Diverse Types Of Network Attacks and the Describing Security Mechanisms

Madhava Rao K¹ And Prof. Ramakrishna S²

Department Of Computer Science, Svu College Of Cm & Cs,Tirupati-517502, A.P. India, Corresponding Author: Prof. Ramakrishna S


Keywords: Authentication, Data Transformation, Integrity, Monitor, Privacy

I. Introduction


II. Possibility Of Primary Security Schemes In Networks


A) Access – Make Available The Means Of Communication To The Authorized Users From An Exacting Network
B) Authentication – Make Sure The Users Of The Network Are Who They Say They Are Or If Not
C) Confidentiality And Secrecy – Make Certain That The Information In The Network Is Privacy.
D) Integrity – Ensure That Alteration In The Communication Ought To Never Happen While Transit.
E) Non-Repudiation – Ensure That The User Never Refutes The Network He Used.
2.1 Cryptography
Cryptography is transmitting the information in an undisclosed coded approach. At this time in cryptography, the content of the communication is hidden from view. On the other hand, the techniques of encryption-decryption are devised for the conventional wired networks not potential to be applied directly for the wireless networks. Wireless networks consist of minute sensors which truly suffer from the lack of processing, memory, and battery power [4-8]. Therefore, extra processing, extra memory, and extra battery power are required for the application of encryption techniques.

2.2 Steganography
Whereas cryptography aims at hiding the content of the message, steganography [9,10] aims at hiding the being of the message. Steganography is the art of hidden communication by embedding a message into the multimedia data in the form of image, sound, video, etc. [11]. Considerably, this method is used in the situation where there is a need of conveying the undisclosed data publicly.

III. Diverse Kinds Of Attacks In Networks
Obviously, the attacks occurred in the physical layer are jamming and tampering [12]. When an attacker blocks the radio frequencies that are using by legitimate sensor nodes, then jamming will take place. Otherwise, if the attacker blocks the complete network, a whole denial of service (DoS) occurs. Tampering is material damage that is alteration or replacement of either a node or part of a node. Sensors' damage, modification or alteration of circuitry, changing of hardware of the node or of the entire node, and altering of sensors with malicious sensors are examples of tampering. In addition to, an attacker can cross-examine the nodes electronically to get hold of access to cryptographic data and the information which is going to access on other communication layers. Major attacks are explaining visibly in the below with separate headings.

3.1 Denial Of Service (DoS)
Obviously, this will happen by the unintentional or unplanned failure of nodes or malicious action [13, 14]. The simple DoS attack try to drain the resources which are accessible to the victim node, through transfer of unnecessary extra packets, as a result prevents authorized network users from available services to which they are entitled. DoS attack intended not only for the attacker's effort to subvert, interrupt, or demolish a network, but also for any incident that destroy the network's facility to make available a service. Quite a few types of DoS attacks are performed in different layers. At physical layer jamming and tampering could be performed, at link layer, collision, exhaustion, unfairness, at network layer, ignore and greed, homing, misdirection, black holes and at transport layer attack might be performed by malicious flooding.

3.2 Attacks On Information In Transit
Obviously in a sensor network, the variations of specific parameters or values monitor by sensors and then inform to the sink based to the requirement. At the time of transferring the report, the information in transit might be changed, deceived, replayed again or missing will takes place. As we know networks are vulnerable to eavesdropping. Adversary can observe or listen the networked messages or might interfere to break off, intercept, vary or formulate the packets consequently providing counterfeit information or data to the destiny stations or sinks [15].

3.3 Sybil Attack
In a sensor network, the sensors might have to work in concert to complete a task in some conditions consequently they can use allocation of subtasks and redundant of information. In such a state, a node can act as if to be more than one node using the identities of other authorized nodes. This kind of attack where as a node forges the identities of more than one node is sybil attack [16, 17].

3.4 Black Hole Attack or Sink Hole Attack
In this attack, the aim is to lure all the traffic to a malicious node of the network [18]. It is achievable by making of a compromised (malicious) node appear alluring to its neighbors in terms of routing of packets. Particularly in an flooding based protocol, the adversary lists to requests for routes and replies the target node that it encompass the large quality or shortest path to the base station. Once the compromised node is in a position to place in itself connecting the communicating nodes then it is capable of doing whatever with the packets passing between them. Actually, this might affect even the nodes that are significantly far from the base stations.
3.5 Hello Flood Attack

This Attack Uses The Hello Packets As A Weapon To Induce The Sensors In Sensor Network. In This Type Of Attack An Adversary With A Large Radio Communication (Laptop-Class Attacker In [19]) Range And Processing Power Transmit Hello Packets To More Number Of Sensor Nodes Which Are Scattered In A Large Area Within A Sensor Network. The Sensors As A Result Convinced The Attacker Is Their Neighbor. As An Outcome, While Transferring The Data To The Base Station, The Victim Nodes Try To Go Through The Adversary As They Know It Is Their Neighbor And Are Eventually Deceived By The Adversary.

3.6 Wormhole Attack

Wormhole Attack Is A Significant Attack, In This Attack Adversary Records The Packets At One Locality Or Spot In The Network And Tunnels Or Retransmits These To Another Locality [20]. The Retransmitting Of Packets Might Be Made Selectively. This Attack Is A Considerable Threat To Wireless Sensor Networks [Wsn], For The Reason That This Type Of Attack Does Not Necessitate Compromising A Sensor In The Networks Rather; It Could Be Performed Yet At The Primary Phase When The Sensors Begin To Find Out The Neighboring Information.

IV. Security Mechanisms For Sensor Networks


V. Architecture Of Classification Of Attacks

The Architecture Of General Classification Of Network Attacks Has Been Explained In Fig.1 After An Obvious Explanation Of Few Words Involved In The Architecture.


Camouflage: An Attacker Might Compromise A Sensor Node In A Sensor Networks And In A While Use That Node To Deception A Regular Node In The Network. This Camouflaged Node Then Might Broadcast
Fake Routing Information And Attract Packets Or Bits From New Nodes For Further Forwarding. After The Packets Begin Incoming At The Compromised Node, It Starts Forwarding Them To Intentional Nodes Where Confidential Analysis On The Packets Might Be Passed Out Systematically.

**Viruses:** These Are Self-Replication Programs Infect The Files And Propagate, Once A File Is Disclosed, The Virus Will Activate In To The System [32].

**Worms:** A Worm Is Analogous To A Virus As They Both Are Self-Replicating, However The Worm Never Need A File To Allow It To Propagate [32]. Two Major Types Of Worms Are There, Mass-Mailing Worms And Network Aware Worms. Mass Mailing Worms Use Email As A Way To Infect Other Computers. Network-Aware Worms Are A Most Important Problem For The Internet. A Network-Aware Worm Selects A Target And Once The Worm Accesses The Target Host, It Can Infect It By Means Of A Trojan Or Otherwise.

**Trojans:** Trojans Emerge To Be Benign Programs To The User, However Will Really Have Some Malicious Purpose. Trojans Generally Transmit Some Payload Such As A Virus [32].

**Node Subversion:** Capture Of A Node Might Disclose Its Information As Well As Revelation Of Cryptographic Keys And As A Result Compromise The Entire Sensor Network. A Specific Sensor May Be Captured, And Information That Is Key Stored On It May Get By An Attacker. [33]

**Node Malfunction:** A Malfunctioning Node Will Create Incorrect Data That Might Represent The Integrity Of Sensor Network In Particular If It Is A Data-Aggregating Node Such As A Cluster Leader [33].

**Node Outage:** When A Node Stops Its Function Then This Situation, Node Outage Is Possible To Occur. In This Case Where As Cluster Leader Stops Performing, The Sensor Network Protocols Must Be Robust Enough To Moderate The Effects Of Node Outages By An Alternate Route [33].
**Message Corruption:** Any Alteration Of The Content Of A Communication By An Adversary Compromises Its Reliability Or Integrity [34]

**False Node:** A Fake Node Involves The Adding Up A Node By A Challenger And Causes The Insertion Of Malicious Data. An Interloper May Add A Node To The System That Includes Bogus Data Or Restricts The Route Of True Data. Inclusion Of Malicious Node Is One Of The Most Hazardous Attacks That Can Takes Place. Malicious Code Injected In The Network Might Extend To All Nodes, Significantly Destroying The Entire Network, Or Yet Worse, Taking Over The Network On Behalf Of A Challenger [34].


**VI. Architecture Of The Required Security Mechanism**

The Architecture Of Necessitate Security Mechanism Has Been Given In Fig.2 Following This Terms In Architecture Is Explained In An Insight Manner.

**Low-Level Mechanism:** Primary Issues For Securing Sensor Networks In Low-Level Mechanism Are,
A. Cryptographic Key Establishment And Trust Setup
B. Privacy And Authentication
C. Secrecy And Confidentiality
D. Robustness In Communication Denial Of Service
E. Protection Of Routing
F. Resilience Or Flexibility To Node Capture

**Cryptographic Key Establishment And Trust Setup:** The Crucial Requisite For Setting Up The Sensor Network Is The Founding Of Cryptographic Keys. By And Large The Sensor Devices Have Inadequate Computational Power And The Public Key Cryptographic Primitives Are Very Expensive To Go After. Key-Establishment Techniques Have To Scale To Networks With Hundreds Or Thousands Of Nodes. In Addition, The Communication Patterns Of Sensor Networks Vary From Conventional Networks; Sensor Nodes Might Require To Set Up Keys With Their Neighbors And With Data Aggregation Nodes. The Drawback Of This Approach Is That Attackers Who Compromised Adequately And Many Nodes Might Also Renovate The Whole Key Collection And Crack The Scheme [35].

Secrecy And Confidentiality: Be Fond Of Other Conventional Networks, The Sensor Networks Have Also Compelled Confidential Concerns. In The Beginning The Sensor Networks Are Deployed For Legitimate Purpose Could Afterward Be Used In Unanticipated Ways. As Long As Awareness Of The Existence Of Sensor Nodes And Data Acquisition Is Predominantly Essential [35].


Table 1: Different Types Of Network Attacks , Required Security Mechanisms And Major Features Are Summarized In The Below Table

<table>
<thead>
<tr>
<th>S.No</th>
<th>Network Attacks</th>
<th>Security Mechanisms</th>
<th>Major Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Dos Attack (Jamming)</td>
<td>Jam [25]</td>
<td>Prevention Of Jammed Region By Using Coalesced Neighbor Nodes</td>
</tr>
<tr>
<td>2</td>
<td>Dos Attack (Jamming)</td>
<td>Wormhole Based [26]</td>
<td>Uses Wormholes To Keep Away From Jamming</td>
</tr>
<tr>
<td>3</td>
<td>Information Deceiving</td>
<td>Statistical En-Route Filtering [27]</td>
<td>Detects And Drops Fake Reports During Forwarding Process</td>
</tr>
<tr>
<td>5</td>
<td>Hello Flood Attack</td>
<td>Bidirectional Verification, Multi-Path Multi-Base Station Routing [29]</td>
<td>Adopts Probabilistic Undisclosed Sharing, Uses Bidirectional Confirmation And Multi-Path Multi-Base Station Routing</td>
</tr>
<tr>
<td>7</td>
<td>Information Spoofing Or Data Spoofing And Wormhole Attack</td>
<td>Tik [37]</td>
<td>Depends On Symmetric Cryptography, Requires Exact Time Synchronization Among All Communicating Parties, Implements Temporal Leashes</td>
</tr>
<tr>
<td>8</td>
<td>Attacks In Information In Transit And Data And Information Deceive</td>
<td>Random Key Pre-Distribution [38], [39], [42]</td>
<td>Make Available Resilience Of The Network, Protect The Network Even If Part Of The Network Is Compromised, Provide Authentication Measures For Sensor Nodes</td>
</tr>
<tr>
<td>10</td>
<td>Blackhole Attacks</td>
<td>Reward [44]</td>
<td>Uses Geographic Routing, Takes Benefit Of The Broadcast Inter-Radio Performance To Watch Neighbor Transmissions And Discover Black Hole Attacks</td>
</tr>
<tr>
<td>11</td>
<td>Data And Information Deceiving, Message Replay Attack</td>
<td>Tinysec [41]</td>
<td>Focuses On Giving Message Legitimacy, Reliability And Confidentiality, Works In The Link Layer</td>
</tr>
<tr>
<td>12</td>
<td>Data Spoofing And</td>
<td>Snp &amp; µtesla [28]</td>
<td>Semantic Security, Data</td>
</tr>
</tbody>
</table>
Diverse Types Of Network Attacks And The Describing Security Mechanisms

VII. Conclusion

Network Security Is A Vital Field That Is More And More Gaining Attention As The Internet Expands. The Security Fear And Internet Protocol Were Analyzed To Find Out The Required Security Technology. The Security Technology Is Typically Software Based, However Lots Of General Hardware Devices Are Used. The Existing Development In Network Security Is No Very Extraordinary. This Paper Summarizes The Attacks And Their Classifications In Sensor Networks And Also An Effort Has Been Made To Investigate The Security Mechanism Extensively Used To Handle Those Attacks. This Survey Will Optimistically Stimulate Future Researchers To Come Up With Smarter And Additional Vigorous Security Mechanisms And Make Their Network Safe.

References

1. Main Types Of Attacks In Wireless Sensor Networks Teodor-Grigore Lupu* *Department Of Computer And Software Engineering University “Politehnica” Of Timisoara, Faculty Of Automatics And Computers Vasile Parvan 2, 300223, Timisoara Romania E-Mail: Teodor.Lupu@Hd.Politiamonar. Ro
Diverse Types Of Network Attacks And The Describing Security Mechanisms
