SECURITY ISSUES AND CHALLENGES, PREVENTION, DETECTION MECHANISMS IN WIRELESS SENSOR NETWORKS - SURVEY

S Jagadeesan, B. Amutha
Dept. of CSE, SRM University
Jagadeesan81@gmail.com, amutha.b@ktr.srmuniv.ac.in

Abstract - The wireless detector networks want secure communication to get up being in open field and being supported broadcasting technology. The detector node’s resource constraints ancient security mechanisms with computation and communication area unit impracticable in WSNs. During this network a threat analyze and to report numerous analysis, labor in finding out a range of routing attacks that focus on the network layer. The protection needs area unit conferred and relationships between the network security and lifelong restricted, lean resources of the network nodes. The analytical community has recently lots of interest attracted lots of applications in detector networks. There is a unit several security attacks in Manet and DDoS is seeing the result of DDoS in routing load, packet drop rate and finish to finish delay attributable to attacks on networks. The DDoS attacks area unit associate degree entropy primarily based detection mechanism to assure the transmission of traditional traffic and stop the abnormal traffic. In each hollow and Denial of Service attack the attackers build a coffee latency association between 2 nodes within the network.

I. INTRODUCTION

A detector network is Associate in Nursing infrastructure comprised of sensing; computing Associate in Nursing communication port provides an administrator observe and react to events and development in an exceedingly explicit surroundings. The administrator generally could be a public, lawmaking, marketable or industrial entity. The atmosphere may be the physical world, a biological system, Associate in Nursing info technology framework. There square measure four basic elements in an exceedingly wireless detector network.

1) Distributed or localized sensors
2) Associate with the Nursing interconnecting network
3) A central purpose, so as of bunch
4) A collection of computing resources at the central purpose to handle the information association, event trending, standing querying and data processing.

II. DEVELOPMENT OF AN EVALUATION FRAMEWORK FOR SENSOR NETWORKS

The device networks gift own model and assumptions that typically cowl a distinct set of the planning state house. The subsequent assumptions are given below

- The range of nodes
- Mobility of nodes
- Node properties
- Possibility of sudden node failures
- non-homogeneous nodes occur
- The offered base stations function gateways to additional networks
- The sensing application in flora and fauna

The development of protocols for device networks be expected that one protocol can do higher than all others attainable models, this discretionary fragmentation of the planning state house makes it tough to search out the protocols and compare them to every alternative. The authors check their protocol with unplanned metrics that create comparison even more difficult. Wireless device networks use stratified design, Characteristics and functions of their each layer are given below.

A. PHYSICAL LAYER

To reduce the trail loss impact and shadowing increase the reliableness. It's answerable for established association, data speed, modulation, encoding, signal recognition, frequency generation and reception.

B. DATA LINK LAYER

To assure the communication between one node to a different node is answerable for error finding.
multiplexing, interference of Collision packets and recurrent communication, etc. To secure this layer planned link layer security design for wireless device networks. Within the link layer stands for hardware based mostly regular key coding and the use of public key cryptography. The key constructs amount of network consumption and protection.

C. NETWORK LAYER
To discover the foremost glorious path permanently routing mechanism and answerable for routing the info from one node to a different node, one node to attack node and contrariwise. Each LEACH and PEGASIS protocols describe the techniques to save lots of the energy consumption on improving the sensor's life. LEACH offers cluster primarily based transmission, whereas PEGASIS is chain protocol. To form a secure routing protocol for secret writing and decipherment techniques used for routing secure.

D. TRANSPORT LAYER
To establish the communication for sensing element networks connected to the net and most difficult problems in wireless sensing element networks.

E. APPLICATION LAYER
The output ensures sleek data flow to lower layers. This layer is accountable for information assortment, management and process of the information throughout the appliance software package for obtaining reliable results. SPINS provides information authentication and replay protection must secure blocks square measure SNEP and μTESLA. SNEP provides baseline security primitives square measure information authentication and information freshness. Localized coding and Authentication Protocol may be a key management.

<table>
<thead>
<tr>
<th>LAYER</th>
<th>ATTACKS</th>
<th>SECURITY APPROACHES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Layer</td>
<td>Denial of Service</td>
<td>Priority Messages</td>
</tr>
<tr>
<td></td>
<td>Tampering</td>
<td>Tamper Proofing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hiding, Encryption</td>
</tr>
<tr>
<td>Data Link Layer</td>
<td>Jamming</td>
<td>Use Error Correcting Codes</td>
</tr>
<tr>
<td></td>
<td>Collision</td>
<td>Use spread spectrum techniques</td>
</tr>
<tr>
<td></td>
<td>Traffic manipulation</td>
<td></td>
</tr>
<tr>
<td>Network Layer</td>
<td>Sybil attacks</td>
<td>Authentication</td>
</tr>
<tr>
<td></td>
<td>Wormhole attack</td>
<td>Authorization</td>
</tr>
<tr>
<td></td>
<td>Sinkhole</td>
<td>Identity certificates</td>
</tr>
<tr>
<td></td>
<td>Flooding</td>
<td></td>
</tr>
<tr>
<td>Transport Layer</td>
<td>Resynchronization</td>
<td>Packet Authentication</td>
</tr>
<tr>
<td></td>
<td>Packet injection attack</td>
<td></td>
</tr>
<tr>
<td>Application Layer</td>
<td>Aggregation based attacks</td>
<td>Cryptographic approach</td>
</tr>
<tr>
<td></td>
<td>Attacks on reliability</td>
<td></td>
</tr>
</tbody>
</table>

A wireless sensing element network may be a wireless network consisting of spatially distributed freelance devices mistreatment sensors to observe physical or environmental conditions. These systems incorporate a gap that has wireless property back to the wired world and distributed nodes. every sensing element node has Associate in Nursing sometimes variety of components are a radio transceiver with an indoor projection, a microcontroller, Associate in Nursing electronic circuit for interfacing with the sensing element Associate in Nursing embedded sort of energy harvest. The elemental aspects of wireless sensing element networks cowl wireless sensing element network technology, applications, communication techniques, networking protocols, middleware, security, and system management. The most characteristic of a wireless sensing element network includes the subsequent.

1) Ability to deal with node failures.
2) Power consumption constraints for node mistreatment batteries are energy harvest.
3) Mobility of nodes.
4) Heterogeneity of nodes.
5) Communication failures.
6) Ease of use.
7) Scalability to the massive scale of preparation.
8) Ability to survive cruel environmental conditions.

Many of those applications share some basic characteristics and clear distinction between sources and sinks. In supply information the particular nodes that sense information and a sink node wherever the info ought to be delivered. The communication pattern between sources and sinks show some typical patterns. The relevant ones are

(i) **Event Detection**: sensor nodes ought to report back to the Sink once they need to detect the incidence of a such event. The best events will be detected domestically by one device node in isolation. A lot of difficult forms of event need near or remote sensors.

(ii) **Periodic Measurements**: Sensors may be sporadically reportage measured values. These reports may be triggered by a detected event. Function approximation and edge detection: a cost like temperature changes from one place to a different may be recorded as a perform on location. A wireless detector network may be used a restricted range of samples taken at every individual detector node and approximate mapping ought to be created out there at the sink. Associate example to seek out the equal points in an exceedingly fireplace application to find the border of the particular fire. This may be generalized to finding edges in such functions or to causing messages on the boundaries of patterns in each house and time.

(iii) **Tracking**: the supply of an incident may be mobile. The wireless device network may be wanting to report updates on the event supply position to the sink. Distributed Deny of Service (DDOS) is one amongst the foremost vital threats to the protection of the web. A key observation in defense against DDOS attack traffic tends to use spoofed supply addresses to hide up their true identities, that conceals assaultive sources and dilute localities in assaultive traffic. The vulnerability and Security deficiency of the TCP/IP set brings the initiating DDOS attacks a straightforward and very laborious to guard. The analysis, detection and defense against DDOS attacks has been explored wide within the analysis community. There are unit 2 classes during this field area unit invasion detection and attack packet filtering. The final science spoofing shorts may be classified into 3 includes random spoofing, subnet spoofing and glued spoofing. It's dangerous to acknowledge attack packets from valid web traffic and filter them once a DDOS attack happens. There's one single path between the supply and destination node. Thus, if any packet with the supply and destination address that start during a router not within the path ought to be discarded. All web service suppliers (ISPs) facing the mother of skyrocketing Associate in Nursing quantity of unwanted traffic area unit the information packets that consume restricted resources and reduce the performance of the network. A flooding DDoS attack is Associate in Nursing attack a sender machine will send an oversized quantity of unwanted traffic. DDoS is one amongst the foremost threats for current web as a result of the flexibility to make a large volume of unwanted traffic. The large-scale DDOS attack packs up the network for over 2 days and additionally stopped many major business websites.

III. **SECURITY REQUIREMENTS FOR WIRELESS SENSOR NETWORKS**

A. **DATA CONFIDENTIALITY**

A standard approach to shield the confidentiality of sensing element

---

S Jagadeesan and B. Amutha
information to inscribe it employing a cryptological key. The cryptological key square measure used Associate in Nursing either cruciform or uneven. The character resource of sensing element node makes it difficult to come up with and store keys. The classified, sensitive information will be generated by sensing element node.

B. DATA AUTHENTICATION

To modify the info packet stream by adding additional packets. The receiver has to ensure the info used method} process of the approved supply. It identifies the communication should be capable of accepting Associate in Nursing rejecting the info from an unauthorized nodes. Authentication is needed for several body tasks.

C. DATA FRESHNESS

The user ensures that the information communicated is recent messages, however couldn't replayed previous messages. It is classified into 2 varieties supported the message ordering area unit weak and robust freshness. Weak freshness provides partial message ordering, however, no data associated with the delay and latency. Sturdy freshness offers the whole request and response with delay. A timestamp is hooked up to the freshness of a packet. The destination node will compare with time stamp with its own clock and checks the packet area unit valid or not. A secure intrusion detection system against DDOS attack in Wireless Mobile Adhoc Network offers the assorted varieties of attacks in wireless sensing element network area unit.

D. WORMHOLE ATTACK

The most powerful attacks in the wireless device network involve the cooperation between 2 malicious nodes within the network. It captures routing traffic at one purpose of the network and tunnels to a different purpose within the network (3). AN appeaser tunnel messages received in one a {part of} the network over a coffee latency link and replay them in another part of the network. Every message includes a time stamp and also the location of the sender. The receiver compares with its own location and time to see the most transmission vary has been exceeded. The answer that needs clock synchronization and correct location verification (13).

E. BLACKMAIL ATTACK

The routing protocols, mechanisms for the identification of malicious nodes and propagate messages. Associate offender could fabricate such news messages and check out to isolate legitimate nodes from the network (3).

F. ROUTING TABLE POISONING:

In routing protocols maintain route tables for hold data concerning the network. The poisoning attacks generate malicious nodes and send fictional signal traffic. During this attack, the choice of non best routes from routing tables (3).

G. REPLAY:

An offender listening the spoken communication or group action between 2 nodes. The necessary message like countersign or authentication messages (3).

H. LOCATION DISCLOSURE

This attack targets the privacy necessities of AN adhoc network. The employment of traffic analysis technique with straightforward inquiring and observation. Assailant ready to discover the situation of a node (3).

I. BLACKHOLE ATTACK

A malicious node injects the false route to the route request and fake replies can fabricate to divert network traffic through the malicious node. To attract all traffic in order to perform a denial of service attack by dropping the received packets (3).

J. DENIAL OF SERVICE

Attacks embody the routing table overflow and also the sleep deprivation. In routing table overflow attack the malicious node floods the network phony route creation packets. The sleep deprivation
torture attack aims at the consumption of batteries of specific node (3).

K. DISTRIBUTED DENIAL OF SERVICE

This attack is analogous to a DoS attack is performed by one node, however DDOS attack is performed by the mixture of the many nodes. All nodes attack on the victim node by causing vast packets consume the victim's information measure and not enable to receive the necessary information from the network (3).

L. MASQUERADE

An interloper who gains the privilege of the Union system as associate degree each user by stealing user passwords (3).

M. PASSIVE LISTENING AND TRAFFIC ANALYSIS

An attack cannot have an effect on the operation of routing protocols. The sensitive routing info ought to be protected and also the confidentiality of user information isn't the responsibility of routing protocol (3).

N. FLOODING ATTACK

To consume network resources like information measure, process resources and battery power in order that network rating goes down and actual user cannot use network resources. In RREQ flooding attack, the wrongdoer transmits several RREQ packets for the node which may be existing or not within the network. To execute RREQ flooding the interloper increase the RREQ rate, that consumes network information measure and stop real users from exploiting it. In information flooding information packets want to flood the network. During this attack, wrongdoer node 1st of all builds a pathway to all or any the opposite nodes within the network, then send the unwarranted quantity of solid information packets and this solid information packet fail the network resources in order that nobody will use them and it'll terribly arduous to suit (8).

O. JAMMING ATTACK

The idea of ECM attack is to top off the channel with useless signals, attributable to that act or legitimate user cannot use it. ECM retards the causation and receiving of messages at the destination. It's terribly arduous to forestall and cite the ECM attacks, however, still some detection algorithms try to forestall the chances of ECM attack (8). The 5 main metrics to estimate the performance of our economical schemes, particularly energy spent, delay, throughput, packet delivery quantitative relation and packet loss in each flood and ECM attacks(8).

P. SYBIL ATTACK

A Sybil attack is outlined as a consistent attack whereby malicious devices illegitimately defy multiple identities within the network. The malicious device's further identities ensuing from such associate degree attack are termed as Sybil nodes. All messages received by Sybil nodes are sent by the malicious device. The method of identity stealing to launch a Sybil attack is performed in one in every of the 2 ways that (22).

(i) Fabricated Identity: The attacker can create arbitrary Sybil identities by generating arbitrary random numbers as indents for the Sybil nodes (22).

(ii) Stolen Identity: The attacker initially identifies the legitimate nodes of the network. Subsequently, the stolen legitimate identities are assigned to the attacker-generated Sybil nodes (22).

Q. NODE REPLICATION ATTACKS

A node replication attack is outlined as an attack whereby somebody injects one or additional nodes within the network as AN existing node. During this attack was a collection of citations nodes created by the somebody node. It involves physical insertion of scallywag nodes into the network. This attack assumes the contestant nodes have the capabilities forever-changing and subverting existing topological data like route and trust within the network.
(i) **Route-based Attacks** Directed delusion is outlined as a mechanism to facilitate information retrieval from device nodes. It’s supported the principle of data-centric, whereby the bottom station broadcasts a call for participation in a selected information kind within the device network. In existing DDOS machine learning is split into 2 elements they're supervised learning and unsupervised methodology. A supervised methodology includes learning step, however, in unsupervised methodology doesn't learn step. In proposing a DDOS attack detection methodology by victimization entropy. Within the commencement, time window controls the quantity of traffic flowed in router is measured. If the time window is over volume threshold. It judges 1st danger and send it to next detective work step. Within the second step, if the entropy of destination informatics address is smaller than entropy threshold. It judged as second danger. The third step, entropy of transmission port variety supported destination informatics address has exceeded the entropy threshold of transmission port variety is over, it's classified into third danger (7). The nodes that are employed in performing arts DDoS attacks are assailable, master, zombies and victim make a case for in table I.

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacker</td>
<td>All attacks operate instrument by remote control and delivery command directly</td>
</tr>
<tr>
<td>Master</td>
<td>Receiving the command from an attacker and orders attack zombies managed by it</td>
</tr>
<tr>
<td>Zombie</td>
<td>They are controlled by the master. An attack program operates the command from each master and finally performs their attack to the victim</td>
</tr>
<tr>
<td>Victim</td>
<td>At the same time attacked from several hosts</td>
</tr>
</tbody>
</table>

### IV. CLASSIFICATIONS BY ACTIVITY LEVEL

#### A. PREVENTIVE MECHANISMS

The goal of protective mechanism is either to remove the chance of DDoS attacks is to enable potential victims to continue the attack without denying services to valued clients. The preventive mechanisms can be divided into attack prevention and denial of service.

#### B. ATTACK PREVENTION MECHANISMS

Modify the system configuration to reduce the possibility of a DDoS attack.

#### C. SYSTEM SECURITY MECHANISMS

The security of the system increases, illegal accesses to the mechanism, removing purpose bugs and updating protocol installations to prevent intrusions and misuse of the system. DDoS attacks are power to large numbers of subvert machines and generate the attack streams. The attackers would be unable to find their armed forces and the DDoS threat.

#### D. PROTOCOL SECURITY MECHANISMS

With these mechanisms address the difficulty of bad protocol design. Protocols control operations that are not expensive for the client, but expensive for the server. Protocols can be altered to the resources of a server by initiating large numbers of concurrent transactions. The authentication server attack and the fragmented packet attack, the attacker bombard the victim with abnormal packet fragments to waste its resources.

#### E. REACTION MECHANISMS

It struggles to improve the impact of an attack on the victim. They need to detect the attack and respond to it. The attack detection is to detect each attempt DDoS
attack as early as possible and to have a low quantity of false positives.

**F. MECHANISMS WITH PATTERN ATTACK DETECTION**

The pattern detection stores the signatures of known attacks in a database. Each communication is monitored and compared with database entry to discover the occurrence of DDoS attacks. The database is efficient with new attack signature. The drawback of this detection mechanism only detects known attacks and helpless against new attacks or even a small variation of older attacks cannot be matched to the store's signature. Known attacks are easily and reliably detected and no fake positives are encountered.

**G. MECHANISMS WITH ANOMALY ATTACK DETECTION**

A model of normal system behavior as a model of usual traffic dynamics or likely scheme performance. The current state of the system is from time to time compared with the model to detect.

**H. MECHANISMS WITH HYBRID ATTACK DETECTION**

In hybrid detection, merge the pattern-based and anomaly-based detection using information about attacks exposed through an inconsistency detection mechanism to devise new attack signatures and inform the database.

**I. MECHANISMS WITH THIRD-PARTY ATTACK DETECTION**

The third-party detection does not handle the detection process, but rely on an outer message that signals the occurrence of the attack and provides attack categorization.

**J. AGENT IDENTIFICATION MECHANISMS**

The victim with information about the uniqueness of the technology that are performing the attack. This information can be combined with other reply approaches to improve the force of the attack.

**K. FILTERING MECHANISMS**

The characterization provided a detection mechanism to pass through a filter the attack stream finally.

**L. AUTONOMOUS MECHANISMS**

These perform independent attack detection and response. At a distinct point in the Internet and take steps in the surrounding area. Firewalls and intrusion detection systems provide an easy example of autonomous mechanisms.

**V. CLASSIFICATION BY DEPLOYMENT LOCATION**

**A. VICTIM-NETWORK MECHANISMS**

The victim networks protect from DDoS attacks and respond to detected attacks by the impact on the victim. The majorities of defense systems were situated at the victim and suffered the greatest impact of the attack and motivated to give up some resources for better security.

**B. INTERMEDIATE-NETWORK MECHANISMS**

At the middle network provide infrastructural services to a large number of Internet hosts. Victims of DDoS attacks can contact the transportation and request the service that's possibly providing sufficient costs.

**C. SOURCE-NETWORK MECHANISMS**

The DDoS defense mechanisms deployed the source network is to prevent customers using this network from generating DDoS attacks. Such mechanisms are necessary and desirable motivation for their consumption is low because indistinct who would pay the operating cost associated with this service.

| Table II Comparison of DDoS attacks, Defense architectures |
| --- | --- | --- |
| Defense Method | Advantages | Disadvantages |

S Jagadeesan and B. Amutha
In an existing system, CUSUM algorithm is applied to detect SYN flooding attacks. Detection approach is used in many off-line based. But in proposed system a new nonparametric CUSUM algorithm is applied to detect SYN flooding attacks. The system can make a real-time detection for flooding attacks at the early stage and take effective measures. A pre-IP traffic behavior analysis is easier to differentiate the attackers from the normal users. The approach needs less computation and memory the system could be on-line DDOS detection and prevention. By applying the non-parametric CUSUM algorithm and decision algorithm can detect accurately at the earlier stage.

VI. CONCLUSION

The wireless detector networks, maintain to boost and become unremarkably utilized in several applications. Security problems with wireless detector Network are a lot of more vital than another issue. Within the past years there was no security in wireless detector networks, however, in recent years, several algorithms used for securing the network. Currently we tend to face differing types of DDOS attacks are a lot of complicated and high drawback comparable with DOS attacks as a result of a DDOS poignant in smart victim’s purchasers. The DDOS defense approach wishes to achieve information of a way to solve the matter within the public should facilitate to counter the threat international exploitation of defense mechanisms. A lot of reliable mechanisms are needed to attest the sources of the web traffic so malicious users may be known and command in order to protect their resources for valid users.

REFERENCES


