International Journal of Advance Engineering and Research Development (IJAERD)
Volume 1,Issue 5,May 2014, e-ISSN: 2348 - 4470 , print-ISSN:2348-6406

EFFICIENT CLUSTER HEAD ELECTION FOR DETECTION AND PREVENTION OF MISDIRECTION ATTACK IN WIRELESS SENSOR NETWORK

Purvi Jani [1], Yask Patel[2]

[1]*M.E. 4th SEM (I.T.), Parul Institute Of Engineering & Technology, Waghodiya,Vadodara, India, pnjani91@gmail.com*

[2]*Department of Information Technology, Parul Institute Of Engineering & Technology, Waghodiya,Vadodara, India patelyask@gmail.com*

Abstract: Wireless sensor networks are gaining their popularity in application like consumer, defense, industrial sectors monitoring and collecting environmental data. Wireless Sensor networks are in areas which are not having any human monitoring. Being unmonitored, wireless sensor networks are vulnerable to different kinds of the attack. Misdirection attack in one the Denial of Service Attack, which causes the nodes to route information on long paths and ultimately creates situations of network jam. Misdirection attack that reduces throughput, network life time and increases the delay. There is only one solution to misdirection attack is third party monitoring. The work here in this dissertation proposes third party monitoring by cluster head and also monitoring of cluster head by source and destination transmission. Furthermore the work also improves the cluster head election procedure for security, so that initially intruder should not be selected as a cluster head.

Keywords: hidden web crawler, query optimization, search engines, metadata, document frequency, term weights

I. INTRODUCTION

Sensor networks refer to a heterogeneous system combining tiny sensors and actuators with general-purpose computing elements. Typical multi-hop wireless sensor network architecture is shown in figure 1. These networks will consist of thousands of self-organizing, low-power, low cost wireless nodes deployed to monitor and affect the environment. WSNs are quickly gaining popularity due to low cost solutions to a variety of real world challenges. Their low cost provides large sensor arrays in a variety of conditions capable of performing both the military and the civilian tasks. But the sensor networks also introduce severe resource constraints due to their lack of data storage and power. Both of these represent major obstacles to the implementation of traditional computer security techniques in WSN. The unreliable communication channel and unattended operation make the security defenses more even harder. Wireless sensors often have the processing characteristics of machines that are very old, and the industrial trend is to minimize the cost of wireless sensors while maintaining similar computing power. There are many researchers have started to address the challenges of increasing the processing capabilities and energy reserves of wireless sensor nodes while also securing them against attackers. In this the WSNs are being examined involving secure and efficient routing. To those traditional security issues, we examine that many general-purpose sensor network techniques predict that all nodes are cooperative and trustworthy. This is not the case for most, real-world wireless sensor networking applications, which require a fix amount of trust in the application in order to maintain proper network functionality. Researchers therefore started to focus on modeling a sensor trust model to solve the problems beyond the capability of cryptographic security [1]. There are number of attacks designed to exploit the unreliable communication channels and unattended operation of WSNs. Due to the inherent unattended feature of WSNs, so argument is that physical attacks to sensors play a very important role in the operation of WSNs. Thus, I have include a detailed discussion of the physical attacks and their corresponding defenses topics ignored in

most of the current research on sensor security. I am presenting a survey on the study of various aspects of WSN security in this process. Wherever possible, classification of work is also completed. Issues need to be addressed in future research are also identified, which provide a vital information for future researchers.[2]

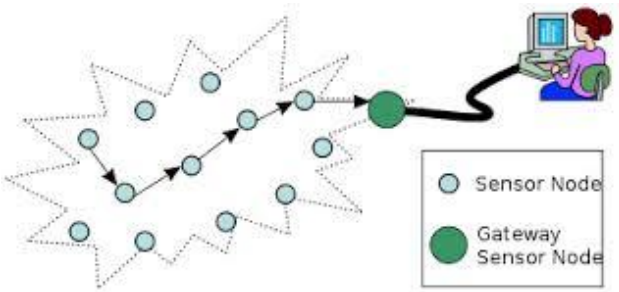

Fig:1 A typical multi-hop wireless sensor network architecture

II. LITERATURE WORK

1. Security Requirements

A sensor network is a very special type of network. It shares some common functionality with a computer network, but also poses some unique requirements. Therefore, i think of the requirements of a wireless sensor network as encompassing both the typical network requirements and the unique requirements suited solely to wireless sensor networks. The goal of security services in WSNs is to protect the information and resources from attacks and misbehavior. The security requirements in WSNs include:

- Availability: which ensures that the desired network services are available even in the presence of denial-of-service attacks
- Authorization: which ensures that only authorized sensors can be involved in providing information to network services
- Authentication: which ensures that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network node
- Confidentiality: which ensures that a given message cannot be understood by anyone other than the desired recipients
- Integrity: which ensures that a message sent from one node to another is not modified by malicious intermediate nodes
- Nonrepudiation: which denotes that a node cannot deny sending a message it has previously sent
- Freshness: Which implies that the data is recent and ensures that no adversary can replay old messages Moreover, as new sensors are deployed and old sensors fail, forward and backward secrecy should also be considered:
    - Forward secrecy: Sensors should not be able to read any future messages after it leaves the network.
    - Backward secrecy: A joining sensor should not be able to read any previously transmitted message.

The security services in WSNs are usually centered around cryptography. However, due to the constraints in WSNs, many already existing secure algorithms are not practical for use. [3]

2. Attacks in Sensor Networks

WSNs are vulnerable to various types of attacks. According to the security requirements in WSNs, these attacks can be categorized as [4]:

• Attacks on secrecy and authentication: Standard cryptographic techniques can protect the secrecy and authenticity of communication channels from outsider attacks such as eavesdropping, packet replay attacks, and modification or spoofing of packets.

• Attacks on network availability: Attacks on availability are often referred to as denial-of-service (DoS) attacks. DoS attacks may target any layer of a sensor network.

• Stealthy attacks against service integrity: The goal of the attacker is to make the network accept a false data value. Like, an attacker compromises a sensor node and injects a false data value through that sensor node. In these attacks, keeping the sensor network available for its intended use is essential.

3. Denial of Service And Denial Of Service Attack

We consider any type of intentional activity that can disrupt, subvert or even destroy the network as a Denial of Service (DoS) attack.In the context of WSN, DoS attacks that target the network resources are one of the most significant: the hardware of sensor nodes is usually very constrained, and attackers can try to overload them. Consider any kind of attempt of an adversary to disrupt, subvert, or destroy the network as a denial of service attack. In practicality, a DoS situation can occur due to any kind of incident that diminishes, eliminates, or hinders the normal activities of the network. Say for example, any kind of hardware failure, software bug, resource exhaustion, environmental condition, or any type of complicated interaction of these factors can create denial of service. It should be noted that the term 'DoS' indicates to a particular situation in the Denial of Service in Wireless Sensor Networks: Issues and Challenges 3 network and when DoS situation occurs due to an intentional attempt of an adversary, it is called DoS attack. DoS attacks can mainly be categorized into three types:

- Consumption of scarce, limited, or non-renewable resources
- Destruction or alteration of configuration information
- Physical destruction or alteration of network resources

The first one is the most significant for wireless sensor networks as the sensors in the network suffer from the lack of enough resources. Other than this type of categorization, layer wise categorization of DoS attacks can also be done. An attacker can choose different targets at different layers to stop proper functioning of legitimate nodes so that they cannot get the services they are entitled to.

III. NETWORK AND ROUTING LAYER

The network and routing layer of sensor networks is usually designed according to the following principles [4]:

• Power efficiency
• Sensor networks are mostly data-centric.
• An ideal sensor network has attribute-based addressing and location awareness.

Misdirection Attack: It is the most popular Denial of Service Attack. This attack can be performed in different ways. A malicious node could deny a valid route to a particular node

thereby denying service to the destination. A. Types of Misdirection attack. It can be performed in two ways:

- Packets forwarded to a node near to the destination: This kind of misdirection attack is less intense, because packets reach to the destination but from a different route which further produces long delay, thus decreasing throughput of network (bit transfer per second).
- Packets forwarded to a node far away from the destination: This kind of misdirection attack is very harmful because all packets are forwarded to a node far away, preventing them to reach the destination so packets will not reach destination. Due to the attack the delay becomes infinite and further results in zero throughputs [4].

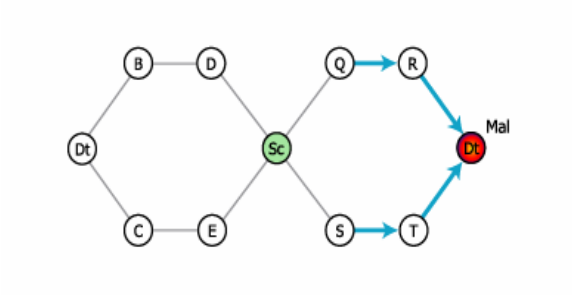

Fig 2: Misdirection Attack

IV. PROBLEM STATEMENT

In misdirection attack malicious nodes misdirect packets to other nodes but not to the intended recipient. As the malicious intermediate node (routing node) begins misdirecting packets due to this packets reach destination but not from the actual path but from some other path producing long delay in the network due to which throughput is also decreased. The Cluster based intrusion detection and prevention technique introduced in this paper detects the misdirection attacker node and also prevents this attack from occurrence. In the proposed technique we build clusters from mobile nodes. Cluster contains nodes which are in the communication range of each other. A cluster head is elected by these nodes for each cluster. When cluster is formed, cluster head is elected and it becomes the responsibility of the cluster head to detect the intruder node in that cluster. Source node maintains a FIFO buffer corresponding to each packet. This buffer contains entry of each sent packet with time stamp value corresponding to each packet sequence number. Source node also shares this buffer to the cluster head. Cluster head compares all sequence numbers of packets stored in its buffer to the sequence numbers of packets stored in buffer of all intermediate nodes with stamp value. If packet mismatch or empty entry is found in the buffer at a particular node, then the previous node will be omitted. The detection process again starts right from the beginning. It again searches for another optimum route for the secure communication. Thus any misdirection attack is easily detected and prevented with the proposed technique.

V. PROPOSED WORK

This section provides brief description about the proposed work. It contains definitions algorithm and flow chart for elaboration. In this chapter several experimental parameters are discussed with their expected outcome. Final section consists of design constraints which includes minimum Hardware and Software specifications.

Cluster Head Election Method

To elect proper cluster head using following method which makes the system more secure and can prevent it from the misdirection attack.

Proposed approach for Privacy in Cluster Head Election

Cluster Head Election Algorithm starts execution simultaneously at each node in the network and also each node in network has capacity to be elected as a cluster head.
There is time synchronization between the nodes so each node start executing at the same time. Then the protocol terminates after a predefined fixed amount of time during execution. If any node that has not received any cluster head announcement it broadcast a CH announcement message announcing it self as cluster head and this message is announce in the cluster. If the node that has neither announced itself as cluster head nor received any announcement will considered as the sender of announcement as it is cluster head. In order to prevent message originators' identity as cluster head the nodes (cluster members) are required to send dummy messages that cannot be distinguished from the announcements by the external observer (Messages are encrypted in the same way as the announcements).

Private cluster head election algorithm

```
Start T1, expires in rand(0,τ ) //timer, expires in round 1
Start T2, expires in rand(τ ,2τ ) //timer, expires in round 2
X = (rand(0,1) <= Y) // Node sends
CHID = -1 // ID of the cluster head of the node
while T1 NOT expired do
        if receive ENC(announcement) AND (CHID = -1) then
                CHID = ID of sender of announcement
        end if
end while
// T1 expired
    if X AND (CHID == -1) then
        broadcast ENC(announcement);
        CHID = ID of node itself;
    else
        broadcast ENC(dummy);
    end if
while T2 NOT expired do
        if receive ENC(announcement) AND (CHID = -1) then
                CHID = ID of sender of announcement
        end if
    end while
// T2 expired
    if (NOT X) AND (CHID = -1) then
        broadcast ENC(announcement);
        CHID = ID of node itself;
    else
        broadcast ENC(dummy);
        end if
```


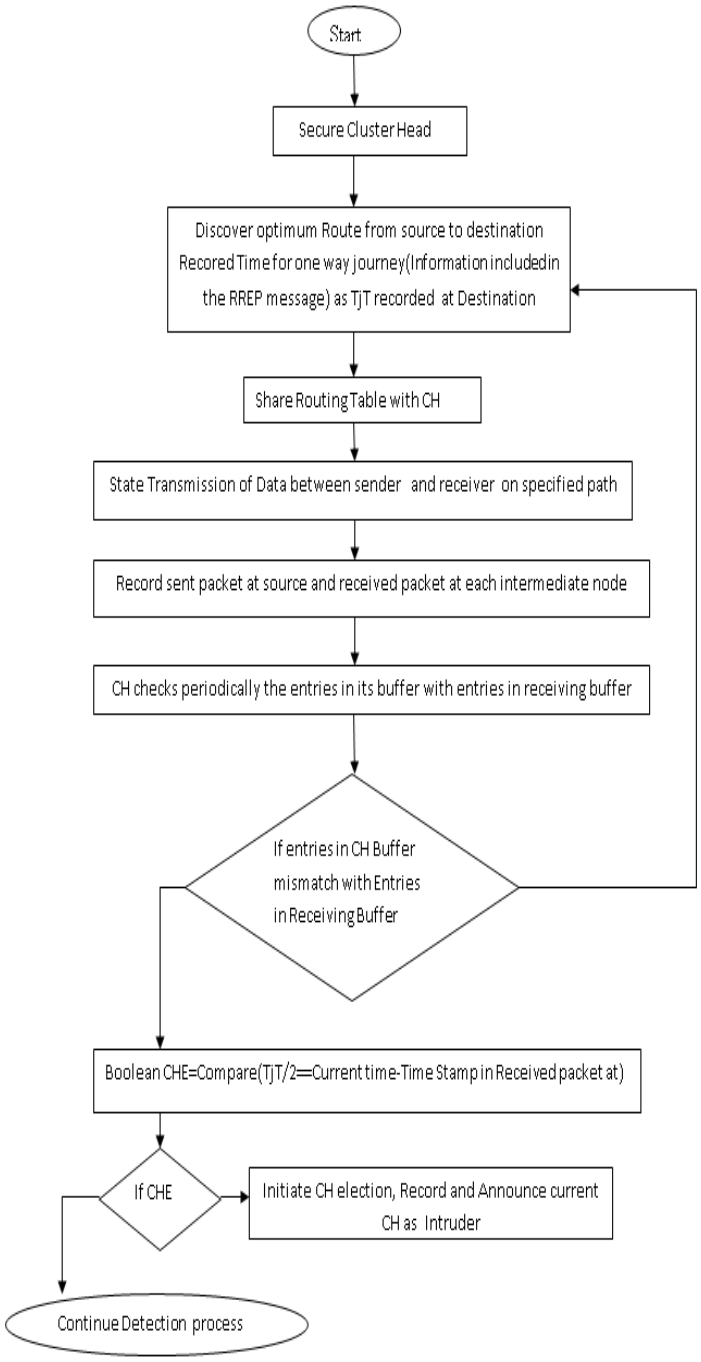

Figure: Flow chart of Proposed method

VI. RESULT & ANALYSIS

This section provides brief description about the implementation of Existing method, proposed method & result analysis. Implementation of both Existing algorithm and proposed algorithm is carried out using Ns2 2.35.

Parameter	Opnet Modeler 14.5	Ns_2 2.35
Platform	Windows XP SP2	Ubuntu 14.1
Network Size	14 Sensor Nodes	14 Sensor Nodes
Simulation Time	1800 Seconds	150 Seconds
Packet Size (bits)	Constant (1024)	Constant (1024)
Throughput (kbps)	12.72729	224.01
Packet Delivery Ration (pdf)	0.3733	0.9821

Table 1: Results of Exiting System in Different Simulators

VII. CONCLUSION

Misdirection attack is one of the most challanging attack in wireless sensor network. The work on the IDS for Misdirection attack in specifying the important aspect of securing cluster head from being intruder and misdirecting other nodes in network. The work proposed here is the required design for IDS that can protect cluster head from two points of view that is intruder should not be elected as a cluster head and if cluster head becomes intruder then it should be identified. The former is realized by inserting private cluster election and later proposal is realized by two-way third party monitoring. Throughput has increased considerably while increasing number of nodes in wireless sensor networks in future focus on two parameters like minimizing end to end delay and increasing packet delivery ratio with minimal compromization in throughput.

REFERENCES

[1] Roshan Singh Sachan "A Cluster Based Intrusion Detection and Prevention Technique for Misdirection Attack inside WSN", IEEE April 3-5, 2013.
[2] Guangjie Han, IDSEP: A Novel Intrusion Detection Scheme Based on Energy Prediction in Cluster Based Wireless, IEEE, 2013
[3] Abror Abduvaliyev, Al-Sakib Khan Pathan, On vital areas of intrusion detection systems in wireless sensor networks, IEEE communications & survey, VOL.15, NO.3,Third Quarter, 2013.
[4] Ismail Butun, Salvatore D. Morgera, and Ravi Sankar, A Survey of Intrusion Detection Systems in Wireless Sensor Networks, IEEE 2013
[5] Xuxun Liu, A Survey on Clustering Routing Protocols in Wireless Sensor Networks, Sensors, 2012.
[6] Wireless Sensor Networks: Security Issues and Challenges, Dr. Manoj Kumar Jain, IJCIT 2011,Volume 02
[7] Denial of service in wireless sensor network: Issues and challanges, Al-Sakib Khan Pathan1, Advances in Communications and Media Research, 2010
[8] A Survey of security issues in wireless sensor network, Yong Wang, Garhan Attebury, and Byrav Ramamurthy,IEEE 2006, Volume 8
[9] J. Kong, Z. Ji, W. Wang, M. Gerla, R. Bagrodia and B. Bhargava, Low-cost Attacks Against Packet Delivery, Localization and Time Synchronization Services in Underwater Sensor Networks, in 4th ACM Workshop on Wireless Security, 2005, pp. 87-96.
[10] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. First IEEE Int'l Wksp. Sensor Network Protocols and Applications, May 2003, pp. 113–27.
[11]Http://Www.Cs.Wustl.Edu/~Jain/Cse567-08/Ftp/Simtools/Index.Html

[12] "Adhoc wireless networks architecture & protocols" by C. Siva Ram Murthy, B.S Manoj Pearson Publication
[13] "Fundamentals of wireless sensor networks: theory and practice" by wiley publication

