elected based on the energy level. The cluster head is the one which possess highest energy among all. Then every node sends a request message to become the member of cluster head. Cluster head then check the authenticity of each node and maintain the list of its member.

Steady-phase: In this phase, actual transmission of packets starts via one cluster head to another. The elected cluster head is responsible for all the communication. The node first sends the request packet to its CH and then it is forwarded to the destination node after passing through authentication phase of CH.

Local negotiated clustering approach (LNCA) [14]: LNCA clustering could be explained as follows.

1. Election phase of cluster head is done by nodes which are randomly deployed irrespective their size.
2. Each node sends a physical value to its immediate number.
3. Total number of immediate neighbors are calculated which is called node degree calculation.
4. The sensor node which possesses highest node degree is selected as cluster head.
5. Every node sends the join request to become the member of cluster head. When cluster head receive the request, it checks the authenticity and adds the node Id in its member table.

Underwater density based clustering sensor network (UWDBCSN) [15]: It is one of the clustering algorithm which perform clustering for both underwater sensor networks and WSN. It groups together the cluster nodes in such a way that high energy sensors cover the maximum of low energy sensors and vice versa. The high-density node becomes cluster head and selection is done randomly based on the basis of energy possessed by individual sensor node. This clustering algorithm gives better performance as compared to LEACH.

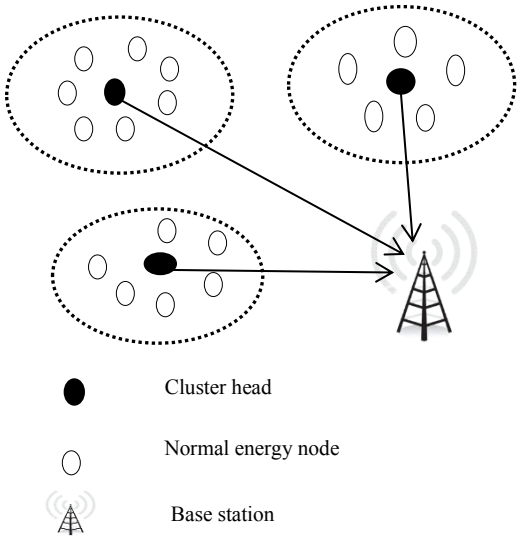

Figure 1.6: UWDBCSN clustering

2. Mobility aware clustering [16]: This clustering defines the mobility changes of sensor nodes. Formation of clusters is based on the relative motion of nodes. The inter and intra links are connected more densely and packet loss is also less. Mobile leach (M-LEACH) is advancement over LEACH which is based on the mobility speed of cluster-head. Each cluster head selects its member nodes during set-up phase. If cluster head moves away from its member node then they change their cluster head by handover mechanism provides by M-LEACH protocol in order to avoid the overlapping between clusters.

3. Load balancing clustering: load balancing clustering handles the large amount of sensor nodes in clusters in order to achieve the optimal performance and increase the lifetime. If cluster size increases or we can say that cluster head is overloaded with extra number of nodes then load balancing introduce new clusters and switch the nodes from the overloaded cluster to new cluster in order to maintain the balance. Adaptive multi-hop cluster based scheme (AMC) [17] is an example of load balancing clustering which is based on the maintenance of each cluster. Every cluster head keeps the information of all the sensor nodes and their neighbor cluster head. Cluster head must need to maintain the specific node's count in their cluster. If the nodes of a cluster are less in number then they start to merge with its neighbor cluster head and if they are more in number then they start to split into two clusters.

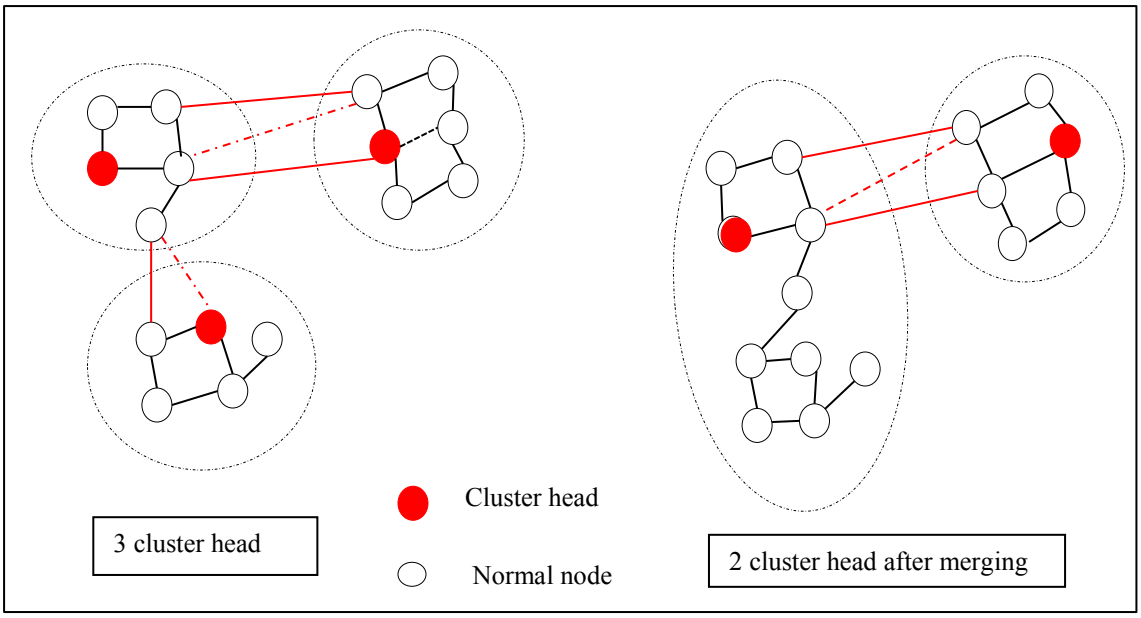

Figure 1.7: AMC clustering

Figure 1.7 represents the AMC clustering in which there are 3 clusters with their cluster heads. The clusters which have lesser nodes start merge together to form one cluster as shown in figure.

4. Energy efficient clustering: Energy efficient clustering is one of the types which increases the network lifetime because they tend to minimize the energy used between the cluster heads and their nodes. HEED [12] [18] is energy efficient clustering protocol which utilizes the resources and energy of sensor nodes efficiently. The primary parameter used by this approach is residual energy of each sensor and cluster size, communication cost are the secondary parameters. Cluster head is elected on the basis of energy. When two cluster heads possess equal energy then the one with less communication cost is considered as cluster head. When the sensor node is low in energy then they can be removed from the network and other sensor nodes may join the network and request to become the member of cluster head. The network lifetime in this clustering decreases because the main focus of this approach is to make the communication more energy efficient. Table 1.1 shows the comparison of different Clustering routing protocols.

Table 1.1: Comparison of different clustering protocols in WSN

Clustering protocols	**Cluster head distribution**	**Network lifetime**	**Overhead on cluster head**	**Complexity**
LEACH-C	Uniform	good	High	constant
LEACH	non-uniform	good	Low	constant
LNCA	non-uniform	low	high	variable
UWDBCSN	uniform	good	Medium	constant
AMC	Uniform	good	Low	variable
HEED	Uniform	low	Medium	constant

1.7 Organization of Dissertation

The organization of thesis is as follows:

- Chapter 2 explains security in WSNs
- Chapter 3 give detailed explanation of the literature review of different node replication attack detection protocols in Wireless sensor network
- Chapter 4 defines the problem statement and objectives
- Chapter 5 explains the implementation
- Chapter 6 explains simulation and result analysis
- Chapter 7 concludes the research work and its future scope

CHAPTER 2

SECURITY IN WSN

2.1 Security issues in WSNs

Security is the major concern in WSN as an attacker can launch various types of attacks because they can be able to get the useful information which may be beneficial for them.There are different types of attackers which are responsible to weaken the security of sensor network [19]. Attackers are classified into different types according to their nature which are defined below:

Active attackers: In this, an attacker try to change the actual information of the message or modify the useful information indefinitely. Masquerade attack is the one which is launced by active attackers.

Passsive attackers: They hide themselves and listen to all the conversation between the sender node and the reciever node and collect all the required information in order to launch further attacks.

Insider attackers: They are the one who has the authority to work inside the network. so it is easy for them to perform attacking operation as they know all the information which can be altered maliciously.

Outsider attackers: They are less harmful as compared to other attackers because they do not know much information but they have the ability to harm the network by taking help from other attackers.

Local attackers: There are some attackers who perform attack on a particular area of interest or we can say a confined area.

2.2 Security requirements

There are security requirements that must be taken into consideration before deploying the sensor nodes which are explained below:

Data confidentiality: Data confidentiality means data should be encrypted in such a way that messsage is only understood by intended reciever. The important information or keys can only be accessed by authorized users. Different cryptographic algorithms are used to perform encryption/decryption on data.

Data authenticity: Authentication means message is generated by authentic user or message is received by authentic user. There is a private key and digital signatures that are shared between the sender and reciever which later verified by some security mechanism. If the message received is not generated by authentic users, then that packet must be discarded.

Availability: Data availabilty means that data must be available when required by authorized users without affecting the network performance. The data must be original which cannot be altered in any way.

Non-repudiation: Non-repudiation means that data sent cannot be denied by anybody who perform transmission. If any authorized person deny that this data is not sent by him/her then it is obvious that there is presence of attackers inside the network which sent the packets. Then we can say that authenticity of the message is somewhere disrupted

Privacy: Data privacy means that the information must be placed in a secure place where none other than authorized users can find the important data and also we must add some security mechanism by the use of combined keys which cannot be easily guesssed by attackers.

Integrity: Integrity means that data over the network should not be altered during communication between sender and reciever. Digital signatures can be used to preserve the integrity of message.

2.3 Attacks on WSNs

Sensor nodes are exploited due to various types of attacks which harm the security of wsn. Figure 2.1 shows the different types of attacks which are explianed below:

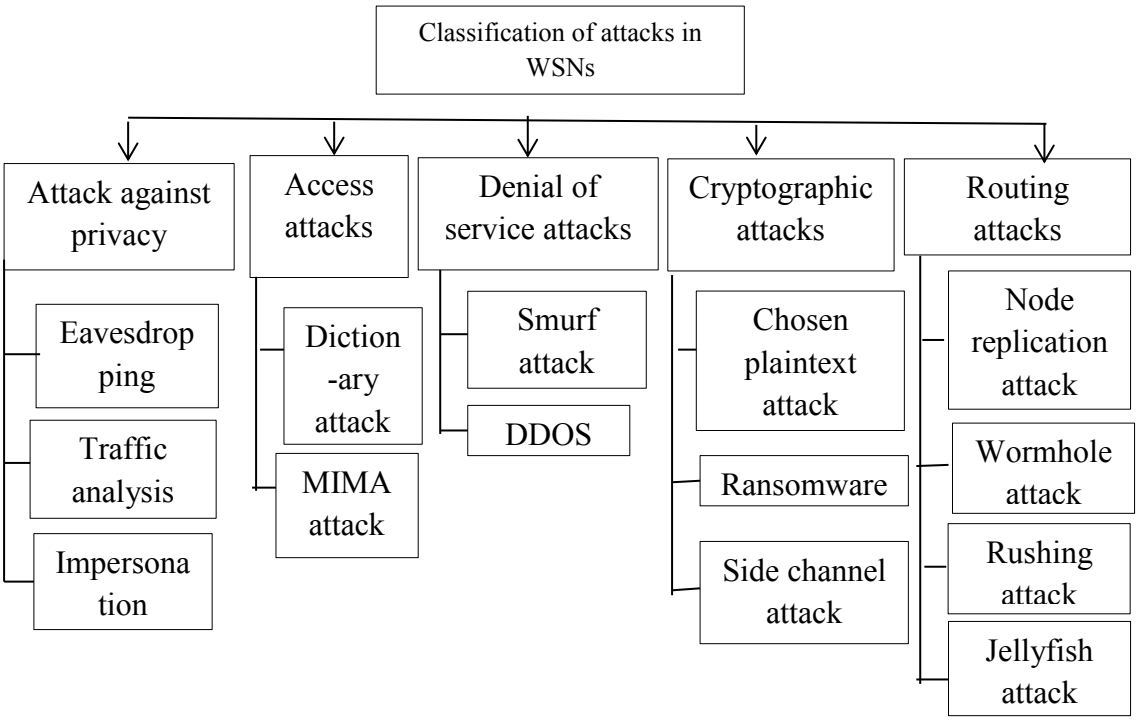

Figure 2.1: different types of attacks in WSN

2.3.1 Attack against privacy: Attacker may gain the access of the private information of nodes present in the network. Following are the examples of privacy attacks:

- **Eavesdropping attack [20] [27]:** Eavesdropping is unauthorized listening or monitoring of other people's communication. It is kind of man in the middle attack in which both sender and reciever is unaware from the attacker's activity. If preventive measures are not used then risk of becoming victim of eavesdrop attack will increase.
- **Traffic analysis attack [21] [27]:** In traffic analysis attack, attacker has the capability to discover the communication pattern between sender and reciever node. They can perform these type of attacks using some hijacking tools and capture each traffic information and analyze their behavior in order to get the useful information.
- **Impersonation attack [22] [27]:** Impersonation attack is one in which an attacker becomes successful to gain the access of legitimate sensor node and may

distrupt the network by launching various insider threats or modify the data in a malicious way.

2.3.2 Access attack: This type of attacks can be launced when attackers becomes successful to access the internal communication between the source and destination nodes and may destroy all the available resources required by the authorized users. The access attack can be dictionary attack, denial of service attack, man in the middle attack etc.

- **Dictionary attack:** A dictionary attack is one in which an attacker try to use the combination of different- different strings and match with the encryption key used in order to decrypt the embedded data. It is like cracking the key to get the useful information.
- **Man in the middle attack (MIMA) [23]:** In MIMA attack, an attacker may sit in between the legitimate users and listen to all the conversation between them and can be able to modify the conversation. An attacker may inject his/her malicious information, may send a corrupted file or virus, alter the content of message and use the important information in an unethical way to launch further dangerous attacks.

2.3.3 Denial of service attack (DOS) [24]: In DOS attack, an attacker tries to send multiple request packets and overload the reciever so that communication will not take place on time. The sender or reciever cannot able to access the data timely and important data may lost. In this attack, single attacker takes control of single sensor node. There is distributed DOS attack and smurf attack which are the example of denial of service attack.

- **DDOS [25] [26]:** Instead of targeting one sensor node or user, an attacker may utilize many sensor nodes link which are randomly distributed in order to distrupt the whole network. Attacker tries to introduce this type of attack by injecting some malicious files into the network which later perform many insider attacking operation and it could be very dangerous as attacker's main aim is to disrupt the functioning of whole network.
- **Smurf attack [26]:** In smurf attack, an attacker continuously send the number of spoofed request packets to halt the communication between the

legitimate users. That spoofed request packets are further forwarded to the sensor nodes connected which degrade the performance of whole network and hence decrease the lifetime of network.

2.3.4 Cryptographic attacks [27]: In cryptographic attack, an attacker try to weaken the security of network by analyzing or guessing the cipher text or code and other cryptographic materials. It is also known as cryptanalysis. The following attacks are cryptographic attacks described below:

- **Chosen plaintext attack:** In plaintext attack, an attacker try to match the encryption key used during the conversation. They try to decipher the text by analyzing it or by using many decryption tools.
- **Ransomware:** In ransomware attack, an attacker may lock your computer or gain access to your network and later ask for money to unlock it. The legitimate users can not able to access their own system. Wanna cry is cyber attack which recently launched by attackers in order to disrupt the security worldwide.
- **Side channel attack:** In side channel attack, an attacker can produce the attack by gaining information from physical sources such as electromagnetic leaks, even sound can produced some important information and other physical weakness can leak the important information. Side channel attacks may include cache attack, acoustic cryptanalysis, timing attack and electromagnetic attack.

2.3.5 Routing attack: [28] In routing attack, attackers may launch the different types of attack by spoofing the information contained by sensor nodes within the network. There are different types of routing attacks explained below:

- **Jellyfish attack [29]:** In jellyfish attack, an attacker introduce a malicious node which is called jellyfish node that impose the problem of delay in communication among the sender and reciever. Jellyfish nodes are difficult to detect because they look like as legitimate node as they follow all the rules of routing protocol. figure 2.2 shows the jellyfish attack inside the network.

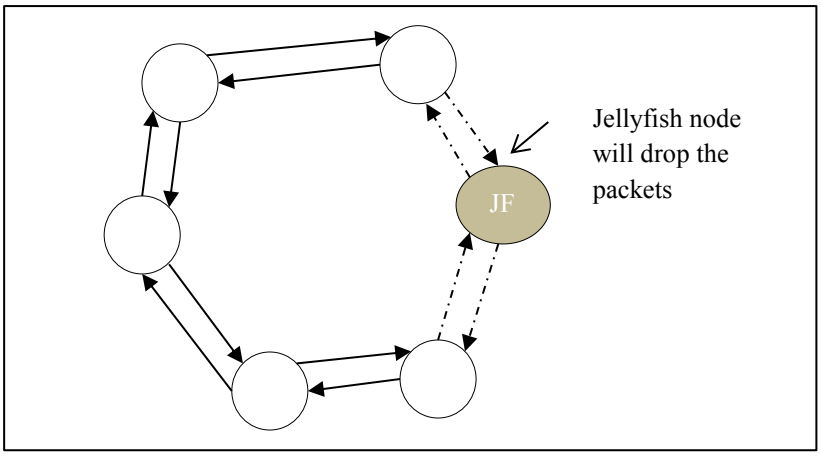

Figure 2.2: Jellyfish attack

- **Rushing attack:** In rushing attack, an attacker or malicious node tries to increase the speed of routing process. Attacker quickly gain the access by duplicating the supression mechanism and exploit the network. Figure 2.3 shows the rushing attack.

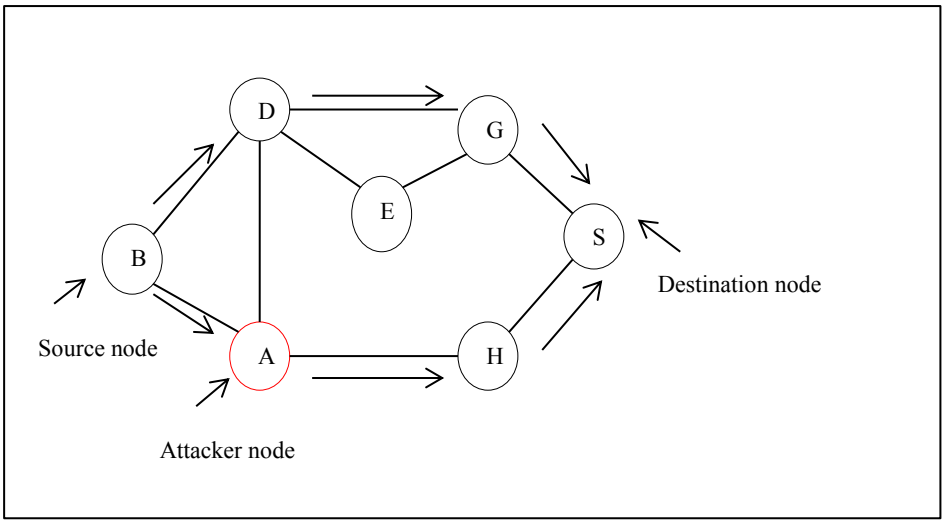

Figure 2.3: Rushing attack

When a node wants to send a packet to the reciever then it generate the request which can be received by an attacker, attacker then forward the packets to the other sensor nodes by establishing the route with maximum speed as compared to the speed of other sensor nodes. Destination node will receive the request fast from the attackers and then it will discard the other node's requests. In this way attacker successfully gain the access to

the legitimate nodes. In figure 2.3, A node is an attacker node which will perform rushing attack.

- **Wormhole attack [24]:** In wormhole attack, an attacker create a bidirectional link between the sender and reciever nodes in adhoc networks. This bidirectional link which is also called tunnel is used to access the communication and transfer the request packets from one node to another. These malicious nodes attract the other legitimate users to forward the packets through this tunnel [30]. It is very difficult to detect because sender nodes believe that they are passing the packets through shortest path. In reality, they are not the part of network. Figure 2.4 shows the wormhole attack. There are two clusters in a network which are communicating through cluster head and an attacker create a tunnel AB between these two clusters to access the state of network and perform wormhole attack.

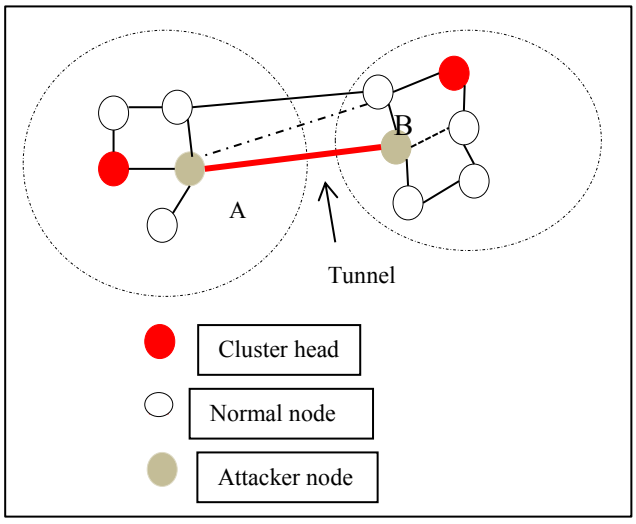

Figure 2.4: wormhole attack

- **Node replication attack [31]:** In node replication attack, a malicious person's aim is to capture a sensor node from the network and generates its replica in the same network. Attacker's aim is to extract all the cryptographic materials of a capture node and by using this information he/she becomes able to generate as many replicas as he wants. It is very difficult to detect the replicas as they possess same node ids in the network. The receiver cannot able to identify whether the request is

coming from the legitimate sender or not. Figure 2.5 shows the node replication attack inside the network.

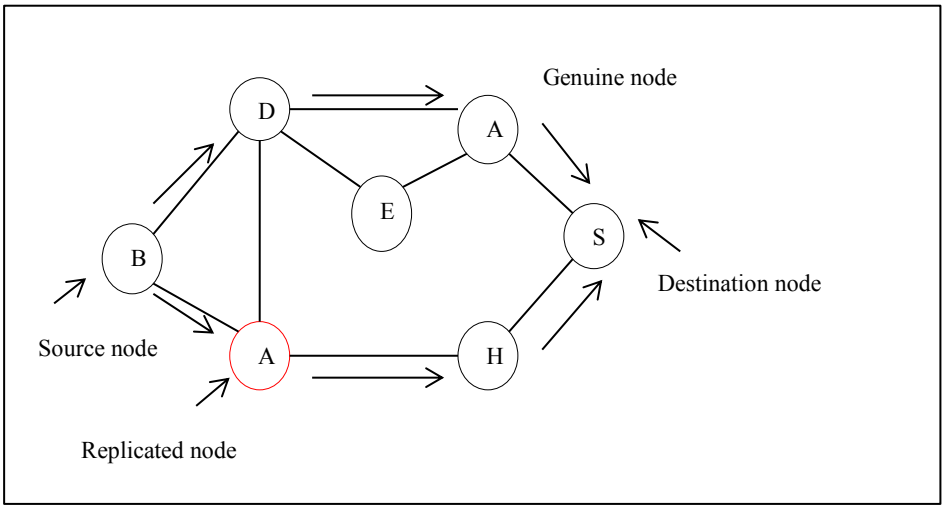

Figure 2.5: node replication attack

An attacker captures node A, extracts the information of node A and generates its replica which also take part in transmission process and the receiver thought that it is node A which is a genuine node. Figure 2.6 shows the attacker's step to perform node replication attack.

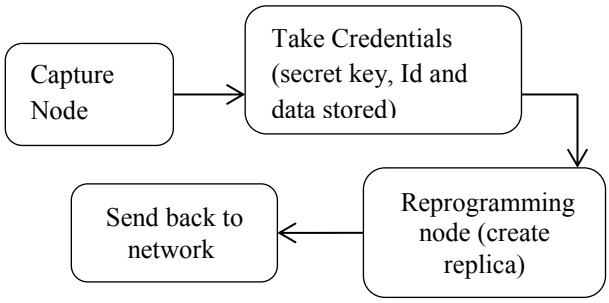

Figure 2.6: attacker's step to perform replication attack

2.4 Countermeasure against Node Replication attack

Several identification schemes are proposed to defend against node replication attack. It is very difficult to find the replicas and they may harm the functioning of entire network. It is important to identify the replicated nodes and remove them from the network [32]. The node replication identification could be divided into following three categories.

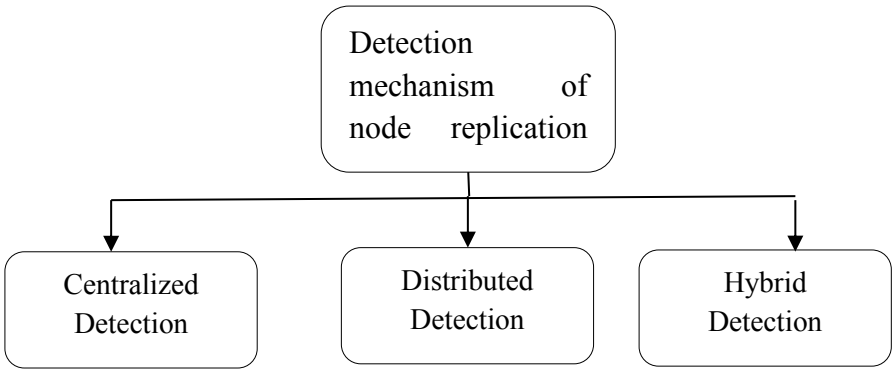

Figure 2.7: node replication attack detection mechanism

- **Centralized detection:** In the centralized network, all sensor nodes are joined to the intermediate node which is called as central base station. All the nodes depend upon the central base station for their communication and base station generate an alert message if any replicated node is detected.

- **Distributed detection:** There is no particular base station, rather they select a random node which is responsible for the detection and it may be any node and hence every node has the equal authority to participate in detection.

- **Hybrid detection:** The hybrid approach combines both centralized and distributed detection schemes and provides efficient detection against node replication attack.

Table 2.1 represents the comparison of different detection approaches of node replication attack in sensor network.

Table 2.1: Comparison of different detection approaches

Centralized	Distributed	Hybrid
Pros		
-Less communication overhead -Low sensor cost -High accuracy -Increase network lifetime	-High probability of detection -Less node movements	-Prolong network lifetime -More secure
Cons		
-Single point of failure -Low probability of detection	-Low accuracy -Decrease network lifetime - High sensor cost	-Expensive -More complex network -Does not consider a standard approach

CHAPTER 3

LITERATURE REVIEW

3.1 Literature Review

In this section, the details about various different node replication attack detection protocols are discussed which are proposed by several researchers. At the end of this section, Table 3.1 shows the comparison of different node replication attack detection protocols.

Y.Lou et al. [33] proposed single hop detection (SH-detection) which is considered to be highly resilient against replication attack. It is distributed protocol which depends on the assumption that a sensor node cannot appear at two different neighborhoods, if so then there may be presence of replicas in the network. First every sensor node signs and maintains a nearby neighbor node list which is the fingerprint description of its neighbor that shows the node Id present in its neighbor. This claim is forwarded to the one hop neighbor. Then selected witness node verifies the signature and stores it. If witness node finds out the two-clashed signature claim with similar node Id having different neighborhood, then there is presence of replicas.

C.M.Yu et al. [34] proposed extremely efficient node replica detection protocol (XED). This protocol is based on strategically approach which is remembered and challenge. Each node participates in detection procedure and tries to find the replicated node. In other protocols, the whole network is mobilized. In addition, the communication cost remains constant and does not necessarily require the location claim of every node. So this protocol is more proficient in terms of communication cost.

Y.Zeng et al. [35] proposed Random walk approach which proved to be highly proficient in Memory and communication overhead is less as compared to Randomized multicast (RM) [19]. In random walk (RAWL), every node announce their signed location information. Then neighbor node bypasses this information to the nodes in random fashion, if any of the witness nodes find the duplicate location information for the similar node value and then it can alert that this sensor node is replicated and must be discarded. Table assisted random walk (TRAWL) decreases

the excess amount of memory used in RAWL. In addition, a table is maintained by each node to cover the traces. If any replicated entry in the record is found, then digest of message claim is recorded and computed which is compare with the digest in the table, if they both are different, then it indicates the presence of replicated node.

A.K.Mishra et al. [36] proposed zone based defending scheme, it is the Hierarchical clustering based detection scheme which is location independent. In zone based replica detection scheme (ZBNRD), a public key cryptographic system is used which contain message signatures and node IDs. ZBNRD consists of two stages. In Registration stage, all the nodes choose their zone leader and registered themselves in their membership list. In defending stage, if the zone leader finds the survival of similar node Id in two different zones, then this generates clash and then revocation message is broadcasted among zones. This approach minimizes the message overhead as this approach is location independent. All the cryptographic material is send among the different zones, so there is no overhead of maintaining the large number of nodes as they are divided into different zones.

Y.Zhou et al. [37] proposed random verification scheme which is energy efficient as compared to previously discussed. Two distributed protocols are introduced namely Global deterministic liner propagation verification protocol (GDL) and Randomized multiple cells linear propagation verification protocol (RMC). GDL scheme does not effectively detect the attack as compared to RMC which gives better results. In GDL, location information travel along horizontal and vertical direction and whenever witness node detects the intersection between these two lines, then they send the revocation message to all the nodes. In RMC, the nodes can be removed and added randomly during detection process and they locate themselves using positioning algorithms. Here detection rate is high, so this is more effective as compared to GDL scheme.

W.Xie et al. [38] proposed matrix decomposition and bloom filter based detection protocol, Fingerprint is calculated using bloom filter and message is represented as matrix. The clustered nodes share their fingerprint and matrix representation with other cluster nodes and verification is done by cluster head itself. If there is any conflict in the fingerprints and cluster head detects the collision, then there is presence of replicas inside the network. So this approach decreased the storage cost of

information contained by nodes present at different location but it has drawback that it cannot detect replicas in mobile sensor network.

M.C.Geetha et al. [39] proposed distributed token based approach which is considered to be highly proficient in detecting replicated nodes and also have less overhead in terms of communication. The transmitting rate is also low because messages are combined into one token. A token is generated by the node which starts the transmission process and that token contain encrypted message which is later decrypted by the receiving node. If any of the neighbor node which receive the token having similar node Id but with different token then it can be detected easily. In this algorithm, all the nodes participate and transmission is done sequentially.

C.P. Abinaya et al. [40] proposed X-RED which is a protocol which dynamically detects the replica. X-RED has lesser memory overhead and high replication detection rate as compared to previous protocols. X-RED executes in following steps, first the starting node send its cryptographic data and location information to the node which is randomly selected. After receiving cryptographic information, verification is done by calculating the time variance between original message and replicated message. If conflict arises, then it confirms that replica is present. So this scheme is better than RM and LSM.

G.Cheng et al. [41] proposed NI-LEACH protocol which has the capability to reduce the cluster size, only the selected member of clustered nodes participates in the detection process. There is another concept introduced is intrusion detection process which includes pre- processing phase, selection of monitored nodes, observing transmission and monitoring cluster head nodes. So this improved clustering algorithm provides better results as compared to LEACH protocol for the defense of node replica attack.

J.W.Ho et al. [42] proposed sequential probability ratio test for fast detection of replication attack. Sequential Probability Ratio Test (SPRT) is a speed measurement test which has scenario that a genuine node's speed will always be lesser than the system. SPRT performs hypothesis test which include two hypothesis, one is null hypothesis which tells that replicated node is not present and another is an alternate hypothesis which tells that replicated node is present.

W.N.Y.Ji et al. [43] proposed Area based approach that is applied on clustering network. ABCD method for node replication detection achieves greater efficiency in

terms of communication overhead as compared to previous methods. There is a witness node which gathers the positioning claim of each sensor node that will be redirected to the intermediate node; this will decrease overall transmission overhead. While collecting the claims, if the witness node finds any confliction in location information then it will generate an alert to all the sensor nodes. So the message storage overhead will decrease and this approach is considered to be highly proficient as compared to Line Selected Multicast (LSM).

C.S.C.Yu et al. [44] proposed compressed sensing identification for clone based attack detection scheme (CSI). In this scheme, one fixed threshold value is marked similar to speed test. Every sensing node sends the cryptographic information and then forward to their nearest neighbor. When the base station receives all the information and senses it, if it finds the sensor reading more than that of marked threshold value, then it is considered to be replicated node.

W.Znaidi et al. [45] proposed clustering hierarchical based approach using bloom filter for replica detection. The clustering protocol used is Local Negotiated Clustering Algorithm (LNCA). For the detection of replicas, each cluster head shared their cryptographic materials (node Ids, signature, messages) with other cluster head through bloom filter mechanism and cluster head is the one which check all the cryptographic materials and verify later with the other cluster heads [5]. If there is any confliction, it generates the revocation message and alerts the other cluster heads.

P.Kaur et al. [46] proposed LEACH-C clustering defending protocol. In this detection scheme, replicas are detected in whole cluster and LEACH-C protocol is used for clustering. After clustering, one witness node is introduced which is responsible for the detection of replicas. This provides less packet movements, communication overhead and energy consumption.

Y.L.M.Wang et al. [47] proposed patrol replication detection protocol, one is with base station and another is without base station. In this detection scheme, mobile nodes are considered as patrollers who increase the overall lifetime of the network. The sensors receive their cryptic data from the patroller. Patrol nodes measure the distance between the location of genuine node and clone node and accordingly discard the replicated nodes.

Table 3.1: Comparison of different node replication attack detection algorithms

Detection Scheme	**Communication cost**	**Memory cost**	**Approach/Algorithm used**	**Simulation results**
SHD [33]	O(d.n.√n.g.p)	O(p.g.d)	Fingerprinting approach	More replicas mean high rate of detection
XED [34]	O(1)	O(n)	Remember and challenge approach	Constant communication cost
RAWL, TRAWL [35]	O(√n log n)	O(1)	Random walk approach	Lowest communication and memory overhead
RED [48]	O(d.n.√n.g.p)	O(p.g.d)	Random value generation	Average storage overhead of network increases
ZBNRD [36]	O(n √n)	O(d)	Zone based detection based on trust values	Decreased memory overhead and complexity
GDL, RMC [37]	O(√n *√m /2)	O(√n)	Intersection among cells	High detection rate and less energy consumption
Matrix and bloom filter based [38]	O (n log n)	O (n)	Matrix decomposition and bloom filter mechanism	Less storage overhead

X-RED [40]			Dynamic detection and time variance calculation	High detection probability and decreased memory overhead
Token based [39]	O (n^2)		Encryption/decryption at genuine and clone node	Less transmission overhead
NI-LEACH [41]	O(l(1+m'^{2}))	O (k.e)	Clustering based intrusion detection	Balanced throughput, more secure and less delay
LEACH-C [46]			Centralized based detection	Less energy consumption, packet loss and overhead
Random key predistribution [49]		O(n log n)	Random key value and hypothesis test	Detect and remove replica, highly secure
SPRT [42]	O(1)	O(√n)	Speed measurement test	Less detection overhead
ABCD [43]	O(n)	O(n log n)	Area clustering based	High communication overhead, increase the network lifetime
CSI [44]	O(n)	O(n √n)	Speed measurement test	Less communication burden

Hierarchical [45]	O(t)	O(√t)	LNCA and bloom filter mechanism	Better communication overhead
Patrol detection [47]		Centralized- O (n), Distributed- O (n√k)	Positioning test	Give better detection for same cost

Abbreviations: n = Nodes in the sensor network, d = Degree of neighbor node, g= Randomly selected witness node, l= Number of bit transmitted message, k= Number of clusters, m'= Distance between destination and receiver nodes, e= Energy consumed per node, k = Number of regions or zones, NDFD= Non-deterministic and fully distributed

3.2 Gaps in Study

The security of clustered wireless sensor network need to be taken into consideration because attackers may directly target the cluster head which include the number of sensor nodes and they may gain access to the multiple sensor nodes in one go. They can capture the multiple sensor nodes, produce the replica and inject into the same cluster which may disrupt the functioning of whole cluster or network. Several node replication attack identification schemes have been proposed as discussed in literature survey. There are some gaps in literature which could be summarized as follows:

- Y. Lou et al. [33] proposed single hop detection operation that performs detection in their neighborhood. So, communication cost is high.
- XED, SPRT detection approaches are only for mobile sensor network [34] [42].
- Detection approaches are not energy efficient as each node is active even when they do not take participate in transmission.
- Detection approaches do not able to find the multiple replicas in one go [41].
- The time taken by algorithm to perform detection is more as compared to the time taken by attacker to perform attack.
- Detection approaches only perform detection on single sensor node but they ignore to perform detection on clustered network which could be more dangerous. [51]
- Memory efficient protocols reduced the amount of memory space needed and energy consumption [35].

- UWDBCSN [15] is not yet used for the clustering in wireless sensor network and analyzed for any type of attacks.

3.3 Conclusion

There should be some more identification schemes in addition to the various algorithms produced by researchers related to node replication attack detection. An efficient solution should be developed to defend against this attack.

CHAPTER 4

PROBLEM STATEMENT AND OBJECTIVES

4.1 Problem Statement

As discussed in chapter 1, security is a major concern in wireless sensor network because the sensor nodes are deployed in a random area which can be easily affected by number of attacks. So there is a need to enhance the security of sensor network by using security methods to ensure the confidentiality, authenticity and integrity of the information provided by sensors. The attack can be in any form, one of the types is node replication attack in which a malicious user may able to generate many insider threats which halt the routing operations of sensor nodes either by injecting the replica or by duplicating the packets coming from sensor node or by dropping the packets. Clustered wireless sensor network is easily destroyed by this type of attack because an attacker can produce the replica of whole cluster and directly attack on the multiple sensor nodes. A lot of defending techniques against node replication attack have been developed as discussed in literature review which tends to provide the effective solution but yet there is a need of improvement. The defending approach is based on cryptography, intrusion detection and bloom filter mechanism. But cryptography methods do not give satisfactory solution to detect replicas. So in the research work, some work is done to detect the node replication attack in which multiple replicas can be detected using Dydog method which is dynamic intrusion detection and also UWDBCSN algorithm is used for the formation of clusters. In addition, the approach is combined with sleep/wake scheduling algorithm in order to make the algorithm more energy efficient. Later this detection approach is compared with hierarchical based detection which has used LNCA clustering as discussed in section 3.1.

4.2 Motivation

Wireless sensor network is an emerging area including large amount of sensor nodes which perform various important tasks. Sensors are communicating through wireless link consist of power sources, transceiver and radio signal and there is a base station which acts as a task manager to take care of all the communication between the sensor

nodes. There is a concept of clustering in sensor network which organize the sensor nodes into clusters to decrease the overhead on the network. Each sensor node consists of a leader called cluster head which is responsible for all the communication between nodes. Clustered sensor network is used in many applications like military application, habitat monitoring etc. in which data has to be transmitted over long distances. As clustering provides efficient solution, there are many challenges related to clustered network. In past few years, wireless sensor network is growing rapidly in the world of communication. The wireless sensor network is considered favorite area of interest by researchers. WSNs deals with physical changes and open challenges occurring in an environment and provide appropriate solution. But due to increase in the number of applications, the technical challenges are also increased that need to be overcome. One of the technical challenges is to increase and maintain the overall security of wireless sensor network which is weakening by number of attacks or threats produce by malicious users. The one of the most threatening attack is node replication attack that may generate many insider threats by duplicating the id of legitimate node or by extracting the cryptographic materials in order to produce a replica of that node inside the same network and confuse the receiver that who is genuine node among them. They may target the whole cluster and generate the multiple replicas simultaneously. According to the security perspective, it is important to maintain the security of network especially in ad-hoc networks which are more susceptible to many attacks. Many researchers have proposed detection algorithm to remove or detect these types of attacks but the security algorithm still need to be improved.

4.3 Objectives

- To create clusters using UWDBCSN algorithm
- To simulate node replication attack and detect the replicated nodes by using Dydog method
- To check the effect on the network, compute the performance metrics such as end to end delay, throughput, energy used, network lifetime and overhead
- To compare the performance of UWDBCSN with LNCA

CHAPTER 5

IMPLEMENTATION

5.1 Proposed algorithm

In network devices, the multiple sensor nodes are grouped together to perform routing operation of data packets through cluster heads which is known as clustering. Communication among cluster heads can be done using various clustering routing protocols such as LEACH, LNCA, UWDBCSN etc. when the communication starts, each sensor node sends the data request packets to their cluster head and then cluster head will forward the packets to the base station. In this scenario attacker may be present and extract the node id of one of the legitimate nodes and try to send the requests and may drop the packets through the route. In this way attacker nodes aim to disrupt the whole network. Some efforts have been applied to mitigate the node replication attack in WSNs. Our proposed algorithm uses the concept of clustering and later the detection schemes used is dynamic intrusion detection i.e. Dydog method which is based on the monitoring nodes in order to detect the replicas in the network.

5.1.1 Brief explanation of Implementation

The proposed work explains the different modules used during implementation. The figure 5.1 represents the flowchart of proposed work which could be explained below:

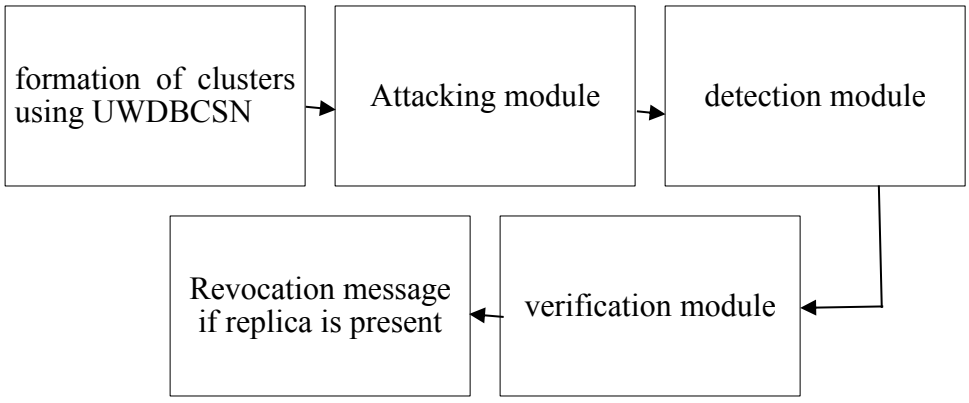

Figure 5.1: Steps of implementation work

5.1.1.1 Formation of clusters using UWDBCSN algorithm

As we discussed in chapter 1, UWDBCSN [15] is a clustering algorithm which is used to perform clustering on under water sensor networks [50]. Now we implement this clustering on wireless sensor networks in which nodes are arranged into number of clusters which are headed by cluster heads. Among randomly deployed n number of sensor nodes, n_h is the high energy senor nodes and n_l is the low energy sensor nodes. Node degree n_{deg} is used to differentiate the density of sensor nodes in the network. n_{deg} can be calculated as [15]:

$$n_{deg}(i) = \text{count}\,(n_h(j) \mid \text{distance}\,(i,j) < T_r)$$

$$\text{where } i \in n_h \text{ and } j \in n_l$$

node i and j are separated by distance(i,j), count is the total number of elements and T_r is the transmission range of node.

The algorithm works as follows:

1. All nodes n is randomly deployed. (n=50)
2. The n_h node sends the hello request to their immediate neighbor in T_r.
3. n_l node give the response and every node in n_h calculates the node degree.
4. The one with high n_{deg} is elected as cluster head and other behaves like their member.
5. Data migration will start in which nodes first send the request packets to cluster head and then it forwards the data to base station.

1.Start

2.n_h : high energy sensor nodes

n_l : low energy sensor nodes

3. do

for $\forall$ $i \in n_h$ send hello request in T_r

while $T < T_{max}$

4. calculate $n_{deg}(i) \in n_h$

5. do

Transmit $m_{deg}(i)$ to $\forall\ i \in n_h$

While $T < T_{max}$

6. if $n_{deg}(i) < n_{deg}(j)$ then

i becomes CH

else

i works as member node

7. broadcast unique Id

Figure 5.2: pseudo code for UWDBCSN

The following screenshot shows the election phase of cluster head which is done randomly because every time when node sends the packet the energy is decreased. In our scenario, four cluster heads are formed using UWDBCSN and routing of packets start. In the following figure 44 node is elected as cluster head.

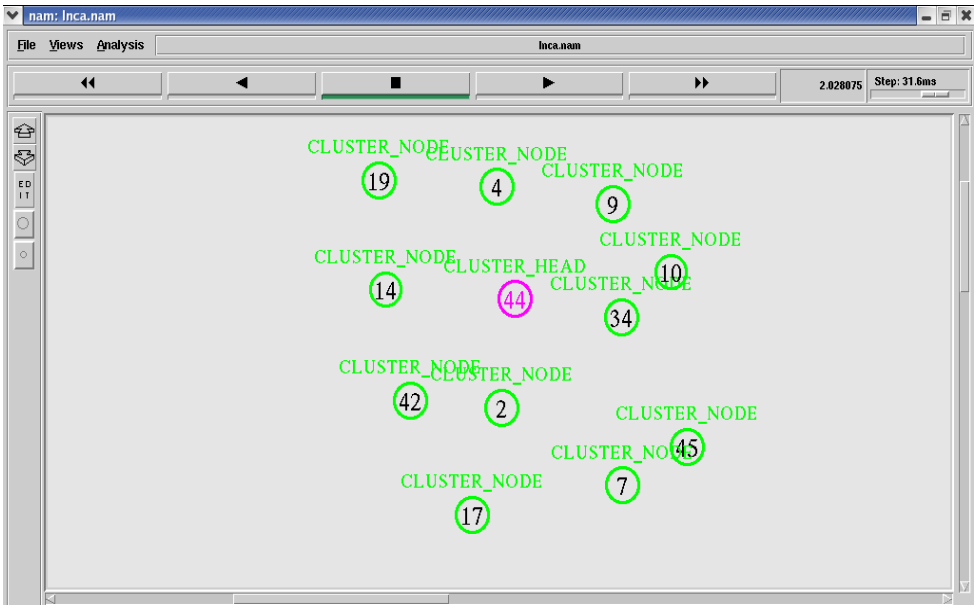

Figure 5.3: Election of cluster head using UWDBCSN

In the next step, the attacking nodes are introduced to create a malicious environment in the network which will further be detected using Dydog method implement with monitoring nodes.

5.1.1.2 Attacking module

When the sensor node wants to send the request then it first sends the hello message request to the elected CH and then it will forward the packet to the destination node or sink node. Sink node will send the acknowledgement message in return to the cluster head [7]. If there is the presence of attacker nodes in the network, then they attract the packet towards them. So, end to end delay increases as these packets are never forwarded to the sink node or cluster head [51]. The attacker nodes which are present in between the region try to send the multiple requests to the sink node in order to generate the flood of packets and pretend to be a legitimate user. The base station will halt the communication and packet dropping will start. This decreases the network performance.

The node replication attack is implemented in ns2 simulator. A malicious behavior is created in clustering environment. Two attacker nodes are injected into the network which possess the random motion and has the property to randomize the node ids. They can take the node id of legitimate sensor node and extract the information in order to generate the replica in the same network. In this scenario two attacking nodes 50 and 51 are injected into network which are given random motion and having the replication functionality. This attacking procedure shown in figure 5.4 is introduced to make the environment malicious as below:

```
$ns at 0.0 "$n(50) setdest 226.0 226.0 10000.0"
$ns at 0.0 "$n(51) setdest 470.0 221.0 10000.0"
$ns at 4.0 "$n(50) setdest 442.0 67.0.0 50.0"
$ns at 4.0 "$n(51) setdest 266.0 228.0 50.0"
$ns at 6.0 "$n(50) setdest 465.0 232.0 50.0"
$ns at 6.0 "$n(51) setdest 428.0 45.0 50.0"
$ns at 8.0 "$n(50) setdest 442.0 67.0.0 50.0"
$ns at 8.0 "$n(51) setdest 266.0 225.0 50.0"
```

Figure 5.4: Injecting two attacker nodes

Figure 5.5 is the screenshot taken in ns2 utilizing NAM (network animator) depicts the graphic view of node replication attack where node 50 and 51 are attacker nodes which perform replication operation. These attacking nodes threaten the security of the network by dropping the packets instead of forwarding them to the sink node.

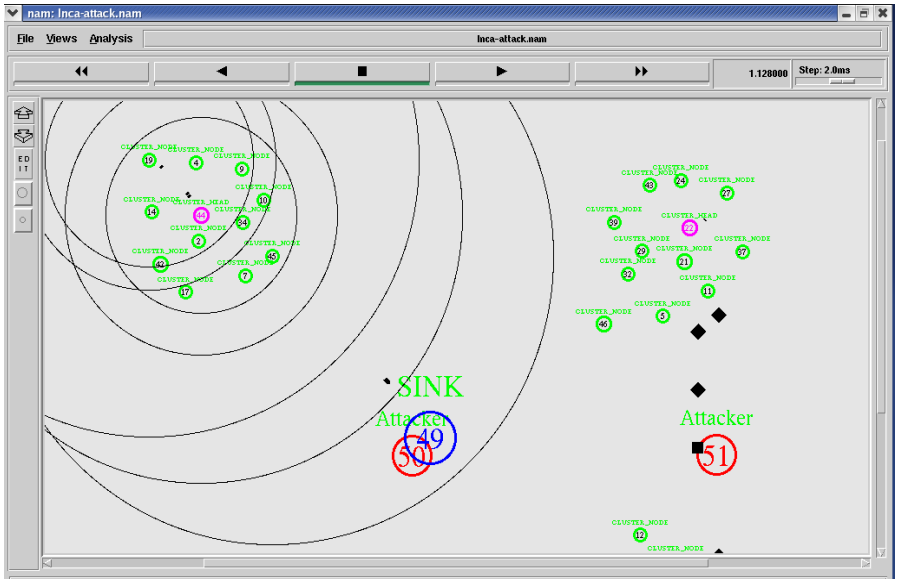

Figure 5.5: packet dropping start due to attacker nodes

5.1.1.3 Detection module

The detection of attacker nodes is done through Dydog method [52] which is an intrusion detection approach in which dynamically monitoring nodes are selected that will check the flow of data packets inside the network. The attack can be easily identified by this method. This is also known as watchdog mechanism because the monitoring nodes which will take care of all the data forwarding process are watchdog [52] [53].

The detection steps taken by monitoring nodes could be explained as follows:

1. The selection of monitoring nodes are done using secure key management algorithm in which sensor nodes will exchange their secret keys with cluster head so that any attacking node will not act as monitoring node and disrupt the overall functioning. When the node wants to send the packet to the destination, then the node which is not in the forwarding path or one hop away from the sensor node will act as monitoring nodes. So there are multiple monitoring node which can even detect the multiple replica present inside the network. the nodes which do not take participate in monitoring process may go to idle start to decrease the energy consumption. For every packet drop each node in its neighbor or may be cluster head become watchdog nodes and start generating

the alert or the packets will be rerouted in secured manner. Figure 5.6 shows the code for building the shared secret key for entire network.

```
# Build the key
   switch -exact -- $opts(mode) {
      encode { DydogKey -encrypt $opts(key) key }
      decode { DydogKey -decrypt $opts(key) key }
      default {
         return -code error "bad option \"$opts(mode)\": \
               must be either \"encode\" or \"decode\""
      }
   }
```

Figure 5.6: Built the shared secret keys

2. The monitoring node will listen to the traffic coming from both the destination and receiver nodes, if they found confliction in the message packet then alert is broadcasted to the cluster head.
3. When the attacker nodes are identified by the monitoring nodes then there is selection of one intrusion detection node which will decide how to securely send the packet to the destination node by choosing the secure route. The one with low TTL value is selected as decision making intrusion detection nodes [52].

1.Start

2. CH_s *: Cluster head (sender)*

CH_R*: Cluster head (receiver)*

N: Number of nodes

3. For each node n apply UWDBCSN

4.CH_s *sends request packet to* CH_R

5.For every i lies between CH_s *and* CH_R

Check TTL (time to live)

If (TTL (node (i) < TTL (node (j)))

Select node (i) as intrusion detection node

Else

Node (i) <- normal node

6. node (i) listen to both CH_s and CH_R, deciding module: checks authenticity;

If(CH_R(decrypt_packet) ==CH_S(encrypt_packet))

Reroute the packet through secure routes

Else

Generate the alerts and discard the request

7. end

Figure 5.7: Pseudo code for detection module

5.1.1.4 Verification Module

After the detection of malicious node has been done then the reply packets which are coming from the destination node is also verified by cluster head before sending them to the sender node. There may be the case that attacker nodes try to send the reply packets in that case the cluster head becomes the monitoring node and verify the reply packets by detecting the misbehaving node.

```
set messageapp new_app
proc signature_sending_message { $chiper } {
Agent/MessagePassing/Flooding instproc send_message {size message_id data port} {
    $self instvar messages_seen node_
    global ns DYDOG_KEY_no ENCRYPT

    lappend messages_seen $message_id
    $ns trace-annotate "[$node_ node-addr] sending message ygsgstgsy"
    $self sendto $size "$message_id:$data" $ENCRYPT $port
}
for {set i 0} {$i < $num_nodes} {incr i} {
    set n($i) [$ns node]
    $n($i) set Y_ [expr 230*floor($i/$DYDOG_KEY_no) + 160*(($i%$DYDOG_KEY_no)>=($DYDOG_KEY_no/2))]
    $n($i) set X_ [expr (90*$DYDOG_KEY_no)*($i/$DYDOG_KEY_no%2) + 200*($i%($DYDOG_KEY_no/2))]
    $n($i) set Z_ 0.0
    $ns initial_node_pos $n($i) 20
}
}
```

Figure 5.8: deployed cryptography for enhanced security performance

5.1.1.5 Sleep/Wake scheduling algorithm

The Dydog method is integrated in sleep/wake scheduling algorithm. Sleep/wake scheduling [54] is considered to be an efficient algorithm which save the network lifetime and reduce the energy consumption [55]. In this scenario, all those nodes who do not take participation in forwarding process or detection process go to inactive state or sleep state and other nodes will remain active in order to save the amount of energy they used. The figure shows the sleep/wake scheduling implemented in clustering algorithm using ns2 simulator. The grey nodes are in sleep state and the green nodes will perform the data forwarding process. Figure 5.9 shows the procedure of sleep/wake scheduling algorithm.

1. *Start*
2. *BS: Base station*
   CH: Cluster head
3. *BS send REQ_PACKET to CH*
4. *For every i lies between BS and CH*
   Check for i belong to ROUTING_PATH
   If (i belongs ROUTING_PATH)
   CH sends REQ_MSG
   Else
   CH sends SLEEP_MSG
5. *End*

Figure 5.9: Pseudo code for sleep/wake procedure

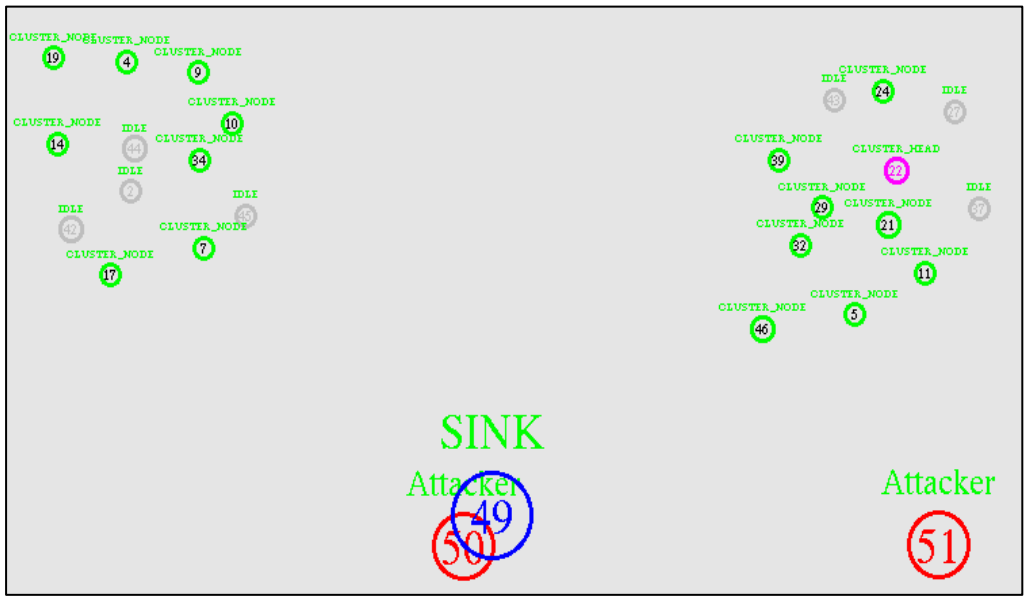

Figure 5.10: Sleep/wake procedure in nam

5.2 Summary

The proposed algorithm is based on the detection of replicas which is created by the two attacking nodes present in the network. The attacker nodes randomize the node id by utilizing their replication functionality. In order to detect the replicas, the Dydog method is introduced which is based on the intrusion detection nodes which will act as watchdog when they see any packet drop in the network. The proposed algorithm is integrated with sleep/wake scheduling algorithm which enhance the network performance and give better results that will be discussed in chapter 6. The whole analysis is done on the clustered network in which we use UWDBCSN for clustering.

CHAPTER 6

SIMULATION AND RESULT ANALYSIS

6.1 Simulator used

Network simulator version 2 (ns2) is the discrete event simulator which is developed by UC Berkely and found to be popular in scientific environment. It is useful to provide the information in dynamic network topology. All the wired and wireless network protocols such as TCP, UDP, FTP can be implemented using ns2 simulator. Two languages supported by ns2 simulator are OTcl and C++ which can be used to implement the basic scripts. OTcl is the object-oriented programming tcl/tk script which is used for the configuration of the network system. It is used to develop the environment structure and topology of the network. the kernel part of the system is C++ which implement the actual code. Ns2 can be implemented on UNIX and LINUX based platform. To use the network simulator, you need to develop the program in OTcl script language which initialize the object modules and scheduler objects which setup the environment or network topology that control the processing of data packets by considering the start and stop time with the help of event scheduler. Then the compilation of object modules and scheduler objects is done in C++ compiler [56]. Figure 6.1 represents the user view of ns2.

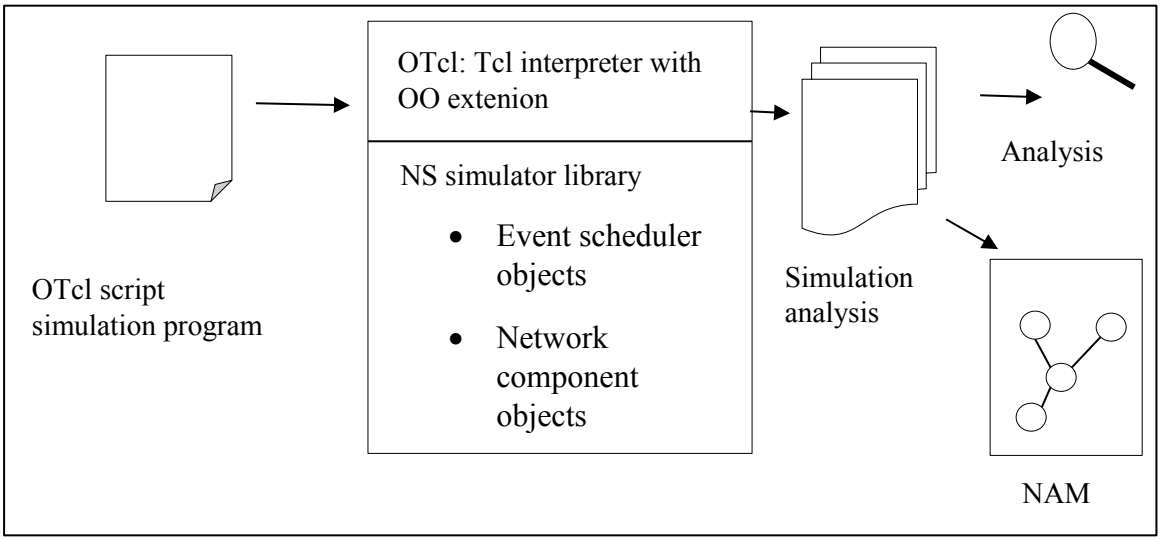

Figure 6.1: User view

6.1.1 Tool Command Language (TCL): Tool command language is a scripting language which is similar to PERL, Python etc. contains tcl scripts. OTcl is an extension of tcl whose library objects can be extended to add c++ code. This is used to create web and desktop application dynamically.

6.1.2. Network Animator (NAM): It is a network animation tool which is tcl/tk based which shows the actual view of transmission of packets. It supports various animated and inspection tools. It provides the information about number of packet drop inside the network.

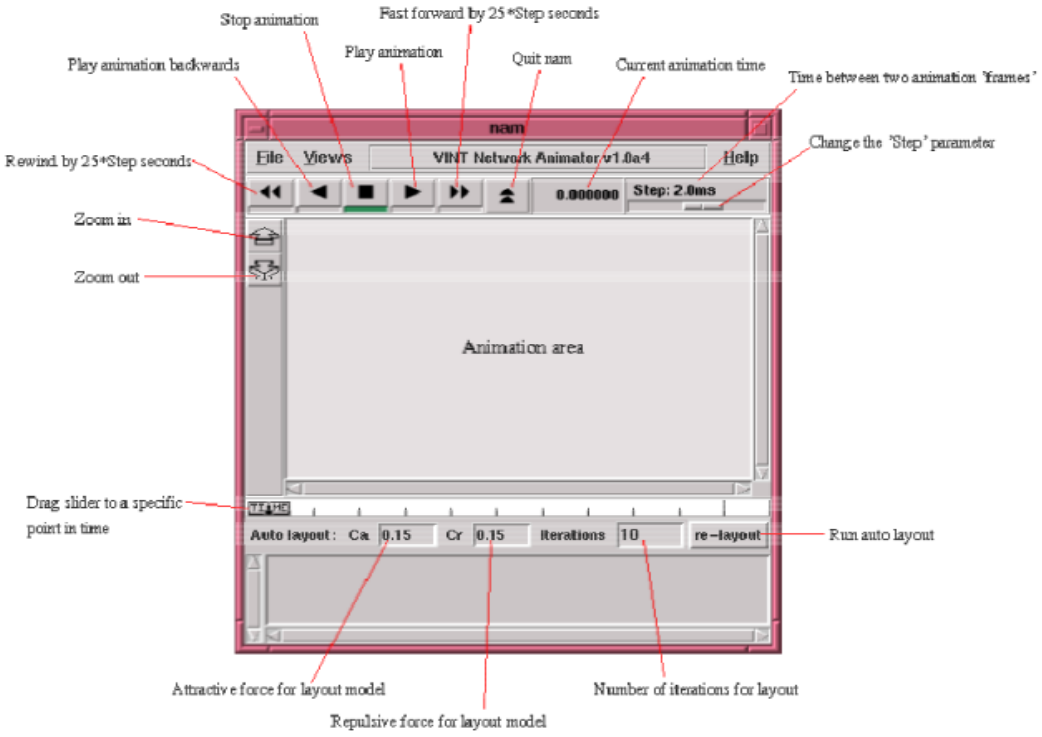

Figure 6.2: NAM

6.1.3 Xgraph: Xgraph is used to create the graphs of simulation results.

6.1.4 Energy model in NS2: The model which maintains the overall energy of the sensor network is called energy model. It includes the transmitting and receiving power associated with each node. Following table shows the attribute associated with each node for energy model in ns2:

TABLE 6.1: Attributes in Energy model

Attribute	Meaning	Value
energyModel	Energy model type	EnergyModel
rxPower	Receiving power	Power in watts
txPower	Transmitting power	Power in watts
initialEnergy	Energy of the node in the beginning	Energy in joule
sleepPower	Energy of the node during sleep state	Power in watts
transmissionPower	Consumption of power from sleep state to idle state	Power in watts
transmissionTime	Time taken during transmission	Time in seconds

6.2 Simulation Topology and Parameters

The ns2 simulator is used for implementing our proposed work. A hierarchical environment is set up which consist of 52 mobile nodes with 500× 500 grid topology. The mobile nodes are associated with energy model attributes which consists of power of each node such as transmitting power, receiving power etc. the results of simulation are discussed and will be shown in graphs. The performance metrics are compared with the previous proposed algorithms and computed based on five parameters such as packet delivery ratio, average throughput, end to end delay, energy consumption and network overhead. The simulation parameters taken during implementation are shown in following table:

Table 6.2: Simulation Parameters

Parameters	Values
Channel Type	Wireless Channel
Radio-Propagation Model	TwoRay Ground
Antenna Type	Omni Antenna

Link Layer Type	LL
Interface Queue Type	Queue/Droptail/PriQueue
Max packets in ifq	200
Network Interface Queue	WiressPhy
MAC_Type	IEEE 802.11
Number of Mobile Nodes	52
Energy Model	EnergyModel
Speed	20
Simulation Time	1000s

6.3 Performance Metrics

- **Packet delivery ratio (PDR):** PDR is the ratio of the total number of packets received by the destination to the total number of packets delivered by the source. Mathematically, it can be defined as:
  PDR = Total number of received packets/ Total number of delivered packets
- **Throughput:** Throughput is the successful delivery of the data packets sent by the sender node.
- **Average Delay:** The data transmitted during the average time period from one end to another end.
- **Average Network Overhead:** The increased amount of memory, time, bandwidth and other resources used by the sensor node is the overhead of the network.
- **Average Energy Spent:** The amount of total energy used by each sensor node in the network.

All the above metrics parameters are calculated using awk scripts and results are shown in Figure 6.3 to Figure 6.7.

6.4 Simulation Results

Figure 6.3 represents the PDR values with respect to time. When there is no attacker activity in the network then packets are delivered in normal time. When the attacker nodes are present then they decrease the PDR. Then the Dydog method is used to detect the attacking nodes which increase the rate at which packets are delivered and sleep/wake scheduling algorithm is used to increase the packet delivery ratio which is very close or more than the normal environment.

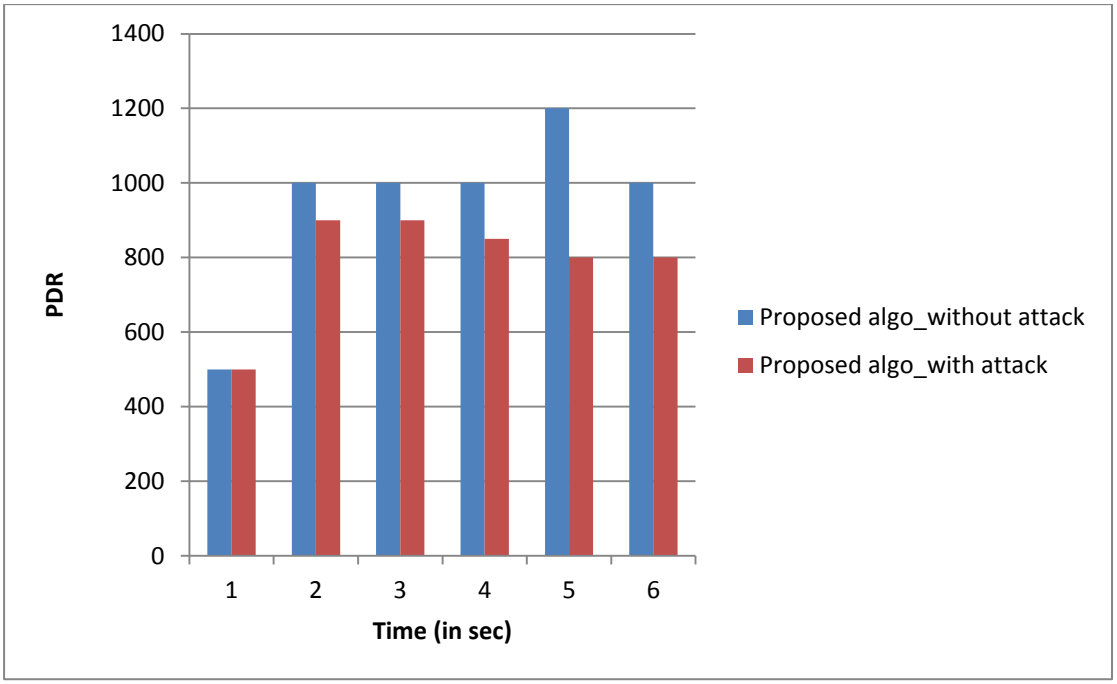

Figure 6.3: PDR versus time

Figure 6.4 represents the energy spent by the sensor nodes in three modules. The energy consumed by attacking nodes is more as compared to normal environment. When we used the Dydog method to detect the replicated nodes which is integrated with sleep/wake scheduling algorithm then it decreases the amount of energy used by the sensor nodes as they put all those nodes in sleep state who does not take participate in transmission and also the intrusion detection nodes are active which are looking forward to all the attacking activities. The average energy spent without attack is 832.91 with attack is 920.858 and when the proposed algorithm is used the total energy spent is 717.352 which is less as compared to others.

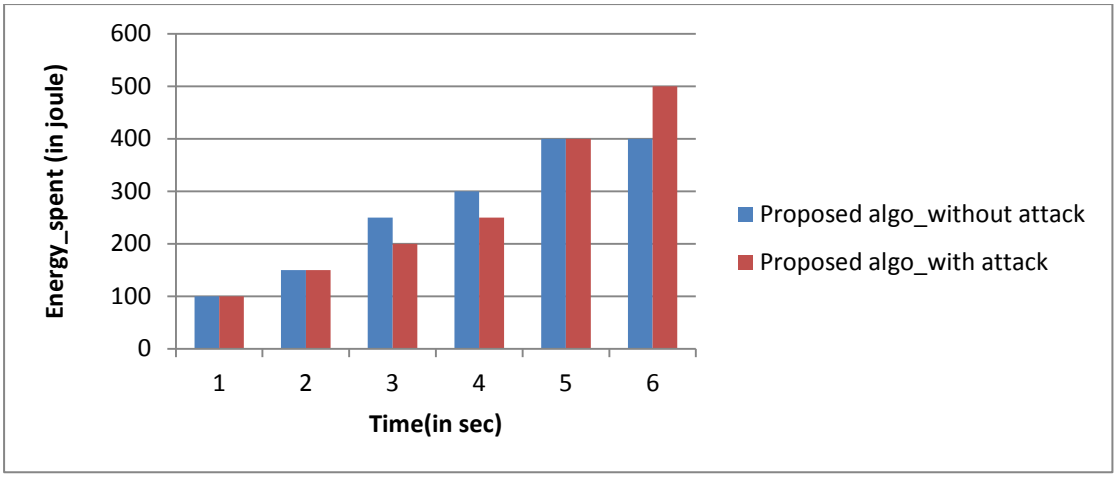

Figure 6.4: Energy_spent versus time

Figure 6.5 represents the successfully delivery of packets in time which is more in case of our implementation algorithm. The attacking nodes halt the communication in between when they try to send the flood of requests to the sink node but when we used Dydog detection then the monitoring nodes detect the malicious behavior and continue to process the packets through secure routes. The proposed algorithm increases the throughput from 20 to 179. Average throughput for the proposed algorithm is 252.59 while in case when the attack is introduced it is 125.47 which is less as compared to the throughput of proposed algorithm.

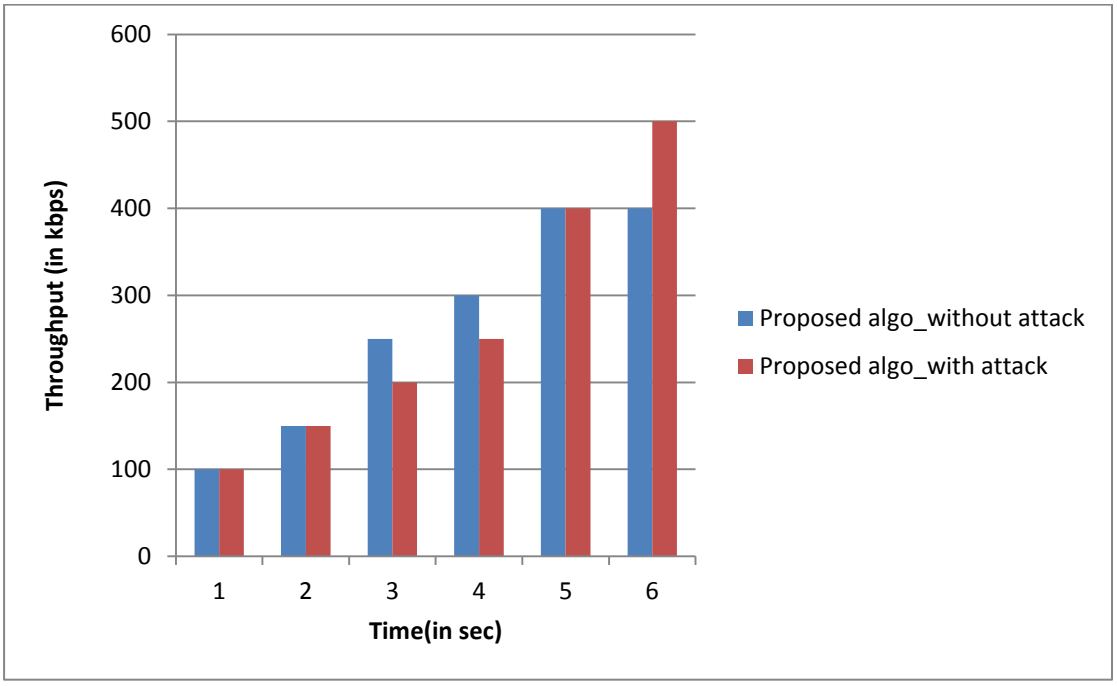

Figure 6.5: Throughput versus time

Figure 6.6 represents the delay of packets which is more when there is presence of attacker nodes in the network which increases the delay by performing some attacking activities from 50 to 2200. Delay in case of proposed algorithm is less because the algorithm tries to reduce the number of malicious replicas and also achieve better performance by sleep/wake method as compared to the normal environment when attacker is not present. The graph is showing the better performance when sleep/wake is used. The average delay in case pf normal environment is 1551.42 and when the attack is introduced the delay increased to 1794.76.

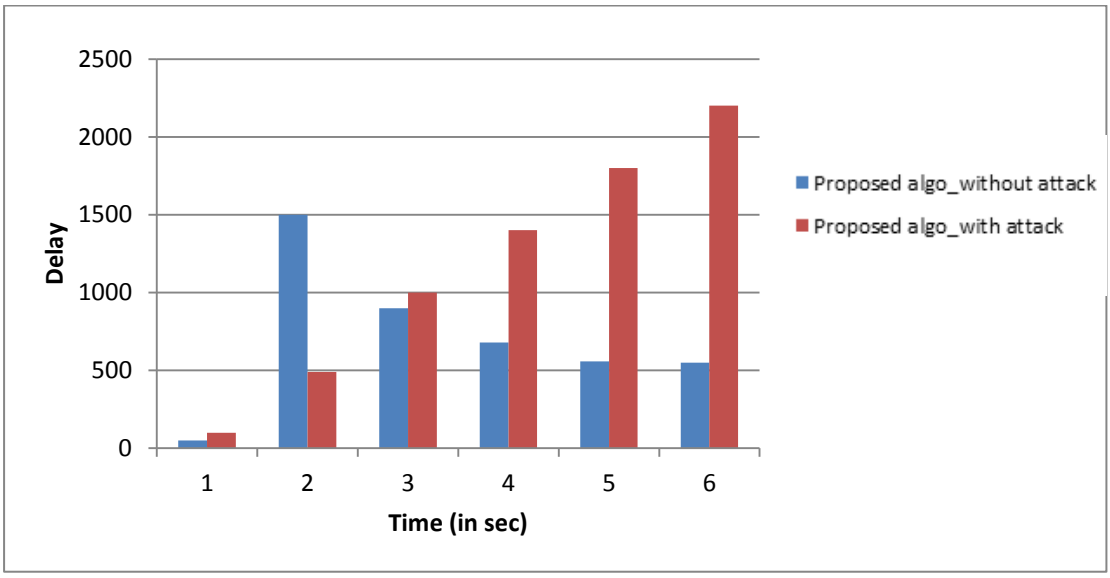

Figure 6.6: Delay versus time

Figure 6.7 represents the overhead during the overall communication in the clustering environment. The overhead in the network increases during attack from 100 to 1100. When the proposed algorithm is used, the overhead is high at 4500 because here the malicious node performs their attacking operations, it tends to decrease the overhead slowly when the selection of monitoring nodes is done and they start performing their detection operation. The overhead decreases to 100. The network overhead increases from 4.443 to 4.688 and when we use the Dydog method followed by the sleep/wake scheduling algorithm then the total network overhead reduced to 0.242.

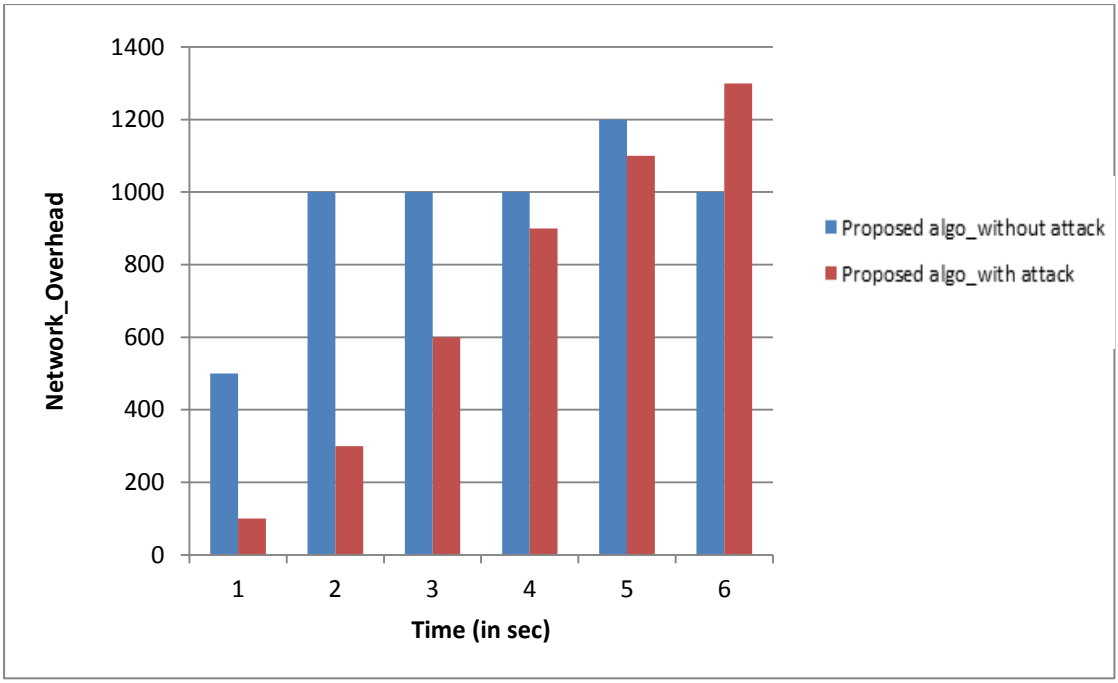

Figure 6.7: Network_overhead versus time

6.5 Comparison results of LNCA and UWDBCSN

Figure 6.8 represents the comparative PDR values of both UWDBCSN and LNCA. The two different clustering approaches are used and then detection method is used to compare the results. It can be clearly shown in the graph that packet delivery ratio in case of UWDBCSN based detection is more as compared to LNCA.

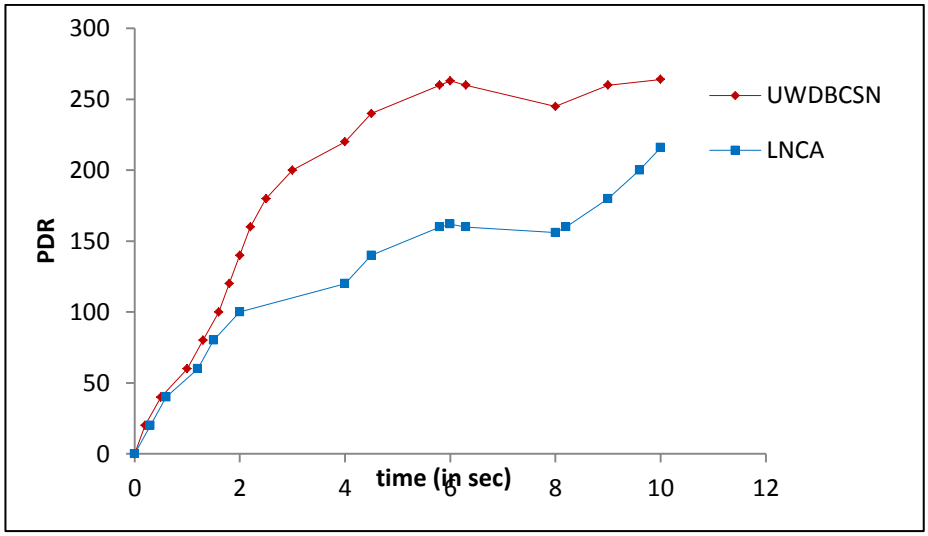

Figure 6.8: PDR versus time (LNCA versus UWDBCSN)

Figure 6.9 represents the comparison graph of end to end delay which is more in case of LNCA as compared to UWDBCSN as shown in the graph.

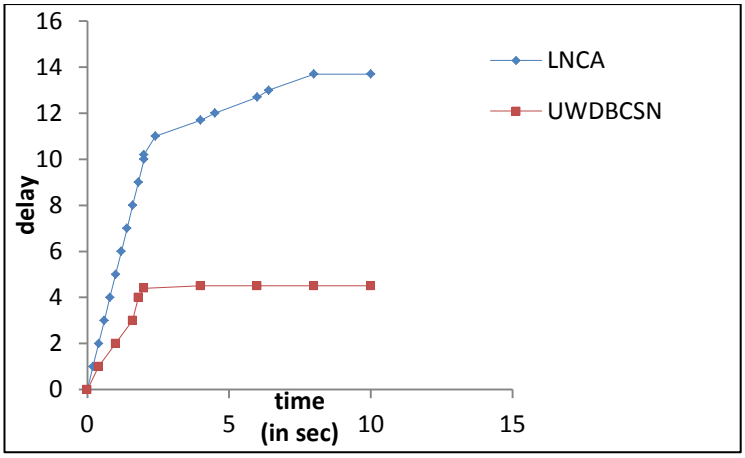

Figure 6.9: Delay versus time (LNCA versus UWDBCSN)

Figure 6.10 shows the energy spent during the packet transmission which is more in case of LNCA as compared to UWDBCSN. Hence UWDBCSN is more energy efficient as shown in the graph.

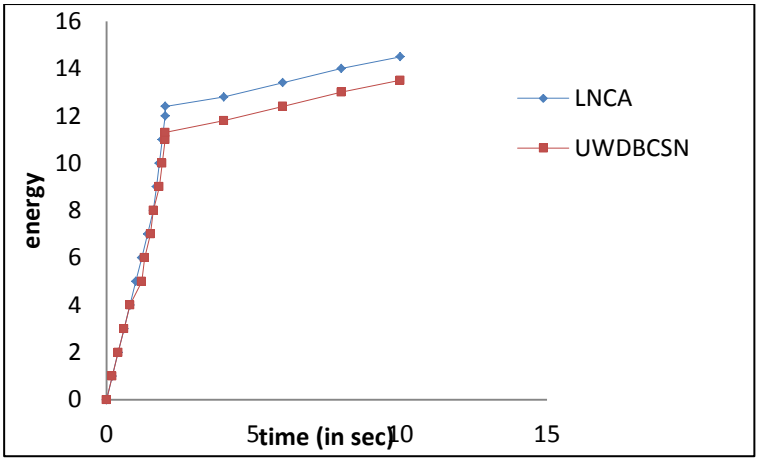

Figure 6.10: Energy_spent versus time (LNCA versus UWDBCSN)

Figure 6.11 shows the comparison graph of average throughput which is more in case of UWDBCSN as compared to LNCA. UWDBCSN tend to increase the packet delivery ratio. Therefore, throughput also increases.

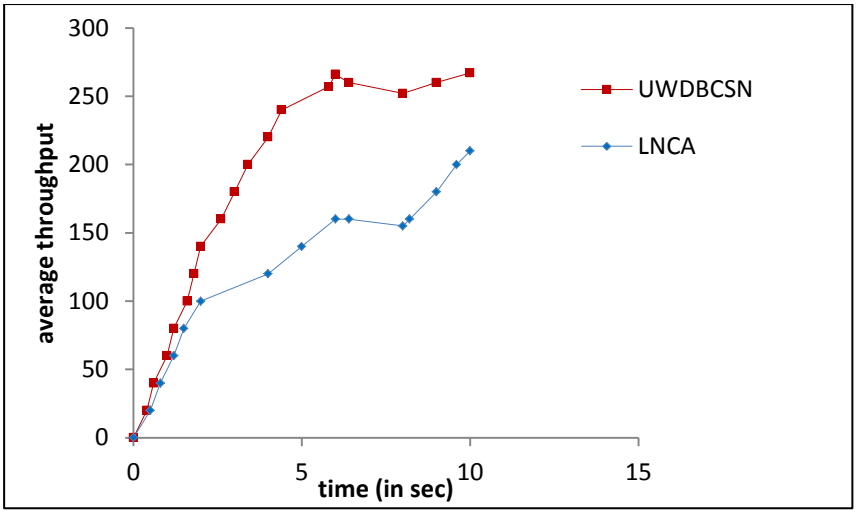

Figure 6.11: Throughput versus time (LNCA versus UWDBCSN)

Figure 6.12 shows the overhead of memory, power, energy and other resources which is more in case of LNCA because every time we have to compute the hash function for authentication of packets and this is more time consuming.

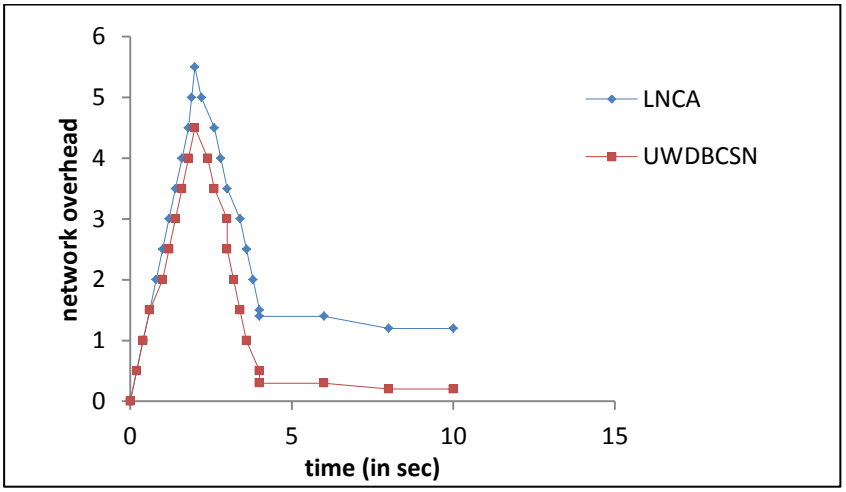

Figure 6.12: Overhead versus time (LNCA versus UWDBCSN)

6.6 Summary

From the simulation results, we conclude that the Dydog method along with sleep/wake scheduling increases the performance and life span of the network. The attacking nodes decrease the network performance and energy spent is more. We also compared our UWDBCSN analysis for node replication attack with previous LNCA clustering.

CHAPTER 7

CONCLUSION AND FUTURE SCOPE

.

7.1 Conclusion

Security is the important consideration in WSNs because it is vulnerable to dangerous attacks. The security of every sensor node should be maintained because the attacker's first aim is to inject their malicious activity to sensor nodes and then they try to disrupt the functioning of whole network. The node replication attack is one of the type of dangerous attacks which misbehave in the network by injecting the malicious nodes and lead to many insider attacks. In this work, we have performed the UWDBCSN clustering analysis of randomly deployed nodes and then attacker behavior is detected using Dydog method which is implemented using monitoring nodes. The detection method is then integrated with sleep/wake scheduling algorithm which will enhance the network lifetime. We have discussed the performance metrics such as end to end delay, throughput, overhead, energy used and packet delivery ratio and also compared with LNCA based detection. The simulation results show the successful implementation of proposed algorithm in sensor environment and able to give desired results. The main advantage of the proposed algorithm is that it can detect the multiple replicas present in the network and having high detection rate.

7.2 Future Scope

The proposed algorithm is proved to be effective detection method against node replication attack in WSNs by efficiently improving the performance and lifespan of the network. In future, the algorithm can also be used to perform detection of other attacks like Sybil attack, wormhole attack, jellyfish attack, rushing attack etc.

REFERENCES

[1] S.Sharma, P.Mittal, "Wireless Sensor Networks: Architecture, Protocols," *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 3, no. 1, pp. 303-308, 2013.

[2] S.Hasan, Z.Hussain, R.K.Singh, "A Survey of Wireless Sensor network," *International Journal of Emerging Technology and Advanced Engineering,* vol. 3, no. 3, pp. 487-492, 2013.

[3] A.Munir, A.G-Ross, S.Ranka, "Multi-Core Embedded Wireless Sensor Networks: Architecture and Applications," *IEEE Transactions on Parallel and Distributed Systems,* vol. 25, no. 6, pp. 1553-1562, 2014.

[4] R.C.Manjunath, A.Sindhu, S.N.Y.Jeevan, "Secure Transmission in MANET and Wireless Sensor Network," *International Journal of Advanced Research in Electrical, Electronic and Instrumentation Engineering,* vol. 3, no. 5, pp. 9415-9418, 2014.

[5] P.B.Hari, S.N.Singh, "Security issues in Wireless Sensor Networks: Current Research and Challenges," in *International Conference on Advances in Computing, Communication & Automation (ICACCA) (Spring)*, Dehradun, India, 2016.

[6] M.Kuorilehto, M.Hannikainen, T.D.Hamalainen, "A Survey of Application Distribution in Wireless Sensor Networks," *EURASIP Journal on Wireless Communications and Networking,* pp. 774-788, 2005.

[7] O.Boyinbode et al., "A Survey on Clustering Algorithms for Wireless Sensor Networks," in *Network-Based information Systems (NBiS)*, Takayama, Gifu,Japan, 2010.

[8] Y.Liao, H.Qi, C.Chen, "Clustering Algorithms of Wireless Sensor Networks," in *2nd International Workshop on Intelligent Systems and Applications (ISA)*, Wuhan,China, 2010.

[9] C.Gherbi, Z.Aliouat, M.Benmohammed, "A Survey on clustering routing protocols in Wireless Sensor Networks," *Sensor Review,* vol. 37, no. 1, pp. 12-25, 2016.

[10] L.N.Devi, A.N.Rao, "Optimization of Energy in Wireless Sensor Networks using Clustering techniques," in *International Conference on Communication and*

Electronic Systems (ICCES), Coimbatore, India, 2017.

[11] M.Tripathi, M.S.Gaur et al., "Energy efficient LEACH-C protocol for wireless sensor network," in *Third International Conference on Computational Intelligence and Information Technology (CIIT)*, Mumbai, India, 2013.

[12] S.K.Gupta, N.Jain, P.Sinha, "Clustering protocols in Wireless Sensor Networks: A Survey," *International Journal of Applied Information Systems (IJAIS),* vol. 5, pp. 41-50, 2013.

[13] S.Ali, .Madani, "Distributed Efficient Multi-Hop Clustering protocol for Mobile Sensor Networks," *The International Arab Journal of Information Technology,* vol. 8, no. 3, pp. 303-309, 2011.

[14] D.Xia, N.Vlajic, "Near-Optimal Node Clustering in Wireless Sensor Networks," in *Advanced Information Networking and Applications*, Niagara Falls, ON, Canada, 2007.

[15] S.Saxena, S.Mishra, M.Singh, "Clustering based on Node Density in Hetrogenous Under-Water Sensor Network," *Information Technology and Computer Science,* vol. 07, pp. 49-55, 2013.

[16] V.Kumawat, Dr.Kavita, B.S.Jangra, "Extended LEACH-Based Clustering Routing Protocols for WSN: A Survey," *International Journal of Engineering Development and Research,* vol. 5, no. 1, pp. 362-367, 2012.

[17] S.Tanessakulwattana, C.Pornavalai, G.Chakraborty, "Adaptive multi-hop routing for Wireless Sensor Networks," in *10th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, Maha Sarakham, Thailand, 2013.

[18] O.Younis, S.Fahmay, "HEED: a hybrid, energy-efficient, distributed clustering approach for adhoc sensor networks," *IEEE Transactions on Mobile Computing,* vol. 3, no. 4, pp. 366-379, 2004.

[19] A.Gaware, S.B.Dhonde, "A Survey on Security attacks in wireless sensor networks," in *3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, 2016.

[20] J.Grover, S.Sharma, "Security issues in Wireless Sensor Network- A Review," in *5th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)* , Noida, India, 2016.

[21] X.Luo, X.Ji, M.Park, "Location Privacy against Traffic Analysis Attacks in Wireless Sensor Networks," in *International Conference on Information Science*

and Applications (ICISA), Seoual, Korea, 2010.

[22] A.Tayebi, S.Berber, A.Swain, "Wireless Sensor Network Attacks: An Overview and Critical Analysis," in *Seventh International Conference on Sensing Technology*, Auckland, New Zealand, 2013.

[23] R.Dubey, V.Jain, R.S.Thakur, .D.Choubey, "Attacks in Wireless Sensor Network," *International Journal of Scientific & Engineering,* vol. 3, no. 3, pp. 1-4, 2012.

[24] N.Alajmi, "Wireless Sensor Networks Attacks and Solutions," *International Journal of Computer Science and Information Securirty,* vol. 12, no. 7, 2014.

[25] X.Chen, "Distributed denial of service attack and defense," in *International Conference on Educational and Information Technology (ICEIT)*, chongqing, China, 2010.

[26] M.Malik, Y.Singh, "A Review: DOS and DDOS Attacks," *International Journal of Computer Science and Mobile Computing ,* vol. 4, no. 6, pp. 260-265, 2015.

[27] A.Araujo et al., "Security in cognitive wireless sensor networks: Challenges and open problems," *EURASIP Journal on Wireless Communications and Networking,* pp. 2-8, 2012.

[28] S.Mohammadi, R.E.Atani, H.Jadidoleslamy, "A Comparison of Routing attacks on Wireless Sensor Networks," *Journal of Information Assurance and Security,* vol. 6, pp. 195-215, 2011.

[29] M.Kaur, M.Sarangal, A.Nayyar, "Simulation of Jelly Fish Periodic Attack in Mobile Ad hoc Networks," *International Journal of Computer Trends and Technology (IJCTT),* vol. 15, no. 1, pp. 20-22, 2014.

[30] M.G.Sanaei et al., "ROUTING ATTACKS IN MOBILE AD HOC NETWORKS: An OVERVIEW," *Sci.Int. (Lahore),* vol. 25, no. 4, pp. 1031-1034, 2013.

[31] A.K.Mishra, A.K.Turuk, "A Comparative Analysis of Node Replica Detection Scheme in Wireless Sensor Networks," *Journal of Network and Computer Applications,* vol. 6, pp. 21-32, 2015.

[32] W.T.Zhu et al., "Detecting node replication attacks in Wireless Sensor Network: A Survey," *Journal of Network and Computer Applications,* pp. 1022-1034, 2012.

[33] Y.Lou, Y.Zhang, S.Liu, "Single Hop Detection of Node Clone Attack in Mobile

Wireless Sensor Networks," in *International Workshop on Information and Electronic Engineering*, China,2012.

[34] C.M.Yu, C.S.Lu, S.Y.Kuo, "Mobile sensor network resilient against node replication attack," *IEEE Communication on Sensor,Mesh and Adhoc Communications and Networks,* pp. 597-599, 2008.

[35] Y.Zeng et al., "Random walk based approach to detect clone attack in wireless sensor networks," *IEEE Journal on Selected Area in Communications,* vol. 28,pp.677-691, 2010.

[36] A.K.Mishra, A.K.Turuk, "Zone based Replica Detection Scheme," in *third IEEE International Conference of Wireless and Mobile Computing,Networking and Communications*, 2007.

[37] Y.Zhou et al., "An energy efficient random verification protocol for the detection of node clone attack in wireless sensor," *EURASIP Journal on Wireless Communications and Networking,* 2014.

[38] W.Xie, L.Wang, M.Wang, "a bloom filter and matrix based node replication attack detection in wireless sensor networks," *Journal of Networks,* vol. 9, pp. 1471-1476, 2014.

[39] M. C. Geetha, "A token based approach for detecting replica node attack in static WSNs," *International Journal of Innovative Research in Computer and Communication Engineering,* vol. 2, 2014.

[40] C. P.Abhinaya, "Dynamic detection of node replication attacks using X-RED in wireless sensor networks," in *IEEE Conference on Information Communication and Embedded Systems (ICICES)*, 2014.

[41] G.Cheng, S.Guo, Y.Yang, F.Wang, "Replication attack detection with monitor nodes in clustered wireless sensor networks," in *IEEE 34th International Performance (IPCCC)*, 2015.

[42] J.W.Ho, M.Wright, S.K.Das, "Fast detection of replica node attacks in wireless sensor networks using sequential hypothesis testing," *IEEE Transactions on Mobile Computing,* vol. 10, 2011.

[43] W.N.Y.Ji, C.Charnsripiniyo, "A area-based approach for node replica detection in wireless sensor networks," in *IEEE 11th International Conference on Trust,Security and Privacy in Computing and Communications*, 2012.

[44] C. S. C.Yu, "CSI: Compressed sensing based clone identification in sensor networks," in *IEEE International Conference on Pervasive Computing and*

Communications, 2012.

[45] W.Znaidi, M.Minier, S.Ubeda, "Hierarchical node replication attack detection in wireless sensor networks," *International Journal of Distributed Sensor Networks,*vol.2013 pp. 82-86, 2013.

[46] P.Kaur, A.Sharma, "Avoidance of replication attack in clusters through witness node," *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 5, 2015.

[47] Y. L.M.Wang, "Patrol detection for replica attacks on wireless sensor networks," *Sensors 2011,* vol. 11, pp. 2496-2504, 2011.

[48] M.Conti, R.D.Pierto, L.V.Mancini, A.Mei, "Distributed detection of clone attacks in wireless sensor networks," in *IEEE Transactions on Dependable and Secure Computing*, 2011.

[49] R.Brooks, P.Y.Govindaraju, M.Pirretti, N.Vijaykrishnan, M.T.Kandemir, "On the detection of clones in sensor networks using random key predistribution," *IEEE transactions on Systems,Man and Cybernetics-Part C: Applications and Reviews,* vol. 37, 2007.

[50] F.Salva-Garau, M.Stojanovic, "Multi-Cluster Protocol for Ad-hoc Mobile Underwater Acoustic Network," in *IEEE OCEANS'03 Conference*, 2003.

[51] J.Ho, "Distributed Detection Replica Cluster Attacks in Sensor Networks using Sequential Analysis," in *Performance,Computing and Communication Conference (IPCCC)*, Austin, Texas, USA, 2009.

[52] S.Janakiraman, S.Rajasoundaran, P.Narayanasamy, "The Model- Dynamic and Flexible Intrusion Detection Protocol for high error rate Wireless Sensor Networks based on data flow," in *in Computing,Communication and Applications(ICCCA)*, Dindigul, Tamilnadu, India, 2012.

[53] T.Varshney, T.Sharma, P.Sharma, "Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network," in *Communication Systems and Network Technologies (CSNT)*, Bhopal, India, 2014.

[54] R.Manirajan, R.K.Sathishkumar, "Sleep/Wake Scheduling for Target Coverage Problem in Wireless Sensor Networks," *International Journal of Advanced Research in Computer and Communication Engineering,,* vol. 4,pp.400-405, 2015.

[55] B.Nazir, H.Hasbullah, "Dynamic sleep scheduling for minimizing delay in Wireless Sensor Network," in *Electronics, Communications and Photonics Conference (SIECPC)*, Riyadh, Saudi Arabia, 2011.

[56] E.Altman and T.Jimenez, "NS Simulator for beginners," Lecture notes, France, 2003.

LIST OF PUBLICATIONS

[1] Harpreet Kaur, Sharad Saxena, "A Review on Node Replication Attack Identification Schemes in WSN," in *8th International Conference on Computing, Communication and Networking Technologies (8th* ICCCNT 2017*)* (Accepted).

[2] Harpreet Kaur, Sharad Saxena, "Comparing UWDBCSN Clustering with LNCA for Node Replication Attack," *in Journals of Mobile Computing, Communication & Mobile Networks, vol.4, issue 2, August* 2017.

[3] Harpreet Kaur, Sharad Saxena, "UWDBCSN Analysis during Node Replication Attack on Cluster Heads," *in information Security in Biomedical Signal Processing (IGI Global Book Submission)* 2017 (Book Chapter proposal accepted).

VIDEO LINK

https://www.youtube.com/watch?v=vEHgV_pVVPM&feature=youtu.be

PLAGIARISM REPORT

ORIGINALITY REPORT

%6	%3	%5	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Saxena, Sharad, Shailendra Mishra, and Mayank Singh. "Clustering Based on Node Density in Heterogeneous Under-Water Sensor Network", International Journal of Information Technology and Computer Science, 2013. Publication	<%1
2	dione.lib.unipi.gr Internet Source	<%1
3	ijcsit.com Internet Source	<%1
4	Carli, M., S. Panzieri, and F. Pascucci. "A joint routing and localization algorithm for emergency scenario", Ad Hoc Networks, 2012. Publication	<%1
5	Lecture Notes in Electrical Engineering, 2015. Publication	<%1
6	Malik Tubaishat. "A secure hierarchical model for sensor network", ACM SIGMOD Record, 3/1/2004	<%1